



**Consorci  
Administració Oberta  
de Catalunya**

**Declaració de Pràctiques de Certificació  
Entitat de Certificació Sector Públic  
(EC-SECTORPUBLIC)**

Referència: D1111\_E0650\_N-DPC EC-SECTORPUBLIC  
Versió: 2.0  
Data: 09/05/2018

# Índex

<b>1. Introducció</b>	<b>11</b>
1.1. Presentació	11
1.1.1. Tipus i classes de certificats	11
1.1.1.1. Certificats d'infraestructura	12
1.1.1.2. Certificats personals	12
1.1.1.3. Certificats de dispositiu	13
1.1.1.4. Certificats de proves	14
1.1.2. Relació entre la Declaració de Pràctiques de Certificació (DPC) i altres documents	14
1.2. Nom del document i identificació	14
1.2.1. Identificació d'aquest document	14
1.2.2. Identificació de polítiques de certificació cobertes per aquesta DPC	14
1.3. Comunitat d'usuaris de certificats	16
1.3.1. Prestadors de serveis de certificació	16
1.3.2. Entitat de Certificació Arrel	17
1.3.3. EC-SECTORPUBLIC	17
1.3.4. Entitats de Registre	17
1.3.5. Usuaris finals	17
1.3.5.1. Sol·licitants de certificats	18
1.3.5.2. Subscriptors de certificats	18
1.3.5.3. Posseïdors de claus	18
1.3.5.4. Usuaris de certificats	18
1.3.5.5. Verificadors de certificats	18
1.4. Ús dels certificats	18
1.4.1. Ús típic dels certificats	19
1.4.1.1. Certificats d'infraestructura	19
1.4.1.1.1. Certificat personal d'Infraestructura personal d'identificació i signatura qualificada (CIPISQ)	19
1.4.1.1.2. Requisits específics per al CIC	19
1.4.1.1.3. Requisits específics per al CIO	19
1.4.1.2. Requisits específics pels Certificats personals	19
1.4.1.2.1. Certificat electrònic de treballador públic de nivell alt d'autenticació	19

1.4.1.2.2. Certificat qualificat de signatura de treballador públic de nivell alt	19
1.4.1.2.3. Certificat electrònic de persona vinculada de nivell alt	19
1.4.1.2.4. Certificat electrònic de treballador públic de nivell mig	19
1.4.1.2.5. Certificat electrònic de persona vinculada de nivell mig	19
1.4.1.2.6. Certificat electrònic de treballador públic amb pseudònim de nivell alt d'autenticació	19
1.4.1.2.7. Certificat qualificat de signatura de treballador públic amb pseudònim de nivell alt	20
1.4.1.2.8. Certificat electrònic de representant davant les AAPP de nivell alt	20
1.4.1.3. Certificats de Dispositiu	20
1.4.1.3.1. Certificats de dispositiu SSL (CDS-1)	20
1.4.1.3.2. Certificats de dispositiu SSL EV (CDS-1 EV)	20
1.4.1.3.3. Certificat de seu electrònica de nivell mig (CDS-1 SENM)	20
1.4.1.3.4. Certificat d'aplicació (CDA-1)	21
1.4.1.3.5. Certificat de segell electrònic nivell mig (CDA-1 SGNM)	21
1.4.2. Aplicacions prohibides	21
1.4.2.1. Informacions per a tots els tipus de certificats	21
1.4.2.2. Certificats d'infraestructura	21
1.4.2.3. Certificats personals	21
1.4.2.4. Certificats de dispositiu	21
1.5. Administració de la Declaració de Pràctiques	22
1.5.1. Organització que administra l'especificació	22
1.5.2. Dades de contacte de l'organització	22
1.5.3. Persona que determina la conformitat d'una Declaració de Pràctiques de Certificació (DPC) amb la política	22
1.5.4. Procediment d'aprovació	22
<b>2. Publicació d'informació i directori de certificats</b>	<b>24</b>
2.1. Directori de certificats	24
2.2. Publicació d'informació de l'EC-SECTORPUBLIC	24
2.3. Freqüència de publicació	24
2.4. Control d'accés	24
<b>3. Identificació i autenticació</b>	<b>25</b>
3.1. Gestió de nom	25
3.1.1. Tipus de noms	25
3.1.2. Significat dels noms	25

3.1.3. Utilització d'anònims i pseudònims	25
3.1.4. Interpretació de formats de noms	25
3.1.5. Unicitat dels noms	25
3.1.6. Resolució de conflictes relatius a noms	26
3.2. Validació inicial de la identitat	26
3.2.1. Prova de possessió de clau privada	26
3.2.2. Autenticació de la identitat d'una organització	26
3.2.2.1. Entitats de Registre	26
3.2.2.2. Les entitats subscriptores de certificats corporatius	26
3.2.2.3. Altres entitats subscriptores	26
3.2.2.3.1. Requisits per a certificats de persona vinculada	26
3.2.2.3.2. Requisits específics per als certificats de dispositiu	26
3.2.3. Autenticació de la identitat d'una persona física	27
3.2.3.1. Elements d'identificació	27
3.2.3.2. Validació dels elements d'identificació	27
3.2.3.3. Necessitat de presència personal	27
3.2.3.4. Vinculació de la persona física amb l'organització	27
3.2.4. Informació no verificada	27
3.3. Identificació i autenticació de sol·licituds de renovació	28
3.3.1. Validació per a la renovació de certificats	28
<b>4. Característiques d'operació del cicle de vida dels certificats</b>	<b>29</b>
4.1. Sol·licitud d'emissió de certificat	29
4.1.1. Legitimació per a sol·licitar l'emissió	29
4.1.2. Procediment d'alta; Responsabilitats	29
4.2. Procediment de sol·licitud de certificació	30
4.2.1. Requisits generals per a tots els certificats	30
4.3. Emissió de certificat	31
4.3.1. Accions de l'EC-SECTORPUBLIC durant el procés d'emissió	31
4.3.2. Comunicació de l'emissió al subscriptor	31
4.4. Acceptació del certificat	31
4.4.1. Responsabilitats de l'Ens subscriptor	32
4.4.1.1. Per a Certificats personals	32
4.4.1.2. Per a certificats de dispositiu	32
4.4.2. Conducta que constitueix acceptació del certificat	32
4.4.3. Publicació del certificat	33

4.4.4. Notificació de l'emissió a tercers	33
4.5. Ús del parell de claus i del certificat	33
4.5.1. Ús per part dels posseïdors de claus	33
4.5.2. Ús pel tercer que confia en certificats	33
4.6. Renovació de certificats sense renovació de claus	33
4.7. Renovació de certificats amb renovació de claus	33
4.8. Renovació telemàtica	33
4.9. Modificació de certificats	33
4.10. Revocació i suspensió de certificats	34
4.10.1. Causes de revocació de certificats	34
4.10.2. Legitimació per a sol·licitar la revocació	34
4.10.3. Procediments de sol·licitud de revocació	34
4.10.4. Termini temporal de sol·licitud de revocació	35
4.10.5. Termini màxim de processament de la sol·licitud de revocació	35
4.10.6. Obligació de consulta d'informació de revocació de certificats	35
4.10.7. Freqüència d'emissió de llistes de revocació de certificats (CRL's)	35
4.10.8. Període màxim de publicació de CRL's	35
4.10.9. Disponibilitat de serveis de comprovació d'estat de certificats	35
4.10.10. Obligació de consulta de serveis de comprovació d'estat de certificats	36
4.10.11. Altres formes d'informació de revocació de certificats	36
4.10.12. Requeriments especials en cas de compromís de la clau privada	36
4.10.13. Causes de suspensió de certificats	36
4.10.14. Efecte de la suspensió de certificats	36
4.10.15. Qui pot sol·licitar la suspensió	36
4.10.16. Procediments de sol·licitud de suspensió	36
4.10.17. Període màxim de suspensió	36
4.10.18. Habilitació d'un certificat suspès	36
4.11. Serveis de comprovació d'estat de certificats	37
4.11.1. Característiques d'operació dels serveis	37
4.11.2. Disponibilitat dels serveis	37
4.11.3. Altres funcions dels serveis	37
4.12. Finalització de la subscripció	37
4.13. Dipòsit i recuperació de claus	37
4.13.1. Política i pràctiques de dipòsit i recuperació de claus	37
4.13.2. Política i pràctiques d'encapsulament i recuperació de claus de sessió	37

4.14. Notificació de problemes amb certificats d'autenticació de lloc web	37
<b>5. Controls de seguretat física, de gestió i d'operacions</b>	<b>39</b>
5.1. Controls de seguretat física	39
5.1.1. Localització i construcció de les instal·lacions	39
5.1.2. Accés físic	39
5.1.3. Electricitat i aire condicionat	39
5.1.4. Exposició a l'aigua	39
5.1.5. Advertència i protecció d'incendis	39
5.1.6. Emmagatzematge de suports	39
5.1.7. Tractament de residus	39
5.1.8. Còpia de seguretat fora de les instal·lacions	40
5.2. Controls de procediments	40
5.2.1. Funcions fiables	40
5.2.2. Nombre de persones per tasca	40
5.2.3. Identificació i autenticació per a cada funció	40
5.2.4. Rols que requereixen separació de tasques	40
5.3. Controls de personal	40
5.3.1. Requisits d'historial, qualificacions, experiència i autorització	41
5.3.2. Requisits de formació	41
5.3.3. Requisits i freqüència d'actualització formativa	42
5.3.4. Seqüència i freqüència de rotació laboral	42
5.3.5. Sancions per accions no autoritzades	42
5.3.6. Requisits de contractació de professionals	42
5.3.7. Subministrament de documentació al personal	42
5.4. Procediments d'auditoria de seguretat	42
5.4.1. Tipus d'esdeveniments registrats	42
5.4.2. Freqüència de tractament de registres d'auditoria	42
5.4.3. Període de conservació de registres d'auditoria	42
5.4.4. Protecció dels registres d'auditoria	43
5.4.5. Procediments de còpies de seguretat	43
5.4.6. Localització del sistema d'acumulació de registres d'auditoria	43
5.4.7. Notificació de l'esdeveniment d'auditoria al causant de l'esdeveniment	43
5.4.8. Anàlisi de vulnerabilitats	43
5.5. Arxiu d'informacions	43
5.5.1. Tipus d'esdeveniments registrats	44

