Consorci
Administració Oberta
de Catalunya

Política General de Certificació
Consorci AOC

Referència:	D1111_E0650_N-PGdC
Versió:	5.0
Data:	09/05/2018

Index

1. Introducció

1.1. Antecedents

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

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

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

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

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

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

En data 2 d'agost de 2011, el Govern de la Generalitat de Catalunya va aprovar l'acord sobre mesures de racionalització i simplificació de l'estructura del sector públic de Catalunya, en el marc de les quals s'instava als departaments competents a formular i implantar estratègies de reordenació del seu sector públic que incidissin especialment en la millora de l'eficiència organitzativa de la que s'ha de derivar una eficiència econòmica.

En aquesta línia, dintre d'una llarga llista d'actuacions que afectaven a un elevat nombre d'entitats que integren el sector públic de la Generalitat de Catalunya, es va acordar promoure les actuacions necessàries pera la integració de CATCert en el Consorci AOC i procedir a l'extinció de CATCert com a organisme autònom.

En conseqüència, la Comissió Executiva del Consorci AOC, va acordar la reversió al Consorci dels serveis gestionats fins a la data per CATCert, amb la incorporació a aquell dels mitjans materials, econòmics i humans corresponents, així com la gestió directa del servei de certificació digital i totes les funcions generals del conjunt de l'organització.

De manera que ara el Consorci Administració Oberta de Catalunya és el prestador dels serveis de certificació (TSP) públics de Catalunya i el propietari de la infraestructura de clau pública (PKI) que abans era titularitat de CATCert.

1.2. Presentació

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

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

L'adequació a la llei 39/15 de 1 d'Octubre, de Procediment Administratiu Comú de les Administracions Públiques, la Llei 40/2015 de 1 d'octubre, de Règim Jurídic del Sector Públic (LRJ) i el Reglament (UE) 910/2014, relatiu a la identificació electrònica i els serveis de confiança per les transaccions electròniques en el mercat interior (eIDAS), ha donat lloc a una nova versió d'aquesta política general i tots els documents que hi estan relacionats. En particular, dels perfils dels certificats digitals.

Més enllà, el servei de certificació digital del Consorci AOC compleix amb la versió actual de les pautes del CA/Browser Forum per a l'emissió i la gestió de certificats de validació estesa (*extended validation*), i amb les pautes de Baseline Requirements d'aquest mateix organisme per la emissió de certificats CDS, publicades a: http://www.cabforum.org.

1.2.1. Termes habituals utilitzats en aquest document

A continuació, s'aporten breus explicacions del significat que alguns termes tenen en l'àmbit d'aquest document:

Certificat	Document electrònic signat per una entitat de certificació que vincula unes dades de verificació de signatura electrònica a una persona (física o jurídica) i confirma la seva identitat.
Declaració de pràctiques de certificació	Document exigit per la Llei de signatura electrònica, que detalla els requisits que compleix el prestador de serveis de certificació quan emet certificats.
Entitat de certificació	Persona física o jurídica que emet certificats, d'acord amb la Llei de signatura electrònica. Amb freqüència es tracta com un sinònim d'autoritat de certificació, que és un component tècnic del servei.
Entitat de certificació arrel	Entitat de certificació superior de la jerarquia de certificació, que garanteix legalment tots els certificats emesos per les entitats de certificació vinculades a la jerarquia.
Entitat de certificació vinculada	Entitat de certificació que ha sigut vinculada a una jerarquia de certificació, de manera que l'entitat de certificació arrel garanteix els certificats emesos per l'entitat vinculada.
Entitat de certificació virtual	Entitat de certificació que ha delegat totes les operacions tècniques per a l'emissió dels certificats al Consorci AOC, en la seva qualitat de prestador de serveis de certificació.
Entitat de registr	Persona jurídica que executa els procediments de comprovació de la identitat de la resta de circumstàncies dels subscriptors i dels posseïdors de claus dels certificats. A vegades es tracta com un sinònim d'autoritat de registre, que és un component tècnic del servei.
Entitat de registre col·laboradora	Entitat de registre que col·labora amb les entitats de certificació en l'emissió dels certificats als subscriptors.
Ens subscriptor	Entitat de registre d'una administració subscriptora de certificats, que registra els seus posseïdors de claus.

Entitat de registre virtual	Entitat de registre interna que ha delegat en l'entitat de certificació o en una entitat de registre col·laboradora els treballs tècnics del procediment de comprovació de la identitat i de la resta de circumstàncies personals dels subscriptors i dels posseïdors dels certificats.
Jerarquia pública de certificació de Catalunya	Conjunt d'entitats públiques catalanes de certificació, entitats de registre i altres que emeten certificats, organitzades en un sistema públic controlat i garantit pel Consorci AOC, que actua com a entitat de certificació arrel per delegació de les institucions d'autogovern de Catalunya i de les administracions públiques catalanes.
Llista de revocació de certificats	Document electrònic signat per una entitat de certificació que detalla els certificats que, temporalment o definitivament, no són vàlids.
Perfil de certificat	Document que detalla els continguts dels certificats, sintàctica i semànticament.
Posseïdor de claus	Persona física que rep un certificat emès a un subscriptor (que serà una entitat, quan es tracti de certificats corporatius, o la pròpia persona física, quan es tracti de certificats individuals), i que l'utilitza sota la responsabilitat del dit subscriptor.
Prestador de serveis de certificació	Persona jurídica que actua legalment com a entitat de certificació i/o que presta serveis de certificació a tercers, per delegació d'una entitat de certificació.
Segell electrònic	D'acord amb la Llei 11/2007, de 22 de juny, d'Accés Electrònic dels Ciutadans als Serveis Públics, es tracta d'un sistema de signatura electrònica pera l'actuació administrativa automatitzada, basada en certificat electrònic.
Seu Electrònica	D'acord amb la Llei 11/2007, de 22 de juny, d'Accés Electrònic dels Ciutadans als Serveis Públics, és l'adreça electrònica disponible per als ciutadans a través de les xarxes de telecomunicacions la titularitat, gestió i administració de la qual correspon a una Administració Pública, òrgan o entitat administrativa en l'exercici de les seves competències.
Sistema públic català de certificació	

	Conjunt de totes les entitats, públiques i privades, catalanes, nacionals i internacionals, de certificació, entitats de registre i altres que emetin certificats, organitzades en un sistema públic controlat i garantit pel Consorci AOC, que actua com a entitat de classificació per delegació de les institucions d'autogovern de Catalunya i de les administracions públiques catalanes.
Subscriptor de certificats electrònics	És el seu titular. En certificats expedits a persones físiques, que actuen individualment, és la persona física que sol·licita el seu certificat i que tindrà accés exclusiu a les dades de creació de signatura (la clau privada). En el cas de certificats corporatius, el subscriptor és la persona jurídica a la qual està vinculat el posseïdor de claus.

1.2.2. Tipus i classes de certificats

El Consorci AOC presta els seus serveis de certificació amb la finalitat d'expedir certificats digitals per a diversos usos i diferents usuaris finals.

Per això es van definir i s'emeten diferents tipus i classes de certificats digitals, que són els que es descriuen a continuació. En primer lloc, dintre de la jerarquia pública de certificació de Catalunya, s'expedeixen certificats a altres Entitats de Certificació, que d'aquesta forma queden vinculades a la jerarquia. Aquests certificats es denominen Certificats d'Infraestructura d'Entitat de Certificació (CIC) i permeten que les entitats de certificació subscriptores dels certificats CIC puguin expedir certificats a altres Entitats de Certificació o a usuaris finals.

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

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

Cada certificat CIC rebrà un nivell adequat al període de durada de dit certificat, que s'usarà pera la programació de la renovació periòdica de la infraestructura de certificació.

Els certificats d'usuaris finals es divideixen en:

- Certificats personals, caracteritzats pel fet que el posseïdor de la clau privada és una persona física, que actua en 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 les operacions de signatura i desxifrat de forma

automàtica, sota la responsabilitat d'una persona física o jurídica (anomenat subscriptor o titular del certificat).

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

Les diferents polítiques de certificació previstes es descriuen a la Declaració de Pràctiques de Certificació (DPC) de l'Entitat de Certificació corresponent.

1.2.3. Relació entre la política de certificació i altres documents

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

La política de certificació estableix les regles mínimes que s'han de complir per part de les Entitats de Certificació, els subscriptors i altres usuaris dels certificats emesos per la jerarquia de certificació del Consorci AOC.

D'altra banda, cada Entitat de Certificació ha de disposar d'una Declaració de Pràctiques de Certificació amb els procediments que aplica en la prestació dels seus serveis, en compliment d'allò establert a la legislació aplicable, descrita a 9.15 Conformitat amb la Llei aplicable, indicant el grau d'aplicació dels requisits establerts per les polítiques de certificats que gestiona i detallant les seves pràctiques professionals en relació amb la provisió dels serveis de certificació.

L'Entitat de Certificació arrel EC-ACC aplicarà les normes i principis de la present Política General de Certificació que acomplirà, en aquest cas, les funcions de Declaració de Pràctiques de Certificació.

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

1.3. Nom del document i identificació

Aquest document de polítiques de certificació de la jerarquia s'anomena "Política General de Certificació – Consorci AOC".

Aquesta Política General de Certificació s'identifica amb el següent OID:

```
1.3.6.1.4.1.15096.1.2.1
```

Cada política de certificat (bàsica, resultant d'una combinació de polítiques o d'una política específica de certificat d'aplicació general) rep el seu propi OID,, i que s'ha d'incloure dintre del certificat, en el camp "Informació de política" (*Policy Information*), excepte quan no resulti possible tècnicament.

Cada Entitat de Certificació Vinculada, abans de començar a emetre certificats, podrà establir la seva pròpia política de certificat pera cada tipus i classe de certificat, a partir de

l'establert en aquest document, concretant o establint noves normes de certificació, amb absolut respecte a les normes d'aquesta política.

Les polítiques específiques poden ser de dos tipus:

a) Polítiques que defineixen normes aplicables a tota la comunitat d'usuaris, amb independència de l'Entitat de Certificació que emeti el certificat, per exemple, la creació d'un tipus específic de certificat CPSQ, incloent el càrrec, política que pot ser aplicable a altres Entitats de Certificació.

b) Polítiques que defineixin o adaptin normes aplicables a una part de la comunitat d'usuaris, generalment dependent d'una Entitat de Certificació concreta, per exemple l'adaptació d'un CPSQ a les necessitats concretes d'una Entitat de Certificació, que pot no tenir sentit pera altres Entitats de Certificació.

