



**Consorci
Administració Oberta
de Catalunya**

Declaració de Pràctiques de Certificació
Entitat de Certificació Secretaria d'Administració i Funció Pública

(EC-SAFP)

Referència: D1111_E0650_N-DPC EC-SAFP
Versió: 5.0
Data: 05/08/2016

Control documental

Estat formal	Elaborat per: Servei de Certificació Digital	Aprovat per: Direcció del Consorci AOC
Data de creació	26/09/2006	
Control de versions	Data:	05/08/2016
	Descripció:	Revisió global – integració de CATCert a Consorci AOC
Nivell accés informació	pública	
Títol	Declaració de Pràctiques de Certificació – Entitat de Certificació Secretaria d'Administració i Funció Pública	
Fitxer	D111 E0650 N-DPC EC-SAFP v5r0 CAT	
Control de còpies	Només les còpies disponibles a https://www.aoc.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 3.0 Espanya de Creative Commons. Per veure'n una còpia, visiteu http://creativecommons.org/licenses/by-nc-nd/3.0/es/deed.ca envieu una carta a Creative Commons, 171 Second Street, Suite 300, San Francisco, California 94105, USA.</p>	

Índex

Índex.....	3
1. Introducció.....	11
1.1 PRESENTACIÓ	11
1.1.1 Tipus i classes de certificats	12
1.1.2 Relació entre la Declaració de Pràctiques de Certificació (DPC) i altres documents.....	19
1.2 NOM DEL DOCUMENT I IDENTIFICACIÓ.....	19
1.2.1 Identificació d'aquest document	19
1.2.2 Identificació de polítiques de certificació cobertes per aquesta DPC	19
1.3 COMUNITAT D'USUARIS DE CERTIFICATS.....	21
1.3.1 Prestadors de serveis de certificació	22
1.3.2 Entitat de Certificació Arrel	22
1.3.3 EC-SAFP	22
1.3.4 Entitats de Registre	22
1.3.5 Usuaris finals.....	23
1.4 ÚS DELS CERTIFICATS.....	24
1.4.1. Usos típics dels certificats.....	24
1.4.2. Aplicacions prohibides.....	32
1.5 ADMINISTRACIÓ DE LA DECLARACIÓ DE PRÀCTIQUES	35
1.5.1 Organització que administra l'especificació	35
1.5.2 Dades de contacte de l'organització	35
1.5.3 Persona que determina la conformitat d'una Declaració de Pràctiques de Certificació (DPC) amb la política	35
1.5.4 Procediment d'aprovació	35
2. Publicació d'informació i directori de certificats	36
2.1. DIRECTORI DE CERTIFICATS	36
2.2. PUBLICACIÓ D'INFORMACIÓ DE L'EC-SAFP	36
2.3. FREQUÈNCIA DE PUBLICACIÓ	36
2.4. CONTROL D'ACCÉS.....	37
3. Identificació i autenticació.....	38
3.1. GESTIÓ DE NOM	38
3.1.1. Tipus de noms.....	38
3.1.2. Significat dels noms	38
3.1.3. Utilització d'anònims i pseudònims	38
3.1.4. Interpretació de formats de noms	38

3.1.5.	Unicitat dels noms	38
3.1.6.	Resolució de conflictes relatius a noms	38
3.2.	VALIDACIÓ INICIAL DE LA IDENTITAT	38
3.2.1.	Prova de possessió de clau privada	38
3.2.2.	Autenticació de la identitat d'una organització	39
3.2.3.	Autenticació de la identitat d'una persona física	39
3.2.4.	Informació no verificada	40
3.3.	IDENTIFICACIÓ I AUTENTICACIÓ DE SOL·LICITUDS DE RENOVACIÓ	40
3.3.1.	Validació per a la renovació de certificats	40
3.3.2.	Validació per a la renovació de certificats després de la revocació	40
4.	Característiques d'operació del cicle de vida dels certificats	41
4.1	SOL·LICITUD D'EMISSIÓ DE CERTIFICAT	41
4.1.1	Legitimació per sol·licitar l'emissió	41
4.1.2	Procediment d'alta; Responsabilitats	42
4.2	PROCESSAMENT DE LA SOL·LICITUD DE CERTIFICACIÓ	42
4.2.1.	Requisits generals per a tots els certificats	42
4.2.2.	Requisits específics per al CEIXSA	43
4.2.3.	Informacions addicionals per al CDS-1, el CDS-1 EV, el CDSCD y el CDS-1 de Seu electrònica EV	43
4.2.4.	Requisits específics per al CIPISR	43
4.3	EMISSIÓ DE CERTIFICAT	44
4.3.1	Accions de l'EC-SAFP durant el procés d'emissió	44
4.3.2.	Notificació de l'emissió al subscriptor	45
4.4.	ACCEPTACIÓ DEL CERTIFICAT	45
4.4.1.	Responsabilitats de l'Entitat de Registre	45
4.4.2.	Conducta que constitueix acceptació del certificat	46
4.4.3.	Publicació del certificat	46
4.4.4.	Notificació de l'emissió a tercers	47
4.5.	ÚS DEL PARELL DE CLAUS I DEL CERTIFICAT	47
4.5.1.	Ús del parell de claus pels posseïdors de claus i ús dels certificats pels subscriptors	47
4.5.2.	Ús pel tercer que confia en certificats	49
4.6.	RENOVACIÓ DE CERTIFICATS SENSE RENOVACIÓ DE CLAUS	49
4.7.	RENOVACIÓ DE CERTIFICATS AMB RENOVACIÓ DE CLAUS	49
4.8.	MODIFICACIÓ DE CERTIFICATS	49
4.9.	REVOACIÓ I SUSPENSÍO DE CERTIFICATS	49
4.9.1.	Causes de revocació de certificats	49

4.9.2.	Legitimació per a sol·licitar la revocació	51
4.9.3.	Procediments de sol·licitud de revocació.....	52
4.9.4.	Període temporal de sol·licitud de revocació	52
4.9.5.	Període màxim de processament de la sol·licitud de revocació.....	52
4.9.6.	Obligació de consulta de informació de revocació de certificats	52
4.9.7.	Freqüència d'emissió de llistes de revocació de certificats (LRCs).....	53
4.9.8.	Període màxim de publicació de LRCs.....	53
4.9.9.	Disponibilitat de serveis de comprovació d'estat de certificats.....	53
4.9.10.	Obligació de consulta de serveis de comprovació d'estat de certificats.....	53
4.9.11.	Altres formes d'informació de revocació de certificats	54
4.9.12.	Requisits especials en cas de compromís de la clau privada.....	54
4.9.13.	Causes de suspensió de certificats.....	54
4.9.14.	Legitimitat per sol·licitar la suspensió.....	55
4.9.15.	Procediments de sol·licitud de suspensió	55
4.9.16.	Període màxim de suspensió.....	56
4.9.17.	Habilitació d'un certificat suspès	56
4.10.	SERVEIS DE COMPROVACIÓ D'ESTAT DE CERTIFICATS.....	56
4.10.1.	Característiques d'operació dels serveis.....	56
4.10.2.	Disponibilitat dels serveis.....	56
4.10.3.	Altres funcions dels serveis.....	56
4.11.	ACABAMENT DE LA SUBSCRIPCIÓ.....	57
4.12.	DIPÒSIT I RECUPERACIÓ DE CLAUS.....	57
4.12.1.	Política i pràctiques de dipòsit i recuperació de claus	57
4.12.2.	Política i pràctiques d'encapsulament i recuperació de claus de sessió	57
5.	Controls de seguretat física, de gestió i d'operacions	58
5.1.	CONTROLS DE SEGURETAT FÍSICA	58
5.1.1.	Localització i construcció de les instal·lacions	58
5.1.2.	Accés físic.....	58
5.1.3.	Electricitat i aire condicionat	58
5.1.4.	Exposició al'aigua.....	58
5.1.5.	Advertència i protecció d'incendis	58
5.1.6.	Emmagatzematge de suports.....	58
5.1.7.	Tractament de residus.....	58
5.1.8.	Còpia de seguretat fora de les instal·lacions	58
5.2.	CONTROLS DE PROCEDIMENTS	58
5.2.1.	Funcions fiables	59

5.2.2.	Nombre de persones per tasca	59
5.2.3.	Identificació i autenticació per a cada funció.....	59
5.2.4.	Rols que requereixen separació de tasques.....	59
5.3.	CONTROLS DE PERSONAL	59
5.3.1.	Requisits d'historial, qualificacions, experiència i autorització.....	60
5.3.2.	Requisits de formació	60
5.3.3.	Requisits ifreqüència d'actualització formativa	60
5.3.4.	Seqüènciaifreqüència de rotació laboral.....	60
5.3.5.	Sancions per accions no autoritzades	61
5.3.6.	Requisits de contractació de professionals.....	61
5.3.7.	Subministrament de documentació al personal	61
5.4.	PROCEDIMENTS D'AUDITORIA DE SEGURETAT.....	61
5.4.1.	Tipus d'esdeveniments registrats	61
5.4.2.	Freqüència de tractament de registres d'auditoria	61
5.4.3.	Període de conservació de registres d'auditoria	61
5.4.4.	Protecció dels registres d'auditoria	61
5.4.5.	Procediments de còpies de seguretat.....	61
5.4.6.	Localització del sistema d'acumulació de registres d'auditoria	62
5.4.7.	Notificació del'esdeveniment d'auditoria al causant del'esdeveniment	62
5.4.8.	Anàlisi de vulnerabilitats	62
5.5.	ARXIU D'INFORMACIONS.....	62
5.5.1.	Tipus d'esdeveniments registrats	62
5.5.2.	Període de conservació de registres	62
5.5.3.	Protecció del'arxiu	63
5.5.4.	Procediments de còpia suport	63
5.5.5.	Requisits de segellat de data i hora.....	63
5.5.6.	Localització del sistema d'arxiu	63
5.5.7.	Procediments d'obtenció i verificació d'informació d'arxiu	63
5.6.	RENOVACIÓ DE CLAUS	63
5.7.	COMPROMÍS DE CLAUS I RECUPERACIÓ DE DESASTRE	63
5.7.1.	Procediment de gestió d'incidències i compromisos.....	63
5.7.2.	Corrupció de recursos, aplicacions o dades	63
5.7.3.	Compromís de la clau privada de l'Entitat.....	63
5.7.4.	Desastre sobre les instal·lacions	64
5.8.	FINALITZACIÓ DEL SERVEI	64
5.8.1.	EC-SAFP.....	64

5.8.2.	Entitat de Registre	64
6.	Controls de seguretat tècnica	65
6.1.	GENERACIÓ I INSTAL·LACIÓ DEL PARELL DE CLAUS	65
6.1.1.	Generació del parell de claus	65
6.1.1.	Tramesa de la clau privada al subscriptor	66
6.1.3.	Enviament de la clau pública a l'emissor del certificat	66
6.1.4.	Distribució de la clau pública del Prestador de Serveis de Certificació	66
6.1.5.	Mides de claus	67
6.1.6.	Generació de paràmetres de clau pública	67
6.1.7.	Comprovació de qualitat de paràmetres de clau pública.....	67
6.1.8.	Generació de claus en aplicacions informàtiques o en bens d'equip	67
6.1.9.	Propòsits d'ús de claus.....	67
6.2.	PROTECCIÓ DE LA CLAU PRIVADA	67
6.2.1.	Mòduls de protecció de la clau privada.....	67
6.2.2.	Control per més d'una persona (n de m) sobre la clau privada.....	68
6.2.3.	Dipòsit de la clau privada	68
6.2.4.	Còpia de seguretat de la clau privada	68
6.2.5.	Arxiu de la clau privada	68
6.2.6.	Introducció de la clau privada en el mòdul criptogràfic.....	69
6.2.7.	Emmagatzematge de la clau privada en el mòdul criptogràfic	69
6.2.8.	Mètode d'activació de la clau privada	69
6.2.9.	Mètode de desactivació de la clau privada	69
6.2.10.	Mètode de destrucció de la clau privada	69
6.2.11.	Classificació dels mòduls criptogràfics	69
6.3.	ALTRES ASPECTES DE GESTIÓ DEL PARELL DE CLAUS	69
6.3.1.	Arxiu de la clau pública.....	69
6.3.2.	Períodes d'utilització de les claus pública i privada	70
6.4.	DADES D'ACTIVACIÓ.....	70
6.4.1.	Generació i instal·lació de les dades d'activació	70
6.4.2.	Protecció de les dades d'activació	70
6.4.3.	Altres aspectes de les dades d'activació	70
6.5.	CONTROLS DE SEGURETAT INFORMÀTICA.....	71
6.5.1.	Requisits tècnics específics de seguretat informàtica	71
6.5.2.	Avaluació del nivell de seguretat informàtica	71
6.6.	CONTROLS TÈCNICS DEL CICLE DE VIDA	71

