



**Agència Catalana
de Certificació**

Declaració de Pràctiques de Certificació IdCAT
Agència Catalana de Certificació

Referència: D1111 N-DPC-EC-IDCAT
Versió: 3.5
Data: 02/12/2011

Control documental

Estat formal	Elaborat per: Carlos Alonso – Núria Mombiola (Àrea d'Assessorament)	Aprovat per: Marta Cruellas
Data de creació	30/07/2009	
Control de versions	Data:	02/12/2011
	Descripció:	Modificació del certificat idCAT-CEX
Nivell accés informació	pública	
Títol	Declració de Pràctiques de Certificació EC-idCAT v3r5 cat	
Fitxer	D1111 E0650 N-DPC EC-idCAT v3r5 cat.pdf	
Control de còpies	Només les còpies disponibles a https://www.catcert.cat/ garanteixen l'actualització dels documents. Tota còpia impresa o desada en ubicacions diferents es consideraran còpies no controlades.	
Drets d'autor	 <p>Aquesta obra està subjecta a una llicència Reconeixement-No comercial-Sense obres derivades 2.5 Espanya de Creative Commons. Per veure'n una còpia, visiteu http://creativecommons.org/licenses/by-nc-nd/2.5/es/deed.ca o envieu una carta a Creative Commons, 171 Second Street, Suite 300, San Francisco, California 94105, USA.</p>	

Índex

1. INTRODUCCIÓ	10
1.1 Presentació	10
1.1.1 Tipus i classes de certificats	10
1.1.2 Relació entre la Declaració de pràctiques de certificació i altres documents	10
1.2 Nom del document i identificació	10
1.2.1 Identificació d'aquest document	10
1.2.2 Identificació de polítiques específiques	10
1.2.3 Identificació de combinacions de polítiques	11
1.2.4 Identificació de polítiques bàsiques	11
1.3 Comunitat d'usuaris de certificats	11
1.3.1 Prestadors de serveis de certificació	12
1.3.2 Entitats de Registre	12
1.3.3 Usuaris finals	12
1.4 Ús dels certificats	13
1.4.1 Usos típics dels certificats	13
1.4.2 Aplicacions prohibides	14
1.5 Administració de la política	14
1.5.1 Organització que administra l'especificació	14
1.5.2 Dades de contacte de l'organització	14
1.5.3 Persona que determina la conformitat d'una DPC amb la política	14
1.5.4 Procediment d'aprovació	14
2. PUBLICACIÓ D'INFORMACIÓ I DIRECTORI DE CERTIFICATS.....	15
2.1 Directori de certificats	15
2.2 Publicació d'informació de l'EC-idCAT	15
2.3 Freqüència de publicació	15
2.4 Control d'accés	15
3. IDENTIFICACIÓ I AUTENTICACIÓ	17
3.1 Gestió de noms	17
3.1.1 Tipus de noms	17
3.1.2 Significat dels noms	17
3.1.3 Utilització d'anònims i pseudònims	17
3.1.4 Interpretació de formats de noms	17
3.1.5 Unicitat dels noms	17

3.1.6	Resolució de conflictes relatius a noms.....	17
3.2	Validació inicial de la identitat.....	18
3.2.1	Prova de possessió de clau privada	18
3.2.2	Autenticació de la identitat del subscriptor	18
3.2.3	Informació de subscriptor no verificada.....	20
3.3	Identificació i autenticació de sol·licituds de renovació	20
3.3.1	Validació per a la renovació rutinària de certificats	20
3.3.2	Validació per a la renovació de certificats després de la revocació.....	20
4.	EL CICLE DE VIDA DELS CERTIFICATS	21
4.1	Sol·licitud d'emissió de certificat	21
4.1.1	Legitimació per a sol·licitar l'emissió	21
4.1.2	Procediment d'alta; Responsabilitats	21
4.2	Processament de la sol·licitud de certificació	22
4.3	Emissió de certificat	22
4.3.1	Accions de l'EC-idCAT durant el procés d'emissió	22
4.3.2	Comunicació de l'emissió al subscriptor.....	23
4.4	Acceptació del certificat	23
4.4.1	Responsabilitats del Prestador de Serveis de Certificació.....	23
4.4.2	Conducta que constitueix acceptació del certificat.....	23
4.4.3	Publicació del certificat.....	23
4.4.4	Notificació de l'emissió a tercers.....	23
4.5	Ús del parell de claus i del certificat.....	24
4.5.1	Ús pels subscriptors	24
4.5.2	Ús pel tercer que confia en certificats.....	24
4.6	Renovació de certificat sense renovació de claus	24
4.7	Renovació de certificat amb renovació de claus	24
4.8	Modificació de certificats	25
4.9	Revocació i suspensió de certificats	25
4.9.1	Causas de revocació de certificats.....	25
4.9.2	Legitimació per a sol·licitar la revocació	26
4.9.3	Procediments de sol·licitud de revocació	26
4.9.4	Termini temporal de sol·licitud de revocació	27
4.9.5	Termini màxim de processament de la sol·licitud de revocació.....	27
4.9.6	Obligació de consulta de informació de revocació de certificats	27
4.9.7	Freqüència d'emissió de llistes de revocació de certificats (LRCs)	27
4.9.8	Període màxim de publicació de LRCs	27
4.9.9	Disponibilitat de serveis de comprovació d'estat de certificats	27

4.9.10	Obligació de consulta de serveis de comprovació d'estat de certificats.....	28
4.9.11	Altres formes d'informació de revocació de certificats	28
4.9.12	Requisits especials en cas de compromís de la clau privada.....	28
4.9.13	Causes de suspensió de certificats	28
4.9.14	Legitimitat per sol·licitar la suspensió	29
4.9.15	Procediments de sol·licitud de suspensió	29
4.9.16	Termini màxim de suspensió.....	29
4.9.17.	Habilitació d'un certificat suspès	30
4.10	Serveis de comprovació d'estat de certificats.....	30
4.10.1	Característiques d'operació dels serveis	30
4.10.2	Disponibilitat dels serveis.....	30
4.10.3	Altres funcions dels serveis	30
4.11	Acabament de la subscripció	30
4.12	Dipòsit i recuperació de claus	30
5.	CONTROLS DE SEGURETAT FÍSICA, DE GESTIÓ I D'OPERACIONS	31
5.1	Controls de seguretat física	31
5.1.1	Localització i construcció de les instal·lacions	31
5.1.2	Accés físic.....	31
5.1.3	Electricitat i aire condicionat	32
5.1.4	Exposició al aigua.....	32
5.1.5	Advertència i protecció d'incendis	32
5.1.6	Emmagatzematge de suports	32
5.1.7	Tractament de residus.....	32
5.1.8	Còpia de seguretat fora de les instal·lacions	33
5.2	Controls de procediments	33
5.2.1	Funcions fiables	33
5.2.2	Nombre de persones per tasca	33
5.2.3	Identificació i autenticació per a cada funció	33
5.2.4	Rols que requereixen separació de tasques.....	33
5.3	Controls de personal	34
5.3.1	Requisits d'historial, qualificacions, experiència i autorització	35
5.3.2	Requisits de formació	35
5.3.3	Requisits i freqüència d'actualització formativa.....	35
5.3.4	Seqüència i freqüència de rotació laboral	35
5.3.5	Sancions per accions no autoritzades.....	36
5.3.6	Requisits de contractació de professionals	36
5.3.7	Subministrament de documentació al personal.....	36
5.4	Procediments d'auditoria de seguretat.....	36
5.4.1	Tipus d'esdeveniments registrats	36
5.4.2	Freqüència de tractament de registres d'auditoria.....	37
5.4.3	Període de conservació de registres d'auditoria	37

5.4.4	Protecció dels registres d'auditoria	37
5.4.5	Procediments de còpies de seguretat	37
5.4.6	Localització del sistema d'acumulació de registres d'auditoria	38
5.4.7	Notificació de l'esdeveniment d'auditoria al causant de l'esdeveniment.....	38
5.4.8	Anàlisi de vulnerabilitats	38
5.5	Arxiu d'informacions	38
5.5.1	Tipus d'esdeveniments registrats	38
5.5.2	Període de conservació de registres.....	39
5.5.3	Protecció de l'arxiu	39
5.5.4	Procediments de còpia de suport.....	39
5.5.5	Requisits de segellat de cautela de data i hora	40
5.5.6	Localització del sistema d'arxiu	40
5.5.7	Procediments d'obtenció i verificació d'informació d'arxiu	40
5.6	Renovació de claus.....	40
5.7	Compromís de claus i recuperació de desastre.....	40
5.7.1	Procediment de gestió d'incidències i compromisos	40
5.7.2	Corrupció de recursos, aplicacions o dades	40
5.7.3	Compromís de la clau privada de l'EC-idCAT	40
5.7.4	Desastre sobre les instal·lacions.....	40
5.8	Acabament del servei.....	41
5.8.1	Entitat de Certificació	41
5.8.2	Entitat de Registre	41
6.	CONTROLS DE SEGURETAT TÈCNICA.....	42
6.1	Generació i instal·lació del parell de claus.....	42
6.1.1	Generació del parell de claus.....	42
6.1.2	Tramesa de la clau privada al subscriptor	42
6.1.3	Tramesa de la clau pública a l'emissor del certificat	42
6.1.4	Distribució de la clau pública del Prestador de Serveis de Certificació	42
6.1.5	Mides de claus	42
6.1.6	Generació de paràmetres de clau pública	43
6.1.7	Comprovació de qualitat de paràmetres de clau pública	43
6.1.8	Generació de claus en aplicacions informàtiques o en bens d'equip.....	43
6.1.9	Propòsits d'ús de claus	43
6.2	Protecció de la clau privada.....	43
6.2.1	Mòduls de protecció de la clau privada.....	43
6.2.2	Control per més d'una persona (n de m) sobre la clau privada	44
6.2.3	Dipòsit de la clau privada.....	44
6.2.4	Còpia de seguretat de la clau privada	44
6.2.5	Arxiu de la clau privada	44
6.2.6	Introducció de la clau privada en el mòdul criptogràfic	44
6.2.7	Emmagatzematge de la clau privada en el mòdul criptogràfic	44
6.2.8	Mètode d'activació de la clau privada.....	44