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

a) Nivell alt: la generació, custòdia i aplicació de la clau privada s'ha de realitzar:

    a. Per als certificats personals en dispositiu qualificat de creació de signatura, d'acord amb el Reglament eIDAS..

    b. Per als certificats de dispositiu, en maquinari criptogràfic que compleix els requisits establerts a qualsevol perfil de protecció o *security targeta*, escrit d'acord amb CC EAL 3 o FIPS 140-1 o -2 nivell 2, que incorpori els requisits del CEN *Workshop Agreement* CWA14167-1 per a certificats no qualificats (reconeguts) o de conformitat amb altres esquemes de certificació (ITSEC), que incorpora els requisits de CEN *Workshop Agreement* CWA14167-1 per a certificats no qualificats (reconeguts).

b) Nivell mig: la generació, custòdia i aplicació de la clau privada pot realitzar-se en mòduls criptogràfics en programari i els algoritmes i els seus paràmetres seran els comunament utilitzats.

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

Aquest OID serà assignat pel Consorci AOC, dins la seva branca d'OIDs 1.3.6.1.4.1.15096.1.3.1. D'aquesta manera es declararà la conformitat del tipus de certificat amb aquesta política general.

1.4. Comunitat d'usuaris de certificats

Aquesta política de certificació regula una comunitat d'usuaris, que poden obtenir certificats pera diverses relacions administratives i privades, d'acord amb la Llei aplicable que es descriu a l'apartat 9.15 Conformitat amb la Llei aplicable i la normativa administrativa corresponent.

S'expedeixen, doncs, certificats a les institucions d'autogovern de Catalunya, les institucions que integren el món local i la resta d'entitats que integren el Sector Públic de Catalunya (en endavant "LES INSTITUCIONS" "); els reben i els utilitzen el seu personal, les seves entitats i els seus dispositius.

També poden expedir-se, en lliure concurrència amb altres prestadors de serveis de certificació, a persones físiques i jurídiques, incloses aquelles subjectes a una relació administrativa de subjecció especial – com la dels estudiants universitaris amb la universitat pública en la qual cursen els seus estudis superiors, o la de les empreses privades quan contracten amb l'Administració pública.

1.4.1. Prestadors de serveis de certificació

D'acord amb les lleis aplicables, que es descriu a 9.15 Conformitat amb la Llei aplicable , 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.

El Consorci AOC és el prestador de serveis de certificació públic de Catalunya.

Conforme a aquesta funció, el Consorci AOC ofereix serveis a diverses entitats de certificació d'entitats del Sector Públic de Catalunya, mitjançant sistemes tècnics d'autoritat de certificació diferenciats i vinculats a la jerarquia pública de certificació de Catalunya.I és responsable per l'actuació d'aquests sistemes davant els seus usuaris finals i davant els tercers verificadors dels certificats digitals emesos.

1.4.2. Entitat de Certificació Arrel

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

Aquesta vinculació tècnica s'aconsegueix mitjançant l'emissió de certificats CIC de nivell 1 i de nivell 2, d'acord amb l'establert en aquesta Política General de Certificació.

1.4.3. Entitats de Certificació Vinculades

Les Entitats de Certificació Vinculades són les entitats del Sector Públic de Catalunya a les quals el Consorci AOC, en qualitat de prestador de serveis de certificació, presta els serveis d'expedició i gestió dels certificats pera les seves autoritats de certificació.

Les Entitats de Certificació Vinculades es troben inscrites en la jerarquia pública de certificació de Catalunya.

Mitjançant una Entitat de Certificació Vinculada, l'entitat emet certificats a usuaris finals.

Quan una entitat del Sector Públic de Catalunya encarrega al Consorci AOC l'operació tècnica de l'entitat de certificació vinculada i dels corresponents sistemes tècnics d'autoritat de certificació, la institució roman responsable de l'organització i les decisions de gestió referides a l'entitat de certificació. Aquesta funció, que no pot ser objecte de delegació, s'anomena Entitat de Certificació Virtual.

Quan no existeixi una institució única responsable d'una comunitat d'usuaris que precisin certificats,el Consorci AOC pot crear sistemes tècnics d'autoritat de certificació de la seva pròpia titularitat, vinculats a la jerarquia pública de certificació de Catalunya.

En el cas que una entitat de certificació sigui operada directament per una entitat del Sector Públic de Catalunya, constituïda aquesta com a prestador de serveis de certificació, amb el seu propi sistema tècnic d'autoritat de certificació, aquesta entitat de certificació podrà integrar-se en el sistema públic català de certificació mitjançant la vinculació tècnica del mencionat sistema d'autoritat de certificació en la jerarquia pública de certificació de Catalunya – segons el descrit en l'apartat 1.4.2.

1.4.4. Entitats de Registre

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.

Existeixen els següents tipus d'Entitats de Registre:

1) Les Entitats de Registre Internes, operades per una institució subscriptora.
2) Les Entitats de Registre Col·laboradors, que col·laboren amb Entitats de Certificació Vinculades al procés d'emissió dels certificats.

La constitució d'una Entitat es regula mitjançant els instruments jurídics corresponents.

El Consorci AOC és responsable del procés de creació d'entitats de registre: 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 pera poder operar (típicament, seran CIPISQ);el Consorci AOC validarà les peticions de certificats pera 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 de la Declaració de Pràctiques de Certificació.

Les institucions, per a ser Entitats de Registre Internes, 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 programari i al cicle de vida dels certificats que emetin. Aquests components i procediments seran prèviament aprovats pel Consorci AOC.

1.4.5. Usuaris finals

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

a) Els sol·licitants de certificats
b) Els subscriptors o titulars de certificats
c) Els posseïdors de claus
d) Els verificadors de signatures, segells i certificats

1.4.5.1. Sol·licitants de certificats

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

Poden ser sol·licitants:

a) De certificats personals: la persona que serà el futur posseïdor de claus.

b) De certificats corporatius: una persona autoritzada a l'efecte per la futura entitat subscriptora.

c) Una persona autoritzada per l'Entitat de Certificació – típicament, el Consorci AOC actuant d'ofici.

L'autorització del sol·licitant podrà realitzar-se tant de forma expressa com tàcita; si bé, en aquells casos en els que l'entitat de certificació ho consideri convenient, es formalitzarà documentalment.

1.4.5.2. Subscriptors de certificats

Els subscriptors són les persones, físiques o jurídiques (les entitats)així identificades en el camp "Subject" del certificat.

Quan es tracta de certificats corporatius de persona física o jurídica,l'entitat subscriptora del certificat actua a través d'un posseïdor de claus, degudament autoritzat, i que figura identificat en el certificat.

El subscriptor té llicència d'ús del certificat.

1.4.5.3. Posseïdors de claus

Els posseïdors de claus són les persones físiques que posseeixen de forma exclusiva les claus de generació de signatura digital de certificats personals o, que es troben degudament autoritzades pera això pel subscriptor i que han estat degudament identificades en el certificat mitjançant el seu nom i cognoms o mitjançant un pseudònim.

1.4.5.4. Verificadors de certificats

Els verificadors són les persones (físiques o jurídiques) que reben signatures digitals, segells electrònics i certificats digitals i han de verificar-los, com a pas previ per confiar en els mateixos.

1.5. 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.

1.5.1. Usos típics dels certificats

1.5.1.1. Requisits específics per al CIC

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

- Signatura de peticions de renovació, suspensió i revocació de certificats CIC.
- Emissió i signatura de certificats d'infraestructura, personals, i de dispositiu
- Emissió i signatura de llistes de revocació de certificats (LRC).

Els CIC s'obtenen després d'un procés d'admissió de l'Entitat de Certificació Vinculada als serveis de certificació del Consorci AOC.

1.5.1.2. Requisits específics per al CIPISQ

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

1.5.1.3. Requisits específics per al CIDS

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

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

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

1.5.1.4. Requisits específics per al CIDA

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

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

1.5.1.5. Requisits específics per al ClO

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

Els certificats CIO són certificats ordinaris, que garanteixen la identitat del servidor *OCSP Responder,*de l'entitat responsable d'aquest servei, així com la integritat i l'autenticitat de les dades signades per aquest.

1.5.1.6. Requisits específics per al CIT

Els certificats d'infraestructura d'entitat de segells de temps (CIT) s'emeten a entitats responsables de l'operació de servei de segellat de temps, pera signar els segells de temps que emeten.

Els certificats CIT són certificats ordinaris que garanteixen la identitat del servidor de signatura de segells de temps, de l'entitat responsable d'aquest servei, així com la integritat i l'autenticitat de les dades signades per aquest.

1.5.1.7. Requisits específics per al CIV

Els certificats d'infraestructura d'entitat de validació (CIV) s'emeten a entitats responsables de l'operació d'un servei de validació de signatures i certificats digitals pera signar els seus informes de validació.

Els certificats CIV són certificats ordinaris que garanteixen la identitat del servei de validació, de l'entitat responsable d'aquest servei, així com garanteixen la integritat i l'autenticitat de les dades signades.

1.5.1.8. Requisits específics per al CPSQ

Els certificats personals de signatura qualificada (en endavant CPSQ) són certificats qualificats d'acord amb les lleis aplicables, que es descriuen a 9.15 Conformitat amb la Llei aplicable.

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

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

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

Els certificats CPSQ es podran emetre per al seu ús amb pseudònim, tot garantint la seguretat i l'anonimat del posseïdor de claus, havent-se d'indicar aquesta circumstància en el certificat en el camps que descrigui la seva tipologia

1.5.1.9. Requisits específics per al CPSA

Els certificats personals de signatura avançada (en endavant *CPSA*) són certificats qualificats d'acord amb el que s'estableix la legislació aplicable, que es descriu a 9.15 Conformitat amb la Llei aplicable

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

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

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

1.5.1.10. Requisits específics per al CPI

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

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

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

1.5.1.11. Requisits específics per al CDS

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

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

Els certificats CDS són certificats ordinaris i que garanteixen la identitat de la persona responsable i del servidor concret on funcionen.

Els certificats CDS-1 Seu electrònica només es poden subministrar a les administracions públiques, òrgans o entitats administratives.

1.5.1.12. Requisits específics per al CDA

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

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

Els certificats CDA-1 Segell electrònic només es poden subministrar a les administracions públiques, òrgans o entitats administratives, per a l'exercici de la competència administrativa de forma automatitzada.

1.5.2. Aplicacions prohibides

1.5.2.1. Prohibicions generals

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

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

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

1.5.2.2. Certificats d'infraestructura

1.5.2.2.1. Requisits específics per al CIC

Els certificats CIC s'atendran a allò disposat en aquesta política i, en tot cas, les limitacions estaran delimitades per la classe del certificat CIC, així com s'especifica en aquest punt i, en el seu cas, per la política de certificat concreta.

1.5.2.2.2. Requisits específics per al CIO

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

1.5.2.2.3. Requisits específics per al CIT

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

1.5.2.2.4. Requisits específics per al CIV

Els CIV no es poden utilitzar en sistemes diferents dels d'una Entitat de Validació.