6.6.1.	Controls de desenvolupament de sistemes	71
6.6.2.	Controls de gestió de seguretat	72
6.6.3.	Avaluació del nivell de seguretat del cicle de vida	72
6.7.	CONTROLS DE SEGURETAT DE XARXA.....	72
6.8.	SEGELL DE TEMPS	72
7.	Perfils de certificats illistes de certificats revocats	73
7.1.	PERFIL DE CERTIFICAT	73
7.2.	PERFIL DE LA LLISTA DE REVOCACIÓ DE CERTIFICATS.....	73
8.	Auditoria de conformitat	74
8.1.	FREQÜÈNCIA DE L' AUDITORIA DE CONFORMITAT	74
8.2.	IDENTIFICACIÓ I QUALIFICACIÓ DEL ' AUDITOR	74
8.3.	RELACIÓ DEL ' AUDITOR AMB L' ENTITAT AUDITADA	74
8.4.	RELACIÓ D' ELEMENTS OBJECTE D' AUDITORIA	74
8.5.	ACCIONS A EMPRENDRE COM A RESULTAT D' UNA FALTA DE CONFORMITAT	74
8.6.	TRACTAMENT DELS INFORMES D' AUDITORIA	74
9.	Requisits comercials i legals	75
9.1.	TARIFES	75
9.1.1.	Tarifa d'emissió o renovació de certificats	75
9.1.2.	Tarifa d'accés a certificats	75
9.1.3.	Tarifa d'accés a informació d'estat de certificat	75
9.1.4.	Tarifes d'altres serveis.....	75
9.1.5.	Política de reintegrament.....	75
9.2.	CAPACITAT FINANCERA.....	75
9.2.1.	Assegurança de responsabilitat civil.....	75
9.2.2.	Altres actius.....	75
9.2.3.	Cobertura d'assegurament per a subscriptors i tercers que confiïn en certificats	75
9.3.	CONFIDENCIALITAT	76
9.3.1.	Informacions confidencials	76
9.3.2.	Informacions no confidencials	76
9.3.3.	Responsabilitat per a la protecció d'informació confidencial	76
9.4.	PROTECCIÓ DE DADES PERSONALS	76
9.4.1.	Política de Protecció de Dades Personals.....	76
9.4.2.	Dades de caràcter personal no disponibles a tercers	76
9.4.3.	Dades de caràcter personal disponibles a tercers	76
9.4.4.	Responsabilitat corresponent a la protecció de dades personals	76
9.4.5.	Gestió d'incidències relacionades amb les dades de caràcter personal	77
9.4.6.	Prestació del consentiment per al tractament de les dades personals.....	77
9.4.7.	Comunicació de dades personals.....	77

9.5.	DRETS DE PROPIETAT INTEL·LECTUAL	77
9.5.1.	Propietat dels certificats i informació de revocació	77
9.5.2.	Propietat de la Política de Certificació i Declaració de Pràctiques de Certificació.....	77
9.5.3.	Propietat de la informació relativa a noms	77
9.5.4.	Propietat de claus.....	77
9.6.	OBLIGACIONS I RESPONSABILITAT CIVIL.....	77
9.6.1.	Entitats de Certificació.....	77
9.6.2.	Obligacions i altres compromisos de les Entitats de Registre	78
9.6.3.	Garanties oferides a subscriptors i verificadors	78
9.6.4.	Subscriptors	78
9.6.5.	Verificadors	78
9.6.6.	Altres participants.....	79
9.7.	RENÚNCIES DE GARANTIES.....	79
9.7.1.	Rebuig de garanties de l'EC-SAFP.....	79
9.8.	LIMITACIONS DE RESPONSABILITAT	79
9.8.1.	Limitacions de responsabilitat de l'EC-SAFP	79
9.8.2.	Cas fortuït i força major	79
9.9.	INDEMNITZACIONS	79
9.9.1.	Clàusula d'indemnitat de subscriptor	79
9.9.2.	Clàusula d'indemnitat de verificador	79
9.10.	TERMINI I FINALITZACIÓ	80
9.10.1.	Termini.....	80
9.10.2.	Finalització.....	80
9.10.3.	Supervivència	80
9.11.	NOTIFICACIONS	80
9.12.	MODIFICACIONS	80
9.12.1.	Procediment per a les modificacions.....	80
9.12.2.	Termini i mecanismes per a notificacions.....	80
9.12.3.	Circumstàncies en les que un OID ha de ser canviat	80
9.13.	RESOLUCIÓ DE CONFLICTES	80
9.13.1.	Resolució extrajudicial de conflictes.....	80
9.13.2.	Jurisdicció competent	81
9.14.	LLEI APLICABLE.....	81
9.15.	CONFORMITAT AMB LA LLEI APLICABLE.....	81
9.16.	CLÀUSULES DIVERSES	81
9.16.1.	Acord íntegre	81

9.16.2.	Subrogació	81
9.16.3.	Divisibilitat.....	81
9.16.4.	Aplicacions	81
9.16.5.	Altres clàusules.....	81
ANNEX – Control documental		82
CONTROL DE VERSIONS DPC EC-SAFP 1ER SEMESTRE 2016		82

1. Introducció

Aquest document és la Declaració de Pràctiques de Certificació de l'Entitat de Certificació 'Secretaria d'Administració i Funció Pública' (d'ara endavant, EC-SAFP), Entitat de Certificació de l'Administració de la Generalitat de Catalunya.

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

Els apartats amb el contingut "Sense estipulacions addicionals" indiquen que s'ha de consultar la Política General de Certificació del Consorci AOC.

1.1 Presentació

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

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

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

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

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

Aquestes institucions emetran certificats per mitjà d'una infraestructura tècnica proporcionada per CATCert, denominada "jerarquia pública de certificació de Catalunya", i

podran admetre i utilitzar certificats d'altres prestadors mitjançant els serveis de classificació i validació de CATCert.

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

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

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

L'EC-SAFP és l'Entitat de Certificació Vinculada a la jerarquia pública de certificació de Catalunya encarregada d'emetre certificats a les organitzacions, dispositius i personal al servei de l'Administració de la Generalitat de Catalunya.

L'Acord de Govern de 16 d'octubre de 2013, assigna la prestació de serveis de certificació al Consorci Administració Oberta de Catalunya (AOC), com a mesura de racionalització del sector públic, que es concreta en la integració de l'Agència Catalana de Certificació en el Consorci AOC, en el qual revertiran totes les marques, drets, deures i serveis gestionats fins a la data per CATCert.

La integració es va fer efectiva mitjançant l'esmentat acord amb efectes comptables i jurídics el 30 de juny de 2013, data en la qual el Consorci AOC assumeix els drets i obligacions així com la prestació del servei, incloent el Servei de Certificació Digital, responsable de l'emissió i gestió del cicle de vida dels certificats digitals. En endavant, el Consorci Administració Oberta de Catalunya és el prestador dels serveis de certificació (TSP) públics de Catalunya i el propietari de la infraestructura de clau pública (PKI) que abans era titularitat de CATCert.

1.1.1 Tipus i classes de certificats

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

Els certificats d'usuaris finals es divideixen en:

- Certificats d'infraestructura, caracteritzats pel fet que el posseïdor de la clau privada és un operador d'una infraestructura, i que s'utilitza per autoritzar operacions relacionades amb els serveis de certificació, com l'aprovació de sol·licituds de certificació.
- Certificats personals, caracteritzats pel fet que el posseïdor de la clau privada és una persona física, que en certificats de classe 1 actua habitualment en representació o per compte d'una persona jurídica.
- Certificats d'entitat, caracteritzats pel fet que el subscriptor del certificat i, d'acord amb la llei, el signant, és una persona jurídica, que actua per mitjà d'un posseïdor de claus.
- Certificats de dispositiu, caracteritzats pel fet que no hi ha un posseïdor de la clau privada sinó que són utilitzats per dispositius informàtics, que en certificats de classe 1 es troben sota la responsabilitat d'una persona jurídica.

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

La resta de certificats són certificats de classe 2. El registre de les dades per a l'emissió dels certificats de classe 2 el realitza sempre l'Entitat de Certificació o una entitat de Registre sota la responsabilitat de l'Entitat de Certificació, mitjançant la certificació administrativa prèvia de les dades, quan l'emissió es produeixi a un públic restringit, o mitjançant la captació directa de tota la informació necessària per a l'emissió dels certificats.

1.1.1.1. Certificats d'infraestructura

- Certificat d'infraestructura personals d'identificació i signatura electrònica reconeguda d'operadors (CIPISR), que s'empra per autoritzar operacions relacionades amb els serveis de certificació, com l'aprovació de sol·licituds de certificació.
- Certificat d'infraestructura de dispositiu servidor segur (CIDS), que és utilitzat per una aplicació informàtica servidor de SSL o de TLS d'infraestructura per identificar-se davant les aplicacions client que s'hi connecten i per protegir el secret de les comunicacions entre el client i el servidor, com per exemple els servidors de les entitats de certificació.
- Certificat d'infraestructura de dispositiu d'aplicació digitalment assegurada (CIDA), que és utilitzat per aplicacions informàtiques de la infraestructura que s'identifiquen digitalment, signen electrònicament webservices o altres protocols i que reben documents i missatges xifrats, com per exemple les aplicacions de notificació de missatges de les entitats de certificació.
- Certificat d'infraestructura de servidor d'estat de certificats en línia (CIO), que és utilitzat per un servidor *OCSP Responder* per signar les seves respostes sobre l'estat de validesa dels certificats.
- Certificat d'infraestructura d'entitat de segells de temps (CIT), que és utilitzat per una entitat per signar els segells de temps que emet.
- Certificat d'infraestructura d'entitat de validació (CIV), que és utilitzat per un servidor d'entitat de validació per signar els seus informes.

1.1.1.2. Certificats personals

L'EC-SAFP emet els següents tipus de certificats personals:

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

signar missatges amb dispositiu segur de creació de signatura, així com missatges d'autenticació i d'accés segur a sistemes informàtics.

- Certificats personals d'identificació i signatura electrònica reconeguda de classe 1 amb càrrec per a ús concret (CPISR-1 amb Càrrec ús), que identifiquen la persona que els posseeix, la seva organització subscriptora, el seu càrrec en aquesta, i les limitacions materials d'ús, i que serveixen per signar missatges amb dispositiu segur de creació de signatura, així com missatges d'autenticació i d'accés segur a sistemes informàtics
- Certificats personals d'identificació i de signatura electrònica reconeguda de classe 2 amb càrrec (CPISR-2 Càrrec), que identifiquen la persona que els posseeix, la seva organització subscriptora, i el seu càrrec en aquesta, i que serveixen per signar missatges amb dispositiu segur de creació de signatura, així com missatges d'autenticació i d'accés segur a sistemes informàtics.
- Certificats personals de xifrat de classe 1 (CPX-1), que identifiquen la persona que els posseeix, la seva organització subscriptora, i que s'utilitzen per produir o rebre missatges o documents confidencials, en qualsevol format. No permeten la signatura electrònica de missatges de dades.
- Certificats personals de xifrat de classe 1 amb càrrec (CPX-1 Càrrec), que identifiquen la persona que els posseeix, la seva organització subscriptora, i el seu càrrec en aquesta, i que s'utilitzen per rebre o produir missatges o documents confidencials en qualsevol format. No permeten la signatura electrònica de missatges de dades.
- Certificats personals de xifrat de classe 2 amb càrrec (CPX-2 Càrrec), que identifiquen la persona que els posseeix, la seva organització subscriptora, i el seu càrrec en aquesta, i que s'utilitzen per rebre o produir missatges o documents confidencials en qualsevol format. No permeten la signatura electrònica de missatges de dades.
- Certificats personals d'identificació, xifrat i signatura avançada, amb càrrec, de classe 1 (CPIXSA-1 Càrrec EP), que identifiquen la persona que els posseeix, la seva organització subscriptora, i que serveixen per signar missatges d'autenticació i d'accés segur a sistemes informàtics.

El certificat personal d'identificació i signatura reconeguda de classe 1 és un certificat reconegut d'acord amb l'establert a l'article 11.1 de la Llei 59/2003, de 19 de desembre, de signatura electrònica, amb el contingut prescrit per l'article 11.2, i emès complint les obligacions dels articles 12, 13, 18 i 20 de la Llei esmentada. Funciona amb dispositiu segur de creació de signatura electrònica, d'acord amb l'article 24.3 de la Llei 59/2003, de 19 de desembre, i donen compliment al disposat per la normativa tècnica de l'Institut Europeu de Normes de Telecomunicacions. Garanteixen la identitat del subscriptor i del posseïdor de la clau privada d'identificació i signatura, i permeten la generació de la "signatura electrònica reconeguda"; és a dir, la signatura electrònica avançada que es basa en un certificat reconegut i que ha estat generada utilitzant un dispositiu segur, per la qual cosa, de conformitat amb el que estableix l'article 3 de la Llei 59/2003, de 19 de desembre, s'equipara a la signatura escrita per efecte legal, sense necessitat de cap compliment de requisit addicional.