5.5.2. Període de conservació de registres	44
5.5.3. Protecció de l'arxiu	44
5.5.4. Procediments de còpia suport	44
5.5.5. Requisits de segellat de data i hora	44
5.5.6. Localització del sistema d'arxiu	44
5.5.7. Procediments d'obtenció i verificació d'informació d'arxiu	45
5.6. Renovació de claus	45
5.7. Compromís de claus i recuperació de desastre	45
5.7.1. Procediment de gestió d'incidències i compromisos	45
5.7.2. Corrupció de recursos, aplicacions o dades	45
5.7.3. Compromís de la clau privada de l'Entitat	45
5.7.4. Desastre sobre les instal·lacions	45
5.8. Finalització del servei	46
5.8.1. EC-SECTORPUBLIC	46
5.8.2. Entitat de Registre	46
<b>6. Controls de seguretat tècnica</b>	<b>47</b>
6.1. Generació i instal·lació del parell de claus	47
6.1.1. Generació del parell de claus	47
6.1.1.1. Requisits per a tots els certificats	47
6.1.1.2. Informació per als certificats CPI, CPSQ, CPPI, CPPSQ I CPRISQ	47
6.1.1.3. Informació per als certificats CPISA	47
6.1.1.4. Informació per als certificats CDS-1, CDS-1 EV, CDS-1 SENM, CDA-1, CDA-1 SENM	47
6.1.2. Enviament de la clau privada al subscriptor	47
6.1.3. Enviament de la clau pública a l'emissor del certificat	48
6.1.4. Distribució de la clau pública del Prestador de Serveis de Certificació	48
6.1.5. Mides de claus	48
6.1.6. Generació de paràmetres de clau pública	48
6.1.7. Comprovació de qualitat de paràmetres de clau pública	48
6.1.8. Generació de claus en aplicacions informàtiques o en béns d'equip	48
6.1.9. Propòsits d'ús de claus	49
6.2. Protecció de la clau privada	49
6.2.1. Mòduls de protecció de la clau privada	49
6.2.1.1. Estàndards dels mòduls criptogràfics	49
6.2.1.2. Cicle de vida de les targetes amb circuit integrat	49

6.2.2. Control per més d'una persona (n de m) sobre la clau privada	49
6.2.3. Dipòsit de la clau privada	49
6.2.4. Còpia de seguretat de la clau privada	49
6.2.5. Arxiu de la clau privada	49
6.2.6. Introducció de la clau privada en el mòdul criptogràfic	49
6.2.7. Emmagatzematge de la clau privada en el mòdul criptogràfic	49
6.2.8. Mètode d'activació de la clau privada	50
6.2.9. Mètode de desactivació de la clau privada	50
6.2.10. Mètode de destrucció de la clau privada	50
6.2.11. Classificació dels mòduls criptogràfics	50
6.3. Altres aspectes de gestió del parell de claus	50
6.3.1. Arxiu de la clau pública	50
6.3.2. Períodes d'utilització de les claus pública i privada	50
6.4. Dades d'activació	50
6.4.1. Generació i instal·lació de les dades d'activació	50
6.4.2. Protecció de les dades d'activació	50
6.4.3. Altres aspectes de les dades d'activació	51
6.5. Controls de seguretat informàtica	51
6.5.1. Requisits tècnics específics de seguretat informàtica	51
6.5.2. Avaluació del nivell de seguretat informàtica	51
6.6. Controls tècnics del cicle de vida	51
6.6.1. Controls de desenvolupament de sistemes	51
6.6.2. Controls de gestió de seguretat	51
6.6.3. Avaluació del nivell de seguretat del cicle de vida	51
6.7. Controls de seguretat de xarxa	52
6.8. Segell de temps	52
<b>7. Perfils de certificats i llistes de certificats revocats</b>	<b>53</b>
7.1. Perfil de certificat	53
7.2. Perfil de la llista de revocació de certificats	53
<b>8. Auditoria de conformitat</b>	<b>54</b>
8.1. Freqüència de l'auditoria de conformitat	54
8.2. Identificació i qualificació de l'auditor	54
8.3. Relació de l'auditor amb l'entitat auditada	54
8.4. Relació d'elements objecte d'auditoria	54
8.5. Accions a emprendre com a resultat d'una falta de conformitat	54



8.6. Tractament dels informes d'auditoria	55
<b>9. Requisits comercials i legals</b>	<b>56</b>
9.1. Tarifes	56
9.1.1. Tarifa d'emissió o renovació de certificats	56
9.1.2. Tarifa d'accés a certificats	56
9.1.3. Tarifa d'accés a informació d'estat de certificat	56
9.1.4. Tarifes d'altres serveis	56
9.1.5. Política de reintegrament	56
9.2. Capacitat financera	56
9.2.1. Assegurança de responsabilitat civil	56
9.2.2. Altres actius	56
9.2.3. Cobertura d'assegurament per a subscriptors i tercers que confiïn en certificats	57
9.3. Confidencialitat	57
9.3.1. Informacions confidencials	57
9.3.2. Informacions no confidencials	57
9.3.3. Responsabilitat per a la protecció d'informació confidencial	57
9.4. Protecció de dades personals	57
9.4.1. Política de Protecció de Dades Personals	57
9.4.2. Dades de caràcter personal no disponibles a tercers	57
9.4.3. Dades de caràcter personal disponibles a tercers	57
9.4.4. Responsabilitat corresponent a la protecció de dades personals	58
9.4.5. Gestió d'incidències relacionades amb les dades de caràcter personal	58
9.4.6. Prestació del consentiment per al tractament de les dades personals	58
9.4.7. Comunicació de dades personals	58
9.5. Drets de propietat intel·lectual	58
9.5.1. Propietat dels certificats i informació de revocació	58
9.5.2. Propietat de la Política de Certificació i Declaració de Pràctiques de Certificació	58
9.5.3. Propietat de la informació relativa a noms	58
9.5.4. Propietat de claus	58
9.6. Obligacions i responsabilitat civil	59
9.6.1. Entitats de Certificació	59
9.6.1.1. Obligacions generals de l'EC-SECTORPUBLIC	59
9.6.1.2. Requisits específics per als certificats personals	59

9.6.1.3. Informació addicional per al CDS-1, CDS-1 EV, i CDS-1 Seu electrònica	59
9.6.1.4. Garanties oferides a subscriptors i verificadors	59
9.6.2. Obligacions i altres compromisos de les Entitats de Registre	59
9.6.2.1. Obligacions i altres compromisos	59
9.6.3. Obligacions i altres compromisos de les entitats subscriptores dels certificats corporatius emesos per l'EC-SECTORPUBLIC	59
9.6.4. Garanties oferides a subscriptor i verificadors	60
9.6.4.1. Garantia del Consorci AOC pels serveis de certificació digital	60
9.6.4.2. Exclusió de la garantia	60
9.6.5. Subscriptors	60
9.6.5.1. Obligacions i altres compromisos	60
9.6.5.1.1. Informacions per a tots els tipus de certificats	60
9.6.5.1.2. Informacions específiques per als certificats de signatura electrònica qualificada	60
9.6.5.2. Garanties oferides pel subscriptor	60
9.6.5.3. Protecció de la clau privada	60
9.6.6. Verificadors	60
9.6.6.1. Obligacions i altres compromisos	60
9.6.6.2. Garanties oferides pel verificador	60
9.6.7. Altres participants	61
9.6.7.1. Obligacions i garanties del directori	61
9.6.7.2. Garanties oferides pel directori	61
9.7. Renúncies de garanties	61
9.7.1. Rebuig de garanties de l'EC-SECTORPUBLIC	61
9.8. Limitacions de responsabilitat	61
9.8.1. Limitacions de responsabilitat de l'EC-SECTORPUBLIC	61
9.8.2. Cas fortuït i força major	61
9.9. Indemnitzacions	62
9.9.1. Clàusula d'indemnitat de subscriptor	62
9.9.2. Clàusula d'indemnitat de verificador	62
9.10. Termini i finalització	62
9.10.1. Termini	62
9.10.2. Finalització	62
9.10.3. Supervivència	62
9.11. Notificacions	62

9.12. Modificacions	62
9.12.1. Procediment per a les modificacions	62
9.12.2. Termini i mecanismes per a notificacions	63
9.12.3. Circumstàncies en les que un OID ha de ser canviat	63
9.13. Resolució de conflictes	63
9.13.1. Resolució extrajudicial de conflictes	63
9.13.2. Jurisdicció competent	63
9.14. Llei aplicable	63
9.15. Conformitat amb la llei aplicable	63
9.16. Clàusules diverses	63
9.16.1. Acord íntegre	63
9.16.2. Subrogació	63
9.16.3. Divisibilitat	64
9.16.4. Aplicacions	64
9.16.5. Altres clàusules	64
<b>10. ANNEX – Control documental</b>	<b>65</b>

# 1. Introducció

## 1.1. Presentació

### 1.1.1. Tipus i classes de certificats

El Consorci AOC ha definit una tipologia de serveis de certificació que permeten, a l'EC-SECTORPUBLIC, emetre certificats digitals per a diversos usos i usuaris finals diferents.