1.5.2.2.5. Requisits específics per al CIDS

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

1.5.2.2.6. Requisits específics per al CIDA

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

1.5.2.2.7. Requisits específics per al CIPISQ

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

1.5.2.3. Certificats personals

1.5.2.3.1. Requisits específics per al CPSQ

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

Els CPSQ tampoc poden utilitzar-se pera signar missatges d'autenticació incomprensibles per al signatari, en particular desafiaments de client SSL o TLS, excepte quan es combinin amb un CPI, i tampoc es poden utilitzar per rebre missatges xifrats.

1.5.2.3.2. Requisits específics per al CPSA

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

Els CPSA tampoc poden utilitzar-se pera signar missatges d'autenticació incomprensibles per al signador, en particular desafiaments de client SSL o TLS, excepte quan es combinin amb un CPI, i tampoc es poden utilitzar per rebre missatges xifrats.

1.5.2.3.3. Requisits específics per al CPI

Els CPI no poden utilitzar-se pera signar peticions d'emissió, renovació, suspensió o revocació de certificats CIC, certificats de cap tipus, o llistes de revocació de certificats (LCR), i tampoc es poden utilitzar per rebre missatges xifrats.

1.5.2.4. Certificats de dispositiu

1.5.2.4.1. Requisits específics per al CDS

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

1.5.2.4.2. Requisits específics per al CDA

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

Tampoc poden utilitzar-se pera assegurar aplicacions diferents a la identificada en el certificat.

1.6. Administració de la política

1.6.1. Organització que administra l'especificació

Consorci Administració Oberta de Catalunya – Consorci AOC.

1.6.2. Dades de contacte de l'organització

Consorci Administració Oberta de Catalunya – Consorci AOC

Domicili social: Via Laietana, 26 – 08003 Barcelona

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

Web del Consorci AOC: www.aoc.cat

Web del Servei de Certificació Digital del Consorci AOC:

www.aoc.cat/Inici/SERVEIS/Signatura-electronica-i-seguretat/CATCert

Servei d'atenció a l'usuari: 902 901 080 en horari 24x7 pera la gestió de suspensions de certificats.

1.6.3. Persona que determina la conformitat d'una DPC amb la política

La persona que determina la conformitat d'una DPC amb la Política General de Certificació és el/la Responsable del Servei de Certificació Digital del Consorci AOC.

1.6.4. Procediment d'aprovació

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

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

La versió inicial de els Declaracions 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 pera aprovar les successives modificacions de les Declaracions de pràctiques.

2. Publicació d'informació i directori de certificats

2.1. Directori de certificats

El servei de directori de certificats estarà disponible durant les 24 hores dels 365 dies de l'any; i, en cas de fallada del sistema fora de control de l'Entitat de Certificació, aquesta realitzarà els seus millors esforços per a que el servei es trobi disponible de nou en el termini establert en la secció corresponent de la DPC aplicable.

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

L'Entitat de Certificació publicarà les següents informacions en el seu web:

a. Les llistes de certificats revocats i altres informacions d'estat de revocació dels certificats.

b. La política general de certificació.

c. Els perfils dels certificats.

d. La Declaració de Pràctiques de Certificació.

e. Els instruments jurídics vinculants amb subscriptors i verificadors.

Tot canvi en les especificacions o condicions del servei serà comunicat als usuaris per l'Entitat de Certificació a través del seu web i, quan sigui oportú, a través de l'adreça de correu electrònic proporcionada a l'efecte pel posseïdor de les claus.

En tots els casos es farà una referència explícita als canvis en la pàgina principal del Web del servei.No es retirarà la versió anterior del document objecte del canvi, però s'indicarà que ha estat substituït per la versió nova. Després de 15 (quinze) dies des de la publicació de la nova versió, es podrà retirar la referència al canvi de la pàgina principal.

Les versions antigues de la documentació i de les llistes de certificats revocats seran conservades per un període de 15 (quinze) anys per l'Entitat de Certificació, podent ser consultades, per causa raonada, pels interessats, sol·licitant-les a l'adreça de contacte del Consorci AOC.

2.3. Freqüència de publicació

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

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

La informació d'estat de revocació de certificats emesos per l'Entitat de Certificació es publicarà d'acord amb allò establert en les seccions corresponents d'aquesta política.

2.4. Control d'accés

L'Entitat de certificació no limita l'accés de lectura a la informació d'estat de revocació dels certificats emesos per ella.

L'Entitat de Certificació protegeix la integritat i l'autenticitat de la informació d'estat de revocació dels certificats.

També estableix controls pera mantenir la integritat del directori dels certificats expedits. Més concretament, utilitza sistemes fiables per al Directori, de manera tal que:

- Es pugui comprovar l'autenticitat dels certificats.

- Les persones no autoritzades no puguin alterar les dades.

- Els certificats solament estiguin accessibles en els supòsits o pera les persones autoritzades.

- Es pugui detectar qualsevol canvi tècnic que afecti als requisits de seguretat.

3. Identificació i autenticació

3.1. Gestió de noms

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

3.1.1. Tipus de noms

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

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

3.1.2. Significat dels noms

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

En certificats corresponents a persones jurídiques, aquesta identificació es realitzarà mitjançant la seva denominació o raó social i el seu NIF.

3.1.3. Utilització d'anònims i pseudònims

No es poden utilitzar pseudònims pera identificar una organització.

Els certificats personals, tant els individuals com els corporatius, poden indicar pseudònims en lloc del nom verdader del posseïdor de la clau del certificat.

El pseudònim constarà com a tal de manera inequívoca i s'indicarà aquesta naturalesa en la descripció del tipus de certificat.

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

Els noms dels posseïdors de claus de certificats seran únics, en l'àmbit del servei de generació de certificats prestat per una Entitat de Certificació Vinculada i pera cada tipus(perfil) de certificat.És a dir, una persona podrà tenir al seu nom certificats de perfils diferents expedits per la mateixa Entitat de Certificació Vinculada; també podrà tenir

certificats al seu nom del mateix perfil expedits per diferents Entitats de Certificació Vinculades.

No es podrà tornar a assignar el nom d'un posseïdor de claus que ja hagi sigut ocupat, a un usuari diferent.

3.1.6. Resolució de conflictes relatius a noms

En **certificats individuals**, els conflictes de noms de posseïdors de claus que apareguin identificats en els certificats amb el seu nom real se solucionen mitjançant la inclusió, en el nom diferenciat (*distinguished name*) del certificat, de:

- En cas de nacionals espanyols, el número de DNI del subscriptor.

  V.gr.: (C) = ES; (SN) = #DNI

- En cas d'estrangers amb algun tipus de vinculació amb Espanya, com pot ser la residència en territori espanyol, el número de NIE del subscriptor.

  V.gr.: francès (C) = ES; (SN) = #NIE

  V.gr.: argentí (C) = ES; (SN) = #NIE

- En cas d'estrangers nacionals d'Estats que són part de l'Acord Schengen i que no tenen NIE, el número de document nacional d'identitat del país d'origen o de procedència o passaport vigent del subscriptor. També es podrà consignar, abans del número del document identificador citat, el codi del país del que el subscriptor és nacional, de conformitat amb els paràmetres establerts per la norma ISO 3166 Codes (Countries), separat per un guió.

  V.gr.: italià (C) = IT; (SN) = #Document nacional d'identitat

  V.gr.: italià (C) = IT; (SN) = IT-#Document nacional d'identitat

- En cas d'estrangers nacionals d'Estats que no són part de l'Acord Schengen i que no tenen NIE, el número de passaport ordinari, diplomàtic, oficial o de servei, del subscriptor vàlidament expedit i en vigor. També es podrà consignar, abans del número del document identificador citat, el codi del país del que el subscriptor és nacional, de conformitat amb els paràmetres establerts per la norma ISO 3166 Codes (*Countries*), separat per un guió.

  V.gr.: xinès (C) = CN; (SN) = #Passaport

  V.gr.: xinès (C) = CN; (SN) = CN-#Passaport

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

- En cas que la "Organization" del camp "Subject" (això és, l'entitat subscriptora) estigui sotmesa a Dret espanyol:
  - En cas de nacionals espanyols, el número de DNI del posseïdor de claus.

    V.gr.: (C) = ES; (SN) = #DNI

- En cas d'estrangers, amb algun tipus de vinculació amb Espanya, com pot ser la residència en territori espanyol, el número de NIE del posseïdor de claus.

  V.gr.: francès (C) = ES; (SN) = #NIE

  V.gr.: argentí (C) = ES; (SN) = #NIE

- En cas d'estrangers nacionals d'Estats part de l'Acord Schengen i que no tenen NIE, el número de document nacional d'identitat del país d'origen o de procedència o passaport vigent del posseïdor de claus. També es podrà consignar, abans del número del document identificador citat, el codi del país del que el posseïdor de claus és nacional, de conformitat amb els paràmetres establerts per la norma ISO 3166 Codes (Countries), separat per un guió.

  V.gr.: italià (C) = ES; (SN) = #Document nacional d'identitat

  V.gr.: italià (C) = ES; (SN) = IT-#Document nacional d'identitat

- En el cas d'estrangers nacionals d'Estats que no són part de l'Acord Schengen i que no tenen NIE, el número de Passaport ordinari, diplomàtic, oficial o de servei del posseïdor de claus vàlidament expedit i en vigor. També es podrà consignar, abans del número del document identificador citat, el codi del país del que el posseïdor de claus és nacional, de conformitat amb els paràmetres establerts per la norma ISO 3166 Codes (Countries), separat per un guió.

  V.gr.: xinès (C) = ES; (SN) = #Passaport

  V.gr.: xinès (C) = ES; (SN) = CN-#Passaport

- Qualsevol altre número d'identificador assignat al posseïdor de claus pel subscriptor.

  V.gr.: un número de col·legiat.

- En cas que l'"Organizational Unit" del "Subject" (això és, l'entitat subscriptora) no estigui sotmesa a Dret espanyol, la semàntica del "SerialNumber" dependrà de la normativa aplicable conforme al "countryName" de l'Entitat.

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

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

3.2. Validació inicial de la identitat

3.2.1. Prova de control exclusiu de clau privada

S'ha de garantir, amb un alt nivell de confiança, que únicament el subscriptor de certificats individuals (o bé el posseïdor de claus de certificats corporatius) pot fer servir la clau privada (que permet la generació de signatures o el desxifrat de dades, segons el tipus de certificat de què es tracti).

Aquesta secció descriu els mètodes a utilitzar pera demostrar que es posseeixen els mitjans per fer servir per part del el subscriptor de certificats individuals (o bé el posseïdor de claus de certificats corporatius), amb un alt nivell de confiança, la clau privada corresponent a la clau pública objecte de certificació.

Aquest requisit no s'aplica quan el parell de claus és generat per l'Entitat de Registre Col·laboradora, durant el procés de generació del certificat – típicament en un dispositiu qualificat de creació de signatura que s'entregarà al posseïdor de les claus. En aquest cas, la possessió de la clau privada es demostra en virtut del procediment fiable d'entrega i acceptació del dispositiu segur i del corresponent certificat i parell de claus emmagatzemades en el seu interior.