També es poden utilitzar en aplicacions que no requereixen la signatura electrònica equivalent a la signatura manuscrita, sinó només la identificació del posseïdor de claus, en nom de la Institució

El certificat personal d'identificació i de signatura electrònica reconeguda de classe 1 amb càrrec (CPISR-1 Càrrec), i el certificat d'identificació i de signatura electrònica reconeguda de classe 1 amb càrrec per a ús concret (CPISR-1 Càrrec ús) són certificats reconeguts d'acord amb l'establert a l'article 11.1 de la Llei 59/2003, de 19 de desembre, de signatura electrònica, amb el contingut prescrit per l'article 11.2, i emesos complint les obligacions dels articles 12, 13, 18 i 20 de la Llei esmentada. Funcionen amb dispositiu segur de creació de signatura electrònica, d'acord amb l'article 24.3 de la Llei 59/2003, de 19 de desembre, i donen compliment al disposat per la normativa tècnica de l'Institut Europeu de Normes de Telecomunicacions. Garanteixen la identitat del subscriptor i del posseïdor de la clau privada d'identificació i signatura, i permeten la generació de la "signatura electrònica reconeguda"; és a dir, la signatura electrònica avançada que es basa en un certificat reconegut i que ha estat generada utilitzant un dispositiu segur, per la qual cosa, de conformitat amb el que estableix l'article 3 de la Llei 59/2003, de 19 de desembre, s'equipara a la signatura escrita per efecte legal, sense necessitat de cap compliment de requisit addicional. A més inclouen una manifestació relativa a la categoria de personal i càrrec del posseïdor de claus, que ha estat comprovada abans d'emetre el certificat, i és correcta. Tanmateix, aquesta indicació no és, per si sola, suficient per determinar les facultats que té el posseïdor de claus per signar en nom del subscriptor; per tant, l'usuari del certificat comprova les facultats i poders de signatura del posseïdor mitjançant altres mitjans, diferents del certificat. També es poden utilitzar en aplicacions que no requereixen la signatura electrònica equivalent a la signatura escrita, sinó només la identificació del posseïdor de claus, en nom de la Institució.

El certificat personal d'identificació i de signatura electrònica reconeguda de classe 2 amb càrrec (CPISR-2 Càrrec), és un certificat reconegut d'acord amb l'establert a l'article 11.1 de la Llei 59/2003, de 19 de desembre, de signatura electrònica, amb el contingut prescrit per l'article 11.2, i emès complint les obligacions dels articles 12, 13, 18 i 20 de la Llei esmentada. Funciona amb dispositiu segur de creació de signatura electrònica, d'acord amb l'article 24.3 de la Llei 59/2003, de 19 de desembre, i dóna compliment al disposat per la normativa tècnica de l'Institut Europeu de Normes de Telecomunicacions. Garanteixen la identitat del subscriptor i del posseïdor de la clau privada d'identificació i signatura, i permet la generació de la "signatura electrònica reconeguda"; és a dir, la signatura electrònica avançada que es basa en un certificat reconegut i que ha estat generada utilitzant un dispositiu segur, per la qual cosa, de conformitat amb el que estableix l'article 3 de la Llei 59/2003, de 19 de desembre, s'equipara a la signatura escrita per efecte legal, sense necessitat de cap compliment de requisit addicional. A més, inclou una manifestació relativa al càrrec del posseïdor de claus, que ha estat comprovada abans d'emetre el certificat, i és correcta. Tanmateix, aquesta indicació no és, per si sola, suficient per determinar les facultats que té el posseïdor de claus per signar en nom del subscriptor; per tant, l'usuari del certificat comprova les facultats i poders de signatura del posseïdor mitjançant altres mitjans, diferents del certificat. També es pot utilitzar en aplicacions que no requereixen la signatura electrònica equivalent a la signatura escrita, sinó només la identificació del posseïdor de claus, en nom de la Institució.

El certificat personal de xifrat de classe 1 (CPX-1) és un certificat reconegut de conformitat amb el que s'estableix a l'article 6 i 11.1, amb el contingut prescrit per l'article 11.2 i emès

complint les obligacions dels articles 12, 13, i 17 a 20 de la Llei 59/2003, de 19 de desembre, de signatura electrònica. Funciona amb dispositiu segur de creació de signatura electrònica, d'acord amb l'article 24.3 de la Llei 59/2003, de 19 de desembre, i que compleixen allò disposat per la normativa tècnica de l'Institut Europeu de Normes de Telecomunicacions. Garanteixen la identitat del subscriptor i del posseïdor de la clau privada d'identificació i signatura, i permeten xifrar documents i rebre missatges de dades confidencials, en qualsevol format.

El certificat personal de xifrat de classe 1 amb càrrec (CPX-1 Càrrec) es un certificat reconegut de conformitat amb el que s'estableix a l'article 6 i 11.1, amb el contingut prescrit per l'article 11.2 i emès complint les obligacions dels articles 12, 13, i 17 a 20 de la Llei 59/2003, de 19 de desembre, de signatura electrònica. Funciona amb dispositiu segur de creació de signatura electrònica, d'acord amb l'article 24.3 de la Llei 59/2003, de 19 de desembre, i compleix allò disposat per la normativa tècnica de l'Institut Europeu de Normes de Telecomunicacions. Garanteix la identitat del subscriptor i del posseïdor de la clau privada d'identificació i signatura, i permet xifrar documents i rebre missatges de dades confidencials, en qualsevol format. A més inclouen una manifestació relativa a la categoria de personal i càrrec del posseïdor de claus, que ha estat comprovada abans d'emetre el certificat, i és correcta. Tanmateix, aquesta indicació no és, per si sola, suficient per determinar les facultats que té el posseïdor de claus per signar en nom del subscriptor; per tant, l'usuari del certificat comprova les facultats i poders de signatura del posseïdor mitjançant altres mitjans, diferents del certificat. També es pot utilitzar en aplicacions que no requereixen la signatura electrònica equivalent a la signatura escrita, sinó només la identificació del posseïdor de claus, en nom de la Institució.

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

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

1.1.1.3. Certificats d'entitat

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

- Certificats d'entitat d'identificació i signatura electrònica reconeguda de classe 1 (CEISR-1), d'acord amb l'establert en l'article 7 de la Llei 59/2003, de 19 de desembre, de signatura electrònica, que permet que Institucions públiques i privades, corporacions de dret públic i persones juridico-públiques (col·lectivament anomenades "entitats") signin documents amb dispositiu segur de creació de signatura, missatges d'autenticació (confirmació de la identitat) i d'accés segur a sistemes informàtics.

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

Adicionalment, en funció dels requeriments tècnics y de les necessitats dels usuaris, és possible que aquests tipus de certificats puguin incorporar altres funcionalitats que, en tot cas, seran identificades en una política específica de certificació, que serà desenvolupada o aprovada pel Consorci AOC.

1.1.1.4. Certificats de dispositiu

L'EC-SAFP emet els següents tipus de certificats de dispositiu:

- Certificat de dispositiu servidor segur de classe 1 (CDS-1), que s'utilitza per una aplicació informàtica, servidor de SSL o de TLS, perquè s'identifiqui davant de les aplicacions client que es connecten i per protegir el secret de les comunicacions entre el client i el servidor.
- Certificat de dispositiu servidor segur de classe 1 Extended Validation (CDS-1EV), que s'utilitza per una aplicació informàtica, servidor de SSL o de TLS, perquè s'identifiqui davant de les aplicacions client que es connecten i per protegir el secret de les comunicacions entre el client i el servidor, tot oferint la validació automàtica al navegador.
- Certificat de dispositiu de seu electrònica nivell mig de classe 1 Extended Validation (CDS-1 SENMEV), que serveix per identificar i garantir una comunicació segura amb la seu electrònica d'un ens, entenent seu electrònica en els termes que la descriu l'article 10 de la Llei 11/2007 d'accés electrònic dels ciutadans als serveis públics.

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

El certificat de nivell mig, amb unes claus de 1024 bits, és recomanable per a la majoria de les administracions públiques que poden tenir els següents riscos: infracció de seguretat (p.ex. robatori de la identitat), pèrdues econòmiques moderades, pèrdua d'informació sensible o crítica o refutació d'una transacció amb impacte econòmic significatiu.

El certificat de nivell mig es lliurarà en suport programari.

- Certificat de dispositiu de seu electrònica nivell alt de classe 1 Extended Validation (CDS-1 SENA EV), que serveix per identificar i garantir una comunicació segura amb la seu electrònica d'un ens, entenent seu electrònica en els termes que la

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

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

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

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

- Certificat de dispositiu segur de controlador de domini de classe 1 (CDSCD-1), s'utilitza per una aplicació informàtica, servidor SSL o TLS, per a autenticar en una xarxa Windows als usuaris que pertanyen a un determinat domini, mitjançant un certificat digital de signatura amb targeta criptogràfica.
- Certificat de dispositiu d'aplicació (CDA), que emmagatzemat en un servidor i requerit per una aplicació, signa documents o missatges.
- Certificat de dispositiu de segell electrònic de Administració, òrgan o entitat de dret públic nivell mig de classe 1 (CDA-1 SENM), És un certificat digital que serveix per a la identificació i l'autenticació de l'exercici de la competència en l'actuació administrativa automatitzada, en els termes descrits en l'article 18 de la Llei 11/2007 d'accés electrònic dels ciutadans als serveis públics. Aquest certificat es pot utilitzar per a l'intercanvi de dades entre administracions, la identificació i autenticació d'un sistema, servei web o aplicació, l'arxiu electrònic automatitzat, les compulses i còpies electròniques, entre d'altres.

El certificat de nivell mig, amb unes claus de 1024 bits, és recomanable per a la majoria de les administracions públiques que poden tenir els següents riscos: infracció de seguretat (p.ex. robatori de la identitat), pèrdues econòmiques moderades, pèrdua d'informació sensible o crítica o refutació d'una transacció amb impacte econòmic significatiu.

- Certificat de dispositiu de segell electrònic de Administració, òrgan o entitat de dret públic nivell alt de classe 1 (CDA-1 SENA), serveix per a la identificació i l'autenticació de l'exercici de la competència en l'actuació administrativa automatitzada, en els termes descrits en l'article 18 de la Llei 11/2007 d'accés electrònic dels ciutadans als serveis públics.

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

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

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

- Certificat de dispositiu de programari o de signatura d'aplicacions informàtiques de classe 1 (CDP-1), que serveix per signar electrònicament les aplicacions informàtiques o programari a transmetre a través d'Internet. Així, els usuaris finals poden signar elements com applets, scripts, executables, etc.

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

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

L'EC-SAFP emet certificats dins de la Jerarquia pública de certificació de l'Agència Catalana de Certificació. Per tant, disposa d'una Declaració de Pràctiques de Certificació (DPC) d'acord amb la Política General de Certificació del Consorci AOC.

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

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

1.2 Nom del document i identificació

1.2.1 Identificació d'aquest document

Aquest document s'anomena "Declaració de Pràctiques de Certificació (DPC) de l'EC-SAFP".

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

1.3.6.1.4.1.15096.1.2.4

1.2.2 Identificació de polítiques de certificació cobertes per aquesta DPC

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

- **CIPISR** – Certificat d'infraestructura d'operador, emès per l'EC-SAFP
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.15
Classe 2. OID: 1.3.6.1.4.1.15096.1.3.1.16
- **CIC** – Certificat d'infraestructura d'Entitat de Certificació Vinculada, emès per l'EC-SAFP
CIC-1. OID: 1.3.6.1.4.1.15096.1.3.1.11

- CIC-2. OID: 1.3.6.1.4.1.15096.1.3.1.12
- CIC-3. OID: 1.3.6.1.4.1.15096.1.3.1.13
- **CIDS-1** – Certificat de infraestructura de servidor segur, emès per l'EC-SAFP
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.17
- **CIDA-1** – Certificat d'infraestructura d'aplicació, emès per l'EC-SAFP
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.18
- **CIO-1** – Certificat d'infraestructura de servidor d'estat de certificats en línia, emès per l'EC-SAFP
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.19
- **CIV-1** – Certificat d'infraestructura d'entitat de validació, emès per l'EC-SAFP
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.20
- **CIT-1** - Certificat d'infraestructura d'entitat de segells de temps, emès per l'EC-SAFP
Classe 1. 1.3.6.1.4.1.15096.1.3.1.111
- **CPISR-1** - Certificat personal d'identificació i signatura electrònica reconeguda, emès per l'EC-SAFP
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.81
- **CPISR-1 amb Càrrec** – Certificat personal d'identificació i signatura electrònica reconeguda amb càrrec, emès per la EC-SAFP
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.21.2.4.
- **CPISR-1 amb Càrrec Ús**- Certificat personal d'identificació i signatura electrònica reconeguda amb càrrec per a ús concret, emès per l'EC-SAFP
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.81.3.1.
- **CPISR-2 amb Càrrec** – Certificat personal d'identificació i signatura electrònica reconeguda amb càrrec, emès per la EC-SAFP
Classe 2. OID: 1.3.6.1.4.1.15096.1.3.1.82.3.4.
- **CPX-1** - Certificat personal de xifrat, emès per l'EC-SAFP
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.41
- **CPX-1 Càrrec** - Certificat personal de xifrat amb càrrec, emès per l'EC-SAFP
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.41.1.4
- **CPX-2 Càrrec** - Certificat personal de xifrat amb càrrec, emès per l'EC-SAFP
Classe 2. OID: 1.3.6.1.4.1.15096.1.3.1.42.3.4
- **CPIXSA-1 Càrrec EP** - Certificat personal d'identificació, xifrat i signatura avançada amb càrrec d'empleat públic, emès per l'EC-SAFP
OID: 1.3.6.1.4.1.15096.1.3.1.85.2
- **CEISR-1** – Certificat d'entitat d'identificació amb signatura electrònica reconeguda, emès per l'EC-SAFP
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.121.2
- **CEX-1** – Certificat d'entitat de xifrat emès per l'EC-SAFP
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.131.1