6.2.9	Mètode de desactivació de la clau privada	45
6.2.10	Mètode de destrucció de la clau privada	45
6.2.11	Classificació dels mòduls criptogràfics	45
6.3	Altres aspectes de gestió del parell de claus	45
6.3.1	Arxiu de la clau pública	45
6.3.2	Períodes d'utilització de les claus pública i privada	45
6.4	Dades d'activació	45
6.4.1	Generació i instal·lació de les dades d'activació	45
6.4.2	Protecció de les dades d'activació	45
6.4.3	Altres aspectes de les dades d'activació	45
6.5	Controls de seguretat informàtica	45
6.5.1	Requisits tècnics específics de seguretat informàtica	45
6.5.2	Avaluació del nivell de seguretat informàtica	46
6.6	Controls tècnics del cicle de vida	46
6.6.1	Controls de desenvolupament de sistemes	46
6.6.2	Controls de gestió de seguretat	46
6.6.3	Avaluació del nivell de seguretat del cicle de vida	47
6.7	Controls de seguretat de xarxa	47
6.8	Segell de temps	47
7.	PERFILS DE CERTIFICATS I LLISTES DE CERTIFICATS REVOCATS	48
7.1	Perfil de certificat	48
7.2	Perfil de la llista de revocació de certificats	48
8.	AUDITORIA DE CONFORMITAT	49
8.1	Freqüència de l'auditoria de conformitat	49
8.2	Identificació i qualificació de l'auditor	49
8.3	Relació de l'auditor amb l'entitat auditada	49
8.4	Relació d'elements objecte d'auditoria	49
8.5	Accions a emprendre com a resultat d'una falta de conformitat	49
8.6	Tractament dels informes d'auditoria	50
9.	REQUISITS COMERCIALS I LEGALS	51

9.1	Tarifes.....	51
9.1.1	Tarifa d'emissió o renovació de certificats	51
9.1.2	Tarifa d'accés a certificats	51
9.1.3	Tarifa d'accés a informació d'estat de certificat.....	51
9.1.4	Tarifes d'altres serveis	51
9.1.5	Política de reintegrament	51
9.2	Capacitat financera	51
9.2.1	Assegurança de responsabilitat civil.....	51
9.2.2	Altres actius	51
9.2.3	Cobertura d'assegament per a subscriptors i tercers que confien en certificats	51
9.3	Confidencialitat.....	51
9.3.1	Informacions confidencials.....	51
9.3.2	Informacions no confidencials.....	52
9.3.3	Responsabilitat per la protecció d'informació confidencial	52
9.4	Protecció de dades personals	52
9.4.1.	Política de Protecció de Dades Personals	52
9.4.2.	Dades de caràcter personal no disponibles a tercers	54
9.4.3.	Dades de caràcter personal disponibles a tercers.....	54
9.4.4.	Responsabilitat corresponent a la protecció de les dades personals	55
9.4.5.	Gestió d'incidències relacionades amb les dades de caràcter personal	55
9.4.6.	Prestació del consentiment per al tractament de les dades personals.....	56
9.4.7.	Comunicació de dades personals.....	56
9.5	Drets de propietat intel·lectual.....	56
9.5.1	Propietat dels certificats i informació de revocació	56
9.5.2	Propietat de la Política de Certificació i la Declaració de Pràctiques de Certificació.....	57
9.5.3	Propietat de la informació relativa a noms	57
9.5.4	Propietat de claus.....	57
9.6	Obligacions i responsabilitat civil.....	57
9.6.1	Entitats de Certificació.....	57
9.6.2	Entitats de Registre.....	60
9.6.3	Subscriptors	61
9.6.4	Verificadors.....	62
9.7	Renúncies de garanties.....	63
9.7.1	Rebuig de garanties de l'Entitat de Certificació.....	63
9.8	Limitacions de responsabilitat	63
9.8.1	Limitacions de responsabilitat de l'Entitat de Certificació	63
9.8.2	Cas fortuït i força major.....	63
9.9	Indemnitzacions.....	63
9.9.1	Clàusula d'indemnitat de subscriptor.....	63
9.9.2	Clàusula d'indemnitat de verificador.....	63
9.10	Termini i acabament	64

9.10.1	Termini	64
9.10.2	Finalització.....	64
9.10.3	Supervivència	64
9.11	Notificacions	64
9.12	Modificacions.....	64
9.12.1	Procediment per a les modificacions	64
9.12.2	Circumstàncies en les que un OID ha de ser canviat.....	65
9.13	Resolució de conflictes	65
9.13.1	Resolució extrajudicial de conflictes	65
9.13.2	Jurisdicció competent	65
9.14	Llei aplicable	65
9.15	Conformitat amb la llei aplicable	65
9.16	Clàusules diverses	66
9.16.1	Acord íntegre.....	66
9.16.2	Subrogació.....	66
9.16.3	Divisibilitat.....	66
9.16.4	Aplicacions	66
9.16.5	Altres clàusules.....	66
	Control documental.....	67
	Control de versions DPC EC-idCAT 1r semestre 2011	67

1. Introducció

1.1 Presentació

1.1.1 Tipus i classes de certificats

L'EC-idCAT emet certificats idCAT, que són certificats reconeguts d'identificació i signatura electrònica avançada, destinats a ciutadans i ciutadanes catalanes majors d'edat, així com a altres persones (col·lectivament anomenats subscriptors) que necessiten relacionar-se amb les Administracions públiques i altres institucions.

El certificat idCAT és un certificat reconegut d'acord amb l'establert a l'article 11.1 de la Llei 59/2003, de 19 de desembre, de signatura electrònica, amb el contingut prescrit per l'article 11.2, i emès complint les obligacions dels articles 12, 13, 17 a 20 de la Llei esmentada.

El procediment de validació de la identitat requereix la compareixença personal de la persona física que obté el certificat davant d'una oficina de registre col·laboradora de CATCert.

1.1.2 Relació entre la Declaració de pràctiques de certificació i altres documents

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

L'EC-idCAT emet certificats dins de la Jerarquia de l'Agència Catalana de Certificació, per tant ha de disposar d'una declaració de pràctiques de certificació d'acord amb la Política General de Certificació de l'EC-idCAT.

Aquesta Declaració de Pràctiques de Certificació (DPC) inclou els procediments que CATCert i les entitats que col·laboren apliquen en la prestació dels seus serveis, en compliment dels requisits establerts per les polítiques que gestiona i l'article 19 de la Llei 59/2003, de 19 de desembre, de signatura electrònica.

1.2 Nom del document i identificació

1.2.1 Identificació d'aquest document

Aquest document es denomina "Declaració de Pràctiques de Certificació de l'Entitat Pública de Certificació de Ciutadans (EC-idCAT)".

1.2.2 Identificació de polítiques específiques

CATCert ha definit i aprovat la següent especificació de política per als certificats idCAT:

idCAT basat en certificat CPIXSA - Certificat de persona física ciutadà d'identificació, xifrat i signatura electrònica avançada

Classe 2. OID: 1.3.6.1.4.1.15096.1.3.1.86.1

idCAT-CEX basat en certificat CPIXSA - Certificat de persona física de nacionalitat estrangera d'identificació, xifrat i signatura electrònica avançada

Classe 2. OID: 1.3.6.1.4.1.15096.1.3.1.86.2

idCAT-T basat en certificat CPIXSA - Certificat de persona física ciutadà d'identificació, xifrat i signatura electrònica avançada, amb suport targeta o *token*

Classe 2. OID: 1.3.6.1.4.1.15096.1.3.1.86.3

Certificat d'infraestructura personal d'identificació i signatura reconeguda CIPISR –
Certificat d'infraestructura d'operador

Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.15

Classe 2. OID: 1.3.6.1.4.1.15096.1.3.1.16

1.2.3 Identificació de combinacions de polítiques

CATCert ha definit i aprovat les següents combinacions de polítiques de certificació, que són compatibles entre si:

CPISA - Certificat personal d'identificació i signatura electrònica avançada

Classe 2. OID: 1.3.6.1.4.1.15096.1.3.1.84

CPIXSA - Certificat personal d'identificació, xifrat i signatura electrònica avançada

Classe 2. OID: 1.3.6.1.4.1.15096.1.3.1.86

1.2.4 Identificació de polítiques bàsiques

L'Agència Catalana de Certificació, actuant com a Entitat de gestió de polítiques, ha assignat a cada tipus i classe de certificat un identificador d'objecte (OID) que es mostra a continuació:

CIPISR – Certificat d'infraestructura d'operador

Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.15

Classe 2. OID: 1.3.6.1.4.1.15096.1.3.1.16

CPSA - Certificat personal de signatura electrònica avançada

Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.23

Classe 2. OID: 1.3.6.1.4.1.15096.1.3.1.24

CPI - Certificat personal d'identitat

Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.31

Classe 2. OID: 1.3.6.1.4.1.15096.1.3.1.32

CPX - Certificat personal de xifrat

Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.41

Classe 2. OID: 1.3.6.1.4.1.15096.1.3.1.42

1.3 Comunitat d'usuaris de certificats

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

Els certificats idCAT sempre s'expedeixen al públic.

1.3.1 Prestadors de serveis de certificació

El prestador de serveis de certificació és l'Agència Catalana de Certificació (CATCert).

L'EC-idCAT dona serveis d'expedició i gestió de certificats a usuaris finals, mitjançant l'emissió de certificats personals, inscrita en la jerarquia pública de certificació de Catalunya.

Com podem observar en la següent imatge la Jerarquia de Certificats comença en la part superior per l'EC-ACC, l'Entitat de Certificació de l'Agència Catalana de Certificació, considerada com l'EC arrel de la jerarquia.

Seguidament i vinculada a l'EC-ACC, ens trobem amb l'EC-idCAT, l'Entitat de Certificació de ciutadans de Catalunya, de la que tracta aquesta declaració de pràctiques de certificació.

I finalment trobem el subscriptor del certificat idCAT, que és un ciutadà de Catalunya posseïdor del certificat idCAT.

Aquesta informació es pot obtenir als navegadors Firefox de Mozilla, seguint la ruta: Eines - Opcions - Avançat - Gestor de Certificats - Veure, per als diversos sistemes operatius.

A Windows s'observa l'esmentada jerarquia seguint els següents passos:

Inicio - Tauler de Control - Opcions d'Internet - Contingut - Certificats.

Abans de verificar la ruta de la Jerarquia Pública de Certificació de Catalunya hem d'instal·lar les seves claus públiques. Per a això haurem d'anar a la web de CATCert (<http://www.catcert.cat/>) o de l'EC-idCAT (<http://www.idcat.cat/>).

1.3.2 Entitats de Registre

Són Entitats de Registre per a certificats idCAT, totes aquelles entitats que s'hagin adherit a les Condicions del Servei de Certificació Digital de CATCert.

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

1.3.3 Usuaris finals

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

- a) Els sol·licitants de certificats
- b) Els subscriptors o titulars de certificats
- c) Els verificadors de signatures i certificats

1.3.3.1 Sol·licitants de certificats

Els certificats idCAT són sol·licitats per persones majors d'edat, en el seu propi nom.

Poden ser sol·licitants:

-
- a) La persona que serà el futur subscriptor.
 - b) Una persona autoritzada pel futur subscriptor (representant)

L'autorització s'ha de realitzar de forma expressa mitjançant document públic.

1.3.3.2 Subscriptors de certificats

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

El subscriptor té llicència d'ús del certificat.

1.3.3.3 Usuaris de certificats

Els usuaris dels certificats són els verificadors

1.3.3.4 Verificadors de certificats

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

1.4 Ús dels certificats

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

1.4.1 Usos típics dels certificats

Els certificats idCAT de signatura avançada 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 emès complint les obligacions dels articles 12, 13, i 17 a 20 de la Llei 59/2003, de 19 de desembre, de signatura electrònica, i que donen compliment a allò disposat per la normativa tècnica de l'Institut Europeu de Normes de Telecomunicacions, identificada amb la referència TS 101 456.