Possessió de la clau privada

En general, el mètode de demostració de possessió de la clau privada serà l'aportació, per part del posseïdor de la clau privada, d'un fitxer de format PKCS#10, si bé el Consorci AOC pot acceptar una altra prova criptogràfica equivalent o qualsevol altre mètode aprovat per ell.

Claus privades centralitzades

Alternativament a la possessió de la clau privada, el Consorci AOC pot oferir el servei d'hostatjar les claus privades dels el subscriptor de certificats individuals (o bé el posseïdor de claus de certificats corporatius).

En aquest cas, el parell del claus es generarà a un mòdul criptogràfic que compleixi els requisits de Dispositiu Qualificat de Creació de Signatura, per a polítiques de signatura reconeguda i a un mòdul criptogràfic que compleixi els requisits d'acord amb ITSEC, Common Criteria EAL 4+ o FIPS 140-2 Nivell 3 o superior nivell de seguretat, per per a la resta de polítiques.

L'ús exclusiu es garantirà mitjançant l'ús mitjançant l'ús d' usuari i paraula de pas més un segon factor d'autenticació per a les polítiques de signatura qualificada i usuari i paraula de pas per a la resta de polítiques.

3.2.2. Autenticació de la identitat d'una organització

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

En general, l'Entitat de Certificació no haurà de determinar que un sol·licitant de certificats té dret sobre el nom que apareix en una sol·licitud de certificat. Tampoc actuarà com a àrbitre o mediador, ni de cap altra manera haurà de resoldre cap disputa relativa 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

L'Entitat de Certificació ha d'autenticar la identitat de l'organització responsable de l'Entitat de Registre, així com la dels seus operadors, junt amb altres dades establertes en la secció corresponent, amb caràcter previ a l'emissió i entrega de certificats pera qualsevol dels components d'una Entitat de Registre o per als seus operadors.

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

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

2) Comprovació de documentació justificativa aportada pel sol·licitant. En aquest cas, es requerirà la formalització de l'instrument jurídic pertinent.

3.2.2.2. Subscriptors de certificats

Quan els certificats s'expedeixen a LES INSTITUCIONS), o 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 Interna coincideixen.

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 pera certificats corporatius.

L'Entitat de Certificació podrà utilitzar Entitats de Registre pera aquesta tasca.

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

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

3.2.3. Comprovacions a realitzar en el cas de sol·licituds de certificats de dispositiu servidor segur

En el cas de sol·licituds de certificats de dispositiu,addicionalment a la comprovació que s'hagi de fer de l'organització responsable, es comprovarà:

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

3.2.4. Autenticació de la identitat d'una persona física

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

3.2.4.1. Elements d'identificació requerits

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

A. Document Nacional d'Identitat o Número d'Identificació d'estrangers o, de forma equivalent, justificant de renovació o reemissió de DNI (o NIE) més altre document acreditatiu de la identitat amb fotografia

B. Passaport

C. Qualsevol altre dels admesos en dret, sempre que contingui, almenys, la següent informació:

    a) Nom i cognoms de la persona

    b) Lloc i data de naixement

    c) Número d'identitat reconegut legalment

    d) Altres atributs de la persona que hagin de constar en el certificat

    e) Fotografia

3.2.4.2. Validació dels elements d'identificació

Quan s'expedeixen LES INSTITUCIONS, la informació d'identificació de posseïdors de claus de es validarà comparant la informació de la sol·licitud amb els registres interns de l'Entitat de Registre Interna que, coincideix amb l'organització subscriptora del certificat. Aquesta, per tant, ha d'assegurar-se de la correcció de la informació que certifica i adjunta a la sol·licitud dels certificats.

Aquesta tasca la podrà realitzar un proveïdor corporatiu d'informació de recursos humans.

Per a la resta de casos,

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

3.2.4.3. Necessitat de presència personal

La identificació de la persona física que hagi d'obtenir un certificat qualificat(això és, del posseïdor de les claus) podrà realitzar-se:

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

Abans de l'emissió i entrega d'un certificat qualificat, l'Entitat de Certificació– mitjançant la intervenció d'una Entitat de Registre–haurà de comprovar la identitat del posseïdor de claus mitjançant la personació d'aquest.

L'acte de personació pot diferir-se al moment d'entrega i acceptació del certificat, aprofitant-lo per validar llavors la identitat de la persona que serà posseïdora de la clau privada corresponent al certificat que s'entrega.

Es podrà prescindir de la personació si la sol·licitud d'expedició d'un certificat ha estat autenticada mitjançant l'ús d'un certificat electrònic de signatura qualificada classificat pel Consorci AOC, sempre que es trobi vigent i no hagin transcorregut més de cinc anys des de la identificació amb presència personal.

Es podria prescindir de la personació si la signatura continguda en la sol·licitud d'expedició d'un certificat ha estat legitimada notarialment[1] i en els casos previstos per l'article 13.4 de la Llei 59/2003, de 19 de desembre. Però aquesta política no dóna suport a aquest mecanisme per la inexistència d'un procediment a l'efecte per part dels notaris.

3.2.4.3.1. Requisits específics per als CPSQ

Abans de l'emissió i entrega d'un certificat CPSQ, l'Entitat de Certificació – mitjançant la intervenció d'una Entitat de Registre–haurà de comprovar la identitat del posseïdor de claus mitjançant la personació d'aquest.

L'acte de personació d'aquests perfils de certificats es difereix al moment d'entrega i acceptació del certificat, aprofitant-lo pera validar llavors la identitat de la persona que serà posseïdora de la clau privada corresponent al certificat que s'entrega.

Es podrà prescindir de la personació si la sol·licitud d'expedició d'un certificat ha sigut autenticada mitjançant l'ús d'un certificat electrònic de signatura qualificada classificat pel Consorci AOC, sempre que es trobi vigent i no hagin transcorregut més de cinc anys des de la identificació amb presència personal.

3.2.4.4. Vinculació de la persona física amb una organització

Quan es tracta de certificats emesos a LES INSTITUCIONS, donat que l'Entitat de Registre i el subscriptor són la mateixa entitat, no és necessari obtenir una justificació documental específica de la vinculació del posseïdor de la clau amb l'Entitat de Registre, sinó que es podrien utilitzar els registres interns de la institució. Si bé el més habitual i preferible és que s'adjunti a la sol·licitud un certificat, emès per una persona de l'entitat competent a l'efecte, que garanteixi la veracitat i exactitud de les dades consignades en la sol·licitud, referents a l'entitat subscriptora i/o als posseïdors de claus indicats.

Per a la resta de casos, l'Entitat de Certificació– 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.

3.2.5. Informació de subscriptor no verificada

No estipulat en aquest document. A concretar per cada Entitat de Certificació en la seva Declaració de Pràctiques de Certificació (DPC).

[1] Article 13.1 Llei 59/2003

3.3. Identificació i autenticació de sol·licituds de renovació

3.3.1. Validació per la renovació rutinària de certificats

Abans de renovar un certificat, l'Entitat de Certificació haurà de comprovar - mitjançant la intervenció d'una Entitat de Registre - que la informació utilitzada pera verificar la identitat i la resta de dades del subscriptor i del posseïdor de la clau continuen essent 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 corresponent.

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

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

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

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

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

3.5. Autenticació d'una petició de suspensió

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

En el cas dels certificats individuals, aquesta pregunta de desafiament la fixa el posseïdor de les claus en el moment d'entrega del certificat.

En el cas dels certificats corporatius, el codi de suspensió és generat aleatòriament per l'Autoritat de certificació i es comunica al posseïdor de les claus per escrit, en el full d'entrega del certificat que aquest rep en l'acte d'entrega i acceptació del certificat.

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

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

4.1. Sol·licitud d'emissió de certificat

Podran existir els següents tipus de sol·licituds:

1. Sol·licitud de certificat d'ofici (no conté clau pública).
2. Sol·licitud electrònica de certificat per part de l'interessat (el posseïdor de la clau, en el cas de certificats individuals o la persona designada a l'efecte per l'entitat subscriptora, en el cas de certificats corporatius) sense generació prèvia de claus (no aporta clau pública iva signada digitalment).
3. Sol·licitud electrònica de certificat per part de l'interessat(el posseïdor de la clau, en el cas de certificats individuals o la persona designada a l'efecte per l'entitat subscriptora, en el cas de certificats corporatius) amb generació prèvia de clau i aportació de prova de possessió de la corresponent clau privada (PKCS#10 o mecanisme similar, d'acord amb la secció "Prova de possessió de clau privada" de la present política).

4.1.1. Legitimació pera sol·licitar l'emissió

4.1.1.1. Requisits per a tots els tipus de certificats

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

En el cas de certificats individuals, el sol·licitant serà el propi subscriptor qui, a la seva vegada, serà també el posseïdor de les claus privades.

En el cas de certificats corporatius emesos a LES INSTITUCIONS, el sol·licitant serà la persona autoritzada a l'efecte per l'entitat subscriptora.

Per a la resta de casos, el sol·licitant i el subscriptor poden ser entitats diferents. De ser així, ha d'existir una autorització de l'Entitat de Certificació pera realitzar la sol·licitud, que s'instrumentarà jurídicament.

Per tant, podran existir els següents tipus d'autoritzacions:

- Certificats corporatius emesos a LES INSTITUCIONS: l'Entitat de Registre autoritza a personal propi,davant l'Entitat de Certificació.
- Resta: l'Entitat de Registre autoritza, davant l'Entitat de Certificació, que l'emissió de certificats la sol·liciti personal relacionat amb el subscriptor (pot ser un treballador del subscriptor, o un representant extern, o inclús una entitat diferent).

4.1.1.2. Requisits específics del CIC

La futura Entitat de Certificació no podrà sol·licitar el certificat fins que hagi completat favorablement el procediment d'admissió en la Jerarquia d'Entitats de Certificació del Consorci AOC.

4.1.1.3. Requisits pera certificats personals, d'entitat i de dispositiu

4.1.1.3.1. Requisits específics per a certificats emesos a LES INSTITUCIONS

Addicionalment a l'establert anteriorment, l'Entitat de Certificació Vinculada haurà de rebre sol·licituds de certificats, d'acord amb un dels següents casos:

1) La sol·licitud és realitzada per una persona que ha estat autoritzada per l'Entitat de Certificació Vinculada, per indicació de l'entitat subscriptora.

   En aquest cas ha d'haver un document, en suport paper o electrònic, signat per l'entitat subscriptora, que inclourà la indicació de la persona o persones a autoritzar, per part de l'Entitat de Certificació Vinculada, pera realitzar peticions. Aquesta autorització es porta a terme mitjançant la configuració dels permisos necessaris pera poder tramitar sol·licituds dels tipus de certificats indicats, en el sistema de tramitació corresponent, a favor de l'usuari/usuaris indicat/s en el document.