- **CEIXSA-1** – Certificats d'entitat d'identificació, xifrat i signatura electrònica avançada emès per l'EC-SAFP
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.161.2
- **CDS-1** - Certificat de dispositiu servidor segur, emès per l'EC-SAFP
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.51
- **CDS-1EV**- Certificat de dispositiu servidor segur Extended Validation, emès per l'EC-SAFP
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.51.4
- **CDS-1 seu electrònica nivell mig EV** – Certificat de dispositiu servidor segur, seu electrònica nivell mig Extended Validation, emès per l'EC-SAFP
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.51.2
- **CDS-1 seu electrònica nivell alt EV** – Certificat de dispositiu servidor segur, seu electrònica nivell alt Extended Validation, emès per l'EC-SAFP
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.51.3
- **CDA-1** - Certificat de dispositiu d'aplicació digitalment assegurada, emès per l'EC-SAFP
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.91
- **CDA-1 segell electrònic nivell mig** -Certificat de dispositiu d'aplicació digitalment assegurada, segell electrònic nivell mig, emès per l'EC-SAFP
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.91.1
- **CDA-1 segell electrònic nivell alt** -Certificat de dispositiu d'aplicació digitalment assegurada, segell electrònic nivell alt, emès per l'EC-SAFP
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.91.2
- **CDP-1** - Certificat de dispositiu de signatura de programari, emès per l'EC-SAFP
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.71
- **CDSCD-1**- Certificat de dispositiu segur de controlador de domini, emès per l'EC-SAFP
Classe 1. OID: 1.3.6.1.4.1.15096.1.3.1.51.1

Els documents descriptius d'aquests perfils de certificats es publiquen en el web del Consorci AOC.

1.3 Comunitat d'usuaris de certificats

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

Els certificats de l'EC-SAFP no s'expedeixen al públic, sinó a les entitats, al personal i als dispositius de la Administració de la Generalitat de Catalunya.

1.3.1 Prestadors de serveis de certificació

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

El Consorci AOC serà el prestador de serveis de certificació de l'EC-SAFP.

Conforme a aquesta funció, el Consorci AOC serà responsable per l'actuació de l'EC-SAFP, davant els usuaris finals i els tercers verificadors de certificats i signatures electròniques, per l'actuació de les autoritats de certificació que operen en nom de les diferents entitats de certificació.

1.3.2 Entitat de Certificació Arrel

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

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

1.3.3 EC-SAFP

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

1.3.4 Entitats de Registre

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

Els diversos Organismes, Departaments i Empreses Públiques de l'Administració de la Generalitat poden actuar com a Entitats de Registre.

El procés de creació d'entitats de registre és responsabilitat de l'administrador de l'Entitat de Certificació. Mitjançant acord o conveni es constitueix l'entitat de registre. El Consorci AOC 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). El Consorci AOC validarà les peticions de certificats de les Entitats de Registre examinant la sol·licitud i fent les comprovacions necessàries per al compliment d'aquesta Política General de Certificació i de la Declaració de Pràctiques de Certificació.

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

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

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

1.3.5 Usuaris finals

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

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

1.3.5.1 Sol·licitants de certificats

Els sol·licitants dels certificats indicats en aquesta DPC són les persones autoritzades per les entitats subscriptores.

Poden ser sol·licitants:

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

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

1.3.5.2 Subscriptors de certificats

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

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

1.3.5.3 Posseïdors de claus

Els posseïdors de claus són les persones físiques que posseeixen de forma exclusiva les claus privades dels certificats, que estan degudament autoritzades pel subscriptor per al

seu ús i degudament identificades al certificat mitjançant el seu nom i cognoms o mitjançant un pseudònim.

1.3.5.4 Usuaris de certificats

Els usuaris dels certificats són els verificadors.

1.3.5.5 Verificadors de certificats

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

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

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

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

1.4 Ús dels certificats

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

1.4.1. Usos típics dels certificats

1.4.1.1. Certificats d'infraestructura

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

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

Els certificats d'infraestructura d'identificació i signatura reconeguda són certificats reconeguts d'acord amb el que s'estableix a l'article 11.1, amb el contingut prescrit per l'article 11.2 i emesos complint les obligacions dels articles 12, 13, i 17 a 20 de la Llei 59/2003, de 19 de desembre, de signatura electrònica.

Els CIPISR funcionen amb dispositiu segur de creació de signatura electrònica, d'acord amb l'article 24.3 de la Llei 59/2003, de 19 de desembre, i que donen compliment a allò disposat per la normativa tècnica de l'Institut Europeu de Normes de Telecomunicacions, identificada amb la referència TS 101 456.

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

Els CIPIISR són certificat d'operador i el seu ús exclusiu és l'operació dels components de la infraestructura de clau pública del Consorci AOC com, per exemple, els components emprats per les Entitats de Registre per aprovar i generar certificats, o per revocar-los, o pel servei d'atenció a usuaris per suspendre certificats.

Els CIPIISR corresponents a l'Entitat de Certificació seran emesos per la pròpia Entitat de Certificació, amb l'aprovació prèvia del Consorci AOC.

Els CIPIISR corresponents a cada Entitat de Certificació Vinculada a l'Entitat de Certificació seran emesos per la pròpia Entitat de certificació, amb l'aprovació prèvia de l'Entitat de Certificació.

1.4.1.1.2. Requisits específics per al CIDS

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

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

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

1.4.1.1.3. Requisits específics per al CIDA

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

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

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

1.4.1.1.4. Requisits específics per al CIO

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

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

1.4.1.1.5. Requisits específics per al CIT

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

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

1.4.1.1.6. Requisits específics per al CIV

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

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

1.4.1.2. Certificats personals

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

Els certificats personals d'identificació i signatura reconeguda de classe 1, els certificats personals d'identificació i signatura reconeguda de classe 1 amb càrrec, i els Certificats personals d'identificació i signatura electrònica reconeguda de classe 1 amb càrrec per a ús concret, són certificats reconeguts d'acord amb el que s'estableix en l'article 11.1, amb el contingut prescrit per l'article 11.2 i emesos complint les obligacions dels articles 12, 13, i 17 a 20 de la Llei 59/2003, de 19 de desembre, de signatura electrònica, i que donen compliment al disposat per la normativa tècnica de l'Institut Europeu de Normes de Telecomunicacions, identificada amb la referència TS 101 456.

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

Per aquest motiu, aquests certificats garanteixen la identitat del subscriptor i del posseïdor de la clau privada d'identificació i signatura, i permeten la generació de la signatura electrònica reconeguda; és a dir, la signatura electrònica avançada que es basa en un certificat reconegut i que ha estat generada utilitzant un dispositiu segur, per la qual cosa, d'acord amb el que estableix l'article 3 de la Llei 59/2003, de 19 de desembre, s'equipara a

la signatura escrita per efecte legal, sense necessitat de complir cap altre requeriment addicional.

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

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

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

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

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

El certificat personal de xifrat de classe 1 és un certificat reconegut d'acord amb el que s'estableix en l'article 11.1, amb el contingut prescrit per l'article 11.2 i emès complint les obligacions dels articles 12, 13, i 17 a 20 de la Llei 59/2003, de 19 de desembre, de signatura electrònica, i que dóna compliment al disposat per la normativa tècnica de l'Institut Europeu de Normes de Telecomunicacions, identificada amb la referència TS 101 456.

Es tracta d'un certificat reconegut que funciona amb dispositiu segur de creació de signatura electrònica, d'acord amb l'article 24.3 de la Llei 59/2003, de 19 de desembre.

Els certificats personals de xifrat s'utilitzen exclusivament per a xifrar documents i rebre missatges de dades confidencials, en qualsevol format, protegits mitjançant el xifrat del text del missatge, per part del remitent del missatge. El posseïdor de la clau utilitza la seva clau privada per desxifrar el missatge.

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

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

El certificat personal de xifrat de classe 1 amb càrrec és un certificat reconegut d'acord amb el que s'estableix en l'article 11.1, amb el contingut prescrit per l'article 11.2 i emès complint les obligacions dels articles 12, 13, i 17 a 20 de la Llei 59/2003, de 19 de desembre, de signatura electrònica, i que dóna compliment al disposat per la normativa tècnica de l'Institut Europeu de Normes de Telecomunicacions, identificada amb la referència TS 101 456.

Es tracta d'un certificat reconegut que funciona amb dispositiu segur de creació de signatura electrònica, d'acord amb l'article 24.3 de la Llei 59/2003, de 19 de desembre. Els certificats personals de xifrat s'utilitzen exclusivament per a xifrar documents i rebre missatges de dades confidencials, en qualsevol format, protegits mitjançant el xifrat del text del missatge, per part del remitent del missatge.

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

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

El certificat personals d'identificació i signatura reconeguda de classe 2 amb càrrec, és un certificat reconegut d'acord amb el que s'estableix en l'article 11.1, amb el contingut prescrit per l'article 11.2 i emès complint les obligacions dels articles 12, 13, i 17 a 20 de la Llei 59/2003, de 19 de desembre, de signatura electrònica, i que dona compliment al dispostat per la normativa tècnica de l'Institut Europeu de Normes de Telecomunicacions, identificada amb la referència TS 101 456.

Es tracta d'un certificat reconegut que funciona amb dispositiu segur de creació de signatura electrònica, d'acord amb l'article 24.3 de la Llei 59/2003, de 19 de desembre.

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

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

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

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

1.4.1.2.5. Certificats personals de xifrat de classe 2 amb càrrec (CPX-2 càrrec)

El certificat personal de xifrat de classe 2 amb càrrec és un certificat reconegut d'acord amb el que s'estableix en l'article 11.1, amb el contingut prescrit per l'article 11.2 i emès complint les obligacions dels articles 12, 13, i 17 a 20 de la Llei 59/2003, de 19 de desembre, de signatura electrònica, i que dona compliment al dispostat per la normativa tècnica de l'Institut Europeu de Normes de Telecomunicacions, identificada amb la referència TS 101 456.

Es tracta d'un certificat reconegut que funciona amb dispositiu segur de creació de signatura electrònica, d'acord amb l'article 24.3 de la Llei 59/2003, de 19 de desembre.

Els certificats personals de xifrat amb càrrec s'utilitzen exclusivament per xifrar documents i rebre missatges de dades confidencials, en qualsevol format, protegits mitjançant el xifrat del text del missatge, per part del remitent del missatge.

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

1.4.1.2.6 Certificats personals d'identificació, xifrat i signatura avançada, amb càrrec, d'empleat públic de classe 1 (CPIXSA-1 Càrrec EP)

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

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

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

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

Es pot utilitzar per a diversos usos, entre els quals:

- Autenticació en servidors web que requereixin la presentació del certificat digital.
- Autenticació en sistemes de control d'accés, de sistema operatiu o centralitzats.

1.4.1.3. Certificats d'entitat

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

Els certificats d'entitat d'identificació amb signatura reconeguda de classe 1 són certificats reconeguts, no emesos al públic, d'acord amb el que s'estableix en l'article 11.1, amb el contingut prescrit per l'article 11.2 i emès complint les obligacions dels articles 7, 12, 13, i 17 a 20 de la Llei 59/2003, de 19 de desembre, de signatura electrònica, i que donen compliment al disposat per la normativa tècnica de l'Institut Europeu de Normes de Telecomunicacions, identificada amb la referència TS 101 456.

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

Per aquest motiu, aquests certificats garanteixen la identitat del subscriptor i del posseïdor de la clau privada de signatura, essent idonis per a oferir suport a la signatura electrònica reconeguda de l'entitat; això és la signatura electrònica avançada que es basa en un certificat reconegut i que ha estat generada utilitzant un dispositiu segur, per la qual cosa, d'acord amb el que estableix l'article 3.4 de la Llei 59/2003, de 19 de desembre, s'equipara a la signatura escrita per efecte legal, sense necessitat de complir cap altre requeriment addicional.

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

Els certificats de entitat de xifrat de classe 1 són certificats reconeguts, no emesos al públic, que s'expedeixen a subscriptors i s'utilitzen exclusivament per xifrar o rebre missatges de dades confidencials, en qualsevol format, protegits mitjançant el xifrat del text del missatge, utilitzant la clau pública del subscriptor indicada al CEX.

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

El posseïdor de la clau utilitzarà la seva clau privada per a desxifrar els missatges. La clau privada del CEX s'arxivarà per l'entitat de certificació de manera que, en certes circumstàncies, pugui recuperar-se i accedir a la informació xifrada, fins i tot sense la intervenció del subscriptor.