Els perfils recollits en aquest document, s'han creat per complir amb els requeriments previstos a la llei aplicable, que es descriu a l'apartat 9.15 Conformitat amb la llei aplicable

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 a autoritzar operacions relacionades amb els serveis de certificació, com l'aprovació de sol·licituds de certificació
- Certificats personals, caracteritzats pel fet que el posseïdor de la clau privada és una persona física, que actua en nom i representació del subscriptor o titular del certificat (que pot ser ell mateix o una persona jurídica a la qual estigui vinculat)
- Certificats de dispositiu, caracteritzats pel fet que el posseïdor de la clau privada és un dispositiu informàtic que realitza operacions de signatura i desxifrat de forma automàtica, sota la responsabilitat d'una persona física o jurídica (anomenada subscriptor o titular del certificat)

Quan els certificats s'expedeixen a LES INSTITUCIONS, es requereix realitzar procediment d'autenticació de l'organització titular del certificat, ja que es tracta de certificats corporatius, en els quals l'organització subscriptora del certificat i l'Entitat de Registre coincideixen.

En circumstàncies excepcionals, motivades per la necessitat de garantir la seguretat de la persona que s'identifica o signa, es preveu la possibilitat d'usar pseudònims en casos especials com poden ser certificats de cossos de seguretat o de personal vinculat a l'administració de justícia, entre d'altres, de conformitat amb allò establert al Reglament (UE) N° 910/2014 del Parlament Europeu i del Consell, de 23 de juliol de 2014, relatiu a la identificació electrònica i els Serveis de confiança per a les transaccions electròniques en el mercat interior i per la que es deroga la Directiva 1999/93/CEa la llei aplicable, que es descriu a l'apartat 9.15 Conformitat amb la llei aplicable.

En aquests supòsits, s'identificarà el posseïdor de claus de forma indirecta mitjançant un identificador que permeti la identificació de la persona actuant, sota requeriment exprés de l'autoritat competent amb aquesta finalitat.

Per a la resta de casos l'Entitat de Certificació ha d'autenticar, amb caràcter previ a l'emissió i entrega d'un certificat, la identitat del subscriptor i la del posseïdor de claus privades i altres dades, establertes en la secció corresponent per a certificats corporatius. Poden ser individuals (quan s'expedeixen a una persona física, actuant en el seu propi nom

- com per exemple, als ciutadans per a relacionar-se per mitjans electrònics amb les entitats del sector públic de Catalunya) o corporatius (d'organització del sector privat o del sector públic fora de Catalunya - quan s'expedeixen a una organització, que actua per mitjà d'una persona física, identificada en el certificat encara que sigui mitjançant un pseudònim).

#### **1.1.1.1. Certificats d'infraestructura**

L'EC-SECTORPUBLIC podrà emetre els següents tipus de certificats d'infraestructura:

- Certificats d'infraestructura personals d'identificació i signatura electrònica qualificada d'operadors (CIPISQ), que s'usa per a autoritzar operacions relacionades amb els serveis de certificació, com l'aprovació de sol·licituds de certificació
- Certificat d'infraestructura de servidor d'estat de certificats en línia (CIO), que és utilitzat per un servidor *OCSP Responder* per a signar les seves respostes sobre l'estat de validesa dels certificats

#### **1.1.1.2. Certificats personals**

L'EC-SECTORPUBLIC podrà emetre els següents tipus de certificats personals:

- Certificat electrònic de treballador públic de nivell alt d'autenticació: és un certificat qualificat. Funciona amb dispositiu qualificat de creació de signatura electrònica. Garanteixen la identitat del subscriptor i del posseïdor de la clau privada d'identificació i signatura;. Es poden utilitzar en aplicacions que no requereixin la signatura electrònica equivalent a la signatura manuscrita, sinó solament la identificació del posseïdor de claus, en nom dels subscriptors.
- Certificat qualificat de signatura de treballador públic de nivell alt: és un certificat qualificat. Funciona amb dispositiu qualificat de creació de signatura electrònica. Garanteixen la identitat del subscriptor i del posseïdor de la clau privada de signatura, i permeten la generació de la "signatura electrònica qualificada"escrita per efecte legal, sense necessitat de compliment de cap requisit addicional.
- Certificat electrònic de persona vinculada de nivell alt: és un certificat qualificat. Funciona amb dispositiu qualificat de creació de signatura electrònica. Garanteixen la identitat del subscriptor i del posseïdor de la clau privada d'identificació i signatura, i permeten la autenticació i la generació de la "signatura electrònica qualificada".
- Certificat electrònic de treballador públic amb pseudònim de nivell alt d'autenticació: és un certificat qualificat d'acord amb allò establert la llei aplicable, que es descriu a l'apartat 9.15 Conformitat amb la llei aplicable. Funciona amb dispositiu qualificat de creació de signatura electrònica. Garanteixen, de forma indirecta, la identitat del subscriptor i del posseïdor de la clau privada d'identificació,.Es pot utilitzar en aplicacions que no requereixin la signatura electrònica equivalent a la signatura manuscrita, sinó solament la identificació del posseïdor de claus, en nom dels subscriptors

- Certificat qualificat de signatura de treballador públic amb pseudònim de nivell alt: és un certificat qualificat d'acord amb allò establert a la llei aplicable, que es descriu a l'apartat 9.15 Conformitat amb la llei aplicable. Funciona amb dispositiu qualificat de creació de signatura electrònica. Garanteixen, de forma indirecta, la identitat del subscriptor i del posseïdor de la clau privada de signatura, i permeten la generació de la "signatura electrònica qualificada".
- Certificat electrònic de representant davant les AAPP de nivell alt: és un certificat qualificat d'acord amb allò establert a la llei aplicable, que es descriu a l'apartat 9.15 Conformitat amb la llei aplicable. Funciona amb dispositiu qualificat de creació de signatura electrònica. Garanteixen la identitat del subscriptor i del posseïdor de la clau privada d'identificació i signatura, i permeten la generació de la "signatura electrònica qualificada"; També es pot utilitzar en aplicacions que no requereixin la signatura electrònica equivalent a la signatura manuscrita, sinó solament la identificació del posseïdor de claus, en nom dels subscriptors
- Certificat electrònic de treballador públic, i també de persona vinculada, de nivell mig: és un certificat qualificat d'acord amb allò establert a la legislació aplicable, que es descriu a l'apartat 9.15 Conformitat amb la llei aplicable. Garanteix la identitat del subscriptor i del posseïdor de la clau privada d'identificació i signatura i permet la generació de la "signatura electrònica avançada"

### 1.1.1.3. Certificats de dispositiu

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

- Certificat de dispositiu servidor segur (CDS-1), que s'utilitza per una aplicació informàtica, servidor d'SSL o de TLS, per a identificar-se davant les aplicacions client que es connecten i per a protegir el secret de les comunicacions entre el client i el servidor
- Certificat de dispositiu servidor segur de Extended Validation (CDS-1 EV), que s'utilitza per una aplicació informàtica, servidor d'SSL o de TLS, perquè s'identifiqui davant les aplicacions client que es connecten i per a protegir el secret de les comunicacions entre el client i el servidor, oferint la validació automàtica en el navegador
- Certificat de dispositiu de seu electrònica nivell mig de (CDS-1 SENM), que serveix per a identificar i garantir una comunicació segura amb la seu electrònica d'un ens.

Aquest certificat pot utilitzar-se 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, entre d'altres.

El certificat de nivell mig 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

- Certificat de dispositiu aplicació (CDA-1), que emmagatzemat en un servidor i requerit per una aplicació, signa documents o missatges
- Certificat de dispositiu de segell electrònic d'Administració, òrgan o entitat de dret públic nivell mig de 1 (CDA-1 SENM), s'utilitza per a la identificació i l'autenticació de l'exercici de la competència en l'actuació administrativa automatitzada.

Aquest certificat pot utilitzar-se 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 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.

#### **1.1.1.4. Certificats de proves**

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

### **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-SECTOR PUBLIC.

L'EC-SECTORPUBLIC emet certificats dintre de la jerarquia de certificació operada pel Consorci AOC, per tant ha de disposar d'una declaració de pràctiques de certificació, d'acord amb la política general de certificació del Consorci AOC.

Aquesta Declaració de Pràctiques de Certificació (DPC) inclou els procediments que aplica l'EC-SECTORPUBLIC en la prestació dels seus serveis, en compliment dels requisits establerts per les polítiques que gestiona i la legislació aplicable.

Aquesta DPC és coherent amb allò establert en la Política General de Certificació i, fins i tot, inclou múltiples referències a aquesta, per a evitar duplicitats allà on la DPC no introdueix informació addicional.

## **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-SECTORPUBLIC".

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

1.3.6.1.4.1.15096.1.2.10

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

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

### **Certificats personals:**

- **CPI-1** – Certificat electrònic de treballador públic de nivell alt d'autenticació, emès per l'EC-SECTORPUBLIC  
OID: 1.3.6.1.4.1.15096.1.3.2.7.1.2
- **CPSQ-1** – Certificat qualificat de signatura de treballador públic de nivell alt  
OID: 1.3.6.1.4.1.15096.1.3.2.7.1.1
- **CPISQ-2** – Certificat electrònic de persona vinculada de nivell alt  
OID: 1.3.6.1.4.1.15096.1.3.2.82.1
- **CPISA** – Certificat electrònic de nivell mig, emès per l'EC-SECTORPUBLIC  
Treballador públic – CPISA-1 - OID: 1.3.6.1.4.1.15096.1.3.2.7.3.1  
Persona vinculada – CPISA-2 - OID: 1.3.6.1.4.1.15096.1.3.2.86.1
- **CPPI-1** – Certificat electrònic de treballador públic amb pseudònim de nivell alt d'autenticació, emès per l'EC-SECTORPUBLIC  
OID: 1.3.6.1.4.1.15096.1.3.2.4.1.2
- **CPPSQ-1** – Certificat qualificat de signatura de treballador públic amb pseudònim de nivell alt, emès per l'EC-SECTORPUBLIC  
OID: 1.3.6.1.4.1.15096.1.3.2.4.1.1
- **CPRISQ-1** – Certificat electrònic de representant davant les AAPP de nivell alt, emès per l'EC-SECTORPUBLIC  
OID: 1.3.6.1.4.1.15096.1.3.2.8.1.1