   Les dades de l'usuari final necessàries pera realitzar la sol·licitud podran provenir d'una base de dades de l'organització o bé ser introduïdes manualment pel sol·licitant.

2) La sol·licitud és realitzada pel futur posseïdor de claus. En aquest cas han de concórrer les següents circumstàncies:
   - Ha d'existir el document, en suport paper o electrònic, de la sol·licitud del certificat.
   - Respecte al parell de claus criptogràfiques: el sol·licitant pot generar el seu parell de claus o acordar que li siguin generades. En cas que les hagi generat ell mateix, ha d'adjuntar a la sol·licitud la clau pública perquè sigui certificada i també la prova de possessió de la corresponent clau privada.
   - El sol·licitant ha d'acceptar un acord de subscriptor, que pot tenir la forma de Condicions d'ús.

Per a sol·licitar un certificat pot fer-se servir un altre vigent, d'acord amb allò establert a la legislació aplicable, descrita a l'apartat 9.15 Conformitat amb la Llei aplicable.

4.1.1.3.2. Requisits específics per a la resta de certificats

Addicionalment a allò establert anteriorment, l'Entitat de Certificació Vinculada haurà de rebre sol·licituds de certificats, d'acord amb un dels següents casos:

1) En el cas de certificats corporatius: la sol·licitud és realitzada per una persona que ha estat autoritzada per l'Entitat de Certificació Vinculada enlloc del subscriptor.

En aquest cas ha d'haver un document, en suport paper o electrònic, signat per la futura entitat subscriptora, que inclourà la indicació de la persona o persones a autoritzar, per part de l'Entitat de Certificació Vinculada, pera realitzar peticions.

Les dades de l'usuari final necessàries pera realitzar la sol·licitud seran introduïdes pel sol·licitant.

2) En el cas de certificats individuals:la sol·licitud és realitzada pel posseïdor de claus.

   En aquest cas ha d'haver-hi un document, en suport paper o electrònic, signat per l'Entitat de Registre, que inclourà la indicació de la persona o persones a autoritzar, per part de l'Entitat de Certificació Vinculada, pera realitzar peticions.

   Les dades de l'usuari final necessàries pera realitzar la sol·licitud seran introduïdes pel sol·licitant.

3) La sol·licitud és realitzada pel futur subscriptor: en aquest cas han de concórrer les següents circumstàncies:
   - Ha d'existir el document, en suport paper o electrònic, de la sol·licitud del certificat.
   - Respecte al parell de claus criptogràfiques: el sol·licitant pot generar el seu parell de claus o acordar que li seran generades. En cas que les hagi generat ell mateix, ha d'adjuntar a la sol·licitud la clau pública per a que sigui certificada i també la prova de possessió de la corresponent clau privada.
   - El sol·licitant ha d'acceptar un acord de subscriptor, que pot tenir la forma de Condicions d'Ús.

4.1.2. Procediment d'alta; Responsabilitats

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

Abans de l'entrega del certificat, l'Entitat de Certificació Vinculada informarà al posseïdor de claus dels termes i de les condicions aplicables al certificat

En certificats d'organització,aquest requisit es complirà donant un full d'entrega al posseïdor de claus que inclogui aquesta informació.

Aquesta informació es comunicarà en suport perdurable, en paper o electrònicament i en llenguatge fàcilment comprensible.

La sol·licitud es podrà acompanyar de documentació justificativa de la identitat del subscriptor i altres circumstàncies, en cas de certificats individuals,t, d'acord amb allò establert en la secció corresponent d'aquesta política de certificats.

També es podrà acompanyar d'una direcció física, o altres dades, que permetin contactar amb el subscriptor, en cas de certificats individuals.

4.2. Processament de la sol·licitud de certificació

4.2.1. Requisits pera tots els tipus de certificats

Quan rep una petició de certificat, l'Entitat de Certificació ha de verificar la informació proporcionada, conforme a la secció corresponent d'aquesta política.

Si la informació no és correcta, l'Entitat de Certificació ha de denegar la petició. En cas contrari, l'Entitat de Certificació aprovarà la generació del certificat.

4.2.2. Requisits específics per al CIC

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

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

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

4.2.3. Requisits per als certificats personals

L'Entitat de Certificació haurà de:

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

- Protegir la integritat de les dades de registre, especialment en cas que siguin intercanviats amb el subscriptor, en cas de certificats individuals o amb el tercer sol·licitant, en el seu cas.

4.2.3.1. Requisits específics per als certificats personals

Addicionalment, l'Entitat de Certificació haurà de:

- Incloure en el certificat les informacions requerides d'acord amb allò establert en la secció 7 d'aquesta política.
- Garantir la data i l'hora en què es va expedir un certificat.
- En cas que l'Entitat de Certificació aporti el seu dispositiu qualificat de creació de signatura, utilitzar un procediment de gestió de dispositius segurs de creació de signatura que asseguri que aquest dispositiu és entregat de forma segura al posseïdor de claus.
- Utilitzar sistemes i productes fiables que estiguin protegits contra tota alteració i que garanteixin la seguretat tècnica i, en el seu cas, criptogràfica dels processos de certificació als que serveixen de suport.
- Assegurar-se que el certificat és emès per sistemes que utilitzin protecció contra falsificació i, en cas que l'Entitat de Certificació generi claus privades, que garanteixin el secret de les claus durant el procés de generació d'aquestes claus

4.2.4. Requisits per als certificats de dispositiu

L'Entitat de Certificació, o l'Entitat de Registre Col·laboradora autoritzada, abans d'aprovar una sol·licitud de certificat de dispositiu que porti adjunta la clau pública a certificar i la prova de possessió de la corresponent clau privada, ha de comprovar aquesta prova de possessió.

En cas que la comprovació de la prova de possessió de la clau privada sigui satisfactòria, es procedirà a l'emissió del certificat, conforme a allò que s'estipula a continuació.

4.3. Emissió de certificat

4.3.1. Accions de l'Entitat de Certificació durant els processos d'emissió i de renovació

Després de l'aprovació de la sol·licitud de Certificació es procedirà a l'emissió del certificat, de forma segura i es posarà el certificat a disposició del posseïdor de claus, d'acord amb allò establert en la secció corresponent.

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

L'Entitat de Certificació haurà de:

a. Utilitzar un procediment de generació de certificats que vinculi de forma segura el certificat amb la informació de registre, incloent la clau pública certificada.

b. En cas que l'Entitat de Certificació generi el parell de claus, utilitzar un procediment de generació de certificats vinculat de forma segura amb el procediment de generació de claus i entregar de forma segura la clau privada al posseïdor corresponent.

c. Protegir la integritat de les dades de registre, especialment en cas que siguin intercanviats amb el subscriptor.

Addicionalment a allò establert en la secció corresponent, l'Entitat de Certificació haurà de:

a. Incloure en el certificat les informacions requerides, d'acord amb allò establert en la secció corresponent d'aquesta política.

b. Indicar la data i l'hora en les que es va expedir un certificat.

c. En cas que l'Entitat de Certificació aporti el dispositiu qualificat de creació de signatura, utilitzar un procediment de gestió de dispositius segurs de creació de signatura que asseguri que aquest dispositiu és entregat de forma segura al posseïdor de claus.

d. Utilitzar sistemes i productes fiables que estiguin protegits contra tota alteració i que garanteixin la seguretat tècnica i, en el seu cas, criptogràfica, dels processos de certificació als que serveixen de suport.

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

4.3.2. Comunicació de l'emissió al subscriptor

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

També es comunicarà al futur posseïdor de claus que s'ha creat el certificat, es troba disponible i la forma d'obtenir-lo.

4.4. Acceptació del certificat

4.4.1. Responsabilitats de l'Entitat de Certificació

L'Entitat de Certificació haurà de:

- Si no ho ha fet abans, i quan resulti necessari, acreditar la identitat del posseïdor de claus, d'acord amb allò establert en la secció 3.2 d'aquesta política.
- Proporcionar al futur posseïdor de claus, accés al certificat.
- Quan el certificat en qüestió es trobi en un dispositiu criptogràfic de generació de signatura:
    - Entregar al posseïdor de claus aquest dispositiu
    - Entregar-li també un full d'entrega del certificat, amb els següents continguts mínims:
        - Informació bàsica sobre la política i les condicions d'ús del certificat, incloent especialment informació sobre l'Entitat de Certificació Vinculada i la Declaració de Pràctiques de Certificació aplicable, així com les seves obligacions, facultats i responsabilitats.
        - Informació sobre el certificat i el dispositiu criptogràfic.
        - Obligacions del posseïdor de claus.
        - Responsabilitat del posseïdor de claus.
        - Mètode d'imputació exclusiva al posseïdor de la clau privada, de les dades d'activació del certificat i, en el seu cas, del dispositiu

criptogràfic, d'acord amb allò establert en les seccions corresponents d'aquesta política.
        - La data de l'acte d'entrega i acceptació.
- Obtenir del posseïdor de claus l'acceptació del certificat i, en el seu cas, el reconeixement de rebre el dispositiu criptogràfic.
  Això es materialitza mitjançant la signatura, manuscrita i per part del posseïdor de claus, dels següents documents –els quals inclouen menció explícita a aquests reconeixements:
    - Quan el certificat s'entrega emmagatzemat en un dispositiu criptogràfic: el posseïdor de les claus signa un full d'entrega del certificat.
    - Quan el certificat es genera en suport software i el mecanisme d'entrega consisteix en la seva descàrrega, des d'una pàgina web, per part del posseïdor de las claus (com passa amb Els certificats idCAT, per exemple): aquest signa la sol·licitud d'emissió del certificat.

  Un exemplar d'aquests documents seran guardats durant 15 anys per l'Entitat de Certificació – mitjançant la participació de les Entitats de Registre; un altre, s'entregarà al posseïdor de claus.

4.4.2. Conducta que constitueix acceptació del certificat

El certificat es podrà acceptar mitjançant la signatura del full d'entrega o de la sol·licitud d'emissió del certificat, descrits anteriorment.

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

4.4.3. Publicació del certificat

Els certificats emesos a LES INSTITUCIONS es podran publicar en tot cas, sense el consentiment previ dels posseïdors de claus, mentre que la publicació de la resta de certificats requerirà sempre el consentiment dels subscriptors.

4.4.4. Comunicació de l'emissió a tercers

No aplicable.

4.5. Ús del parell de claus i del certificat

Els certificats han d'utilitzar-se d'acord amb la seva funció pròpia i finalitat establerta, i no han d'utilitzar-se en altres funcions i amb altres finalitats; especialment, no s'han dissenyat, no es poden destinar i no s'autoritza el seu ús pera aquelles funcions prohibides explícitament per aquesta política en l'apartat "Aplicacions prohibides".

Els certificats hauran d'utilitzar-se únicament d'acord amb la Llei aplicable.