1.4.1.3.3. Certificat d'Entitat d'Identificació, Xifrat i Signatura Electrònica Avançada de classe 1 (CEIXSA-1)

Els certificats d'entitat d'identificació, xifrat i signatura electrònica avançada de classe 1 són certificats reconeguts, no emesos al públic, d'acord amb el que s'estableix en l'article 11.1, amb el contingut prescrit per l'article 11.2 i emesos complint les obligacions dels articles 7, 12, 13, i 17 a 20 de la Llei 59/2003, de 19 de desembre, de signatura electrònica, i que donen compliment al disposat per la normativa tècnica de l'Institut Europeu de Normes de Telecomunicacions, identificada amb la referència TS 101 456.

S'utilitzen per a signar missatges d'autenticació (confirmació de la identitat) i d'accés segur a sistemes informàtics, per a rebre missatges de dades confidencials, en qualsevol format, protegits mitjançant el xifrat del text del missatge, utilitzant la clau pública del subscriptor indicada en el CEIXSA i per a signatura documents sense dispositiu segur de creació de signatura, donant suport a la signatura electrònica avançada segons l'article 3.2 de la Llei 59/2003, de 19 de desembre.

1.4.1.4. Certificats de Dispositiu

1.4.1.4.1. Certificats de dispositiu de servidor segur de classe 1 (CDS-1)

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

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

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

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

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

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

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

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

Els CDS-1 Seu electrònica Extended Validation s'emeten a les Institucions, responsables de l'operació de servidors segurs SSL o TLS, amb la finalitat d'identificar i garantir una comunicació segura amb la seu electrònica d'un ens, entenent-se seu electrònica en els termes de l'article 10 de la Llei 11/2007 d'accés electrònic dels ciutadans als serveis públics. Es tracta de certificats reconeguts que es poden utilitzar per a la connexió segura dels ciutadans a pàgines web oficials, l'autenticació d'un lloc web, l'allotjament de registres electrònics, la consulta i autorització de registres de representació, etc.

Es distingeixen dos certificats:

- El certificat de nivell mig, lliurat en suport programari, i amb unes claus de 1024 bits, és recomanable per a la majoria de les administracions públiques amb previsió dels següents riscos: infracció de seguretat (per exemple, robatori de la identitat), pèrdues econòmiques moderades, pèrdua d'informació sensible o crítica, o refutació d'una transacció amb impacte econòmic significatiu.
- El certificat de nivell alt, emmagatzemat en un HSM (maquinari criptogràfic), i amb unes claus de 2048 bits, és recomanable per a aquelles administracions públiques que, havent realitzat prèviament una anàlisi de riscos, precisen mesures addicionals de seguretat, al contemplar els següents riscos: infracció de seguretat, pèrdues econòmiques importants, pèrdua d'informació altament sensible i crítica o refutació d'una transacció amb impacte econòmic molt significatiu.

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

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

Els CDSCD s'emeten a les Institucions responsables de l'operació del controlador de domini, amb els següents usos:

- Autenticació del servidor
- Autenticació de l'usuari amb targeta criptogràfica

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

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

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

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

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

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

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

- El certificat de nivell mig, lliurat en suport programari, i amb unes claus de 1024 bits, és recomanable per a la majoria de les administracions públiques que poden tenir els següents riscos: infracció de seguretat (per exemple robatori de la identitat), pèrdues econòmiques moderades, pèrdua d'informació sensible o crítica, o refutació d'una transacció amb impacte econòmic significatiu.
- El certificat de nivell alt amb unes claus de 2048 bits, és recomanable per a aquelles administracions públiques que, havent realitzat prèviament una anàlisi de riscos, precisen mesures addicionals de seguretat, ja que contempnen els següents riscos: infracció de seguretat, pèrdues econòmiques importants, pèrdua d'informació altament sensible i crítica o refutació d'una transacció amb impacte econòmic molt significatiu.

1.4.1.4.6. Certificats de dispositiu de signatura de programari de classe 1 (CDP-1)

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

Aquests són certificats ordinaris, i que garanteixen la identitat de la persona responsable i l'origen i la integritat del programari signat.

1.4.2. Aplicacions prohibides

1.4.2.1. Informacions per a tots els tipus de certificats

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

Els certificats no s'han dissenyat, no es poden destinar i no 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.

1.4.2.2. Certificats d'infraestructura

1.4.2.2.1. Certificat d'infraestructura personal d'identificació i signatura reconeguda

Qualsevol altre ús no especificat a la secció anterior està expressament prohibit i la seva detecció donarà lloc a la immediata revocació del certificat CIPISR.

1.4.2.3. Certificats personals

1.4.2.3.1. Certificats personals d'identificació i signatura electrònica reconeguda

Els certificats CPISR-1, CPISR-1 amb Càrrec, CPISR-1 amb Càrrec ús, i CPISR-2 amb Càrrec no es poden utilitzar per a:

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

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

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

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

1.4.2.3.3. Certificat personal de xifrat

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

1.4.2.4. Certificats d'entitat

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

Els certificats CEISR no es poden utilitzar per a:

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

1.4.2.4.2 Certificats d'entitat de xifrat

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

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

Els CEIXSA no es poden utilitzar per a:

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

Realitzar signatura electrònica reconeguda de documents

1.4.2.5. Certificats de dispositiu

1.4.2.5.1 Certificats de dispositiu de servidor segur

Els CDS-1 i els CDS-1 EV no es poden utilitzar per signar peticions d'emissió, renovació, suspensió o revocació de certificats CIC, certificats de cap tipus o llistes de revocació de certificats (LRC).

1.4.2.5.2. Certificat de dispositiu de servidor segur seu electrònica

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

1.4.2.5.3 Certificats de dispositiu d'aplicació digitalment assegurada

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

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

1.4.2.5.4 Certificats de dispositiu d'aplicació digitalment assegurada segell electrònic

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

1.4.2.5.5 Certificats de dispositiu de signatura de programari

Sense estipulacions addicionals

1.5 Administració de la Declaració de Pràctiques

1.5.1 Organització que administra l'especificació

Consorti Administració Oberta de Catalunya – Consorci AOC

1.5.2 Dades de contacte de l'organització

Consorti Administració Oberta de Catalunya – Consorci AOC

Domicili social: Via Laietana, 26 – 08003 Barcelona

Adreça postal comercial: Tànger, 98, planta baixa (22@ Edifici Interface) - 08018 Barcelona

Web del Consorci AOC: www.aoc.cat

Web del servei de certificació digital del Consorci AOC:

www.aoc.cat/catcert

Servei d'Atenció al'Usuari: 902 901 080, en horari 24x7 per a la gestió de suspensions de certificats.

1.5.3 Persona que determina la conformitat d'una Declaració de Pràctiques de Certificació (DPC) amb la política

La persona que determina la conformitat d'una DPC amb la Política General de Certificació és el/la Responsable del Servei de Certificació Digital del Consorci AOC, basant-se en els resultats d'una auditoria al'efecte, realitzada per un tercer, bianualment.

1.5.4 Procediment d'aprovació

El sistema documental i d'organització de l'EC-SAFP 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.

Això inclou el procediment de modificació d'especificació del servei i el procediment de publicació d'especificacions de servei.

La versió inicial d'aquesta Declaració de pràctiques és aprovada per la Comissió Executiva del Consorci AOC, que és l'òrgan col·legiat de direcció executiva del Consorci.

El Director Gerent del Consorci AOC és competent per a aprovar les successives modificacions d'aquesta Declaració de pràctiques.

2. Publicació d'informació i directori de certificats

2.1. Directori de certificats

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

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

L'EC-SAFP publica les següents informacions, en el web del Consorci AOC (<http://www.aoc.cat/catcert/>):

- a) Les llistes de certificats revocats i altres informacions d'estat de revocació dels certificats.
- b) La política general de certificació
- c) Els perfils dels certificats i de les llistes de revocació dels certificats.
- d) La Declaració de Pràctiques de Certificació.
- e) Els instruments jurídics vinculants amb subscriptors i verificadors.

Tot canvi en les especificacions o condicions del servei es comunica als usuaris per part de l'EC-SAFP, a través del dipòsit.

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

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

2.3. Freqüència de publicació

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

Els canvis en aquest document es regeixen per l'establert a la secció 9.12.1.

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

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

Les versions antigues de la documentació són conservades, per un període de 15 (quinze) anys per l'EC-SAFP, podent ser consultada, per causa raonada pels interessats.

2.4. Control d'accés

Sense estipulacions addicionals.

3. Identificació i autenticació

3.1. Gestió de nom

En aquesta secció s'estableixen requisits relatius als procediments d'identificació i autenticació que s'utilitzen durant les operacions de registre que realitzen, amb anterioritat a l'emissió i lliurament de certificats, les Entitats de Registre.

3.1.1. Tipus de noms

3.1.1.1 Estructura sintàctica

Sense estipulacions addicionals.

3.1.1.2 Perfils dels certificats

Els perfils dels certificats emesos per l'EC-SAFP es publiquen al web del Consorci AOC (<http://www.aoc.cat/catcert/>).

3.1.2. Significat dels noms

Sense estipulacions addicionals.

3.1.3. Utilització d'anònims i pseudònims

No es poden fer servir pseudònims per a identificar una organització.

3.1.4. Interpretació de formats de noms

Sense estipulacions addicionals.

3.1.5. Unicitat dels noms

Sense estipulacions addicionals

3.1.6. Resolució de conflictes relatius a noms

Sense estipulacions addicionals.

Referent al tractament de marques registrades, veure l'apartat 9.5.3.

3.2. Validació inicial de la identitat

3.2.1. Prova de possessió de clau privada

Sense estipulacions addicionals.

3.2.2. Autenticació de la identitat d'una organització

Sense estipulacions addicionals.

3.2.2.1 Entitats de Registre

Sense estipulacions addicionals.

3.2.2.2 Subscriptors de Certificats

Sense estipulacions addicionals.

3.2.3. Autenticació de la identitat d'una persona física

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

3.2.3.1. Elements d'identificació

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

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

- Nom i cognoms de la persona
- Número d'identitat reconegut legalment (DNI, NIF o NIE dels països signants del Acord de Schengen; passaport en el cas dels certificats d'estranger)
- Data i lloc de naixement.
- Qualsevol altra informació que pugui ser utilitzada per a diferenciar a una persona d'altra, dintre del'àmbit de la Institució (per exemple: fotografia, correu-e, categoria, càrrec, etc.).

3.2.3.2. Validació dels elements d'identificació

La informació d'identificació de posseïdors de claus de certificats de Classe 1 és vàlida comparant la informació de la sol·licitud amb els registres interns de l'Entitat de Registre que s'assegura de la correcció de la informació a certificar.

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

La informació del posseïdor registrada la Institució en els últims cinc anys està actualitzada.

3.2.3.3. Necessitat de presència personal

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

Durant el tràmit de lliurament i acceptació del certificat i del corresponent dispositiu segur de creació de signatura, es realitza la validació definitiva de la identitat de la persona de conformitat amb els procediments operatius aprovats i la present DPC.

3.2.3.4. Vinculació de la persona física amb l'organització

En tractar-se de certificats corporatius, en què l'Entitat de Registre i el subscriptor coincideixen, no és necessari obtenir una justificació documental específica de la vinculació del posseïdor de claus.

3.2.4. Informació no verificada

L'EC-SAFP es responsabilitza que tota la informació inclosa en la sol·licitud del certificat sigui exactai completa per a la finalitat del certificat; i que té dret al seu ús (per exemple, dret a utilitzar cert nom en l'adreça de correuelectrònic o la legitimitat en l'ús d'un servidor web).

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

3.3. Identificació i autenticació de sol·licituds de renovació

3.3.1. Validació per a la renovació de certificats

Sense estipulacions addicionals.

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

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

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

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

4.1 Sol·licitud d'emissió de certificat

4.1.1 Legitimació per sol·licitar l'emissió

4.1.1.1 Certificats personals, d'entitat i de xifrat

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

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

- A través de les seves Entitats de Registre T-CAT
- Directament al Servei de Certificació Digital del Consorci AOC, de forma supletòria en cas que l'ens no tingui cap entitat de registre assignada. En aquest cas el Consorci AOC actuarà com a Entitat de Registre.

Aquesta sol·licitud requereix la tramesa d'un document amb la informació exacta i comprovada (certificat) de les persones o dispositius per a les que es demana el certificat. Aquesta sol·licitud se signa per la persona autoritzada pel subscriptor a la fitxa. També s'envia un certificat de dades.

També es pot acompanyar d'una adreça física, o altres dades, que permetin establir contacte directe amb el futur posseïdor de claus.

Tota la documentació es lliurarà a l'Entitat de registre telemàticament. Excepcionalment podrà ser lliurada en suport paper o mitjançant correu electrònic signat i xifrat, per les causes següents:

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

4.1.1.2 Altres certificats

Abans de l'emissió i lliurament d'un certificat, existeix una sol·licitud de certificat, acompanyada de la corresponent documentació acreditativa de les dades a certificar, la qual s'ha de gestionar pel responsable del sistema de certificació digital, encarregat de l'Entitat de Registre, directament al Consorci AOC.