Els certificats idCAT no funcionen necessàriament amb dispositius segurs de creació de signatura electrònica d'acord amb l'article 24.3 de la Llei 59/2003, de 19 de desembre.

Els certificats idCAT garanteixen la identitat del subscriptor 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 (per exemple l'ORDRE HAC/1181/2003, de 12 de maig, per la qual s'estableixen normes específiques sobre l'ús de la signatura electrònica en les relacions tributàries per mitjans electrònics, informàtics i telemàtics amb l'Agència Estatal d'Administració Tributària), que establirà les condicions addicionals necessàries perquè es produeixi l'esmentada equiparació.

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

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

Els certificats idCAT tenen la possibilitat de rebre missatges de dades confidencials, en qualsevol format, protegits mitjançant el xifrat del text del missatge, per part del remitent del missatge, utilitzant la clau pública del subscriptor indicada al certificat.

El subscriptor utilitza la seva clau privada per desxifrar el missatge o document.

1.4.2 Aplicacions prohibides

Els certificats idCAT (a excepció del CIPISR) no es poden utilitzar 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), ni per realitzar cap tipus de transaccions econòmiques.

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

1.5 Administració de la política

1.5.1 Organització que administra l'especificació

CATCert - Agència Catalana de Certificació

Passatge de la Concepció, 11

08008 - Barcelona

1.5.2 Dades de contacte de l'organització

CATCert - Agència Catalana de Certificació

Àrea d'Assessorament

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

Passatge de la Concepció, 11

08008 - Barcelona

1.5.4 Procediment d'aprovació

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

Es preveu, d'aquesta manera, el procediment de modificació d'especificació del servei i el procediment de publicació d'especificacions de servei.

Les modificacions finals de la política són aprovades per CATCert, després de comprovar el compliment dels requisits establerts a les seccions corresponents d'aquesta DPC.

2. Publicació d'informació i directori de certificats

2.1 Directori de certificats

El Directori de certificats està disponible durant les 24 hores dels 7 dies de la setmana i, en cas d'error del sistema fora de control de CATCert, aquesta realitza els seus millors esforços perquè el servei es trobi disponible de nou en el termini establert a la secció 4.10.2 d'aquest document.

2.2 Publicació d'informació de l'EC-idCAT

L'EC-idCAT publica les següents informacions, 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 i, quan sigui convenient, les polítiques específiques.
- Els perfils dels certificats i de les llistes de revocació dels certificats.
- La Declaració de Pràctiques de Certificació.
- Els instruments jurídics vinculants amb subscriptors i verificadors.

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

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

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

2.3 Freqüència de publicació

La informació de l'EC-idCAT es publica quan es troba disponible i en especial, de forma immediata quan s'emeten les mencions relatives a la vigència dels certificats.

Els canvis en aquest document es regeixen per l'establert a la secció corresponent.

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

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

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

2.4 Control d'accés

L'EC-idCAT no limita l'accés de lectura a les informacions establertes a la secció corresponent, però estableix controls per mantenir la integritat del directori actualitzat dels



**Agència Catalana
de Certificació**

Declaració de Pràctiques de Certificació idCAT

certificats expedits i la protecció de la integritat i autenticitat de la informació d'estat de revocació.

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

- Es pugui comprovar l'autenticitat dels certificats.
- Les persones no autoritzades no poden alterar les dades.
- Detecti qualsevol canvi tècnic que afecti els requisits de seguretat.

3. Identificació i autenticació

3.1 Gestió de noms

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

3.1.1 Tipus de noms

3.1.1.1 Estructura sintàctica

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

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

3.1.1.2 Perfils dels certificats

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

3.1.2 Significat dels noms

En certificats corresponents a persones físiques la identificació del signant està formada pel seu nom i cognoms, més el seu DNI, NIF, NIE o passaport.

L'estructura sintàctica i el contingut dels camps de cada certificat, així com el seu significat semàntic es troba descrit al document "perfil de certificat" corresponent, que l'Agència Catalana de Certificació publica en el seu web.

3.1.3 Utilització d'anònims i pseudònims

No es poden utilitzar anònims ni pseudònims.

3.1.4 Interpretació de formats de noms

Sense estipulació addicional.

3.1.5 Unicitat dels noms

Els noms dels subscriptors de certificats seran únics, per a cada servei de generació de certificats operat per l'EC-idCAT i per a cada tipus de certificat.

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

3.1.6 Resolució de conflictes relatius a noms

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

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

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

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

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

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

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

3.2 Validació inicial de la identitat

3.2.1 Prova de possessió de clau privada

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

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

3.2.2 Autenticació de la identitat del subscriptor

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

Per acreditar la identitat del subscriptor, aquest es persona davant d'una Entitat de Registre que elegeix i que pot ser la més propera al seu domicili.

Recordem que en un dels últims passos de la sol·licitud del certificat, la web ofereix al sol·licitant la possibilitat de cercar l'Entitat de Registre, per codi postal o per població.

L'acreditació de la identitat es pot realitzar directament davant de les Entitats de Registre, mitjançant el procés de pre-validació, segons el qual el sol·licitant consigna les dades directament als operadors, que els contrasten amb els documents originals aportats (DNI, NIE, passaport). Una vegada recollides les dades es procedeix a emetre el certificat

El sol·licitant també pot consignar les dades d'identitat en la web de CATCert. Seguidament, el sol·licitant es persona davant l'Entitat de Registre de la seva elecció i que pot ser la més propera al seu domicili.

Una vegada el sol·licitant es trobi a les dependències de l'Entitat de Registre es presenta amb el document que l'identifica i que ha indicat a la sol·licitud (DNI, NIF, NIE o passaport, depenent del cas), amb una fotocòpia de l'esmentat document i, si així ho desitja, una còpia impresa del formulari de confirmació de dades que li mostra la web just al final del procés de sol·licitud.

L'encarregat de rebre l'esmentada documentació a l'Entitat de Registre, comprova visualment que la fotografia del document que identifica el sol·licitant sigui exactament la corresponent al subscriptor i la majoria d'edat.

Seguidament imprimeix el document de compareixença amb les dades de la sol·licitud del certificat perquè el sol·licitant el firmi.

L'encarregat comprova també que la signatura que el subscriptor acaba de realitzar a la sol·licitud de certificat correspon a la signatura que hi ha al document que l'identifica (DNI, NIE, passaport).

Fetes totes aquestes comprovacions es valida la sol·licitud en el sistema informàtic enviant-lo electrònicament i de forma segura a l'EC-idCAT

Tots els documents que porti el subscriptor han d'estar vigents. En el seu cas, haurà d'aportar el comprovant de renovació. Si aquest no conté fotografia, es podrà completar la verificació de la identitat usant el document caducat.

3.2.2.1 Necessitat de presència personal

La identificació de la persona física que obté un certificat idCAT pot realitzar-se

- Mitjançant la seva presència davant dels encarregats de verificar la seva identitat.
- Es pot prescindir de la presència si la signatura continguda a la sol·licitud d'expedició d'un certificat ha estat legitimada notarialment, i en els casos previstos per l'article 13.4 de la Llei 59/2003, de 19 de desembre.
- Mitjançant el procediment que estableix la normativa administrativa, quan la presència es realitzi davant de les Administracions Públiques.

3.2.2.1.1 Informacions addicionals per a subscriptores de nacionalitat espanyola

El subscriptor s'identifica obligatòriament amb el seu Document Nacional d'Identitat.

3.2.2.1.2 Informacions addicionals per a subscriptors de nacionalitat no espanyola residents a Catalunya.

El subscriptor s'identifica obligatòriament amb la seva targeta de residència o document NIE (ciutadans comunitaris i d'altres estats, exempts de la targeta de residència).

3.2.3 Informació de subscriptor no verificada

Els certificats inclouen informació del subscriptor no verificada, com l'adreça electrònica.

3.3 Identificació i autenticació de sol·licituds de renovació

3.3.1 Validació per a la renovació rutinària de certificats

El sistema de certificació comunica al subscriptor la data de la finalització de la vigència del certificat amb una antelació de 60 dies.

La renovació s'inicia quan el subscriptor del certificat idCAT, encara en vigor, demana la renovació seguint la ruta indicada en el missatge electrònic.

Si el certificat va ser emès en suport de programari, i es realitza durant els cinc primers anys des de la primera validació, el subscriptor no s'ha de personar davant les entitats de registre. En cas que el certificat s'hagi emès en suport de maquinari (típicament, clauer IdCAT), o si han passat més de cinc anys des de la primera validació (per exemple, en casos de segona renovació), el subscriptor s'haurà de personar físicament davant l'Entitat de Registre, o aportar l'acta notarial corresponent.

Abans de renovar un certificat, l'EC-idCAT comprova que la informació utilitzada per verificar la identitat i la resta de dades del subscriptor continuen sent vàlides.

Si qualsevol informació del subscriptor ha canviat, es registra adequadament la nova informació, d'acord amb l'establert a la secció 4.7 d'aquest document.

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

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

4. El cicle de vida dels certificats

4.1 Sol·licitud d'emissió de certificat

4.1.1 Legitimació per a sol·licitar l'emissió

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

Tots aquells que desitgen convertir-se en subscriptors realitzen una sol·licitud de certificat idCAT, visitant la web de CATCert (<http://www.catcert.cat/> o <http://www.idcat.cat/>) o directament presentant-se davant de qualsevol de les entitats (Ajuntaments, Diputacions, etc.) que ofereixen aquesta possibilitat, i omplint el formulari de sol·licitud i seguint els passos que allà s'indiquen.

4.1.2 Procediment d'alta; Responsabilitats

L'EC-idCAT s'assegura que les sol·licituds de certificats són completes, precises i estan degudament autoritzades.

Per a certificats i claus en clauer, la presa de dades del sol·licitant es fa a les pròpies instal·lacions de l'Entitat de Registre.

Per realitzar la sol·licitud prèvia, cal accedir a la pàgina web de presentació d'aquest servei que conté un menú amb les passes a seguir per realitzar la sol·licitud.

El primer pas de necessària execució és carregar en el nostre sistema informàtic les claus públiques de la jerarquia pública de certificació.

El següent pas consisteix en el deure de visualització del text divulgatiu de la política de certificació idCAT i la declaració d'intencions d'ús de les dades personals i la seva protecció.

A continuació trobem el formulari on introduïm les nostres dades personals i de contacte. És molt important emplenar el formulari amb les dades exactament com estan escrites als documents que ens identifiquen, que l'operador de l'Entitat de Registre que ens atengui pugui comprovar i validar posteriorment les esmentades dades.