L'extensió Key Usage s'utilitzarà per establir límits tècnics als usos que poden donar-se a una clau privada corresponent a una clau pública continguda en un certificat X.509v3. Encara que s'ha de considerar que l'efectivitat de les limitacions basades en extensions de

certificats depèn en ocasions del tractament que d'aquestes facin aplicacions informàtiques que no han estat fabricades ni poden estar controlades per les Entitats de Certificació.

4.5.1. Ús per part dels posseïdors de claus

Els usos són els següents:

Utilitzar el parell de claus exclusivament pera generar signatures electròniques i/o desxifrar informació i d'acord amb qualsevol altres limitacions que li siguin notificades.

Ser especialment diligent en la custòdia de la seva clau privada i del seu dispositiu qualificat de creació de signatura, amb la finalitat d'evitar usos no autoritzats.

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

a. Generar les seves claus utilitzant un algoritme reconegut com acceptable per a la signatura electrònica reconeguda
b. Crear les claus dins del dispositiu qualificat de creació de signatura
c. Utilitzar longituds i algoritmes de clau reconeguts com acceptables pera la signatura electrònica reconeguda

4.5.2. Ús per al tercer que confia en certificats

Els usos són els següents:

Utilitzar el certificat digital exclusivament pera validar signatures electròniques i/o xifrar informació pera un altre usuari i d'acord amb qualssevol altres limitacions que li siguin notificades.

Comprovar la validesa del certificat digital (vigència i estat) abans de confiar en aquest.

4.6. Renovació de certificats sense renovació de claus

No recomanat per les millors pràctiques del sector i no suportat per l'actual sistema de certificació implantat. No es permet la renovació de certificats sense renovació de claus.

4.7. Renovació de certificat amb renovació de claus

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

El procés pera la renovació d'un certificat és el mateix que se segueix pera l'emissió de nous certificats. Quan se sol·liciti la renovació d'un certificat, l'Entitat de Registre Interna haurà de verificar que les dades de registre continuen sent vàlides i, si ha canviat alguna dada,aquesta ha de ser verificada, s'ha de guardar evidència d'aquesta comprovació i el subscriptor ha d'estar d'acord amb la modificació, tal com s'especifica en la secció corresponent d'aquesta política.

En qualsevol cas, si han passat més de cinc anys des de la darrera vegada que el subscriptor es va identificar presencialment en una oficina d'Entitat de Registre, haurà de personar-se de nou pera portar a terme la renovació.

L'Entitat de Certificació informarà al posseïdor de claus de les condicions jurídiques de prestació del servei, tal com es fa en el procés d'emissió de nous certificats.

Pera certificats individuals en suport clauer, el subscriptor haurà de personar-se en les oficines de l'Entitat de Registre, ja que les noves claus es generaran en aquest dispositiu.

4.8. Renovació telemàtica

El Consorci AOC permet la renovació telemàtica de certificats digitals - a partir d'una autenticació segura i la corresponent signatura electrònica del full d'entrega o de la sol·licitud d'emissió del nou certificat (mitjançant la qual s'accepta aquest), realitzada amb el certificat a renovar dins dels dos darrers mesos de vigència - sempre que no hagin transcorregut més de cinc anys des de la darrera vegada que el posseïdor de claus es va identificar presencialment en una oficina d'Entitat de Registre.

4.9. Modificació de certificats

La modificació de les dades dels certificats comporta la revocació i l'emissió d'un nou certificat. A tots els efectes, la modificació es considerarà renovació.

Quan el subscriptor d'un certificat tingui coneixement de canvis en la informació obligatòria o la relativa a càrrecs, límits d'ús o dispositius usuaris dels certificats (p.ex. adreces IP o dades de servidors o aplicacions); o quan precisi la modificació de la resta de les dades incloses en el certificat (adreça de correu electrònic, etc) podrà gestionar la renovació del certificat pera introduir les modificacions necessàries, incloent la revocació del certificat vigent. En certs casos, en funció de la informació a modificar, aquesta revocació podrà fer-se en data posterior a l'emissió del certificat amb les dades actualitzades.

L'Entitat de Registre requerirà l'acreditació de les condicions justificatives de la modificació.

4.10. Revocació i suspensió de certificats

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

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

4.10.1. Causes de revocació de certificats

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

1. Circumstàncies que afecten la informació continguda en el certificat
    - Modificació d'alguna de les dades contingudes en el certificat.
    - Descobriment que alguna de les dades aportades en la sol·licitud del certificat és incorrecta, així com l'alteració o modificació de les circumstàncies verificades pera l'expedició del certificat.
    - Descobriment que alguna de les dades contingudes en el certificat és incorrecta.
2. Circumstàncies que afecten la seguretat de la clau o del certificat
    - Compromís de la clau privada o de la infraestructura o sistemes de l'Entitat de Certificació que va emetre el certificat, sempre que afecti la fiabilitat dels certificats emesos a partir d'aquest incident.
    - Infracció, per l'Entitat de Certificació, dels requisits previstos en els procediments de gestió de certificats establerts en la DPC de l'Entitat de Certificació.
    - Compromís o sospita de compromís de la seguretat de la clau o del certificat del posseïdor de claus.
    - Accés o utilització no autoritzades per un tercer de la clau privada del posseïdor de claus.
    - L'ús irregular del certificat pel posseïdor de claus, o falta de diligència en la custòdia de la clau privada.
3. Circumstàncies que afecten la seguretat del dispositiu criptogràfic
    - Compromís o sospita de compromís de la seguretat del dispositiu criptogràfic.
    - Pèrdua o inutilització per danys del dispositiu criptogràfic.
    - Accés no autoritzat per un tercer a les dades d'activació del posseïdor de claus.
4. Circumstàncies que afecten al posseïdor de claus.
    - Finalització de la relació entre l'Entitat de Certificació Vinculada iel posseïdor de claus.
    - Modificació o extinció de la relació jurídica subjacent o de la causa que va motivar l'emissió del certificat al posseïdor de claus.
    - Infracció per part del sol·licitant del certificat, dels requisits preestablerts pera la sol·licitud d'aquest.
    - Infracció, per part del posseïdor de claus, de les seves obligacions, responsabilitat i garanties, establertes en l'instrument jurídic corresponent o en la Declaració de Pràctiques de Certificació de l'Entitat de Certificació Vinculada que li va emetre el certificat.
    - La incapacitat sobrevinguda o la mort del posseïdor de claus.
    - En cas de certificats corporatius, l'extinció de la persona jurídica subscriptora del certificat, així com la finalització de l'autorització del subscriptor al posseïdor de claus, o la finalització de la relació entre el subscriptor i el posseïdor de claus.
    - Sol·licitud del subscriptor de revocació del certificat, d'acord amb allò establert en la secció 3.4 d'aquesta política.
5. Circumstàncies relatives als certificats Extended Validation:
    - Sol·licitud del subscriptor de revocació del certificat.

- L'Entitat de Certificació obté proves raonables que la clau privada del subscriptor s'ha vist compromesa o que el certificat ha estat usurpat per un tercer.
- L'Entitat de Certificació rep notificació o comunicació per part d'un tribunal o àrbitre sobre la revocació del dret a utilitzar el nom de domini que figura en el certificat o coneix la impossibilitat de renovar el domini.
- L'Entitat de Certificació té coneixement de l'incompliment de les Condicions Generals d'Ús o d'altres especificacions establertes en la documentació jurídica o operativa.
- L'Entitat de Certificació cessa activitats que donen suport a la revocació de certificats Extended Validation o perd el dret d'emetre certificats Extended Validation. Si l'Entitat de Certificació pot garantir el manteniment dels serveis de validació CRL i OCSP, la revocació no és necessària.
- Compromís o sospita de compromís de les claus de qualsevol Entitat de Certificació de nivell superior en la jerarquia.
- Revocació de les publicacions de les polítiques relatives a certificats Extended Validation.
- Notificació de la inclusió d'un subscriptor en el llistat de subscriptors prohibits (també llistes negres, confeccionades pera víctimes de phishing o activitats d'enginyeria inversa).

6. Altres circumstàncies
   - La suspensió del certificat digital per un període superior a 120 dies.
   - La finalització del servei de l'Entitat de Certificació Vinculada.
   - La finalització de la prestació de serveis per part del Consorci AOC.
   - Resolució judicial o administrativa que ho ordeni.
   - L'Entitat de Certificació Vinculada té coneixement que els certificats CDP han realitzat signatures sobre codi hostil.

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

Si l'Entitat de Certificació Vinculada no disposa de tota la informació necessària pera determinar la revocació d'un certificat, però té indicis del seu compromís, pot decidir la suspensió.

4.10.2. Legitimació pera sol·licitar la revocació

Podran sol·licitar la revocació d'un certificat:

- En cas de certificats individuals, el subscriptor a nom del qual es va emetre el certificat.
- En cas de certificats corporatius, la persona autoritzada a l'efecte per l'entitat subscriptora;en ocasions, a instància del posseïdor de claus.
- L'Entitat de Registre que va sol·licitar l'emissió del certificat.

4.10.3. Procediments de sol·licitud de revocació

La revocació d'un certificat ha de sol·licitar-se a l'Entitat de Certificació Vinculada, a través de l'Entitat de Registre que va aprovar la sol·licitud de certificació; per tant, ha d'adreçar-se a aquesta – presencialment o per mitjans electrònics.

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, que té un horari d'atenció 24x365.

La sol·licitud de revocació ha d'incloure la següent informació:

- Data de sol·licitud de la revocació
- Identitat del posseïdor de claus
- Raó detallada per a la petició de revocació
- Nom i càrrec de la persona que demana la revocació
- Informació de contacte de la persona que demana la revocació

Un cop revocats, els certificats no podran ser reactivats. La revocació no podrà aixecar-se ni anul·lar-se de cap manera; és un estat definitiu del certificat.

4.10.4. Termini temporal de sol·licitud de revocació

Les sol·licituds de revocació s'han de remetre a la major brevetat possible, quan es tingui coneixement de la causa de revocació.

Fora de l'horari d'atenció de les Entitats de Registre, el subscriptor pot sol·licitar la suspensió cautelar del certificat a través del Servei d'Atenció a l'Usuari del Consorci AOC.

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

Quan una Entitat de Registre o una Entitat de Certificació Vinculada rebin una sol·licitud de revocació, aquesta serà processada en el mínim termini possible, i sempre abans de 24 h des de la sol·licitud de la mateixa.

Abans de procedir a la revocació efectiva d'un certificat, el destinatari de la sol·licitud ha d'autenticar-la, d'acord amb els requisits establerts en la secció corresponent d'aquesta política.

Quan la sol·licitud de revocació hagi estat remesa a una Entitat de Registre, aquesta podrà, un cop autenticada la sol·licitud, revocar directament el certificat o remetre una sol·licitud en aquest sentit a l'Entitat de Certificació Vinculada.

S'haurà d'informar sobre el canvi d'estat del certificat que s'ha revocat al posseïdor de claus i també, Quan es tracti de certificats corporatius, al subscriptor.