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

4.1.2 Procediment d'alta; Responsabilitats

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

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

4.2 Processament de la sol·licitud de certificació

4.2.1. Requisits generals per a tots els certificats

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

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

1. Lliurament de la Fitxa del Subscriptor.

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

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

-Descàrrega de la fitxa del subscriptor

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

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

2. Obtenció dels certificats

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

Quan la sol·licitud hagi estat realitzada telemàticament, un cop completada la sol·licitud, cal signar-la digitalment pel sol·licitant, i en els certificats personals, també pel certificador. Un cop signada pel sol·licitant, automàticament s'envia un correu electrònic al certificador de l'ens avisant-lo que ha de verificar les dades de la sol·licitud del certificat.

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

El certificador de l'ens obre la sol·licitud signada anteriorment i, si comprova que les dades són correctes, la signa digitalment finalitzant el procés de sol·licitud. En aquest moment es fa automàticament l'assentament del registre de sortida de l'ens i d'entrada a la seva entitat de registre.

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

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

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

Els certificats es lliuraran dins dels terminis compromesos pel servei ordinari o pel servei urgent d'emissió i renovació de certificat – segons escaigui - al document “Catàleg de certificats i serveis” què es publica al web del Servei de Certificació Digital del Consorci AOC.

4.2.2. Requisits específics per al CEIXSA

Una vegada aprovada la sol·licitud, la EC-SAFP rep l'autorització de l'Entitat de Registre, recupera la corresponent sol·licitud, l'emmagatzema en l'estructura de certificats, sent signada per la EC-SAFP, completant així la generació del certificat.

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

4.2.3. Informacions addicionals per al CDS-1, el CDS-1 EV, el CDSCD y el CDS-1 de Seu electrònica EV

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

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

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

4.2.4. Requisits específics per al CIPISR

Adicionalment, l'Entitat de Certificació haurà de:

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

- Garantir la data i l'hora en què es va expedir un certificat.
- En cas que l'Entitat de Certificació aporti el dispositiu segur de creació de signatura, emprar un procediment de gestió de dispositius segurs de creació de signatura que assegurí que l'esmentat dispositiu és lliurat de forma segura al posseïdor de claus.
- Utilitzar sistemes i productes fiables que estiguin protegits contra tota alteració i que garanteixin la seguretat tècnica i, en el seu cas, criptogràfica dels processos de certificació als que serveixen de suport.
- Assegurar-se que el certificat és emès per sistemes que utilitzin protecció contra falsificació i, en cas que l'Entitat de Certificació generi claus privades, que garanteixin el secret de les claus durant el procés de generació de les esmentades claus.

4.3 Emissió de certificat

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

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

Per a cada sol·licitud de certificat tramitada, l'EC-SAFP 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.
- En cas de que l'Entitat de Certificació aporti el dispositiu segur de creació de signatura, utilitzar un procediment de gestió de dispositius segurs de creació de signatura que assegurí que aquest dispositiu és lliurat de forma segura al posseïdor de claus.
- Utilitzar sistemes i productes fiables que estiguin protegits contra tota alteració i que garanteixin la seguretat tècnica i, en el seu cas, criptogràfica dels processos de certificació als que serveixen de suport.

- Prendre mesures contra la falsificació de certificats i, en cas que l'Entitat de Certificació generi claus privades, que garanteixin el secret de les claus durant el procés de generació d'aquestes claus.

4.3.2. Notificació de l'emissió al subscriptor

El Consorci AOC notifica al subscriptor l'emissió del certificat, o la incidència corresponent.

4.4. Acceptació del certificat

4.4.1. Responsabilitats de l'Entitat de Registre

4.4.1.1. Per a Certificats personals

El Consorci AOC és l'encarregat de crear el parell de claus i el certificat dels subscriptors.

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

L'EC-SAFP generarà el full de lliurament per a cada posseïdor de claus.

El Consorci AOC enviarà mitjançant correu electrònic directament als posseïdors de claus els codis PIN i PUK.

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

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

Al full de lliurament de subscriptor s'indica a aquest:

- que s'ha demanat prèviament al responsable del servei de l'Entitat de Registre documentació completa i adequada de les dades dels respectius posseïdors, per a la seva identificació i relació amb el subscriptor,
- que aquest responsable del servei de l'Entitat de Registre es compromet a lliurar les targetes i els certificats als posseïdors, informar-los de les seves obligacions i responsabilitats, i a custodiar el full de lliurament de posseïdor degudament signat durant 15 anys,
- es demana al posseïdor que estigui informat sobre el tractament de les seves dades, respecte de la normativa de protecció de dades i que doni consentiment per al tractament i la inclusió de certes dades al certificat.

Al full de lliurament i acceptació del posseïdor, s'indica a aquest:

- quin és el règim obligatori d'ús de certificats digitals:
 - l'existència d'aquesta Declaració de Pràctiques de Certificació,
 - que els certificats són únics per a cada persona i estan protegits per un codi secret,

- que els certificats permeten identificar-se, generar signatures electròniques i, en el seu cas, desxifrar missatges,
- que ha de custodiar la targeta i el codi secret,
- que en cas d'indici que la seva identificació pot ser coneguda per altres persones ha de notificar-ho a la seva Entitat de Registre,
- Que en cas de necessitat d'informació addicional, pot dirigir-se a la seva Entitat de Registre,
- que pot exercir els seus drets inclosos en la Llei 15/1999, de 13 de desembre, sobre protecció de dades personals,
- que les seves dades poden ser cedides, en compliment de la legislació vigent sobre signatura electrònica i protecció de dades personals, i
- quins són els certificats inclosos a la targeta i el codi de suspensió
- que signa el document de lliurament, que hi està d'acord, una vegada lligides i enteses les obligacions i responsabilitats

4.4.1.2. Per a certificats de dispositiu

Els certificats de dispositiu es lliuraran mitjançant un fitxer que haurà de descarregar-se el responsable de l'entitat de registre virtual.

L'EC-SAFP generarà el full de lliurament per a cada posseïdor de claus. El Consorci AOC enviarà mitjançant correu electrònic directament als posseïdors de claus els codis PIN i PUK, si escau, segons el tipus de certificat.

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

4.4.2. Conducta que constitueix acceptació del certificat

El certificat s'accepta mitjançant la signatura del full de posseïdor de claus.

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

A través de l'aplicació telemàtica es podran obtenir informes de tots els certificats gestionats per l'Entitat de Registre Virtual en el moment actual o un recull històric.

4.4.2.1. Informacions addicionals per al CEIXSA-1

El subscriptor accepta el certificat, descarregant-lo de la web i no retornant-lo en 7 dies.

4.4.3. Publicació del certificat

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

4.4.4. Notificació de l'emissió a tercers

No aplicable.

4.5. Ús del parell de claus i del certificat

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

4.5.1.1. Informació per a tots els tipus de certificats

Els certificats s'utilitzen per permetre una millor seguretat en les comunicacions telemàtiques internes de les Institucions, entre elles, així com les que es realitzen amb la resta de la societat.

Els certificats s'utilitzen d'acord amb la seva funció pròpia i finalitat establerta, i no es poden utilitzar en altres funcions o amb altres finalitats.

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

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

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

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

4.5.1.2. Informacions addicionals per als certificats personals i de dispositiu

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

4.5.1.3. Informacions addicionals per al CIPISR

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

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

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

4.5.1.4. Informacions addicionals per al CPISR

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

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

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

4.5.1.5. Informacions addicionals per al CPIXSA

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

4.5.1.6. Informacions addicionals per al CPX

Els CPX s'utilitzen en conjunció amb un dispositiu de protecció de la clau privada de desxifrat, d'acord amb les característiques establertes en aquest document.

4.5.1.7. Informacions addicionals per al CEISR

Els CEISR s'utilitzen necessàriament amb un dispositiu segur de creació de signatura electrònica, que compleix les característiques establertes per l'article 24.3 de la Llei 59/2003, de 19 de desembre i aquesta Declaració de Pràctiques de Certificació (DPC).

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

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

4.5.1.8. Informacions addicionals per al CEX

Els CEX s'utilitzen en conjunció amb un dispositiu de protecció de la clau privada de desxifrat, d'acord amb les característiques establertes en aquest document.

4.5.1.9. Informacions addicionals per al CEIXSA

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

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

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

4.5.2. Ús pel tercer que confia en certificats

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

L'ús del certificat permet al tercer que confia, una identificació positiva, rebre i confiar en signatures electròniques i, en el seu cas, xifrar aquells missatges en els quals ha decidit preservar el seu contingut.

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

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

4.6. Renovació de certificats sense renovació de claus

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

4.7. Renovació de certificats amb renovació de claus

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

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

4.8. Modificació de certificats

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

4.9. Revocació i suspensió de certificats.

4.9.1. Causes de revocació de certificats

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

1. Circumstàncies que afecten la informació continguda al certificat
 - Modificació d'alguna de les dades contingudes al certificat.
 - Descobriment que alguna de les dades contingudes a la sol·licitud de certificat és incorrecta.
 - Descobriment que alguna de les dades contingudes al certificat és incorrecte.
2. Circumstàncies que afecten a la seguretat de la clau o del certificat
 - Compromís de la clau privada o de la infraestructura o sistemes de l'EC-SAFP, sempre que afecti la confiança en els certificats emesos a partir d'aquest incident.
 - Infracció, per a l'EC-SAFP, dels requisits previstos en els procediments de gestió de certificats.
 - Compromís o sospita de compromís de la seguretat de la clau o del certificat del subscriptor.
 - Accés o utilització no autoritzat, per un tercer, de la clau privada del subscriptor.
 - L'ús irregular del certificat pel subscriptor o falta de diligència en la custòdia de la clau privada.
3. Circumstàncies que afecten el dispositiu criptogràfic
 - Compromís o sospita de compromís de la seguretat del dispositiu criptogràfic.
 - Pèrdua o inutilització del dispositiu criptogràfic.
 - Accés no autoritzat, per un tercer, a les dades d'activació del subscriptor.
4. Circumstàncies que afecten el subscriptor o el posseïdor de claus
 - Final de la relació entre l'EC-SAFP i el subscriptor.
 - Modificació o extinció de la relació jurídica subjacent o causa que va provocar l'emissió del certificat al subscriptor.
 - Infracció per al sol·licitant del certificat dels requisits preestablerts per a la sol·licitud d'aquest.
 - Infracció per al subscriptor de les seves obligacions, responsabilitat i garanties, establertes a l'instrument jurídic corresponent de l'EC-SAFP.
 - La incapacitat sobrevinguda o la mort del subscriptor.
 - L'extinció de la persona jurídica subscriptora del certificat, així com la finalitat de l'autorització del subscriptor al posseïdor de claus o el final de la relació entre subscriptor i posseïdor de claus.
 - Sol·licitud del subscriptor de revocació del certificat.
5. Circumstàncies relatives als certificats Extended Validation
 - Sol·licitud del subscriptor.
 - L'Entitat de Certificació obté proves raonables de que la clau privada del subscriptor s'ha vist compromesa o que el certificat ha estat usurpat per un tercer.

- L'Entitat de Certificació rep notificació o comunicació per part d'un tribunal o àrbitre sobre la revocació del dret a utilitzar el nom de domini que figura en el certificat, o coneix la impossibilitat de renovar el domini.
 - L'Entitat de Certificació té coneixement de l'incompliment de les Condicions Generals d'Ús o d'altres especificacions establertes a la documentació jurídica o operativa.
 - L'Entitat de Certificació cessa activitats que donin suport a la revocació de certificats Extended Validation o perd el dret d'emetre certificats Extended Validation. Si l'Entitat de Certificació pot garantir el manteniment dels serveis de validació CRL i OCSP, la revocació no és necessària.
 - Compromís o sospita de compromís de les claus de qualsevol Entitat de Certificació de nivell superior en la jerarquia.
 - Revocació de les publicacions de les polítiques relatives a certificats Extended Validation.
 - Notificació de la inclusió d'un subscriptor al llistat de subscriptors prohibits (altrament, llistes negres, confeccionades per a víctimes de phishing o activitats d'enginyeria inversa).
6. Altres circumstàncies
- La suspensió del certificat digital per un període superior a 120 dies.
 - El final del servei de l'EC-SAFP, d'acord amb l'establert a la secció 5.8 d'aquest document.
 - La finalització de prestació de serveis per part del Consorci AOC, d'acord amb el que estableix la Política General de Certificació.
 - Resolució judicial o administrativa que ho ordeni (Art. 8.1 de la Llei 59/2003, de signatura electrònica).
 - L'EC-SAFP té coneixement que els CDP han realitzat signatures sobre codi hostil.

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

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

4.9.2. Legitimació per a sol·licitar la revocació

La sol·licitud de revocació pot ser demanada pel subscriptor del certificat, el Consorci AOC o l'Entitat de Registre que va sol·licitar l'emissió del certificat.