### **Certificats de dispositiu:**

- **CDS-1** – Certificat de dispositiu SSL, emès per l'EC-SECTORPUBLIC  
OID: 1.3.6.1.4.1.15096.1.3.2.51.1
- **CDSQ-1** - Certificat de dispositiu SSL EV, emès per l'EC-SECTORPUBLIC. Aquests certificats no es podran emetre a partir de l'entrada en vigor de la versió 2.0 d'aquest document.  
OID: 1.3.6.1.4.1.15096.1.3.1.51.2



- **CDSQ-1** - Certificat de dispositiu SSL EV, emès per l'EC-SECTORPUBLIC i adaptat per eIDAS  
OID: 1.3.6.1.4.1.15096.1.3.2.51.2
- **CDS-1 SENM** - Certificat de seu electrònica de nivell mig, emès per l'EC-SECTORPUBLIC  
OID: 1.3.6.1.4.1.15096.1.3.2.5.2
- **CDA-1** – Certificat d'aplicació, emès per l'EC-SECTORPUBLIC  
OID: 1.3.6.1.4.1.15096.1.3.2.91.1
- **CDA-1 SGNM** - Certificat de segell electrònic de nivell mig, emès per l'EC-SECTORPUBLIC  
OID: 1.3.6.1.4.1.15096.1.3.2.6.2

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 poder portar a terme relacions administratives per mitjans electrònics, d'acord amb la Llei aplicable i la normativa administrativa corresponent, que es recullen a l'apartat 9.15 Conformitat amb la llei aplicable

Els certificats de l'EC-SECTORPUBLIC no s'expedeixen al públic, sinó a les entitats, al personal i als dispositius de les entitats que integren el Sector Públic 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 aplicable, descrita a l'apartat 9.15 Conformitat amb la llei aplicable.

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

Conforme a aquesta funció, el Consorci AOC serà responsable per l'actuació de l'EC-SECTORPUBLIC, davant els usuaris finals i els tercers verificadors de certificats i signatures electròniques.

### **1.3.2. Entitat de Certificació Arrel**

El Consorci AOC disposa d'una autoritat de certificació principal, que és l'arrel de la jerarquia pública de certificació de Catalunya: l'EC-ACC, la finalitat de la qual és integrar altres entitats de certificació en el sistema públic català de certificació mitjançant la vinculació tècnica de les autoritats de certificació corresponents.

### **1.3.3. EC-SECTORPUBLIC**

L'EC-SECTORPUBLIC és l'Entitat de Certificació per a dotar de certificats digitals a les entitats, al personal i als dispositius dels Organismes, Departaments i Empreses Públiques que integren el Sector Públic de Catalunya.

L'EC-SECTORPUBLIC està vinculada a la jerarquia d'entitats de certificació de les entitats públiques de Catalunya i emet els certificats indicats en el punt 1.1.1.

### **1.3.4. Entitats de Registre**

Conforme a allò establert en la Política General de Certificació, les Entitats de Registre assisteixen a les Entitats de Certificació Vinculades en determinats procediments i relacions amb els sol·licitants i subscriptors de certificats, especialment en els tràmits d'identificació, registre i autenticació dels subscriptors dels certificats i dels posseïdors de claus.

El Consorci AOC és responsable del procés de creació d'entitats de registre de l'EC-SECTORPUBLIC: verifica que l'Entitat de Registre compta amb els recursos materials i humans necessaris; i que ha designat i ha format al personal que serà responsable de l'emissió de certificats (els anomenats operadors de l'entitat de registre). Així mateix, és responsable de l'emissió dels certificats d'operador que aquests necessitaran per a poder operar (típicament, seran CIPISQ); el Consorci AOC validarà les peticions de certificats per a operadors de les Entitats de Registre examinant la sol·licitud i fent les comprovacions necessàries per al compliment de la Política General de Certificació i d'aquesta Declaració de Pràctiques de Certificació.

Existeixen els següents tipus d'Entitats de Registre de l'EC-SECTORPUBLIC:

- 1) Els ens subscriptor , operades per una entitat subscriptora de certificats
- 2) Les Entitats de Registre, que col·laboren amb l'EC-SECTORPUBLIC en el procés d'emissió dels certificats

Per a ser Entitats de Registre, les entitats hauran de dissenyar i implantar els corresponents components i procediments tècnics, jurídics i de seguretat, referents al cicle de vida dels dispositius segurs de creació de signatura o, en el seu cas, de xifrat, al cicle de vida de les claus en suport software i al cicle de vida dels certificats que emetin. Aquests components i procediments seran prèviament aprovats pel Consorci AOC.

### **1.3.5. Usuaris finals**

Els usuaris finals són les persones (físiques o jurídiques) que obtenen i utilitzen els certificats personals, d'entitat i de dispositiu emesos per l'EC-SECTORPUBLIC; concretament, podem distingir els següents usuaris finals:

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

#### **1.3.5.1. Sol·licitants de certificats**

Conforme a allò establert en la Política General de Certificació. Més concretament, poden ser sol·licitants de certificats de l'EC-SECTORPUBLIC:

- a) De certificats corporatius: una persona autoritzada a l'efecte per la futura entitat subscriptora
- b) Una persona autoritzada per l'Entitat de Certificació – típicament, el Consorci AOC actuant d'ofici

L'autorització es formalitzarà documentalment.

#### **1.3.5.2. Subscriptors de certificats**

Conforme a allò establert en la Política General de Certificació.

#### **1.3.5.3. Posseïdors de claus**

Conforme a allò establert en la Política General de Certificació.

#### **1.3.5.4. Usuaris de certificats**

Conforme a allò establert en la Política General de Certificació.

#### **1.3.5.5. Verificadors de certificats**

Conforme a allò establert en la Política General de Certificació.

## **1.4. Ús dels certificats**

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

## **1.4.1. Ús típic dels certificats**

### **1.4.1.1. Certificats d'infraestructura**

#### **1.4.1.1.1. Certificat personal d'Infraestructura personal d'identificació i signatura qualificada (CIPISQ)**

Conforme a allò establert en la Política General de Certificació.

#### **1.4.1.1.2. Requisits específics per al CIC**

Conforme a allò establert en la Política General de Certificació.

#### **1.4.1.1.3. Requisits específics per al CIO**

Conforme a allò establert en la Política General de Certificació.

### **1.4.1.2. Requisits específics pels Certificats personals**

#### **1.4.1.2.1. Certificat electrònic de treballador públic de nivell alt d'autenticació**

Permeten l'autenticació dels usuaris.

#### **1.4.1.2.2. Certificat qualificat de signatura de treballador públic de nivell alt**

Permeten els treballadors públics la creació de signatura electrònica qualificada .

#### **1.4.1.2.3. Certificat electrònic de persona vinculada de nivell alt**

Permeten a persones vinculades autenticar-se, i la creació de signatura electrònica qualificada.

#### **1.4.1.2.4. Certificat electrònic de treballador públic de nivell mig**

Permeten els treballadors públics la autenticació i creació de signatura electrònica avançada.

#### **1.4.1.2.5. Certificat electrònic de persona vinculada de nivell mig**

Permeten les persones vinculades la autenticació i creació de signatura electrònica avançada.

#### **1.4.1.2.6. Certificat electrònic de treballador públic amb pseudònim de nivell alt d'autenticació**

Permeten l'autenticació treballadors públics identificats amb pseudònim

#### **1.4.1.2.7. Certificat qualificat de signatura de treballador públic amb pseudònim de nivell alt**

Permeten a treballadors públics identificats amb pseudònim generar signatures qualificades.

#### **1.4.1.2.8. Certificat electrònic de representant davant les AAPP de nivell alt**

Permeten a treballadors públics autenticar-se amb atribucions de representació d'entitats públiques, i també la generació de signatura electrònica qualificada.

### **1.4.1.3. Certificats de Dispositiu**

#### **1.4.1.3.1. Certificats de dispositiu SSL (CDS-1)**

L'EC-SECTORPUBLIC els podrà emetre certificats a les entitats integrants del Sector Públic de Catalunya que siguin 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

Són certificats ordinaris; i garanteixen l'origen de la comunicació (la identitat del servidor concret on funcionen), així com la de l'entitat responsable d'aquest.

#### **1.4.1.3.2. Certificats de dispositiu SSL EV (CDS-1 EV)**

L'EC-SECTORPUBLIC els podrà emetre certificats a les entitats 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 CAB Forum.

Són certificats ordinaris; i garanteixen l'origen de la comunicació (la identitat del servidor concret on funcionen), així com la de l'entitat responsable d'aquest.

#### **1.4.1.3.3. Certificat de seu electrònica de nivell mig (CDS-1 SENM)**

L'EC-SECTORPUBLIC els podrà emetre certificats a entitats integrants del Sector Públic de Catalunya que siguin responsables de l'operació de servidors segurs SSL o TLS destinats a identificar i garantir la comunicació segura amb la seu electrònica d'aquestes entitats. Es tracta de certificats qualificats que poden utilitzar-se per a garantir l'autenticació d'un lloc web oficial (això és, l'origen de les connexions web establertes per un ciutadà amb una seu electrònica) i la connexió segura amb aquest, l'allotjament de registres electrònics d'entrada/sortida, la consulta i l'autorització de registres de representació, etc.

#### **1.4.1.3.4. Certificat d'aplicació (CDA-1)**

L'EC-SECTORPUBLIC els podrà emetre 1 a entitats integrants del Sector Públic de Catalunya que siguin responsables de l'operació d'aplicacions informàtiques que s'identifiquen digitalment, que signen electrònicament webservices o altres protocols i que reben documents i missatges xifrats.

Són certificats ordinaris que garanteixen la integritat i l'autenticitat de les dades signades. També garanteixen la identitat de l'entitat responsable.

#### **1.4.1.3.5. Certificat de segell electrònic nivell mig (CDA-1 SGNM)**

L'EC-SECTORPUBLIC els podrà emetre c a entitats integrants del Sector Públic de Catalunya, per a la identificació i l'autenticació de l'exercici de la competència en l'actuació administrativa automatitzada.