Després cerquem i indiquem l'Entitat de Registre (normalment la que tenim més propera) per presentar-nos i validar les dades que acabem d'incloure al formulari. Seguidament i una vegada indicada a quina Entitat de Registre anirem, ens apareix una pantalla amb les dades que hem introduït que les puguem visualitzar i si són correctes, enviar-les a l'EC-idCAT activant la casella corresponent (típicament, fent clic en el botó "Enviar dades"). D'aquesta forma s'inicia el procés de creació de les claus del certificat idCAT.

Per acabar ens apareix una pantalla amb les dades introduïdes on se'ns demana que l'imprimim per tenir una còpia escrita de la nostra sol·licitud.

Acabada la nostra sol·licitud de certificat, arriba un missatge electrònic a l'adreça electrònica indicada al formulari, comunicant-nos si la subscripció és satisfactòria o si hi ha algun error en la introducció de les dades, així com els passos a seguir, en ambdós casos.

4.2 Processament de la sol·licitud de certificació

Després que l'Entitat de Registre comprovi la identitat del sol·licitant, verifiqui la documentació i el sol·licitant signi el document de compareixença, s'envia la sol·licitud a l'EC-idCAT.

Si alguna de les comprovacions és errònia, s'introdueixen els canvis, es signa pel sol·licitant el document de rectificació de dades i s'envia l'esmentada sol·licitud a l'EC-idCAT.

L'EC-idCAT rep l'autorització de l'Entitat de Registre, recupera la corresponent sol·licitud de la taula de sol·licituds, l'emmagatzema en l'estructura de certificats, es signada per l'EC-idCAT, i es completa així la generació del certificat.

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

A més l'EC-idCAT té en compte els següents aspectes:

- Genera els certificats vinculant-los de forma segura amb la informació que el futur subscriptor indica al formulari de registre.
- Protegeix el secret i la integritat de les dades de registre.
- Inclou al certificat les informacions establertes a l'article 11 de la Llei 59/2003, d'acord amb l'establert a la secció 7 d'aquest document.
- Garanteix la data i l'hora en què s'expedeix un certificat
- Utilitza sistemes i productes fiables que estan protegits contra tota alteració i que garanteixen la seguretat tècnica i, en el seu cas, criptogràfica dels processos de certificació a què serveixen de suport.
- S'assegura que el certificat és emès per sistemes que utilitzin protecció contra falsificació.

En el cas de certificats en programari (clauers, mòbil), l'emissió i lliurament del certificat es realitza en l'acte de personació davant l'entitat de registre.

4.3 Emissió de certificat

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

Després de l'aprovació de la sol·licitud de certificació es procedeix a l'emissió del certificat, de forma segura i es posa el certificat a disposició del subscriptor en el suport corresponent

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

L'EC-idCAT ha de:

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

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

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

4.3.2 Comunicació de l'emissió al subscriptor

L'EC-idCAT comunica per correu electrònic al sol·licitant, una vegada aquest ha finalitzat i ha estat enviat el formulari d'alta de sol·licitud de certificat idCAT, si la subscripció és satisfactòria o ha sorgit un error en la verificació de les dades introduïdes. L'EC-idCAT també notifica per correu electrònic al subscriptor que s'ha creat el certificat i que es troba disponible.

Per a que el subscriptor obtingui el certificat idCAT (en cas d'emissió en programari) cal que accedeixi a la pàgina web que se li indica al correu electrònic i que procedeixi a descarregar el certificat. La descàrrega del certificat digital es pot efectuar tantes vegades com l'usuari cregui convenient.

4.4 Acceptació del certificat

4.4.1 Responsabilitats del Prestador de Serveis de Certificació

L'EC-idCAT proporciona accés al certificat al subscriptor.

4.4.2 Conducta que constitueix acceptació del certificat

El subscriptor accepta el certificat i les condicions d'ús del mateix en signar el document emès per l'Entitat de Registre.

En el cas de certificat en clau, el certificat es descarrega en la pròpia oficina de l'Entitat de Registre.

4.4.3 Publicació del certificat

La publicació dels certificats idCAT requereix sempre el consentiment dels subscriptors.

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

El certificat idCAT serveix per als ciutadans i ciutadanes catalanes i altres persones físiques majors d'edat que necessitin relacionar-se amb les Administracions públiques catalanes, realitzant els corresponents tràmits telemàtics entre ambdues parts amb totes les garanties jurídiques i tècniques recollides en les normes vigents

A més es pot utilitzar pel subscriptor en les seves relacions telemàtiques amb altres persones físiques o jurídiques que ho acceptin, sempre que el seu ús no impliqui una transferència de valor econòmic directe o indirecte.

També permet enviar correu electrònic segur (signat i xifrat) amb altres ciutadans o organitzacions.

4.5.2 Ús pel tercer que confia en certificats

El certificat idCAT serveix per a ús administratiu (quan el tercer és una Administració pública) o privat (quan el tercer no és Administració pública). El tercer verificador que vulgui permetre l'ús professional de l'IdCAT en els seus sistemes haurà de signar un conveni específic d'extensió de l'ús del certificat, que permeti a CATCert assumir el risc corresponent.

4.6 Renovació de certificat sense renovació de claus

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

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.

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.

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.

En qualsevol cas, si han passat més de cinc anys des de la darrera vegada que el subscriptor es va identificar presencialment a una oficina d'entitat de registre, cal presentar-se de nou per a dur a terme la renovació.

4.8 Modificació de certificats

El subscriptor només pot modificar les dades de contacte associades al certificat però no les dades identificatives del mateix. Per canviar les dades de contacte cal que ho sol·liciti a través de la web, seleccionant el seu certificat i introduint les noves dades.

4.9 Revocació i suspensió de certificats

Seguidament s'informa d'aspectes a tenir en compte per a la revocació i suspensió de certificats

4.9.1 Causes de revocació de certificats

L'EC-idCAT revoca un certificat per les següents causes:

1. Circumstàncies que afecten la informació continguda al certificat
 - Modificació d'alguna de les dades contingudes al certificat.
 - Descobriment que alguna de les dades aportades a la sol·licitud de certificat és incorrecte, 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'EC-idCAT, sempre que afecti la fiabilitat dels certificats emesos a partir d'aquest incident.
 - Infracció, per l'EC-idCAT, dels requisits previstos en els procediments de gestió de certificats, establerts en aquest document.
 - Compromís o sospita de compromís de la seguretat de la clau o del certificat del subscriptor.
 - Accés o utilització no autoritzats, per un tercer, de la clau privada del subscriptor.
 - L'ús irregular del certificat pel subscriptor o falta de diligència en la custòdia de la clau privada.
3. Circumstàncies que afecten el subscriptor.
 - Acabament de la relació entre l'EC-idCAT i subscriptor.
 - Modificació o extinció de la relació jurídica subjacent o causa que va provocar l'emissió del certificat al subscriptor.
 - Infracció pel sol·licitant del certificat dels requisits preestablerts per a la sol·licitud d'aquest.
 - Infracció pel subscriptor, de les seves obligacions, responsabilitat i garanties, establertes a l'eina jurídica corresponent o en aquest document.
 - La incapacitat sobrevinguda o la mort del subscriptor.

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

4. Altres circumstàncies

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

Si l'entitat a 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 considera que les actuacions realitzades durant el període de suspensió no són vàlides, sempre que el certificat finalment sigui revocat. Són vàlides si s'aixeca la suspensió i el certificat torna a passar a la situació de vàlid.

L'eina jurídica que vincula l'EC-idCAT amb el subscriptor estableix que el subscriptor sol·licita la revocació del certificat en cas de tenir coneixement d'alguna de les circumstàncies indicades anteriorment.

4.9.2 Legitimació per a sol·licitar la revocació

Poden sol·licitar la revocació d'un certificat:

- El subscriptor a nom del qual el certificat va ser emès.
- L'Entitat de Registre IdCAT que va intervenir a l'emissió.
- L'EC-idCAT

4.9.3 Procediments de sol·licitud de revocació

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

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

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

La petició de revocació amb la documentació necessària és recollida, registrada i notificada per l'Entitat de Registre.

S'arxiva i es comprova la documentació, s'autentica i s'autoritza el sol·licitant. Finalment es realitza la revocació en l'aplicació informàtica corresponent i, a continuació i de forma

automàtica i immediata, s'indica l'esmentada revocació en l'estat del certificat en la llista de revocacions. S'informa el subscriptor i, en el seu cas, el posseïdor de claus, sobre el canvi d'estat de revocació del certificat d'acord amb l'art. 10.2 de la Llei de signatura electrònica.

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

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

4.9.4 Termini temporal de sol·licitud de revocació

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

4.9.5 Termini màxim de processament de la sol·licitud de revocació

La sol·licitud de revocació es processada en el mínim termini possible, sempre dins dels horaris d'oficina de l'Entitat de Certificació.

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

4.9.6 Obligació de consulta de informació de revocació de certificats

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

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

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

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

L'EC-idCAT emet una LRC almenys cada dotze (12) hores. A més, s'emet una després de cada revocació.

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

Els certificats revocats que expiren són retirats de la LRC transcorreguts seixanta dies des de la seva expiració.

4.9.8 Període màxim de publicació de LRCs

Les LRCs són publicades immediatament en el web de CATCert (<http://www.catcert.cat/>).

4.9.9 Disponibilitat de serveis de comprovació d'estat de certificats

De forma alternativa, els verificadors poden consultar els certificats publicats en el directori de l'EC-idCAT, a través d'una interfície web, que està disponible les 24 hores dels 7 dies de la setmana.

En cas d'error dels sistemes de comprovació de l'estat dels certificats per causes fora del control de l'EC-idCAT, aquesta realitza els seus millors esforços per assegurar que aquest servei es mantingui inactiu el mínim temps possible. L'EC-idCAT subministra informació als verificadors referent al funcionament del servei d'informació d'estat dels certificats.

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

El verificador que no utilitzi LRC per comprovar la validesa d'un certificat, ha d'utilitzar el directori de l'EC-idCAT.

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

Una forma per la qual es pot verificar l'estat dels certificats és consultant la LRC més recent emesa per l'EC-idCAT.

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

4.9.11 Altres formes d'informació de revocació de certificats

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

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

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

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

Aquesta resposta serà signada per l'autoritat de certificació arrel de CATCert (EC-ACC) amb el certificat corresponent (en aquest cas, el certificat d'infraestructura de servidor d'estat de certificats en línia –que rep l'acrònim CIO). Aquesta resposta serà emmagatzemada.

4.9.12 Requisits especials en cas de compromís de la clau privada

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

4.9.13 Causes de suspensió de certificats

L'EC-idCAT pot suspendre un certificat en els següents casos:

- Quan ho sol·liciti el subscriptor.
- En els casos legals previstos a l'article 9.1 de la Llei de Signatura Electrònica, és a dir, en cas que una resolució judicial o administrativa ho ordeni.
- Si el subscriptor no utilitza el certificat durant un període prolongat de temps, conegut prèviament.
- Si se sospita el compromís d'una clau, fins que aquest sigui confirmat. En aquest segon cas, l'EC-idCAT s'assegura que el certificat no està suspès durant més temps del necessari per confirmar el seu compromís.