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

Els verificadors han de comprovar l'estat dels certificats abans de confiar en ells.

Pera verificar l'estat dels certificats ha de consultar-se la llista de certificats revocats (CRL o LCR) vigent emesa per l'Entitat de Certificació que va emetre aquest certificat, o bé

consultar un servei en línia que respongui sobre l'estat de certificats (servei OCSP o altres serveis de validació de certificats) operat per un prestador de serveis de validació en el que es confia.

Les Entitats de Certificació que integren la jerarquia de certificació operada pel Consorci AOC publiquen de manera gratuïta la informació sobre l'estat dels certificats emesos per elles. Les URLs en les quals es publica aquesta informació (llistes CRL i serveis OCSP) s'indiquen entre el contingut dels certificats que emeten.

4.10.7. Freqüència d'emissió de llistes de revocació de certificats (LCRs)

4.10.7.1. Requisits específics del CIC

L'Entitat de Certificació Arrel o entitat de certificació que expedeixi certificats d'entitat de certificació haurà d'emetre una LCR immediatament després de la revocació d'una Entitat de Certificació de la jerarquia. I, en tot cas, emetrà una LCR anualment.

4.10.7.2. Requisits per als certificats personals, d'entitat i de dispositiu

L'Entitat de Certificació Vinculada haurà d'emetre una LCR almenys cada 24 hores.

En la LCR s'indicarà el moment programat d'emissió d'una nova LCR, si bé es podrà emetre una LCR abans d'aquest moment, per necessitats del servei (això és, si s'ha revocat algun certificat).

Es retiraran del contingut de la LCR les referències a certificats que hagin superat el període de validesa previst en el moment de la seva emissió.

4.10.8. Període màxim de publicació de LCRs

Un cop generades, les noves versions de les LCRs seran publicades immediatament a la web del Consorci AOC i a les URLs indicades entre el contingut dels certificats emesos.

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

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

El Consorci AOC ofereix de manera gratuïta un servei *OCSP responder* per a la comprovació en línia de l'estat dels certificats emesos (dintre del seu període de validesa o caducats) per les Entitats de Certificació que integren la jerarquia pública de certificació de Catalunya.

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

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

Els verificadors han de comprovar l'estat d'aquells certificats en els que desitgin confiar, si bé no s'estipula obligació alguna referent al mecanisme utilitzat pera la comprovació d'aquest estat.

4.10.11. Altres formes d'informació de revocació de certificats

Es podran establir altres formes pera informar sobre la revocació dels certificats, que s'hauran de detallar en la DPC de l'Entitat de Certificació Vinculada.

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

El compromís de la clau privada d'una Entitat de Certificació Vinculada serà comunicat, en la mida del possible, a tots els participants en la jerarquia pública de certificació de Catalunya, com mínim mitjançant la inclusió en la LRC corresponent de la referència al certificat digital d'aquesta Entitat de Certificació.

4.10.13. Causes de suspensió de certificats

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

- En els casos legalment previstos en l'article 9.1 de la Llei de Signatura electrònica, això és, en el cas que una resolució judicial o administrativa ho ordeni.
- Quan la documentació requerida en la sol·licitud de revocació sigui suficient, però no es pugui identificar raonablement al posseïdor de claus.
- Quan la documentació requerida en la sol·licitud de revocació no sigui suficient, tot i que es pugui identificar raonablement al posseïdor de claus.
- Quan la documentació requerida en la sol·licitud de revocació no sigui suficient i tampoc permeti identificar raonablement al posseïdor de claus.
- Quan no s'activa el certificat en un termini de 120 dies a partir de la data d'emissió del certificat.
- Si se sospita el compromís d'una clau, fins que aquest sigui confirmat. En aquest cas, l'Entitat de Certificació Vinculada ha d'assegurar-se que el certificat no està suspès durant més temps del necessari pera confirmar el seu compromís.

4.10.14. Efecte de la suspensió de certificats

Es considerarà que les actuacions realitzades durant el període de suspensió d'un certificat no són vàlides, sempre que el certificat finalment sigui revocat. Però si s'aixeca la suspensió (habilitació) i el certificat torna a passar a estat vàlid, les actuacions realitzades durant el període de suspensió del certificat es consideraran vàlides.

La suspensió és reversible en un termini màxim de 120 dies a comptar des de la data de suspensió, transcorregut el qual, si no s'ha sol·licitat la posterior habilitació, passarà automàticament a estat revocat.

Pera portar a terme l'habilitació d'un certificat suspès, el posseïdor de la clau haurà de personar-se davant l'Entitat de Registre que va aprovar la sol·licitud d'emissió d'aquest certificat i presentar el document acreditatiu de la seva identitat, per a que aquesta pugui comprovar-la.

Tot canvi d'estat d'un certificat (suspensió, habilitació, etc.) s'haurà d'informar al posseïdor de claus i també, Quan es tracti de certificats corporatius, al subscriptor.

4.10.15. Qui pot sol·licitar la suspensió

Podran sol·licitar la suspensió d'un certificat:

- En cas de certificats individuals:el posseïdor de claus o l'entitat de registre que va sol·licitar l'emissió del certificat, actuant en nom d'aquest.

- En cas de certificats corporatius: un representant autoritzat per l'entitat subscriptora, l'entitat de registre que va sol·licitar l'emissió del certificat, o el posseïdor de claus.

4.10.16. Procediment de sol·licitud de suspensió

El procediment de suspensió es pot tramitar de les maneres que es detallen a continuació:

1. La suspensió pot ser sol·licitada pel posseïdor de les claus, mitjançant trucada telefònica al Centre d'Atenció a l'Usuari del Consorci AOC.
2. Quan es tracti de certificats corporatius, la suspensió pot ser sol·licitada per l'entitat subscriptora del certificat, mitjançant trucada telefònica al Centre d'Atenció a l'Usuari del Consorci AOC.
3. La suspensió pot ser sol·licitada per l'Entitat de Registre. En cas que l'Entitat de Registre disposi d'autorització del Consorci AOC, pot realitzar ella mateixa el procés de suspensió. En cas contrari, realitza la tramitació de la suspensió a través del Consorci AOC.

Per iniciar la suspensió es requereix la següent informació:

- Data i hora de la sol·licitud de la suspensió.
- Nom i cognoms del posseïdor de claus a qui se li ha de suspendre el certificat digital.
- DNI del posseïdor de claus a qui se li ha de suspendre el certificat digital.
- Número de sèrie (*serialNumber*) del certificat digital que se sol·licita suspendre.
- Raó detallada pera la petició de suspensió.
- Codi de suspensió associat al certificat o, per defecte, pregunta i resposta secreta escollida en el moment d'activar el certificat.
- Quan es tracti de certificats corporatius:
    - Identitat del subscriptor que sol·licita la suspensió (en cas que no sigui el mateix posseïdor).
    - Informació de contacte de la Institució que demana la suspensió.
    - Organisme i departament al que està vinculat el posseïdor de claus.

Un cop suspesa la vigència d'un certificat, s'informarà al subscriptor i, en el seu cas, al posseïdor de claus, sobre el canvi d'estat de suspensió i també que el termini màxim de la mateixa serà de 120 dies.

4.10.17. Termini màxim de suspensió

El termini màxim de suspensió serà de 120 dies naturals.

4.10.18. Habilitació d'un certificat suspès

Pera habilitar el certificat que es manté suspès, el subscriptor podrà personar-se i identificar-se davant l'Entitat de Certificació Vinculada, a través de l'Entitat de Registre que va aprovar la sol·licitud del certificat i signar el corresponent document de sol·licitud d'habilitació pera deixar constància que s'ha extingit el motiu que va provocar la suspensió.

4.11. Serveis de comprovació d'estat de certificats

4.11.1. Característiques d'operació dels serveis

Les LRCs 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'Entitat de Certificació Vinculada.

4.11.2. Disponibilitat dels serveis

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

En cas de fallada dels sistemes de comprovació d'estat de certificats per causes fora del control de l'Entitat de Certificació, aquesta haurà de realitzar els seus millors esforços pera assegurar que aquest servei es manté inactiu el mínim temps possible. L'Entitat de Certificació detallarà en la seva DPC el període màxim de temps en el qual el servei haurà de tornar a operar.

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

4.11.3. Altres funcions dels serveis

Sense estipulació addicional.

4.12. Finalització de la subscripció

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

4.13. Dipòsit i recuperació de claus

4.13.1. Política i pràctiques de dipòsit i recuperació de claus

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

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

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

Sense estipulació addicional.

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

5.1. Controls de seguretat física

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

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

L'Entitat de Certificació establirà controls de seguretat física i ambiental pera protegir els recursos de les instal·lacions on es trobin els sistemes, així com els mateixos sistemes iels equipaments utilitzats pera les operacions. La política de seguretat física i ambiental aplicable als serveis de generació de certificats, de dispositius criptogràfics i de gestió de revocació establirà prescripcions pera les següents contingències:

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

5.1.1. Localització i construcció de les instal·lacions

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

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

5.1.2. Accés físic

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

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

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

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

5.1.3. Electricitat i aire condicionat

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

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

Els equipaments informàtics hauran d'estar ubicats en un entorn on es garanteixi una climatització (temperatura i humitat) adequada a les seves condicions òptimes de treball.

5.1.4. Exposició a l'aigua

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

5.1.5. Advertència i protecció d'incendis

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

En concret, els dispositius criptogràfics i suports que emmagatzemen claus de les Entitats de Certificació, hauran de comptar amb un sistema específic i addicional ala resta de la instal·lació pera la protecció davant de foc.

5.1.6. Emmagatzematge de suports

L'emmagatzematge en suports d'informació ha de realitzar-se de forma que es garanteixi tant la seva integritat, com la seva confidencialitat, d'acord amb la classificació de la informació que s'hagi establert.Haurà de comptar pera ells amb dependències o armaris ignífugues.

L'accés a aquests suports, inclús pera la seva eliminació, haurà d'estar restringit a persones específicament autoritzades.

Cal tenir en compte que les Entitats de Registre es queden amb una còpia signada pel posseïdor de claus del full d'entrega o del full de sol·licitud d'emissió de certificats. Aquesta còpia és guardada durant 15 anys per l'Entitat de Registre, aplicant-li les indicacions de la legislació catalana d'arxius, en relació amb la guarda i custòdia de documentació.

5.1.7. Tractament de residus

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

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

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

5.1.8. Còpia de seguretat fora de les instal·lacions

Periòdicament, l'Entitat de Certificació emmagatzemarà un backup dels sistemes d'informació en dependències físicament separades d'aquelles en les que es trobin els equips.

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

En el moment de realitzar una sortida d'informació de les dependències, s'hauran d'adoptar mesures adequades pera impedir qualsevol recuperació indeguda de la mencionada informació (com per exemple la utilització de carteres amb dispositius segurs de claus o combinacions o la utilització de fitxers xifrats).