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

### **1.4.2. Aplicacions prohibides**

#### **1.4.2.1. Informacions per a tots els tipus de certificats**

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 requereixen actuacions a prova d'errors, com el funcionament d'instal·lacions nuclears, sistemes de navegació o comunicacions aèries, o sistemes de control d'armament, on un error podria directament comportar la mort, lesions personals o danys mediambientals severos.

#### **1.4.2.2. Certificats d'infraestructura**

Els certificats d'infraestructura emesos per l'EC-SECTORPUBLIC – els perfils dels quals es relacionen en l'apartat 1.2.2 *Identificació de polítiques de certificació cobertes per aquesta DPC* – no podran utilitzar-se per als fins descrits en la Política General de Certificació, apartat *Aplicacions prohibides*.

#### **1.4.2.3. Certificats personals**

Els certificats personals emesos per l'EC-SECTORPUBLIC – els perfils dels quals es relacionen a l'apartat *Identificació de polítiques de certificació cobertes per aquesta DPC* – no podran utilitzar-se per als fins descrits en la Política General de Certificació, apartat *Aplicacions prohibides*.

#### **1.4.2.4. Certificats de dispositiu**

Els certificats de dispositiu emesos per l'EC-SECTORPUBLIC – els perfils dels quals es relacionen a l'apartat *Identificació de polítiques de certificació cobertes per aquesta DPC* –

no podran utilitzar-se per als fins descrits en la Política General de Certificació, apartat *Aplicacions prohibides*.

## **1.5. Administració de la Declaració de Pràctiques**

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

Consorci Administració Oberta de Catalunya – Consorci AOC

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

Consorci 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](http://www.aoc.cat)

Servei d'Atenció a l'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 SCD del Consorci AOC, basant-se en els resultats d'una auditoria a l'efecte, realitzada per un tercer, bianualment.

### **1.5.4. Procediment d'aprovació**

El sistema documental i d'organització de l'EC-SECTORPUBLIC 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**

Conforme a allò establert a la Política General de Certificació.

### **2.2. Publicació d'informació de l'EC-SECTORPUBLIC**

Conforme a allò establert a la Política General de Certificació.

### **2.3. Freqüència de publicació**

La informació de l'EC-SECTORPUBLIC 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 allò establert a la secció 9.12.1 *Procediment per a les modificacions*.

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-SECTORPUBLIC, podent ser consultades pels interessats.

La informació d'estat de revocació de certificats es publica d'acord amb allò establert a la secció 4.10.7 *Freqüència d'emissió de llistes de revocació de certificats (CRL's)*.

### **2.4. Control d'accés**

Conforme a allò establert a la Política General de Certificació.

## 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

Conforme a allò establert a la Política General de Certificació.

#### 3.1.2. Significat dels noms

Conforme a allò establert a la Política General de Certificació.

#### 3.1.3. Utilització d'anònims i pseudònims

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

Els certificats personals, així els individuals com els corporatius, podran indicar pseudònims en comptes del nom vertader del posseïdor de la clau del certificat.

El pseudònim constarà com a tal de forma inequívoca, i se'n indicarà aquesta naturalesa a la descripció del tipus de certificat.<sup>1</sup>

El pseudònim es farà constar mitjançant un camp *Pseudonym* del certificat, i estarà vinculat a una adreça de correu electrònic, mitjançant un camp de caràcter obligatori.

En qualsevol cas, l'emissió de certificats amb pseudònim garantirà, en la fase de registre, la disponibilitat de la identificació real del posseïdor de claus, que només podrà ser revelada prèvia sol·licitud de l'autoritat competent

#### 3.1.4. Interpretació de formats de noms

Sense estipulació addicional.

#### 3.1.5. Unicitat dels noms

Conforme a allò establert a la Política General de Certificació.

---

<sup>1</sup> Article 32 Reglament (UE) N° 910/2014 del Parlament Europeu i del Consell, de 23 de juliol de 2014, relatiu a la identificació electrònica i els Serveis de confiança per les transaccions electròniques en el mercat interior, i pel que es deroga la Directiva 1999/93/CE.

### **3.1.6. Resolució de conflictes relatius a noms**

Conforme a allò establert a la Política General de Certificació.

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**

Conforme a allò establert a la Política General de Certificació.

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

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

En general, l'EC-SECTORPUBLIC no haurà de determinar que un sol·licitant de certificats té dret sobre el nom que apareix en una sol·licitud de certificat. Tampoc actuarà com àrbitre o mediador, ni haurà de resoldre cap disputa concernent a la propietat de noms de persones o organitzacions, noms de domini, marques o noms comercials (per exemple, relatius a direccions electròniques).

#### **3.2.2.1. Entitats de Registre**

Conforme a allò establert a la Política General de Certificació.

#### **3.2.2.2. Les entitats subscriptores de certificats corporatius**

No es requereix realitzar procediment d'autenticació de les entitats subscriptores (titular del certificat) en certificats emesos a LES INSTITUCIONS, ja que es tracta de certificats corporatius, en els que l'organització subscriptora del certificat i l'Entitat de Registre Interna coincideixen.

#### **3.2.2.3. Altres entitats subscriptores**

##### **3.2.2.3.1. Requisits per a certificats de persona vinculada**

Conforme a allò establert a la Política General de Certificació.

##### **3.2.2.3.2. Requisits específics per als certificats de dispositiu**

Conforme a allò establert a la Política General de Certificació.

### **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**

El número i tipus de documents necessaris per a acreditar la identitat del posseïdor de claus són els que admet cada organització subscriptora, tal com es recull en la seva normativa reguladora.

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

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

#### **3.2.3.2. Validació dels elements d'identificació**

Conforme a allò establert a la Política General de Certificació.

#### **3.2.3.3. Necessitat de presència personal**

Conforme a allò establert a la Política General de Certificació.

#### **3.2.3.4. Vinculació de la persona física amb l'organització**

Per als certificats de treballador públic: com es tracta 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 la clau amb l'Entitat de Registre, sinó que s'utilitzen els registres interns de l'entitat.

Per als certificats de persona vinculada: l'EC-SECTORPUBLIC – mitjançant la intervenció d'una Entitat de Registre – ha d'obtenir una justificació documental de la vinculació de la persona física que serà posseïdora de la clau privada amb l'organització, mitjançant qualsevol mitjà admès en dret.

### **3.2.4. Informació no verificada**

L'entitat subscriptora del certificat es responsabilitza que tota la informació inclosa en la sol·licitud del certificat sigui exacta i 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 correu electrònic o la legitimitat en l'ús d'un servidor web).

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

#### **3.3.1. Validació per a la renovació de certificats**

Tant si es tracta d'una renovació ordinària, com si és posterior a la revocació del certificat a renovar, el procés a seguir per a la renovació d'un certificat serà el mateix que per a l'emissió de certificats nous: l'EC-SECTORPUBLIC haurà de comprovar – mitjançant la intervenció d'una Entitat de Registre - que la informació utilitzada per a verificar la identitat i la resta de dades del subscriptor i del posseïdor de la clau continuen sent vàlides.

Si qualsevol informació del subscriptor o del posseïdor de la clau ha canviat, es registrarà adequadament la nova informació, d'acord amb allò establert en la secció 3.2 *Validació inicial de la identitat*.

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

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

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

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

En el cas de les Administracions Públiques, la sol·licitud s'enviarà:

- A través de les seves Entitats de Registre T-CAT
- Directament al 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 T-CAT

Aquesta sol·licitud requereix l'enviament d'un document amb la informació exacta i comprovada (certificada) de les persones, entitats o dispositius per a les quals es demana el certificat. Aquesta ha d'anar signada per la persona autoritzada a l'efecte per l'entitat subscriptora; i ha de portar adjunt el certificat d'aquesta informació.

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

Tota la documentació es lliura a l'Entitat de Registre, per mitjans electrònics. Podrà ser remesa en suport paper o mitjançant correu electrònic, excepcionalment, pels següents motius:

- Que l'entitat subscriptora, per raó de la seva naturalesa jurídica, no pugui ser usuari de l'aplicatiu informàtic usat per a remetre les sol·licituds (actualment, EACAT)
- Que sigui una entitat que sol·liciti certificats digitals per primera vegada, de manera que no disposi de cap certificat digital amb el que portar a terme la tramitació de la sol·licitud per mitjans electrònics

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

Conforme a allò establert en la Política General de Certificació en relació a la sol·licitud de certificats d'infraestructura; a la sol·licitud dels certificats corporatius, personals i a la sol·licitud dels certificats de dispositiu.

#### 4.1.2. Procediment d'alta; Responsabilitats

No aplicable.

## 4.2. Procediment de sol·licitud de certificació

### 4.2.1. Requisits generals per a tots els certificats

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

#### 1. Lliurament de la Fitxa del Subscriptor

Per a que una entitat integrant del Sector Públic de Catalunya pugui sol·licitar certificats, prèviament ha de remetre la Fitxa del Subscriptor, degudament complimentada, al Consorci AOC perquè aquest pugui donar-la d'alta en el sistema i configurar les necessàries autoritzacions del personal indicat per l'entitat.

Aquesta remissió es farà, de manera ordinària, per mitjans electrònics, quan tots els rols que intervenen en el procés de sol·licitud (sol·licitant, certificador i responsable del servei) disposin de certificats digitals.

Alternativament, podrà sol·licitar-los, conforme als motius descrits en l'apartat 4.1 *Sol·licitud d'emissió de certificat*, a través del següent procediment alternatiu:

- Descàrrega de la Fitxa del Subscriptor des del web del Consorci AOC
- Enviament de la Fitxa, degudament complimentada i signada digitalment, a l'adreça: [scd@aoc.cat](mailto:scd@aoc.cat); o bé, enviament de la Fitxa, degudament complimentada i signada manuscritament, per correu ordinari a l'adreça que es recull a la secció 1.5.2 *Dades de contacte de l'organització* d'aquest document

El lliurament d'aquesta documentació es farà junt amb la primera sol·licitud de certificats, o quan sigui necessari actualitzar la informació confirmada en ella.