- Quan no s'activa el certificat en un termini de 120 dies a partir de la data d'emissió del certificat.

4.9.14 Legitimitat per sol·licitar la suspensió

Poden sol·licitar la suspensió d'un certificat:

- El subscriptor a nom del qual el certificat va ser emès.
- L'EC-idCAT

4.9.15 Procediments de sol·licitud de suspensió

L'EC-idCAT determina a continuació els procediments i mecanismes d'accés als sistemes de suspensió, tot informant al subscriptor d'acord amb els termes establerts a l'article 10.2 de la Llei de Signatura Electrònica::

- 1) En un primer cas, el subscriptor d'un certificat idCAT fa una crida al telèfon 902 90 10 80 del CAU de CATCert. El subscriptor s'identifica davant de l'operador del CAU indicant-li el número del document que l'identifiqui (DNI, passaport, etc.) amb que va sol·licitar el certificat.
- 2) El operador introdueix aquest número de document identificatiu en la corresponent aplicació informàtica i apareixent-li totes les dades del titular del certificat que pot comprovar amb el subscriptor, li realitza la pregunta de desafiament que el subscriptor va fer i va respondre en el moment de realitzar la sol·licitud del certificat.
- 3) Si el subscriptor respon correctament, l'operador valida el procés de suspensió.
- 4) El titular del certificat rep un correu electrònic, on se li indica que s'ha suspès el seu certificat, i els passos a seguir per habilitar-lo de nou. En cas contrari i si en 120 dies no l'ha habilitat de nou, el seu certificat serà revocat automàticament

El procediment de suspensió es tramita de la mateixa manera que el procediment de revocació, i es realitza per l'EC-IdCAT.

Per iniciar la suspensió es requereix la següent informació:

- Data i hora de la sol·licitud de la suspensió.
- Identitat del subscriptor que sol·licita la suspensió.
- Informació de contacte de l'entitat que demana la suspensió.
- Nom i cognoms del posseïdor de claus a qui se li ha de suspendre el certificat digital.
- DNI del posseïdor de claus a qui se li ha de suspendre el certificat digital.
- Número de sèrie (serial number) del certificat digital que se sol·licita suspendre.
- Raó detallada per a la petició de suspensió
- Codi de suspensió associat al certificat

4.9.16 Termini màxim de suspensió

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

4.9.17. Habilitació d'un certificat suspès

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

4.10 Serveis de comprovació d'estat de certificats

4.10.1 Característiques d'operació dels serveis

Les LRC seran descarregades manualment des del directori de certificació de CATCert instal·lades pels verificadors.

4.10.2 Disponibilitat dels serveis

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

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

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

4.10.3 Altres funcions dels serveis

Sense estipulació addicional.

4.11 Acabament de la subscripció

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

4.12 Dipòsit i recuperació de claus

No es practica.

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

5.1 Controls de seguretat física

L'EC-idCAT ofereix als seus subscriptors el més alt nivell de seguretat física per a la realització de les tasques imprescindibles en la generació i gestió dels certificats.

D'aquesta forma disposa d'instal·lacions amb diversos perímetres de seguretat al voltant dels serveis de generació de certificats, dels dispositius criptogràfics i de la gestió del cicle de vida

Així l'EC-idCAT controla la seguretat física i ambiental de les instal·lacions i els sistemes que es troben a les esmentades instal·lacions, amb les següents mesures:

- Controls d'accés físic
- Protecció davant de desastres naturals
- Mesures de protecció davant d'incendis
- Error dels sistemes de suport (energia elèctrica, telecomunicacions, etc.)
- Demolició de l'estructura
- Inundacions
- Protecció antirobotària
- Conformitat i entrada no autoritzada
- Recuperació del desastre
- Sortida no autoritzada d'equipaments, informacions, suports i aplicacions relatives a components utilitzats pels serveis de l'EC-idCAT.

5.1.1 Localització i construcció de les instal·lacions

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

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

5.1.2 Accés físic

L'Entitat de Certificació estableix 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 duen a terme processos relacionats amb el cicle de vida del certificat, és necessària l'autorització prèvia, identificació en el moment de l'accés i registre del mateix, incloent filmació per circuit tancat de televisió i el seu arxiu.

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

5.1.3 Electricitat i aire condicionat

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

Les instal·lacions compten amb un sistema d'estabilització del corrent, així com d'un sistema de generació propi amb autonomia suficient per mantenir el subministrament durant el temps que requereixi el tancament ordenat i complet de tots els sistemes informàtics.

Els equips informàtics estan ubicats en un entorn on es garanteixi una climatització (temperatura i humitat) adequada a les seves condicions òptimes de treball.

5.1.4 Exposició al aigua

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

5.1.5 Advertència i protecció d'incendis

Totes les instal·lacions i actius de l'EC-idCAT compten amb sistemes automàtics de detecció i extinció d'incendis.

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

5.1.6 Emmagatzematge de suports

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

Es disposa per a ells amb dependències o armaris ignífugs.

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

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

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

5.1.7 Tractament de residus

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

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

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

5.1.8 Còpia de seguretat fora de les instal·lacions

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

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

En el moment de realitzar una sortida d'informació de les dependències s'adopten mesures adients per a impedir qualsevol recuperació indeguda de l'esmentada informació (com per exemple, la utilització de carteres amb dispositius segurs de claus o combinacions, o la utilització de fitxers xifrats).

5.2 Controls de procediments

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

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

5.2.1 Funcions fiables

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

Les funcions fiables inclouen:

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

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

5.2.2 Nombre de persones per tasca

Les funcions fiables identificades en la política de seguretat de l'EC-idCAT, i les seves responsabilitats associades, estan documentades en descripcions de llocs de treball.

5.2.3 Identificació i autenticació per a cada funció

L'EC-idCAT identifica i autentica el personal abans d'accedir a la corresponent funció fiable.

5.2.4 Rols que requereixen separació de tasques

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

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

- Deures associats a la funció
- Nivell d'accés
- Monitoratge de la funció

d. Formació i conscienciació

e. Habilitats requerides

Les citades restriccions s'apliquen en tot cas:

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

b. La persona que actua com a administrador del sistema no pot ser oficial de seguretat ni auditor del sistema.

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

5.3 Controls de personal

L'EC-idCAT té en compte, referent als controls de personal, els següents aspectes:

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

El personal afectat per aquesta normativa és:

- el Responsable del Servei de Certificació Digital
- el Responsable de l'EC-idCAT
- el Responsable de Seguretat

-
- el Responsable d'Operacions
 - l'Operador de Cerimònies de Claus
 - l'Equip tècnic d'administració, operació i explotació
 - els Administradors de la Xarxa
 - i els Operadors de les Entitats de Registre.

5.3.1 Requisits d'historial, qualificacions, experiència i autorització

L'EC-idCAT 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'aplica al personal de gestió de l'EC-idCAT, especialment en relació amb procediments de personal de seguretat.

La qualificació i l'experiència es poden suplir 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 té encomanada.

5.3.2 Requisits de formació

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

La formació inclou 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.

CATCert, a més, proporciona a tot el personal involucrat en les operacions de l'Entitat de Registre, una informació adequada, que inclou els procediments de treball i els de seguretat. També es realitza una instrucció periòdica en normes de seguretat, plans de contingència i gestió d'incidències.

5.3.3 Requisits i freqüència d'actualització formativa

Sense estipulació addicional.

5.3.4 Seqüència i freqüència de rotació laboral

Sense estipulació addicional.

5.3.5 Sancions per accions no autoritzades

L'EC-idCAT disposa d'un sistema sancionador, que depura les responsabilitats derivades d'accions no autoritzades.

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

5.3.6 Requisits de contractació de professionals

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

Quan el professional no es sotmet a aquests controls, està constantment acompanyat per un empleat fiable.

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

Aquests aspectes queden concretats a l'eina jurídica utilitzada per acordar la prestació dels serveis de certificació pel tercer diferent de l'EC-idCAT.

5.3.7 Subministrament de documentació al personal

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

5.4 Procediments d'auditoria de seguretat

5.4.1 Tipus d'esdeveniments registrats

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

- Encès i apagat dels sistemes
- Inici i acabament de l'aplicació d'Autoritat (tècnica) de certificació
- Intents de crear, esborrar, canviar contrasenyes o permisos dels usuaris dins del sistema
- Canvis en les claus de l'Autoritat (tècnica) de certificat
- Canvis en les polítiques d'emissió de certificats
- Intents d'entrada i sortida del sistema
- Intents no autoritzats d'entrada a la xarxa de l'EC-idCAT
- Intents no autoritzats d'accés als fitxers del sistema
- Generació de les claus de l'EC-idCAT.
- Intents nuls de lectura i escriptura en un certificat i en el directori
- Esdeveniments relacionats amb el cicle de vida del certificat, com una sol·licitud, emissió, suspensió, habilitació, revocació i renovació d'un certificat

- Esdeveniments relacionats amb el cicle de vida del mòdul criptogràfic, com a recepció, ús i desinstal·lació d'aquest

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

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

5.4.2 Freqüència de tractament de registres d'auditoria

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

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

5.4.4 Protecció dels registres d'auditoria

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

5.4.5 Procediments de còpies de seguretat

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

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

- Es guarden en armaris ignífugs
- Només persones autoritzades disposen d'accés a les còpies de seguretat
- Les còpies estan identificades

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

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

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

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

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

Es comunica si el resultat de la seva acció ha tingut èxit o no, però no que s'ha auditat l'acció.

5.4.8 Anàlisi de vulnerabilitats

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

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

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

5.5 Arxiu d'informacions

L'EC-idCAT garanteix que tota la informació relativa als certificats es guarda durant un període de temps apropiat.

5.5.1 Tipus d'esdeveniments registrats

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

L'EC-idCAT guarda un registre del següent:

Documents originals:

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

Fotocopies de:

- Full d'entrega de certificats
- Carta PIN y PUK, amb avís de rebuda

5.5.2 Període de conservació de registres

L'EC-idCAT guarda els registres especificats a la secció corresponent d'aquest document durant 15 anys, comptats des del moment de l'expedició del certificat.

5.5.3 Protecció de l'arxiu

L'Entitat de Certificació:

- Manté la integritat i la confidencialitat de l'arxiu que conté les dades referents als certificats emesos.
- Arxiva les dades indicades anteriorment de forma completa i confidencial.
- Manté la privacitat de les dades de registre del subscriptor.

5.5.4 Procediments de còpia de suport

L'EC-idCAT realitza còpies de suport incrementals diàries de tots els seus documents electrònics. A més, realitza còpies de suport completes setmanalment per a casos de recuperació de dades.

Els suports que contenen dades dels fitxers estan clarament identificats amb una etiqueta externa que indica de quin fitxer es tracta, quin tipus de dades conté, el procés que els ha originat i la data de creació.

Aquells mitjans que són reutilitzables, i que contenen còpies de dades dels fitxers, són esborrats físicament abans de la seva reutilització, de manera que les dades que contenen no són recuperables.