4.9.3. Procediments de sol·licitud de revocació

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

La sol·licitud de revocació ha de ser tramitada telemàticament. Excepcionalment es podrà tramitar per correu electrònic signat o per correu certificat convencional. S'ha d'incloure la informació suficient per poder identificar raonablement, a criteri de l'EC-SAFP, el certificat que se sol·licita revocar, i l'autenticitat i autoritat del sol·licitant.

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

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

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

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

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

4.9.4. Període temporal de sol·licitud de revocació

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

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

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

4.9.6. Obligació de consulta de informació de revocació de certificats

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

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

L'EC-SAFP 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-SAFP emet una LRC almenys cada 24 hores. A més s'emet una nova LRC després de cada suspensió o revocació.

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

Els certificats revocats o suspesos són retirats de la LRC transcorreguts seixanta dies des de l'expiració.

4.9.8. Període màxim de publicació de LRCs

Les LRCs es publiquen immediatament en el web del Servei de Certificació Digital del Consorci AOC.

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

Els verificadors de certificats digitals poden consultar un servei en línia que respongui sobre l'estat de certificats (servei *OCSP responder* o d'altres serveis de validació de certificats) operat per un prestador de serveis de validació en qui es confia.

El Consorci AOC ofereix de manera gratuïta un servei *OCSP responder* per a la comprovació en línia de l'estat dels certificats emesos per les Entitats de Certificació que integren la jerarquia pública de certificació de Catalunya.

La URL en la que es troba disponible l'esmentat servei s'indica en el contingut dels certificats emesos. La informació relativa al perfil OCSP i, en general, al funcionament del servei es pot trobar a <http://www.aoc.cat/catcert>.

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

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

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

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

L'EC-SAFP 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-SAFP 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 numero de sèrie del certificat sobre el qual es fa la petició i les dades identificatives de l'autoritat de certificació emissora.

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

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

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

4.9.12. Requisits especials en cas de compromís de la clau privada

El compromís de la clau privada de l'EC-SAFP és notificat, en la mesura possible, a tots els participants en la jerarquia pública de certificació de Catalunya, mitjançant el Dipòsit del Servei de Certificació Digital del Consorci AOC.

4.9.13. Causes de suspensió de certificats

Els certificats es poden suspendre:

- Quan ho sol·liciti el posseïdor de claus o el subscriptor o un tercer autoritzat (art. 9.1.a de la Llei 59/2003)
- En els casos legals previstos a l'article 9.1 de la Llei de Signatura Electrònica, és a dir, en cas que una resolució judicial o administrativa ho ordeni.
- Quan la documentació requerida a la sol·licitud de revocació sigui suficient però no es pugui identificar raonablement el posseïdor de claus.
- Quan la documentació requerida a la sol·licitud de revocació no sigui suficient, encara que es pugui identificar raonablement el posseïdor de claus
- Quan la documentació requerida a la sol·licitud de revocació no sigui suficient i tampoc no permetin identificar raonablement el posseïdor de claus.
- Si el subscriptor no utilitza el certificat durant un període prolongat de temps, conegut prèviament.
- Si se sospita el compromís d'una clau, fins que aquest sigui confirmat. En aquest cas, l'EC-SAFP ha d'assegurar-se que el certificat no està suspès durant més temps del necessari per consignar el seu compromís.

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

4.9.14. Legitimitat per sol·licitar la suspensió

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

4.9.15. Procediments de sol·licitud de suspensió

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

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

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

Per iniciar la suspensió es requereix la següent informació:

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

- Codi de suspensió associat al certificat o, por defecto, pregunta y respuesta secreta escogida en el momento de activar el certificado.

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

4.9.16. Període màxim de suspensió

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

4.9.17. Habilitació d'un certificat suspès

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

4.10. Serveis de comprovació d'estat de certificats

4.10.1. Característiques d'operació dels serveis

Les LCRs es publiquen a la web del Consorci AOC i en les URLs indicades en els certificats emesos.

De forma alternativa, els verificadors podran consultar els certificats publicats en el directori de l'EC-SAFP.

4.10.2. Disponibilitat dels serveis

Els verificadors de certificats digitals poden consultar un servei en línia que respongui sobre l'estat de certificats (servei *OCSP responder* o d'altres serveis de validació de certificats) operat per un prestador de serveis de validació en qui es confia.

El Consorci AOC ofereix de manera gratuïta un servei *OCSP responder* per a la comprovació en línia de l'estat dels certificats emesos per les Entitats de Certificació que integren la jerarquia pública de certificació de Catalunya.

La URL en la que es troba disponible l'esmentat servei s'indica en el contingut dels certificats emesos. La informació relativa al perfil OCSP i, en general, al funcionament del servei es pot trobar a <http://www.aoc.cat/catcert>

4.10.3. Altres funcions dels serveis

Sense estipulacions addicionals.

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

4.12.1. Política i pràctiques de dipòsit i recuperació de claus

No es practica recuperació de claus.

4.12.2. Política i pràctiques d'encapsulament i recuperació de claus de sessió

Sense estipulacions addicionals.

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

5.1. Controls de seguretat física

Sense estipulacions addicionals.

5.1.1. Localització i construcció de les instal·lacions

Sense estipulacions addicionals.

5.1.2. Accés físic

Sense estipulacions addicionals.

5.1.3. Electricitat i aire condicionat

Sense estipulacions addicionals.

5.1.4. Exposició al'aigua

Sense estipulacions addicionals.

5.1.5. Advertència i protecció d'incendis

Sense estipulacions addicionals.

5.1.6. Emmagatzematge de suports

Sense estipulacions addicionals.

5.1.7. Tractament de residus

Sense estipulacions addicionals.

5.1.8. Còpia de seguretat fora de les instal·lacions

Sense estipulacions addicionals.

5.2. Controls de procediments

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

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

5.2.1. Funcions fiables

Sense estipulacions addicionals.

5.2.2. Nombre de persones per tasca

Sense estipulacions addicionals.

5.2.3. Identificació i autenticació per a cada funció

Sense estipulacions addicionals.

5.2.4. Rols que requereixen separació de tasques

Sense estipulacions addicionals.

5.3. Controls de personal

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

- Es manté la 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
- Ésser 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'extrauen suports d'informació a nivells de seguretat inferiors
- Es reporta al Responsable de Seguretat, el més aviat possible, qualsevol incident que es consideri que afecta a la seguretat de la infraestructura, o limitar la qualitat del servei
- S'utilitzen els actius de la infraestructura per a les finalitats que els han sigut 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 les quals està sotmès
- El responsable de seguretat vetlla perquè el punt anterior sigui executat, proveint als responsables d'àrea tota la informació que fos necessària
- No s'instal·len en cap dels sistemes de la infraestructura, software o hardware que no sigui expressament autoritzat per escrit pel responsable de sistemes d'informació.
- No s'accedeix voluntàriament, ni s'elimina o altera informació no destinada a la seva persona o perfil professional

El personal afectat per aquesta normativa és:

- el Responsable del Servei de Certificació Digital
- el Responsable de l'EC-SAFP
- 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
- els Usuaris de l'EC-SAFP

Amés, es veu afectat el següent personal del Consorci AOC:

- qui fa les peticions dels certificats
- qui fa l'aprovació i validació de les peticions de certificats
- qui fa la generació / personalització de certificats
- qui custodia les claus o tokens criptogràfics
- qui custodia les claus o combinacions de seguretat d'accés a la sala d'operacions
- qui accedeix a informació classificada
- el personal de comunicacions i operacions
- el personal de seguretat (física i lògica) involucrats en l'operació
- el responsable del servei

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

Sense estipulacions addicionals.

5.3.2. Requisits de formació

Sense estipulacions addicionals.

5.3.3. Requisits de freqüència d'actualització formativa

Sense estipulacions addicionals.

5.3.4. Seqüència i freqüència de rotació laboral

Sense estipulacions addicionals.

5.3.5. Sancions per accions no autoritzades

Sense estipulacions addicionals.

5.3.6. Requisits de contractació de professionals

Sense estipulacions addicionals.

5.3.7. Subministrament de documentació al personal

Sense estipulacions addicionals.

5.4. Procediments d'auditoria de seguretat

5.4.1. Tipus d'esdeveniments registrats

Sense estipulacions addicionals.

5.4.2. Freqüència de tractament de registres d'auditoria

Sense estipulacions addicionals.

5.4.3. Període de conservació de registres d'auditoria

Sense estipulacions addicionals.

5.4.4. Protecció dels registres d'auditoria

Sense estipulacions addicionals.

5.4.5. Procediments de còpies de seguretat

Amb la finalitat de conservar correctament les còpies de seguretat, s'han implantatels següents punts:

- Es guarden en armaris ignífugues
- Solament 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...) ies volen reutilitzar, s'assegura que les dades que ha contingut siguin totalment esborrades fent impossible la seva recuperació
- S'autoritza expressament l'extracció de les còpies de seguretat fora de l'Entitat de Registre, emplenant una fitxa al respecte i anotant el corresponent detall en un llibre de registre

- Es procura anar dipositant còpies de seguretat periòdicament fora de l'Entitat de Registre

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

Sense estipulacions addicionals.

5.4.7. Notificació del'esdeveniment d'auditoria al causant del'esdeveniment

Sense estipulacions addicionals.

5.4.8. Anàlisi de vulnerabilitats

Sense estipulacions addicionals.

5.5. Arxiu d'informacions

Sense estipulacions addicionals.

5.5.1. Tipus d'esdeveniments registrats

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

L'EC-SAFP guarda registre del següent:

Documents originals:

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

L'EC-SAFP guarda, en relació amb els certificats Extended Validation:

- LOG i pistes d'auditoria
- Documentació relativa a peticions, verificacions i revocacions de certificats Extended Validation

5.5.2. Període de conservació de registres

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

L'EC-SAFP guarda els registres especificats a la secció 5.5.1 en relació amb els certificats Extended Validation per un període de 7 anys, comptats des del moment de l'expedició del certificat.

5.5.3. Protecció del'arxiu

Sense estipulacions addicionals.

5.5.4. Procediments de còpia suport

Sense estipulacions addicionals.

5.5.5. Requisits de segellat de datai hora

Sense estipulacions addicionals.

5.5.6. Localització del sistema d'arxiu

Sense estipulacions addicionals.

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

Sense estipulacions addicionals.

5.6. Renovació de claus

Els certificats de l'EC-SAFP renovats es comuniquen als usuaris finals, mitjançant la seva publicació a la pàgina web del Servei de Certificació Digital del Consorci AOC.

5.7. Compromís de claus i recuperació de desastre

5.7.1. Procediment de gestió d'incidències i compromisos

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

5.7.3. Compromís de la clau privada de l'Entitat

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

En cas de compromís, l'EC-SAFP:

- Informa a tots els subscriptors i verificadors del compromís

- Indica que els certificats i la informació del'estat de revocació lliurats usant la clau de l'EC-SAFPja no són vàlids

5.7.4. Desastre sobre les instal·lacions

L'EC-SAFP desenvolupa, manté, provai, si és necessari, executa un pla d'emergència en cas de desastre, ja sigui per causes naturals o causat per l'home, sobre les instal·lacions, que indiqui 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-SAFP és capaç de restaurar l'operació normal de la PKI en les 24 hores següents al desastre, podent, com a mínim, executar-se les següents accions:

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

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

5.8. Finalització del servei

5.8.1. EC-SAFP

Sense estipulacions addicionals.

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 Entitat de Registre durant 15 anys després de finalitzar les activitats relacionades amb l'Entitat de Registre.

6. Controls de seguretat tècnica

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

6.1. Generació i instal·lació del parell de claus

6.1.1. Generació del parell de claus

6.1.1.1. Requisits per a tots els certificats

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

6.1.1.2. Informació per als certificats CPISR i CEISR

Les claus pública i privada dels certificats CPISR i CEISR es generen per part del Consorci AOC dins d'un dispositiu segur de creació de signatura electrònica (targeta que rep el posseïdor de claus).

6.1.1.3. Informació per als certificats CPIXSA

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

6.1.1.4. Informació per als certificats CPX i CEX

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

Addicionalment una còpia de la clau privada s'emmagatzema al Consorci AOC.

6.1.1.5. Informació per als certificat CEIXSA

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

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

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

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

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

6.1.1.8. Informació per als certificats CDA-1 Segell electrònic

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

6.1.1.9. Informació per als certificats CDP

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

6.1.1. Tramesa de la clau privada al subscriptor

6.1.2.1. Informació per als certificats CPISR, CEISR, CDP, CPX i CEX

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

6.1.2.2. Informació per als certificat CEIXSA

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

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

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

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

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

La clau pública de l'EC-ACC, que és l'arrel de la jerarquia, es publica en el directori de l'EC-SAFP, en forma de certificat auto-signat, al costat d'una declaració referent a que la clau permet autenticar a l'EC-SAFP.

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

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

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-SAFP és almenys de 2.048 bits.

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

6.1.6. Generació de paràmetres de clau pública

Sense estipulacions addicionals.