#### 2. Obtenció dels certificats

Quan la sol·licitud es realitza per mitjans electrònics, una vegada complimentada, ha de ser signada digitalment pel sol·licitant i, quan hagi d'adjuntar-se un certificat de dades, aquest haurà de ser signat digitalment pel certificador:

- Primer, quan el sol·licitant signa la sol·licitud, el sistema envia automàticament un correu electrònic al certificador de l'entitat 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 a 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'entitat obre la sol·licitud en qüestió i, un cop ha comprovat que les dades són correctes, la signa digitalment finalitzant així el procés de sol·licitud
- En aquest moment es fa automàticament l'assentament del registre de sortida de l'entitat i l'assentament del registre d'entrada a l'Entitat de Registre T-CAT que correspongui a l'entitat

L'EC-SECTORPUBLIC rep les dades de la sol·licitud i les carrega a l'aplicació de generació de certificats, on queden a disposició de l'Entitat de Registre corresponent.

Una vegada el certificat ha sigut generat per aquesta Entitat de Registre, s'envia a l'entitat subscriptora.

Si la sol·licitud es realitza per mitjans electrònics, s'han de sol·licitar pel següent procediment alternatiu:

- Descàrrega del model de sol·licitud i el certificat de dades corresponent
- Enviament dels documents, degudament complimentats i signats digitalment, a l'adreça: [scd@aoc.cat](mailto:scd@aoc.cat); o bé, enviament dels documents, degudament complimentats i signats manuscritament, per correu ordinari a l'adreça que es recull en la secció 1.5.2 Dades de contacte de l'organització d'aquest document

### **4.3. Emissió de certificat**

Les sol·licituds rebudes són processades i validades.

En cas que tot sigui correcte, es tramet la sol·licitud a l'Entitat de Registre que correspongui a l'entitat sol·licitant.

Seguidament, i de manera automàtica, s'envia al sol·licitant un missatge informant del resultat positiu o negatiu de l'operació i, en aquest darrer cas, detallant el tipus d'error detectat.

#### **4.3.1. Accions de l'EC-SECTORPUBLIC 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 tramesa, l'EC-SECTORPUBLIC actuarà conforme a allò establert a l'efecte en la Política General de Certificació – apartat 4.3.1 *Accions de l'Entitat de Certificació durant els processos d'emissió i renovació.*

#### **4.3.2. Comunicació de l'emissió al subscriptor**

L'EC-SECTORPUBLIC comunicarà al sol·licitant l'aprovació o denegació de la sol·licitud.

En cas que hagi sigut aprovada, també comunicarà – quan correspongui - al futur posseïdor de claus que s'ha creat el certificat, que es troba disponible i la forma d'obtenir-lo.

### **4.4. Acceptació del certificat**

Per a determinats perfils de certificats, l'EC-SECTORPUBLIC és responsable de crear el parell de claus criptogràfiques; i, per a tots els perfils de certificats, és responsable de generar el certificat digital corresponent.



Per als perfils de certificats per als quals es genera el parell de claus i s'emmagatzema en targetes criptogràfiques, l'EC-SECTORPUBLIC també és responsable de crear els corresponents codis PIN i PUK d'aquestes targetes. Aquests codis s'envien directament al posseïdor de les claus, de manera ordinària per correu electrònic adreçat a aquest o, de manera extraordinària, per correu postal en sobre cec. El posseïdor de les claus podrà, en qualsevol moment, recuperar aquests codis a través de l'aplicació telemàtica a l'efecte.

Paral·lelament, la targeta amb el certificat sol·licitat s'envia per correu postal a l'atenció del responsable de l'entitat de registre interna de l'entitat subscriptora.

L'EC-SECTORPUBLIC generarà el full de lliurament i acceptació del certificat per al posseïdor de claus; en el qual se l'indiquen els continguts descrits en la Política General de Certificació.

#### **4.4.1. Responsabilitats de l'Ens subscriptor**

##### **4.4.1.1. Per a Certificats personals**

L'EC-SECTORPUBLIC delega en els ens subscriptors (més concretament, en la figura del responsable) algunes de les seves responsabilitats, referents al procés d'entrega i acceptació dels certificats digitals que emet.

Concretament, el responsable de l'entitat de registre haurà de:

- informar al posseïdor de les claus de les seves obligacions i responsabilitats en relació al certificat que li lliura
- requerir del posseïdor de les claus el reconeixement de rebre el certificat i, en el seu cas, el dispositiu criptogràfic corresponent, així com el reconeixement de l'acceptació d'aquests elements, mitjançant la signatura del full de lliurament i acceptació del certificat
- En el cas d'aquells perfils que requereixen targeta criptogràfica, lliurar al posseïdor de les claus en persona, una vegada aquest hagi signat el full de lliurament i acceptació del certificat; així com també un exemplar del full de lliurament i acceptació del certificat

##### **4.4.1.2. Per a certificats de dispositiu**

Els certificats de dispositiu es lliuraran mitjançant un fitxer que haurà de descarregar el responsable de l'ens subscriptor.

#### **4.4.2. Conducta que constitueix acceptació del certificat**

El certificat s'accepta mitjançant la signatura, per part del posseïdor de claus, del full de lliurament i acceptació del certificat.

També es considera la possibilitat d'acceptar el certificat mitjançant un mecanisme telemàtic d'activació del certificat.

#### **4.4.3. Publicació del certificat**

Conforme a allò establert a la Política General de Certificació.

#### **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 per part dels posseïdors de claus**

Conforme a allò establert a la Política General de Certificació.

#### **4.5.2. Ús pel tercer que confia en certificats**

Conforme a allò establert a la Política General de Certificació.

### **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**

Conforme a allò establert a la Política General de Certificació.

### **4.8. Renovació telemàtica**

Conforme a allò establert a la Política General de Certificació.

### **4.9. Modificació de certificats**

Conforme a allò establert en la Política General de Certificació.

Més enllà, en determinades circumstàncies (com per exemple, en moments de canvis organitzatius, com a l'inici d'una nova legislatura, quan alguns departaments desapareixen i

les seves funcions s'integren en un altre departament, o simplement canvien de nom), i de manera transitòria, les dades no identificatives que sobre el posseïdor de les claus consten en el certificat (com són: l'adreça de correu-e, el departament al qual està adscrit, etc.) poden no ajustar-se a les noves circumstàncies. En aquests casos, l'organització haurà de planificar la renovació dels certificats dels seus usuaris, la qual cosa podrà demorar-se raonablement atenent a motius econòmics i/o organitzatius, sense que suposi un incompliment de la responsabilitat atribuïda.

## **4.10. Revocació i suspensió de certificats**

### **4.10.1. Causes de revocació de certificats**

Conforme a allò establert a la Política General de Certificació.

### **4.10.2. Legitimació per a sol·licitar la revocació**

Conforme a allò establert a la Política General de Certificació.

### **4.10.3. Procediments de sol·licitud de revocació**

La sol·licitud de revocació ha de ser tramesa telemàticament. Excepcionalment es podrà trametre per correu electrònic signat o per correu certificat convencional. Ha d'incloure's la informació suficient per a poder identificar raonablement, a criteri de l'EC-SECTORPUBLIC, per una banda, el certificat que es sol·licita revocar i, per altra, l'autenticitat i autoritat del sol·licitant.

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

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

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

Les Entitats de Registre atenen les sol·licituds de revocació dintre del seu horari d'oficina. Fora d'aquest horari, quan sigui urgent deixar sense efecte un certificat, es pot sol·licitar la suspensió cautelar del certificat mitjançant trucada telefònica al Centre d'Atenció a l'Usuari del Consorci AOC, l'horari d'atenció del qual és 24x365.

La suspensió està prohibida pels certificats de dispositiu següents, podent ser només revocats:

- Certificat de dispositiu SSL
- Certificat de dispositiu SSL EV

Certificat de seu electrònica de nivell mig

L'acció de revocació la porta a terme un dels operadors de l'Entitat de Registre, qui accedeix a l'aplicació web a l'efecte, autenticant-se mitjançant un certificat digital d'operador (CIPISQ) emès per l'EC-SECTORPUBLIC.

Una vegada registrat el canvi d'estat del certificat en el sistema de l'EC-SECTORPUBLIC, de forma automàtica i a la major brevetat possible, es genera i publica una nova Llista de Certificats Revocats (LCR o CRL) en la qual constarà la referència d'aquest certificat.

S'informa al subscriptor i, en el seu cas, al posseïdor de claus, sobre el canvi d'estat del certificat, d'acord amb l'article 10.2 de la Llei de signatura electrònica.

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

Conforme a allò establert a la Política General de Certificació.

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

Conforme a allò establert a la Política General de Certificació.

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

Conforme a allò establert a la Política General de Certificació.

#### **4.10.7. Freqüència d'emissió de llistes de revocació de certificats (CRL's)**

Conforme a allò establert a la Política General de Certificació.

#### **4.10.8. Període màxim de publicació de CRL's**

Conforme a allò establert a la Política General de Certificació.

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

Conforme a allò establert a la Política General de Certificació.

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

Conforme a allò establert a la Política General de Certificació.

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

Sense estipulació addicional.

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

Conforme a allò establert a la Política General de Certificació.

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

Conforme a allò establert a la Política General de Certificació.

#### **4.10.14. Efecte de la suspensió de certificats**

Conforme a allò establert a la Política General de Certificació.

#### **4.10.15. Qui pot sol·licitar la suspensió**

Conforme a allò establert a la Política General de Certificació en relació a la suspensió de certificats corporatius.

#### **4.10.16. Procediments de sol·licitud de suspensió**

Conforme a allò establert a la Política General de Certificació.

#### **4.10.17. Període màxim de suspensió**

Conforme a allò establert a la Política General de Certificació.

#### **4.10.18. Habilitació d'un certificat suspès**

Conforme a allò establert a la Política General de Certificació.

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

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

Les CRL's 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-SECTORPUBLIC.

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

Conforme a allò establert a la Política General de Certificació.