Els suports que contenen dades dels fitxers són emmagatzemats en llocs en els quals no tenen accés persones no autoritzades per a l'ús dels fitxers.

La sortida de suports informàtics que contenen dades dels fitxers fora dels locals on estan ubicats els fitxers és autoritzada expressament pel responsable dels fitxers, utilitzant per a això el document adequat.

El responsable del fitxer manté un Llibre de registre d'entrades i sortides on es guarden els formularis d'entrades i sortides de suports, amb indicació del tipus de suport, data i hora, emissor, nombre de suports, tipus d'informació que contenen, forma de tramesa, destinatari i persona responsables de la recepció que està degudament autoritzada.

Quan els suports surten fora dels locals on es troben ubicats els fitxers com a conseqüència d'operacions de manteniment, s'adopten les mesures necessàries per impedir qualsevol recuperació indeguda de la informació emmagatzemada en ells.

La distribució dels suports que contenen dades de caràcter personal es realitza xifrant dades o bé, utilitzant qualsevol altre mecanisme que garanteix que l'esmentada informació no és desxifrabla ni manipulada durant el seu transport.

L'EC-idCAT guarda els documents en paper, en un lloc fora de les instal·lacions de la mateixa EC-idCAT per a casos de recuperació de dades.

5.5.5 Requisits de segellat de cautela de data i hora

L'EC-idCAT emet els certificats i les LRC amb informació de temps i hora. No és necessari que aquesta informació es trobi signada.

5.5.6 Localització del sistema d'arxiu

L'EC-idCAT té un sistema de manteniment de dades d'arxiu fora de les seves pròpies instal·lacions.

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

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

5.6 Renovació de claus

Els certificats renovats es comuniquen als usuaris finals, mitjançant la seva publicació en el directori de CATCert.

5.7 Compromís de claus i recuperació de desastre

5.7.1 Procediment de gestió d'incidències i compromisos

L'EC-idCAT estableix els procediments que aplica en la gestió de les incidències que afecten les seves claus i, molt especialment, en els compromisos de la seguretat de les claus.

5.7.2 Corrupció de recursos, aplicacions o dades

Quan tingui lloc un esdeveniment de corrupció de recursos, aplicacions o dades l'EC-idCAT inicia les gestions necessàries, segons els documents Pla de Seguretat, Pla d'Emergència i Pla d'Auditoria, per fer que el sistema torni al seu estat normal de funcionament.

5.7.3 Compromís de la clau privada de l'EC-idCAT

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

En cas de compromís, l'EC-idCAT:

- Informa a tots els subscriptors i verificadors del compromís.
- Indica que els certificats i la informació de l'estat de revocació lliurats usant la clau d'aquesta Entitat de Certificació ja no són vàlids.

5.7.4 Desastre sobre les instal·lacions.

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

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

-
- Revocació de certificats
 - Publicació d'informació de revocació

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

5.8 Acabament del servei

5.8.1 Entitat de Certificació

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

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

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

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

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

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

5.8.2 Entitat de Registre

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

6. Controls de seguretat tècnica

L'EC-idCAT utilitza sistemes i productes fiables, que estan protegits contra tota alteració i que garanteixen la seguretat tècnica i criptogràfica dels processos de certificació a què serveixen de suport.

6.1 Generació i instal·lació del parell de claus

6.1.1 Generació del parell de claus

El parell de claus és generat pel futur subscriptor.

6.1.2 Tramesa de la clau privada al subscriptor

La clau privada és generada pel subscriptor en el seu sistema informàtic o al clauer i no ha de sortir sota cap concepte de l'esmentat sistema, per tant no hi ha cap tramesa de la clau privada, en cap direcció.

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

Una vegada que el subscriptor ha generat el parell de claus del certificat ambdues claus seran emmagatzemades al reposador de claus del sistema operatiu instal·lat a la màquina del Subscriptor o al clauer però a més, la clau pública junt amb les dades de la sol·licitud del certificat s'inseriran en un arxiu PKCS#10 (signat per la clau privada). Aquest arxiu és, en definitiva, la petició de certificació que s'envia a l'EC-idCAT.

Aquest enviament s'efectua mitjançant una comunicació segura a través del protocol SSL versió 2 amb autenticació exclusiva del servidor, i aquesta es emmagatzemada a la Taula de Sol·licituds de l'EC-idCAT.

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

La clau de l'EC-idcat i les claus de les Entitats de Certificació anteriors de la jerarquia pública de certificació de Catalunya estan a disposició dels verificadors, assegurant la integritat de la clau i autenticant l'origen.

La clau pública de l'EC-ACC (Entitat de Certificació de l'Agència Catalana de Certificació) que és l'arrel de la jerarquia, es publica al directori de l'EC-idCAT, en forma de certificat auto-signat, al costat d'una declaració referent a què la clau permet autenticar a l'EC-idCAT.

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

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

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

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

6.1.5 Mides de claus

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

Les claus dels subscriptors de certificats idCAT seran almenys de 2.048 bits.

6.1.6 Generació de paràmetres de clau pública

Sense estipulació addicional.

6.1.7 Comprovació de qualitat de paràmetres de clau pública

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

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

Els parells de claus de les Entitats de Certificació (tant de CATCert com de l'EC-idCAT) estan generades utilitzant maquinari criptogràfic que compleix els requisits establerts en un perfil de protecció de dispositiu segur de signatura electrònica d'autoritat de certificació normalitzat, d'acord amb ITSEC, Common Criteria o FIPS 140-1 Nivell 3 o superior nivell de seguretat.

La generació de claus per als certificats idCAT es realitza mitjançant aplicacions informàtiques.

6.1.9 Propòsits d'ús de claus

L'EC-idCAT inclou l'extensió *KeyUsage* a tots els certificats, indicant els usos permesos de les corresponents claus privades.

6.2 Protecció de la clau privada

6.2.1 Mòduls de protecció de la clau privada

6.2.1.1. Estàndards dels mòduls criptogràfics

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

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

6.2.1.2. Cicle de vida de les targetes amb circuit integrat

Les targetes amb circuit integrat (altrament, targetes intel·ligents) es lliuren per l'emissió de cada nou certificat (en el cas de l'EC-IdCAT, per als certificats d'operador –CIPISR) directament per CATCert.

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

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

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

Dels 5 possibles dispositius criptogràfics que existeixen l'EC-idCAT requereix el concurs de mínim 2 de forma simultània.

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

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

6.2.3 Dipòsit de la clau privada

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

Les claus privades dels certificats idCAT no es poden emmagatzemar a l'EC-idCAT.

6.2.4 Còpia de seguretat de la clau privada

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

6.2.5 Arxiu de la clau privada

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

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

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

6.2.6 Introducció de la clau privada en el mòdul criptogràfic

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

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

6.2.7 Emmagatzematge de la clau privada en el mòdul criptogràfic

Les claus privades es generen directament en els mòduls criptogràfics.

6.2.8 Mètode d'activació de la clau privada.

La clau privada del subscriptor s'activa mitjançant la introducció del PIN en la corresponent aplicació de generació de signatura.

L'esmentada aplicació en els sistemes informàtics basats en windows és el Cryptographic Service Provider.

Necessitem disposar de l'esmentada aplicació en el nostre sistema, així la web de l'EC-idCAT (<http://www.idcat.cat/>) ens ofereix la possibilitat, a la secció "abans de fer la

sol·licitud", d'actualitzar el nostre sistema amb l'esmentada aplicació amb l'enllaç corresponent a la web de Microsoft.

Els sistemes basats en Netscape, poden utilitzar l'aplicació PKCS #11.

6.2.9 Mètode de desactivació de la clau privada

No aplicable.

6.2.10 Mètode de destrucció de la clau privada

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

6.2.11 Classificació dels mòduls criptogràfics

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

6.3 Altres aspectes de gestió del parell de claus

6.3.1 Arxiu de la clau pública

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

6.3.2 Períodes d'utilització de les claus pública i privada

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

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

6.4 Dades d'activació

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

La generació i instal·lació de les dades d'activació es basa en el Cryptographic Service Provider.

6.4.2 Protecció de les dades d'activació

L'usuari és responsable de tenir cura de la seva clau privada, amb una contrasenya el més completa possible, a través de l'aplicació (Cryptographic Service Provider).

S'aconsella que l'esmentada contrasenya no sigui massa curta i formada per números i lletres.

El subscriptor ha de recordar l'esmentada contrasenya.

6.4.3 Altres aspectes de les dades d'activació

Sense estipulació addicional.

6.5 Controls de seguretat informàtica

6.5.1 Requisits tècnics específics de seguretat informàtica

Es garanteix que l'accés als sistemes és limitat a individus degudament autoritzats. En particular:

- L'EC-idCAT garanteix una administració efectiva del nivell d'accés dels usuaris (operadors, administradors, així com de qualsevol usuari amb accés directe al sistema) per mantenir la seguretat del sistema, incloent la gestió de comptes d'usuari, auditoria i modificacions o denegacions d'accés oportunes.
- L'EC-idCAT garanteix que l'accés als sistemes d'informació i aplicacions es restringeix d'acord a l'establert en la política de control d'accés, així com que els sistemes proporcionen els controls de seguretat suficients per implementar la segregació de funcions identificada en les pràctiques de l'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 està restringit i estretament controlat.
- El personal de l'EC-idCAT està identificat i reconegut abans d'utilitzar aplicacions crítiques relacionades amb el cicle de vida del certificat.
- El personal de l'EC-idCAT és responsable i ha de poder justificar les seves activitats, per exemple mitjançant un arxiu d'esdeveniments.
- S'ha d'evitar la possibilitat de revelació de dades sensibles mitjançant la reutilització d'objectes d'emmagatzematge (per exemple fitxers esborrats) que quedin accessibles a usuaris no autoritzats.
- Els sistemes de seguretat i monitoratge permeten una ràpida detecció, registre i actuació davant d'intents d'accés irregulars o no autoritzats als seus recursos (per exemple, mitjançant un sistema de detecció d'intrusions, monitoratge i alarma).
- L'accés als dipòsits públics de la informació de l'EC-idCAT (per exemple, certificats o informació d'estat de revocació) compte amb un control d'accésos per a modificacions o esborrament de dades.

6.5.2 Avaluació del nivell de seguretat informàtica

Les aplicacions de EC i ER són fiables, d'acord amb l'especificació tècnica CEN CWA 14167-1, i s'avalua el grau de compliment mitjançant una auditoria de seguretat informàtica conforme amb l'especificació tècnica CEN CWA 14172-3 i un perfil de protecció adequat, d'acord amb la norma ISO 15408 o equivalent.

6.6 Controls tècnics del cicle de vida

6.6.1 Controls de desenvolupament de sistemes

Es realitza una anàlisi de requisits de seguretat durant les fases de disseny i especificació de requisits de qualsevol component utilitzat en les aplicacions d'Autoritat (tècnica) de certificació i d'Autoritat (tècnica) de Registre, per garantir que els sistemes són segurs.