6.1.7. Comprovació de qualitat de paràmetres de clau pública

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

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

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

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

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

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

6.1.9. Propòsits d'ús de claus

L'EC-SAFP 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 es protegeixen utilitzant maquinari criptogràfic que compleix els requisits establerts per l'especificació tècnica FIPS 140-2 Nivell 3 o superior.

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

6.2.1.2. Cicle de vida de les targetes amb circuit integrat

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

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

Quan el Consorci AOC 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-SAFP requereix el concurs d'almenys 2 de forma simultània.

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

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

6.2.3. Dipòsit de la clau privada

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

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

6.2.4. Còpia de seguretat de la clau privada

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

6.2.5. Arxiu de la clau privada

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

Els controls de seguretat a aplicar en còpies de seguretat de l'EC-SAFP 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, es proveeixen els controls oportuns perquè aquestes mai no puguin abandonar el dispositiu.

No s'emmagatzemen còpies de les claus privades dels certificats.

6.2.6. Introducció de la clau privada en el mòdul criptogràfic

Les claus privades de l'EC-SAFP 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.

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

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

6.2.9. Mètode de desactivació de la clau privada

No aplicable.

6.2.10. Mètode de destrucció de la clau privada

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

6.2.11. Classificació dels mòduls criptogràfics

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

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

6.3. Altres aspectes de gestió del parell de claus

6.3.1. Arxiu de la clau pública

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

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

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

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

6.4. Dades d'activació

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

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

6.4.2. Protecció de les dades d'activació

6.4.2.1. Per a certificats personals i d'entitat

Per protegir al màxim les dades d'activació, el Consorci AOC s'encarrega de distribuir els elements dels certificats per dos canals diferents.

- En primer lloc, el responsable de l'Entitat de Registre lliura al posseïdor de claus el següent material:
 - Full de lliurament de posseïdor
 - Targeta amb els certificats
 - Programari necessari per utilitzar la targeta
 - Carta de lliurament de certificats.
- Al mateix temps, i per correu electrònic, s'envien al posseïdor de claus les dades d'activació del certificat.

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

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

La distribució de les dades d'activació per als certificats de dispositiu CDS-1, CDS-1 EV, CDSCD-1, CDS-1 Seu electrònica de nivell mig EV i CDA-1 Segell electrònic de nivell alt, és diferent a la dels certificats personals (no té ni PIN ni PUK ni targeta), ja que la clau privada la genera el propi subscriptor que ha demanat el certificat.

6.4.3. Altres aspectes de les dades d'activació

Sense estipulacions addicionals.

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-SAFP 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-SAFP garanteix que l'accés als sistemes d'informació i aplicacions es restringeix d'acord a l'establert en la política de control d'accés, així com que els sistemes proporcionen els controls de seguretat suficients per implementar la segregació de funcions identificada en les pràctiques de l'EC-SAFP, 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-SAFP està identificat i reconegut abans d'utilitzar aplicacions crítiques relacionades amb el cicle de vida del certificat.
- El personal de l'EC-SAFP és responsable i pot justificar les seves activitats, per exemple mitjançant un arxiu d'esdeveniments.
- Ha d'evitar-se la possibilitat de revelació de dades sensibles mitjançant la reutilització d'objectes d'emmagatzematge (per exemple fitxers esborrats) que quedin accessibles a usuaris no autoritzats.
- Els sistemes de seguretat i monitoratge permeten una ràpida detecció, registre i actuació davant d'intents d'accés irregulars o no autoritzats als seus recursos (per exemple, mitjançant un sistema de detecció d'intrusions, monitoratge i alarma).
- L'accés als dipòsits públics de la informació de l'EC-SAFP (per exemple, certificats o informació d'estat de revocació) conta amb un control d'accésos per a modificacions o esborrament de dades.

6.5.2. Avaluació del nivell de seguretat informàtica

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

6.6. Controls tècnics del cicle de vida

6.6.1. Controls de desenvolupament de sistemes

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

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

6.6.2. Controls de gestió de seguretat

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

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

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

6.6.3. Avaluació del nivell de seguretat del cicle de vida

Sense estipulacions addicionals.

6.7. Controls de seguretat de xarxa

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

- S'implementen controls (com per exemple tallafocs) per protegir la xarxa interna de dominis externs accessibles per terceres parts. Els tallafocs es configuren de manera que s'impedeixin accessos i protocols que no siguin necessaris per a l'operació de l'EC-SAFP.
- 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 estipulacions addicionals.

7. Perfils de certificats illistes de certificats revocats

7.1. Perfil de certificat

Sense estipulació addicional.

Els documents descriptius dels diversos perfils de certificats digitals que expedeix l'EC-SAFP es publiquen a la web del Consorci AOC <http://www.aoc.cat/catcert/>.

7.2. Perfil de la llista de revocació de certificats

L'accés a la informació relativa a la llista de revocació de certificats es publica al web del Consorci AOC <http://www.aoc.cat/catcert/>.

8. Auditoria de conformitat

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

L'EC-SAFP pot delegar l'execució de les auditories en una tercera entitat contractada pel Consorci AOC. En aquests casos l'EC-SAFP coopera completament amb el personal que porta a terme la investigació.

8.1. Freqüència de l'auditoria de conformitat

Sense estipulacions addicionals.

8.2. Identificació i qualificació del auditor

L'EC-SAFP acut a auditors independents externs per a la realització de les auditories anuals de conformitat. Aquests han de demostrar experiència en seguretat informàtica, en seguretat de Sistemes d'Informació i en auditories de conformitat d'Autoritats de Certificació dels elements relacionats.

8.3. Relació del auditor amb l'entitat auditada

Les auditories externes de conformitat executades per tercers són realitzades per entitats independents de l'EC-SAFP.

8.4. Relació d'elements objecte d'auditoria

Sense estipulacions addicionals.

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

Sense estipulacions addicionals.

8.6. Tractament dels informes d'auditoria

Els informes de resultats de les auditories seran lliurats al Consorci AOC, en tant que és el Prestador de Serveis de Certificació, en un termini màxim de 15 dies després de l'execució de l'auditoria, per a la seva avaluació i gestió diligent.

9. Requisits comercials i legals

9.1. Tarifes

9.1.1. Tarifa d'emissió o renovació de certificats

El Consorci AOC estableix les tarifes que aplica l'EC-SAFP en la prestació dels seus serveis. Les tarifes es poden consultar a la web del servei de certificació digital del Consorci AOC.

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 estipulacions addicionals.

9.1.5. Política de reintegrament

El Consorci AOC no practicarà reembossaments. 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

El Consorci AOC 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, excepte quan es trobi eximit per Llei d'aquesta obligació. Aquesta assegurança cobreix les actuacions del Consorci AOC com a prestador de serveis de certificació.

9.2.2. Altres actius

Sense estipulacions addicionals.

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

En cas d'ús incorrecte o no autoritzat dels certificats, el Consorci AOC (o l'EC-SAFP) no actuarà com a agent fiduciari davant subscriptors i terceres persones, que hauran d'adreçar-se contra l'infractor de les condicions d'ús dels certificats establertes pel Consorci AOC (o l'EC-SAFP).

9.3. Confidencialitat

9.3.1. Informacions confidencials

Sense estipulacions addicionals.

9.3.2. Informacions no confidencials

Sense estipulacions addicionals.

9.3.3. Responsabilitat per a la protecció d'informació confidencial

Sense estipulacions addicionals.

9.4. Protecció de dades personals

9.4.1. Política de Protecció de Dades Personals

Sense estipulacions addicionals.

9.4.2. Dades de caràcter personal no disponibles a tercers

Sense estipulacions addicionals.

9.4.3. Dades de caràcter personal disponibles a tercers

Sense estipulacions addicionals.

9.4.4. Responsabilitat corresponent a la protecció de dades personals

Sense estipulacions addicionals.

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

Sense estipulacions addicionals.

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

Sense estipulacions addicionals.

9.4.7. Comunicació de dades personals

Sense estipulacions addicionals.

9.5. Drets de propietat intel·lectual

9.5.1. Propietat dels certificats i informació de revocació

Sense estipulacions addicionals.

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

Sense estipulacions addicionals.

9.5.3. Propietat de la informació relativa a noms

Sense estipulacions addicionals.

9.5.4. Propietat de claus

Sense estipulacions addicionals.

9.6. Obligacions i responsabilitat civil

9.6.1. Entitats de Certificació

9.6.1.1. Obligacions generals de l'EC-SAFP

Sense estipulacions addicionals.

9.6.1.2. Garanties oferides a subscriptors i verificadors

Sense estipulacions addicionals.

9.6.2. Obligacions i altres compromisos de les Entitats de Registre

9.6.2.1. Obligacions i altres compromisos

Sense estipulacions addicionals, exceptuant l'obligació d'emmagatzemar els fulls de lliurament de certificat durant un període de 15 anys, que és assumida per les entitatssubscriptores dels certificats corporatius que emet l'EC-SAFP.

En quant al nombre d'operadors de l'autoritat de registre que aquesta ha de nomenar: per a l'EC-SAFP hauran de ser quatre o més dels empleats que treballin per a ella.

9.6.3. Garanties oferides a subscriptors i verificadors

9.6.3.1. Garantia del Consorci AOC pels serveis de certificació digital

Sense estipulacions addicionals.

9.6.3.2. Exclusió de la garantia

Sense estipulacions addicionals.

9.6.4. Subscriptors

9.6.4.1. Obligacions i altres compromisos

Sense estipulacions addicionals.

9.6.4.2. Garanties oferides pel subscriptor

Sense estipulacions addicionals.

9.6.4.3. Protecció de la clau privada

Sense estipulacions addicionals.

9.6.5. Verificadors

9.6.5.1. Obligacions i altres compromisos

Sense estipulacions addicionals.

9.6.5.2. Garanties oferides pel verificador

Sense estipulacions addicionals.

9.6.6. Altres participants

9.6.6.1. Obligacions i garanties del directori

Sense estipulacions addicionals.

9.6.6.2. Garanties oferides pel directori

L'EC-SAFP té la responsabilitat civil del directori de certificació.

9.7. Renúncies de garanties

9.7.1. Rebuig de garanties de l'EC-SAFP

L'EC-SAFP 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'EC-SAFP

Més enllà de les limitacions dels prestadors de serveis de certificació establertes a l'article 23 de la Llei 59/2003, de 19 de desembre, l'EC-SAFP 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).

I, per a determinats tipus de certificats, l'EC-SAFP limita la seva responsabilitat mitjançant la inclusió de límits d'ús del certificat i límits de valor de les transaccions per a les que es pot utilitzar el certificat.

9.8.2. Cas fortuït i força major

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

9.9. Indemnitzacions

9.9.1. Clàusula d'indemnitat de subscriptor

No s'establirà clàusula d'indemnitat del subscriptor.

9.9.2. Clàusula d'indemnitat de verificador

No s'establirà clàusula d'indemnitat del verificador.

9.10. Terminii finalització

9.10.1. Termini

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

9.10.2. Finalització

L'EC-SAFP estableix, en els seus instruments jurídics amb els subscriptors, una clàusula que determina les conseqüències de la finalització de la relació jurídica en virtut de la qual els subministradors certificats.

9.10.3. Supervivència

Sense estipulacions addicionals.

9.11. Notificacions

Sense estipulacions addicionals.

9.12. Modificacions

9.12.1. Procediment per a les modificacions

Sense estipulacions addicionals.

9.12.2. Terminii mecanismes per a notificacions

Les modificacions d'aquest document seran aprovades pel Consorci AOC, conforme s'estableix a l'apartat 1.5.

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

Sense estipulacions addicionals.

9.13. Resolució de conflictes

9.13.1. Resolució extrajudicial de conflictes

Sense estipulacions addicionals.

9.13.2. Jurisdicció competent

Sense estipulacions addicionals.

9.14. Llei aplicable

Sense estipulacions addicionals.

9.15. Conformitat amb la llei aplicable

L'EC-SAFP manifesta, en aquest document i en els instruments jurídics amb subscriptors, el compliment de la Llei 59/2003, de 19 de desembre, de signatura electrònica. La prestació de serveis s'ajusta a la Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i comerç electrònic.

9.16. Clàusules diverses

9.16.1. Acord íntegre

Sense estipulacions addicionals.

9.16.2. Subrogació

Sense estipulacions addicionals.

9.16.3. Divisibilitat

Sense estipulacions addicionals.

9.16.4. Aplicacions

Sense estipulacions addicionals.

9.16.5. Altres clàusules

Sense estipulacions addicionals.

ANNEX – Control documental

Control de versions DPC EC-SAFP 1er semestre 2016

Projecte:	Informe modificació del document DPC EC-SAFP
Entitat de destí:	Consorti AOC
Codi de referència:	Revisió 1er semestre 2016
Versió:	Canvis de la v4.1 a la v5.0 en català i en castellà
Data de l'edició:	05/08/2016

Versió	Parts que canvien	Descripció del canvi	Autor del canvi	Data del canvi
5.0	Totes	Revisió global - Integració de CATCert a Consorci AOC	Servei de Certificació Digital - Consorci AOC	05/08/2016