### **4.11.3. Altres funcions dels serveis**

Sense estipulació addicional.

## **4.12. Finalització de la subscripció**

Conforme a allò establert a la Política General de Certificació.

## **4.13. Dipòsit i recuperació de claus**

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

No es practica recuperació de claus per als certificats emesos per EC-SECTORPUBLIC.

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

Sense estipulació addicional.

## **4.14. Notificació de problemes amb certificats d'autenticació de lloc web**

Per notificar qualsevol problema relacionada amb l'ús, correcció, seguretat o altre, relatiu a qualsevol classe de certificat d'autenticació de lloc web o certificat SSL emès pel Consorci Administració Oberta de Catalunya, a saber:

- Certificat de dispositiu SSL,
- Certificat de dispositiu SSL EV,

- Certificat de seu electrònica de nivell mig,

si us plau contacteu amb el Consorci AOC fent servir les Dades de contacte de l'organització o l'adreça electrònica següent:

incident\_pki@aoc.cat,

proporcionant, si és possible:

- Data i hora
- Número de sèrie del certificat
- URL a la que s'està accedint
- adreça IP des de la que s'està intentant accedir a la URL

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

## **5.1. Controls de seguretat física**

Conforme a allò establert a la Política General de Certificació.

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

Conforme a allò establert a la Política General de Certificació.

### **5.1.2. Accés físic**

Conforme a allò establert a la Política General de Certificació.

### **5.1.3. Electricitat i aire condicionat**

Conforme a allò establert a la Política General de Certificació.

### **5.1.4. Exposició a l'aigua**

Conforme a allò establert a la Política General de Certificació.

### **5.1.5. Advertència i protecció d'incendis**

Conforme a allò establert a la Política General de Certificació.

### **5.1.6. Emmagatzematge de suports**

Conforme a allò establert a la Política General de Certificació.

### **5.1.7. Tractament de residus**

Conforme a allò establert a la Política General de Certificació.



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

Conforme a allò establert a la Política General de Certificació.

## **5.2. Controls de procediments**

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

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

### **5.2.1. Funcions fiables**

Conforme a allò establert a la Política General de Certificació.

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

### **5.2.2. Nombre de persones per tasca**

Conforme a allò establert a la Política General de Certificació.

### **5.2.3. Identificació i autenticació per a cada funció**

Conforme a allò establert a la Política General de Certificació.

### **5.2.4. Rols que requereixen separació de tasques**

Conforme a allò establert a la Política General de Certificació.

## **5.3. Controls de personal**

L'EC-SECTORPUBLIC 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-SECTORPUBLIC
- 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 Operadors de l'Entitats de Registre

A més, 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**

Conforme a allò establert a la Política General de Certificació.

### **5.3.2. Requisits de formació**

Conforme a allò establert a la Política General de Certificació.

El Consorci AOC, a més, proporciona a tot el personal involucrat en les operacions de les Entitats de Registre de l'EC-SECTORPUBLIC, una informació adequada, que inclou els procediments de treball i els de seguretat.

També es realitza instrucció periòdica en normes de seguretat, plans de contingència i gestió d'incidències al personal intern.

### **5.3.3. Requisits i freqüència d'actualització formativa**

Conforme a allò establert a la Política General de Certificació.

### **5.3.4. Seqüència i freqüència de rotació laboral**

Sense estipulació addicional.

### **5.3.5. Sancions per accions no autoritzades**

Conforme a allò establert a la Política General de Certificació.

### **5.3.6. Requisits de contractació de professionals**

Conforme a allò establert a la Política General de Certificació.

### **5.3.7. Subministrament de documentació al personal**

Conforme a allò establert a la Política General de Certificació.

## **5.4. Procediments d'auditoria de seguretat**

### **5.4.1. Tipus d'esdeveniments registrats**

Conforme a allò establert a la Política General de Certificació.

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

Conforme a allò establert a la Política General de Certificació.

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

Conforme a allò establert a la Política General de Certificació.

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

Conforme a allò establert a la Política General de Certificació.

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

Conforme a allò establert a la Política General de Certificació.

Amb la finalitat de conservar correctament les còpies de seguretat, s'han implantat els 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 (usb, dvd's...) i es 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**

Conforme a allò establert a la Política General de Certificació.

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

Conforme a allò establert a la Política General de Certificació.

#### **5.4.8. Anàlisi de vulnerabilitats**

Conforme a allò establert a la Política General de Certificació.

### **5.5. Arxiu d'informacions**

Conforme a allò establert a la Política General de Certificació.

### **5.5.1. Tipus d'esdeveniments registrats**

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

L'EC-SECTORPUBLIC guarda registre del següent:

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

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

L'EC-SECTORPUBLIC 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 de l'arxiu**

Conforme a allò establert a la Política General de Certificació.

### **5.5.4. Procediments de còpia suport**

Es fan còpies de seguretat dels logs d'accés lògic al sistema operatiu de la LRA. S'encarrega un tècnic de comunicacions del Consorci AOC.

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

### **5.5.5. Requisits de segellat de data i hora**

Conforme a allò establert a la Política General de Certificació.

### **5.5.6. Localització del sistema d'arxiu**

L'EC-SECTORPUBLIC té un sistema d'emmagatzemament de dades d'arxiu fora de les seves pròpies instal·lacions, així com s'especifica a la secció 5.1.8.

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

Conforme a allò establert a la Política General de Certificació.

## **5.6. Renovació de claus**

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

## **5.7. Compromís de claus i recuperació de desastre**

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

L'EC-SECTORPUBLIC 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-SECTORPUBLIC 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-SECTORPUBLIC (o pla de recuperació de desastres) considera el compromís, o la sospita de compromís, de la clau privada de l'EC-SECTORPUBLIC com un desastre.

En cas de compromís, l'EC-SECTORPUBLIC:

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

### **5.7.4. Desastre sobre les instal·lacions**

L'EC-SECTORPUBLIC desenvolupa, manté, prova i, 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-SECTORPUBLIC 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
- Publicació d'informació de revocació

La base de dades de recuperació de desastres utilitzada per l'EC-SECTORPUBLIC 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-SECTORPUBLIC tenen les mesures de seguretat físiques especificades en el Pla de Seguretat.

## **5.8. Finalització del servei**

### **5.8.1. EC-SECTORPUBLIC**

Conforme a allò establert a la Política General de Certificació.

### **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-SECTORPUBLIC 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 posseïdor de claus o per l'Entitat de Registre.

##### **6.1.1.2. Informació per als certificats CPI, CPSQ, CPPI, CPPSQ i CPRISQ**

Les claus pública i privada dels certificats CPI, CPSQ, CPPI, CPPSQ i CPRISQ les genera el Consorci AOC dintre d'un dispositiu qualificat de creació de signatura electrònica.

##### **6.1.1.3. Informació per als certificats CPISA**

Les claus pública i privada dels certificats CPISA les pot generar el Consorci AOC i són enviades al posseïdor de claus de forma segura. També poden ser generades pel futur posseïdor de claus, qui remetrà la corresponent prova de possessió de clau privada (PKCS#10) a l'EC-SECTORPUBLIC.

Aquestes claus no s'emmagatzemen, de manera que, en cas de suspensió, revocació o expiració del certificat, el Consorci AOC no respondrà per la pèrdua d'informació que hagués estat xifrada amb elles.

##### **6.1.1.4. Informació per als certificats CDS-1, CDS-1 EV, CDS-1 SENM, CDA-1, CDA-1 SENM**

El parell de claus dels certificats CDS-1, CDS-1 EV, CDS-1 SENM, CDA-1, CDA-1 SENM, el genera l'entitat que sol·licita el certificat, el subscriptor, que remetrà la corresponent prova de possessió de clau privada (PKCS#10) a l'EC-SECTORPUBLIC.

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

6.1.2.1. Conforme a allò establert a la Política General de Certificació.



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

Conforme a allò establert a la Política General de Certificació.

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

La clau de l'EC-SECTORPUBLIC i les claus de les Entitats de Certificació anteriors en la jerarquia pública de certificació de Catalunya són comunicades als verificadors, garantint la integritat de la clau i autenticant-ne l'origen.

La clau pública de l'EC-SECTORPUBLIC es publica en el directori de l'EC-SECTORPUBLIC, en forma de certificat CIC signat per l'EC-ACC. Els usuaris poden accedir al directori per a obtenir les claus públiques de l'EC-SECTORPUBLIC.

Aquest mateix certificat també es publica a la web del Consorci AOC.

Addicionalment, en aplicacions S/MIME, el missatge de dades conté una cadena de certificats, incloent els certificats CIC amb les claus públiques de les Entitats de Certificació de la jerarquia (en aquest cas, de l'EC-SECTORPUBLIC i de l'EC-ACC), que d'aquesta manera són distribuïdes als usuaris.

### **6.1.5. Mides de claus**

Les claus de l'EC-SECTORPUBLIC són de mínim de 2.048 bits.

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

### **6.1.6. Generació de paràmetres de clau pública**

Sense estipulació addicional.

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

Conforme a allò establert a la Política General de Certificació.

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

Conforme a allò establert a la Política General de Certificació.

### **6.1.9. Propòsits d'ús de claus**

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

## **6.2. Protecció de la clau privada**

### **6.2.1. Mòduls de protecció de la clau privada**

#### **6.2.1.1. Estàndards dels mòduls criptogràfics**

Conforme a allò establert a la Política General de Certificació.

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

Conforme a allò establert a la Política General de Certificació.

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

Conforme a allò establert a la Política General de Certificació.

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

Conforme a allò establert a la Política General de Certificació.

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

Conforme a allò establert a la Política General de Certificació.

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

Conforme a allò establert a la Política General de Certificació.

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

Conforme a allò establert a la Política General de Certificació.

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

Conforme a allò establert a la Política General de Certificació.

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

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

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

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

Conforme a allò establert a la Política General de Certificació.

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

Conforme a allò establert a la Política General de Certificació.

### **6.2.11. Classificació dels mòduls criptogràfics**

Conforme a allò establert a la Política General de Certificació.