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

6.6.2 Controls de gestió de seguretat

L'EC-IdCAT garanteix que les seves funcions de gestió de les operacions dels mòduls criptogràfics són suficientment segures i, en particular, ha d'assegurar que existeixen instruccions per:

- a. Operar els mòduls de forma correcta i segura.

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

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

La configuració dels sistemes s'audita de forma periòdica.

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

6.6.3 Avaluació del nivell de seguretat del cicle de vida

Sense estipulació addicional.

6.7 Controls de seguretat de xarxa

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

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

6.8 Segell de temps

Sense estipulació addicional.

7. Perfils de certificats i llistes de certificats revocats

7.1 Perfil de certificat

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

7.2 Perfil de la llista de revocació de certificats

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

8. Auditoria de conformitat

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

L'EC-idCAT pot delegar l'execució de les auditories a una tercera entitat, en aquest cas, coopera completament amb el personal que porta a terme la investigació.

8.1 Freqüència de l'auditoria de conformitat

L'EC-idCAT porta a terme una auditoria de conformitat anualment, a més de les auditories internes que realitza sota el seu propi criteri o en qualsevol moment, a causa d'una sospita d'incompliment d'alguna mesura de seguretat o per un compromís de claus.

8.2 Identificació i qualificació de l'auditor

Si l'EC-idCAT disposa d'un departament d'auditoria interna, aquest pot encarregar-se de realitzar l'auditoria de conformitat.

En el cas de no tenir aquest departament, l'EC-idCAT pot acudir a un auditor independent extern, el qual ha de demostrar experiència en seguretat informàtica, en seguretat de Sistemes d'Informació i en auditories de conformitat d'Autoritats de Certificació i els elements relacionats.

8.3 Relació de l'auditor amb l'entitat auditada

Les auditories externes de conformitat executades per tercers estan realitzades per una entitat independent de l'EC-IdCAT auditada. En cas d'auditoria interna, l'EC-IdCAT s'ha d'assegurar que no existeix cap conflicte d'interessos que afecti negativament la seva capacitat de realitzar serveis d'auditoria.

8.4 Relació d'elements objecte d'auditoria

Els elements objecte d'auditoria seran els següents:

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

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

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

Si l'EC-idCAT 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 ha de realitzar-se una de les següents accions:

-
- Revocar la clau de l'EC-idCAT, de la forma com es descriu en aquest document.
 - Acabar el servei de l'EC-idCAT, de la forma com es descriu en aquest document.

8.6 Tractament dels informes d'auditoria

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

9. Requisits comercials i legals

9.1 Tarifes

9.1.1 Tarifa d'emissió o renovació de certificats

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

9.1.2 Tarifa d'accés a certificats

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

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

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

9.1.4 Tarifes d'altres serveis

Sense estipulació addicional.

9.1.5 Política de reintegrament

CATCert no practicarà reintegraments. En cas de productes defectuosos, es procedirà a substituir el producte defectuós per un altre en bon estat.

9.2 Capacitat financera

9.2.1 Assegurança de responsabilitat civil

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

9.2.2 Altres actius

Sense estipulació addicional.

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

En cas d'ús incorrecte o no autoritzat dels certificats, CATCert 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.

9.3 Confidencialitat

9.3.1 Informacions confidencials

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

- a. Informació de negoci subministrada pels seus proveïdors i altres persones amb qui CATCert o l'EC-idCAT té una obligació de guardar secret, establerta legalment o convencionalment.
- b. Registres de transaccions, incloent els registres complets i els registres d'auditoria de les transaccions.

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

9.3.2 Informacions no confidencials

Les següents informacions no tenen caràcter confidencial:

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

9.3.3 Responsabilitat per la protecció d'informació confidencial

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

Aquestes mesures inclouen 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 reglamentaria d'aplicació en matèria de protecció de dades de caràcter personal

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

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

SUBSCRIPTORS DE CERTIFICATS:

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

PERSONES FÍSQUES CERTIFICADES:

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

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

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

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

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

- a. Àmbit d'aplicació del document de seguretat amb especificació detallada dels recursos protegits (article 88 del RD 1720/2007) - secció 6.1
- b. Mesures, normes, procediments, regles i estàndards que garanteixin el nivell de seguretat exigít pel RD 1720/2007 - secció 9.4, i, en general, tots els controls tècnics de les seccions 5 i 6 de la Política General de Certificació de CATCert.
- c. Funcions i obligacions del personal (article 89 del RD 1720/2007) - secció 5.3.
- d. Registre d'incidències (article 90 del RD 1720/2007), procediment de notificació, gestió i resposta davant les incidències – secció 9.4.5
- e. Control d'accés (article 91 del RD 1720/2007) – seccions 5 i 6.
- f. Gestió de suports (article 92 del RD 1720/2007) – secció 5.
- g. Identificació i autenticació (article 93 del RD 1720/2007) – secció 5.2.
- h. Procediments de còpia de seguretat i recuperació de dades (article 94 del RD 1720/2007) - secció 5.5.

9.4.2. Dades de caràcter personal no disponibles a tercers

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

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

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

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

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

9.4.3. Dades de caràcter personal disponibles a tercers

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

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

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

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

- a. Els certificats emesos o en tràmit d'emissió.
- b. La subjecció del subscriptor a un certificat emès per l'Entitat de Certificació.
- c. El nom i els cognoms del subscriptor del certificat, així com qualssevol altres circumstàncies o dades personals del titular, en el supòsit que siguin significatives en funció de la finalitat del certificat, d'acord amb aquest document.
- d. L'adreça electrònica del subscriptor del certificat.
- e. Els usos i límits econòmics ressenyats al certificat.
- f. El període de validesa del certificat, així com la data d'emissió del certificat i la data de caducitat.

-
- g. El número de sèrie del certificat.
 - h. Els diferents estats o situacions del certificat i la data de l'inici de cada un d'ells, en concret: pendent de generació i/o lliurament, vàlid, revocat, suspès o caducat i el motiu que va provocar el canvi d'estat.
 - i. Les llistes de revocació de certificats (LRCs), així com la resta d'informacions d'estat de revocació.
 - j. La informació continguda en la part pública del Registre de l'Entitat de Certificació.

9.4.4. Responsabilitat corresponent a la protecció de les dades personals

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

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

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

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

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

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

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

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

- Quin recurs té la incidència
- El seu codi i descripció
- El dia i l'hora

-
- El tipus d'incidència
 - Els efectes
 - El comunicant i el destinatari
 - La resposta
 - Els procediments previstos a realitzar
 - La persona que els realitzarà
 - El procediment per a la recuperació
 - La persona (i autorització) per a la recuperació
 - Les dades restaurades.

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

Per a la prestació del servei, CATCert necessita recollir i emmagatzemar certes informacions que comporta tractament de dades personals. CATCert informa els subscriptors de l'obtenció de les seves dades personals de conformitat amb l'article 5 de la LOPD.

9.4.7. Comunicació de dades personals

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

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

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

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

9.5 Drets de propietat intel·lectual

9.5.1 Propietat dels certificats i informació de revocació

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

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

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

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

Aquesta normativa resulta d'aplicació en l'ús d'informació de revocació de certificats.

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

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

L'EC-idCAT és propietària de la seva Declaració de Pràctiques de Certificació.

9.5.3 Propietat de la informació relativa a noms

El subscriptor, conserva qualsevol dret, quan existeixi aquest, relatiu a la marca, producte o nom comercial contingut al certificat.

El subscriptor és el propietari del nom distingit del certificat, format per les informacions especificades a la secció 3.1, sense perjudici del dret de tercers.

9.5.4 Propietat de claus

Els parells de claus són propietat dels subscriptors dels certificats.

Quan una clau es trobi fraccionada en parts, totes les parts de la clau són propietat del propietari de la clau.

9.6 Obligacions i responsabilitat civil

9.6.1 Entitats de Certificació

9.6.1.1 Obligacions i altres compromisos

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

- a. L'EC-idCAT garanteix sota la seva plena responsabilitat, que compleix amb tots els requisits establerts en aquest document.
- b. L'EC-idCAT és l'única entitat responsable del compliment dels procediments descrits en aquest document, inclòs quan una part o la totalitat de les operacions són sub-contractades externament.
- c. L'EC-idCAT presta els seus serveis de certificació d'acord amb aquest document, en el qual es detallen 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'EC-idCAT l'informa dels aspectes previstos a l'article 18.b) de la Llei 59/2003, 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
 - b) Forma en que es garanteix la responsabilitat patrimonial de l'EC-idCAT
 - c) Si l'EC-idCAT és declarada d'acord 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 i la certificació dels productes de signatura electrònica utilitzats.
- e. Aquest requisit es compleix mitjançant un "Text divulgatiu de la política de certificat" aplicable, que és transmès electrònicament, utilitzant un mitjà de comunicació que duri en el temps, i llenguatge comprensible.

-
- f. L'EC-idCAT obliga als subscriptors i als verificadors mitjançant instruments jurídics apropiats a cada situació.
- g. Aquests instruments jurídics poden ser transmesos electrònicament, estan en llenguatge escrit i comprensible, i tenen els següents continguts mínims:
- a) Prescripcions per donar compliment a l'establert en la política de certificació.
 - 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.
 - d) Consentiment per a la publicació del certificat en el directori i accés per tercers al mateix.
 - e) Consentiment per a l'emmagatzematge de la informació utilitzada per al registre del subscriptor, 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'EC-idCAT sense revocació de certificats vàlids.
 - f) Límits d'ús del certificat, incloent les establertes a la secció 4.5 d'aquest document.
 - 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 en el certificat, que resulta aplicable quan el subscriptor actua com a verificador.
 - h) Limitacions de responsabilitat aplicables, incloent els usos pels quals l'EC-idCAT accepta o exclou la seva responsabilitat.
 - i) Procediments aplicables de resolució de disputes.
 - j) Llei aplicable i jurisdicció competent.
 - k) L'EC-idCAT ha d'identificar el subscriptor del certificat, d'acord amb els articles 12 i 13 de la Llei 59/2003 i el present document i, en concret:
 - a) La EC-IdCAT comprova per si mateixa o per mitjà d'una Entitat de Registre, la identitat i qualssevol altres circumstàncies personals dels sol·licitants dels certificats, d'acord amb l'establert a l'article 13 de la Llei 59/2003.
 - l) L'EC-idCAT compleix la resta d'obligacions contingudes a l'article 12 de la Llei 59/2003.

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

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 aquest document.

Adicionalment a l'establert a la secció corresponent, l'eina jurídica que vincula l'EC-idCAT i el subscriptor està en llenguatge escrit i comprensible, i té els següents continguts mínims:

- a. Indicació que els certificats s'expedeixen al públic i de la necessitat d'ús de dispositiu segur de creació de signatura, com s'indica a la secció 6.2.8 d'aquest document.
- b. Certificació de serveis de l'EC-idCAT.
- c. Forma que es garanteix la responsabilitat patrimonial de l'EC-idCAT.

9.6.1.2 Garanties ofertes a subscriptors i verificadors

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

- a. El compliment de les seves obligacions legals com a prestador de serveis de certificació, d'acord amb la Llei 59/2003, de 19 de desembre.
- b. Que no hi hagi errors de fet, en les informacions contingudes als certificats, coneguts o realitzats per l'EC-idCAT 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. La responsabilitat de l'EC-idCAT, amb els límits que s'estableixin.
- f. Que els serveis de revocació i l'ús del directori compleixin tots els requisits materials establerts en la DPC.

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

- a. 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.
- b. 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.
- c. La informació que conté o que incorpora per referència al certificat és correcta, excepte quan s'indiqui el contrari.
- d. 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.
- e. Que en l'aprovació de la sol·licitud de certificat i en l'emissió del certificat s'han complert tots els requisits materials establerts en aquest document.
- f. La rapidesa i seguretat en la prestació dels serveis, en especial dels serveis de revocació

Adicionalment, l'EC-idCAT garanteix 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.

9.6.2 Entitats de Registre

9.6.2.1 Obligacions i altres compromisos

9.6.2.1.1 Entitat de Registre

L'EC-idCAT pot delegar algunes funcions a Entitats de Registre, que en aquest cas queden obligades al seu compliment, en les mateixes condicions que l'EC-idCAT.

L'Entitat de Registre actua en el seu propi nom, sense perjudici de la responsabilitat de l'EC-idCAT.

L'Entitat de Registre 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 realitza les comprovacions que considera necessàries sobre la identitat i la resta de dades personals i complementàries dels subscriptors.

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

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

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

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

9.6.2.2 Garanties ofertes a subscriptors i verificadors

9.6.2.2.1 Garantia de CATCert pels serveis de certificació digital

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

CATCert únicament garanteix que:

- a) Els certificats idCAT contenen tota la informació exigida per la Llei 59/2003, de 19 de desembre.
- b) CATCert no ha originat ni ha introduït declaracions falses o errònies en la informació de cap certificat, ni ha deixat d'incloure informació necessària aportada pel subscriptor i validada per CATCert o per l'entitat de registre, en el moment de l'emissió del certificat.
- c) Tots els certificats compleixen els requisits formals i de contingut.
- d) CATCert queda vinculada pels procediments operatius i de seguretat descrits en aquest document.

9.6.2.2.2 Exclusió de la garantia

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

9.6.3 Subscriptors

9.6.3.1 Obligacions i altres compromisos

L'EC-idCAT obliga el subscriptor a:

- a. Facilitar a l'EC-idCAT informació completa i adequada, en especial pel que respecta al procediment de registre.
- b. Manifestar el seu consentiment previ a l'emissió i entrega d'un certificat.
- c. Complir les obligacions que s'estableixen per al subscriptor en aquest document i a l'article 23.1 de la Llei 59/2003, de 19 de desembre, de signatura electrònica.
- d. Utilitzar el certificat d'acord amb l'establert a la secció 1.4.
- e. Notificar a l'EC-idCAT, sense retards injustificables, la pèrdua, l'alteració, l'ús no autoritzat, el robatori o el compromís del seu dispositiu segur de creació de signatura.
- f. Notificar l'EC-idCAT i qualsevol persona que el subscriptor cregui que pugui confiar en el certificat, sense retards injustificables:
 - a) La pèrdua, el robatori o el compromís potencial de la seva clau privada.
 - b) La pèrdua de control sobre la seva clau privada, a causa del compromís de les dades d'activació (per exemple, el codi PIN del dispositiu segur de creació de signatura) o per qualsevol altra causa.
 - c) Les inexactituds o canvis en el contingut del certificat que conegui o pugués conèixer el subscriptor.
- g. Deixar d'utilitzar la clau privada transcorregut el període indicat a la secció corresponent.
- h. No monitorar, manipular o realitzar actes d'enginyeria reversa sobre la implantació tècnica de la Jerarquia de l'Agència Catalana de Certificació, sense permís previ per escrit.
- i. No comprometre intencionadament la seguretat de la Jerarquia de l'Agència Catalana de Certificació.
- j. Utilitzar el parell de claus exclusivament per a firmes electròniques i conforme a qualsevol altres limitacions que li siguin notificades.
- k. Reconèixer que aquestes firmes electròniques són firmes electròniques equivalents a firmes manuscrites, d'acord amb l'article 3.4 de la Llei 59/2003, de 19 de desembre.
- l. 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.
- m. El subscriptor genera les seves pròpies claus, per tant, s'obliga a:

1. Generar les seves claus de subscriptor utilitzant un algoritme reconegut com a acceptable per a la signatura electrònica reconeguda.
2. Crear la claus dins del dispositiu segur de creació de signatura.
3. Utilitzar longituds i algoritmes de clau reconeguts com a acceptables per a la signatura electrònica reconeguda.
- n. Notificar a l'EC, sense retards injustificables, la pèrdua, l'alteració, l'ús no autoritzat, el robatori o el compromís del seu dispositiu segur de creació de signatura.

9.6.3.2 Garanties ofertes pel subscriptor

L'EC-idCAT obliga el subscriptor, mitjançant el corresponent instrument jurídic, a garantir:

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

9.6.3.3 Protecció de la clau privada

L'EC-idCAT obliga el subscriptor, mitjançant el corresponent instrument jurídic, a garantir que el subscriptor és l'únic responsable dels danys causats pel seu incompliment del deure de protegir la clau privada.

9.6.4 Verificadors

9.6.4.1 Obligacions i altres compromisos

L'EC-idCAT ha d'obligar l'usuari de certificats a:

- a. Assessorar-se sobre el fet que el certificat és apropiat per a l'ús que es pretén.
- b. Verificar la validesa, suspensió o revocació dels certificats emesos, per a la qual cosa utilitza informació sobre l'estat dels certificats.
- c. Verificar tots els certificats de la jerarquia de certificats, abans de confiar en la signatura digital o en algun dels certificats de la jerarquia.
- d. Tenir present qualsevol limitació en l'ús del certificat, amb independència que es trobi al mateix certificat o al contracte de verificador.

- e. Tenir present qualsevol precaució establerta en un contracte o en un altre instrument, amb independència de la seva naturalesa jurídica.
- f. No monitorar, manipular o realitzar actes d'enginyeria inversa sobre la implantació tècnica de la jerarquia pública de certificació de Catalunya, sense permís previ per escrit.
- g. No comprometre intencionadament la seguretat de la jerarquia pública de certificació de Catalunya.

9.6.4.2 Garanties ofertes pel verificador

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

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

9.7 Renúncies de garanties

9.7.1 Rebuig de garanties de l'Entitat de Certificació

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

9.8 Limitacions de responsabilitat

9.8.1 Limitacions de responsabilitat de l'Entitat de Certificació

L'EC-idCAT limita la seva responsabilitat restringint el servei a l'emissió i gestió de certificats i, en el seu cas, de parells de claus de subscriptors i dipòsits criptogràfics (de signatura i verificació de signatura, així com de xifrat o desxifrat).

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

9.8.2 Cas fortuït i força major

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

9.9 Indemnitzacions

9.9.1 Clàusula d'indemnitat de subscriptor

No s'estableix clàusula d'indemnitat del subscriptor.

9.9.2 Clàusula d'indemnitat de verificador

No s'estableix clàusula d'indemnitat del verificador.

9.10 Termini i acabament

9.10.1 Termini

L'EC-idCAT estableix, als seus instruments jurídics amb els subscriptors i els verificadors, una clàusula que determina el període de vigència de la relació jurídica en virtut de la qual subministra certificats als subscriptors.

9.10.2 Finalització

L'EC-idCAT estableix, als seus instruments jurídics amb els subscriptors i els verificadors, una clàusula que determina les conseqüències de l'acabament de la relació jurídica en virtut de la que subministra certificats als subscriptors.

9.10.3 Supervivència

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

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

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

9.11 Notificacions

L'EC-idCAT estableix, als seus instruments jurídics vinculants amb subscriptors i verificadors, clàusules de notificació.

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

9.12 Modificacions

9.12.1 Procediment per a les modificacions

L'EC-idCAT pot modificar, de forma unilateral, aquest document, sempre que procedeixi segons el següent procediment:

- La modificació ha d'estar justificada des del punt de vista tècnic, legal o comercial.
- La modificació proposada per l'EC-idCAT no pot anar en contra de la política de certificació establerta per CATCert.

- S'estableix un control de modificacions, per garantir, en tot cas, que les especificacions resultants compleixen els requisits que s'intenten complir i que van donar peu al canvi.
- S'estableixen les implicacions que el canvi d'especificacions té sobre l'usuari, i es preveu la necessitat de notificar-li les esmentades modificacions.
- La nova política ha de ser aprovada per CATCert.

9.12.2 Circumstàncies en les que un OID ha de ser canviat

Sense estipulació addicional.

9.13 Resolució de conflictes

9.13.1 Resolució extrajudicial de conflictes

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

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

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

9.13.2 Jurisdicció competent

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

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

Quan l'EC-idCAT tingui la consideració d'Administració Pública es té en compte la legislació administrativa que resulti aplicable.

9.14 Llei aplicable

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

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

9.15 Conformitat amb la llei aplicable

L'EC-idCAT manifesta el compliment de la Llei 59/2003, en aquest document, i als instruments jurídics amb subscriptors i verificadors.

9.16 Clàusules diverses

9.16.1 Acord íntegre

L'EC-idCAT estableix, als seus instruments jurídics vinculants amb subscriptors i verificadors, clàusules d'acord íntegre.

En virtut de la clàusula d'acord íntegre s'entén que l'eina jurídica reguladora del servei conté la voluntat completa i tots els acords entre les parts.

9.16.2 Subrogació

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

En cas que es produeixi una cessió o subrogació, es procedeix a l'acabament de l'EC-idCAT.

9.16.3 Divisibilitat

L'EC-idCAT estableix, els seus instruments jurídics vinculants amb subscriptors i verificadors, clàusules de divisibilitat.

En virtut de la clàusula de divisibilitat, la invalidesa d'una clàusula no afecta la resta del contracte.

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

9.16.4 Aplicacions

Sense estipulació addicional.

9.16.5 Altres clàusules

Sense estipulació addicional.

ANNEX I

Control documental

Projecte:	Informe modificació del document DPC EC-idCAT
Entitat de destí:	Agència Catalana de Certificació
Codi de referència:	Revisió 1r semestre 2011
Versió:	Canvis de la v3.3 a la 3.4 en català i en castellà
Data de l'edició:	30/06/2011

Control de versions DPC EC-idCAT 1r semestre 2011

Versió	Parts que canvien	Descripció del canvi	Autor del canvi	Data del canvi
3.3	Apartat 4.8	Redactat nou	Oficina de Polítiques	28/06/2011
3.3	Apartat 5.8.2	Redactat nou. Obligació de conservar la documentació per a les ER en cas de finalització de servei	Oficina de Polítiques	30/06/2011
3.3	Apartat 6.1.5	Actualització mides claus	Oficina de Polítiques	30/06/2011