## **6.3. Altres aspectes de gestió del parell de claus**

### **6.3.1. Arxiu de la clau pública**

L'EC-SECTORPUBLIC arxiva les seves claus públiques, d'acord amb allò establert a la secció 6.2.

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

Conforme a allò establert a la Política General de Certificació.

## **6.4. Dades d'activació**

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

Conforme a allò establert a la Política General de Certificació.

### **6.4.2. Protecció de les dades d'activació**

Conforme a allò establert a la Política General de Certificació.

### **6.4.3. Altres aspectes de les dades d'activació**

Sense estipulació addicional

## **6.5. Controls de seguretat informàtica**

### **6.5.1. Requisits tècnics específics de seguretat informàtica**

Conforme a allò establert a la Política General de Certificació.

### **6.5.2. Avaluació del nivell de seguretat informàtica**

L'aplicació d'autoritat de certificació, mitjançant la qual opera l'EC-SECTORPUBLIC (EJBCA Enterprise Edition) és fiable, donat que va obtenir la certificació Common Criteria EAL 4+.

## **6.6. Controls tècnics del cicle de vida**

### **6.6.1. Controls de desenvolupament de sistemes**

Conforme a allò establert a la Política General de Certificació.

### **6.6.2. Controls de gestió de seguretat**

Conforme a allò establert a la Política General de Certificació.

A més, l'EC-SECTORPUBLIC garanteix que les seves funcions de gestió de les operacions dels mòduls criptogràfics són suficientment segures; en particular, existeixen instruccions per a:

- 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 software maliciós per a garantir la integritat i validesa de la informació que processen

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

Sense estipulació addicional.

## 6.7. Controls de seguretat de xarxa

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

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

## 6.8. Segell de temps

Sense estipulació adicional.

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

## **7.1. Perfil de certificat**

Conforme a allò establert a la Política General de Certificació.

Els documents descriptius dels diversos perfils de certificats digitals que expedeix l'EC-SECTORPUBLIC es publiquen a la web del Consorci AOC.

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

Conforme a allò establert a la Política General de Certificació.

## **8. Auditoria de conformitat**

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

### **8.1. Freqüència de l'auditoria de conformitat**

Conforme a allò establert a la Política General de Certificació.

### **8.2. Identificació i qualificació de l'auditor**

L'EC-SECTORPUBLIC 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 i dels elements relacionats.

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

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

### **8.4. Relació d'elements objecte d'auditoria**

Conforme a allò establert a la Política General de Certificació.

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

Conforme a allò establert a la Política General de Certificació.

## **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-SECTORPUBLIC en la prestació dels seus serveis. Les tarifes es poden consultar a la web 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 estipulació addicional.

#### **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 estipulació addicional.

### **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-SECTORPUBLIC) 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-SECTORPUBLIC).

## **9.3. Confidencialitat**

### **9.3.1. Informacions confidencials**

Conforme a allò establert a la Política General de Certificació.

### **9.3.2. Informacions no confidencials**

Conforme a allò establert a la Política General de Certificació.

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

Conforme a allò establert a la Política General de Certificació.

## **9.4. Protecció de dades personals**

### **9.4.1. Política de Protecció de Dades Personals**

Conforme a allò establert a la Política General de Certificació.

### **9.4.2. Dades de caràcter personal no disponibles a tercers**

Conforme a allò establert a la Política General de Certificació.

### **9.4.3. Dades de caràcter personal disponibles a tercers**

Conforme a allò establert a la Política General de Certificació.

#### **9.4.4. Responsabilitat corresponent a la protecció de dades personals**

Conforme a allò establert a la Política General de Certificació.

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

Conforme a allò establert a la Política General de Certificació.

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

Conforme a allò establert a la Política General de Certificació.

#### **9.4.7. Comunicació de dades personals**

Conforme a allò establert a la Política General de Certificació.

### **9.5. Drets de propietat intel·lectual**

#### **9.5.1. Propietat dels certificats i informació de revocació**

Conforme a allò establert a la Política General de Certificació.

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

Conforme a allò establert a la Política General de Certificació.

#### **9.5.3. Propietat de la informació relativa a noms**

Conforme a allò establert a la Política General de Certificació.

#### **9.5.4. Propietat de claus**

Conforme a allò establert a la Política General de Certificació.

## **9.6. Obligacions i responsabilitat civil**

### **9.6.1. Entitats de Certificació**

#### **9.6.1.1. Obligacions generals de l'EC-SECTORPUBLIC**

Conforme a allò establert a la Política General de Certificació.

#### **9.6.1.2. Requisits específics per als certificats personals**

Conforme a allò establert a la Política General de Certificació.

#### **9.6.1.3. Informació addicional per al CDS-1, CDS-1 EV, i CDS-1 Seu electrònica**

Conforme a allò establert a la Política General de Certificació.

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

#### **9.6.1.4. Garanties oferides a subscriptors i verificadors**

Conforme a allò establert a la Política General de Certificació.

### **9.6.2. Obligacions i altres compromisos de les Entitats de Registre**

#### **9.6.2.1. Obligacions i altres compromisos**

Conforme a allò establert a la Política General de Certificació. Exceptuant l'obligació d'emmagatzemar els fulls de lliurament de certificat durant un període de 15 anys, que és assumida per les entitats subscriptores dels certificats corporatius que emet l'EC-SECTORPUBLIC.

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

#### **9.6.3. Obligacions i altres compromisos de les entitats subscriptores dels certificats corporatius emesos per l'EC-SECTORPUBLIC**

Les entitats subscriptores dels certificats emesos per l'EC-SECTORPUBLIC s'obliguen a emmagatzemar els fulls de lliurament de certificat durant un període de 15 anys.

Aquests registres han d'estar a disposició de l'Entitat de Certificació Vinculada.

## **9.6.4. Garanties oferides a subscriptor i verificadors**

### **9.6.4.1. Garantia del Consorci AOC pels serveis de certificació digital**

Conforme a allò establert a la Política General de Certificació.

### **9.6.4.2. Exclusió de la garantia**

Conforme a allò establert a la Política General de Certificació.

## **9.6.5. Subscriptors**

### **9.6.5.1. Obligacions i altres compromisos**

#### **9.6.5.1.1. Informacions per a tots els tipus de certificats**

Conforme a allò establert a la Política General de Certificació.

#### **9.6.5.1.2. Informacions específiques per als certificats de signatura electrònica qualificada**

Conforme a allò establert a la Política General de Certificació.

### **9.6.5.2. Garanties oferides pel subscriptor**

Conforme a allò establert a la Política General de Certificació.

### **9.6.5.3. Protecció de la clau privada**

Conforme a allò establert a la Política General de Certificació.

## **9.6.6. Verificadors**

### **9.6.6.1. Obligacions i altres compromisos**

Conforme a allò establert a la Política General de Certificació.

### **9.6.6.2. Garanties oferides pel verificador**

Conforme a allò establert a la Política General de Certificació.

## **9.6.7. Altres participants**

### **9.6.7.1. Obligacions i garanties del directori**

Conforme a allò establert a la Política General de Certificació.

### **9.6.7.2. Garanties oferides pel directori**

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

## **9.7. Renúncies de garanties**

### **9.7.1. Rebuig de garanties de l'EC-SECTORPUBLIC**

L'EC-SECTORPUBLIC 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-SECTORPUBLIC**

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-SECTORPUBLIC 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-SECTORPUBLIC limita la seva responsabilitat mitjançant la inclusió de límits d'ús del certificat i límits de valor de les transaccions per a les que pot utilitzar-se el certificat.

### **9.8.2. Cas fortuït i força major**

L'EC-SECTORPUBLIC 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. Termini i finalització**

### **9.10.1. Termini**

L'EC-SECTORPUBLIC 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 subministra certificats.

### **9.10.2. Finalització**

L'EC-SECTORPUBLIC 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 subministra certificats.

### **9.10.3. Supervivència**

Conforme a allò establert a la Política General de Certificació.

## **9.11. Notificacions**

Conforme a allò establert a la Política General de Certificació.

## **9.12. Modificacions**

### **9.12.1. Procediment per a les modificacions**

Conforme a allò establert a la Política General de Certificació.

## **9.12.2. Termini i 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 estipulació addicional.

## **9.13. Resolució de conflictes**

### **9.13.1. Resolució extrajudicial de conflictes**

Conforme a allò establert a la Política General de Certificació.

### **9.13.2. Jurisdicció competent**

Conforme a allò establert a la Política General de Certificació.

## **9.14. Llei aplicable**

Conforme a allò establert a la Política General de Certificació.

## **9.15. Conformitat amb la llei aplicable**

Conforme a allò establert en la Política General de Certificació.

## **9.16. Clàusules diverses**

### **9.16.1. Acord íntegre**

Conforme a allò establert a la Política General de Certificació.

### **9.16.2. Subrogació**

Conforme a allò establert a la Política General de Certificació.



### **9.16.3. Divisibilitat**

Conforme a allò establert a la Política General de Certificació.

### **9.16.4. Aplicacions**

Sense estipulació addicional.

### **9.16.5. Altres clàusules**

Sense estipulació addicional.

## 10. ANNEX – Control documental

Projecte:	<b>Informe creació del document DPC EC-SECTORPUBLIC</b>
Entitat de destí:	<b>Servei SCD - Consorci AOC</b>
Codi de referència:	<b>Revisió 2on trimestre 2018</b>
Versió:	<b>Versió inicial</b>
Data de l'edició:	<b>09/05/2018</b>

<b>Versió</b>	<b>Parts que canvien</b>	<b>Descripció del canvi</b>	<b>Autor del canvi</b>	<b>Data del canvi</b>
1.0	Tot el document	Redacció inicial de la Declaració de Pràctiques de Certificació de l'EC-SECTORPUBLIC	Servei CATCert del Consorci AOC	0/08/2015
2.0	Tot el document	Adaptació a requisits eIDAS	Servei SCD del Consorci AOC	09/05/2018