5.2. Controls de procediments

Les Entitats de Certificació han de garantir que els seus sistemes s'operen de forma segura i, per això, hauran d'establir i implantar procediments pera les funcions que afecten a la provisió dels seus serveis.

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

5.2.1. Funcions fiables

Segons l'especificat en les normes ETSI EN 319 401 i CEN/TS 419261, els rols mínims establerts són:

a) Responsable de seguretat (Security Officer): Manté la responsabilitat global sobre l'administració i la implementació de les polítiques i procediments de seguretat.

b) Operador de RA (Registration Officer): Responsables d'aprovar, emetre, suspendre i revocar els certificats d'Entitat final, així com les oportunes verificacions en certificats d'autenticació web.
c) Responsable de revocació (Revocation Officers): Responsable de realitzar els canvis en l'estat d'un certificat.
d) Administradors del sistema de certificació (System Administrators): Autoritzat per realitzar canvis en la configuració del sistema, però sense accés a les dades del mateix.
e) Operadors de sistemes (System Operators): Responsables de la gestió del dia a dia del sistema (Monitoratge, backup, recovery…)
f) Auditor intern (System Auditors): Autoritzat a accedir als logs del sistema i verificar els procediments que es realitzen sobre el mateix.
g) Operador de CA - Operador de Certificació: Responsables d'activar les claus de la CA en l'entorn Online, o dels processos de signatura de certificats i CRL's en l'entorn Root Offline.

5.2.2. Nombre de persones per tasca

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

5.2.3. Identificació i autenticació pera cada funció

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

5.2.4. Rols que requereixen separació de tasques

L'Entitat de Certificació haurà d'identificar, en la seva política de seguretat, funcions o rols fiables.

Aquestes descripcions hauran de realitzar-se tenint en compte que ha d'existir una separació de funcions sensibles, així com una concessió de mínim privilegi, quan sigui possible. Pera determinar la sensibilitat de la funció, es tindran en compte els següents elements:

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

Les citades restriccions s'apliquen en tot cas:

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

5.3. Controls de personal

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

El Consorci AOC ocupa personal qualificat i amb l'experiència necessària pera la prestació dels serveis oferts, en l'àmbit de la signatura electrònica i els procediments de seguretat i de gestió adequada.

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

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

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

5.3.2. Requisits de formació

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

La formació haurà d'incloure els següents continguts:

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

5.3.3. Requisits i freqüència d'actualització formativa

Tot el personal vinculat a les ER té com a requisit imprescindible l'assistència al curs de formació d'Entitats de Registre impartit pel Consorci AOC.

5.3.4. Seqüència i freqüència de rotació laboral

Sense estipulació addicional.

5.3.5. Sancions per accions no autoritzades

L'Entitat de Certificació haurà de disposar d'un sistema sancionador pera depurar les responsabilitats derivades d'accions no autoritzades.

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

5.3.6. Requisits de contractació de professionals

L'Entitat de Certificació podrà contractar professionals pera qualsevol funció, inclús pera un lloc fiable, cas en el que s'haurà de sotmetre als mateixos controls que els empleats restants.

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

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

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

5.3.7. Subministrament de documentació al personal

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

5.4. Procediments d'auditoria de seguretat

5.4.1. Tipus d'esdeveniments registrats

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

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

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

- La cerimònia de generació de claus i les bases de dades de gestió de claus
- Registres d'accés físic
- Manteniments i canvis de configuració del sistema
- Canvis en el personal
- Informes de compromís y discrepàncies

- Registres de la destrucció de material que contingui informació de claus, dades d'activació o d'informació personal del subscriptor, en cas de certificats individuals, o del posseïdor de claus
- Possessió de dades d'activació, pera operacions amb la clau privada de l'Entitat de Certificació
- Informes complets dels intents d'intrusió física en les infraestructures que donen suport a l'emissió i gestió de certificats.

5.4.2. Freqüència de tractament de registres d'auditoria

Els registres d'auditoria s'examinaran al menys un cop per setmana en cerca d'activitat sospitosa o no habitual.

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

5.4.3. Període de conservació de registres d'auditoria

Els registres d'auditoria es retenen durant al menys dos mesos després de processar-los i a partir d'aquest moment s'arxiven d'acord amb la secció corresponent d'aquesta política.

5.4.4. Protecció dels registres d'auditoria

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

5.4.5. Procediments de backup

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

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

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

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

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

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

5.4.8. Anàlisi de vulnerabilitats

Els esdeveniments en el procés d'auditoria hauran de ser guardats, en part, pera monitoritzar les vulnerabilitats del sistema.

Es realitzen anàlisis de vulnerabilitats internes com a mínim trimestralment i externes al menys anualment.

5.5. Arxiu d'informacions

L'Entitat de Certificació ha de garantir que tota la informació relativa als certificats es guarda durant un període de temps apropiat, segons allò establert en la secció corresponent d'aquesta política.

5.5.1. Tipus d'esdeveniments registrats

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

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

- Tipus de document presentat en la sol·licitud del certificat
- Número d'identificació únic proporcionat pel document anterior
- Identitat de l'Entitat de Registre que accepta la sol·licitud de certificat
- La ubicació de les còpies de sol·licituds de certificats i de l'Acord signat pel subscriptor,en cas de certificats individuals.

5.5.2. Període de conservació de registres

5.5.2.1. Requisits pera tots els tipus de certificats

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

5.5.2.2. Requisits específics per als certificats qualificats certificats reconeguts

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

5.5.2.3. Requisits per als certificats CIC

per als certificats CIC els registres es guardaran indefinidament.

5.5.3. Protecció de l'arxiu

L'Entitat de Certificació ha de:

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

5.5.4. Procediments de còpia de suport

5.5.4.1. Requisits pera tots els tipus de certificats

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

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

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

5.5.5. Requisits de segellat de data i d'hora

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

5.5.6. Localització del sistema d'arxiu

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

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

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

5.6. Renovació de claus

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

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

Els certificats CIC renovats es comunicaran als usuaris finals mitjançantla seva publicació en el Registre del Consorci AOC.

5.7. Compromís de claus i recuperació de desastre

5.7.1. Procediment de gestió d'incidències i compromís

L'Entitat de Certificació establirà en la seva DPC 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'Entitat de Certificació ha d'iniciar les gestions necessàries, segons el Pla de Recuperació Desastres del Consorci AOC, 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'Entitat de Certificació (o pla de recuperació de desastres) ha de considerar el compromís o la sospita de compromís de la clau privada de l'Entitat de Certificació com un desastre.

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

- Informar a tots els subscriptors i verificadors del compromís.

- Indicar que els certificats i la informació de l'estat de revocació entregats usant la clau d'aquesta Entitat de Certificació ja no són vàlids.
- Revocar, en el termini que es pacti amb el supervisor nacional, els certificats emesos per aquesta CA, aplicant, si escau, algun dels procediments previstos en el Pla de Cessament o en el Pla de Continuïtat.

5.7.4. Desastre sobre les instal·lacions

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

L'Entitat de Certificació ha de ser capaç de restaurar l'operació normal de la PKI en les 24 hores següents al desastre, podent, 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'Entitat de Certificació ha d'estar sincronitzada amb la base de dades de producció, dintre dels límits temporals especificats en el Pla de Seguretat. Els equips de recuperació de desastres de l'Entitat de Certificació han de tenir les mesures de seguretat físiques especificades en el Pla de Seguretat.

5.8. Finalització del servei

5.8.1. Entitat de Certificació

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

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

- Informar a tots els subscriptors i verificadors (no es requereix que l'Entitat de Certificació tingui alguna relació anterior amb terceres parts).
- Finalitzar tota autorització de subcontractacions que actuïn en nom de l'Entitat de Certificació en el procés d'emissió de certificats.
- Executar les tasques necessàries pera transferir les obligacions de manteniment de la informació de registre i els arxius de registre d'esdeveniments durant els períodes de temps respectius indicats al subscriptor i als verificadors.
- Destruir les claus privades de l'Entitat de Certificació o retirar-les del'ús.

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

- Notificació a les entitats afectades
- Transferència de les obligacions de l'Entitat de Certificació a altres persones
- Com es tractarà l'estat de revocació dels certificats emesos que encara no hagin expirat
- L'Entitat de Certificació podrà transferir els certificats, en els termes previstos en la legislació aplicable.

5.8.2. Entitat de Registre

Sense estipulació addicional.

6. Controls de seguretat tècnica

L'Entitat de Certificació haurà d'utilitzar sistemes i productes fiables que estiguin protegits contra tota alteració i que garanteixin la seguretat tècnica i criptogràfica dels processos de certificació als 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 pera 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. Requisits específics per al CIC

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

6.1.1.3. Requisits específics per als certificats de xifrat

Les claus dels certificats de xifrat seran creades per l'Entitat de Registre i, en el seu cas, emmagatzemades pera la seva posterior recuperació.

6.1.2. Enviament de la clau privada al subscriptor

Per als certificats de signatura qualificada i els certificats de nivell alt, la clau privada haurà de ser entregada al posseïdor de claus, degudament protegida mitjançant una targeta intel·ligent que compleixi l'establert en un perfil de protecció de dispositiu qualificat de creació de signatura electrònica. o emmagatzemada segons els termes de la secció 3.2.1 de la present política i s'haurà de lliurar al posseïdor de claus els mecanismes d'accés a la mateixa.

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

Quan el parell de claus hagi estat generat pel posseïdor de claus, el mètode d'enviament de la clau pública a l'Entitat de Certificació serà mitjançant un fitxer PKCS#10, o mitjançant una altra prova criptogràfica equivalent o qualsevol altre mètode aprovat pel Consorci AOC a l'efecte.

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

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

La clau pública de l'entitat de certificació arrel (*root CA)* de la jerarquia de certificació del Consorci AOC es publicarà al directori de dita Entitat de Certificació, en forma de certificat autosignat, junt amb una declaració referent al fet que la clau permet autenticar l'Entitat de Certificació.

S'hauran d'establir mesures addicionals pera confiar en el certificat autosignat, com ara la comprovació de l'empremta digital del certificat.

Les claus públiques de les Entitats de Certificació Vinculades es publicaran en el web del Consorci AOC, en forma de certificat CIC signat per l'entitat de certificació superior en la jerarquia de certificació del Consorci AOC. També es publiquen, amb el mateix format, en el directori de cada Entitat de Certificació.

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

6.1.5. Mesures de claus

El Consorci AOC gestiona de manera diligent la jerarquia pública de certificació, esforçant-se per mantenir-la conforme a les novetats que s'introdueixin en les especificacions tècniques aplicables.

Concretament, en relació a les mesures de les claus de les Entitats de Certificació Vinculades seran, almenys, de 2.048 bits.

Les claus de tots els certificats emesos per les Entitats de Certificació Vinculades són de 2.048 bits.

6.1.6. Generació de paràmetres de clau pública

Sense estipulació addicional.

6.1.7. Comprovació de qualitat de paràmetres de clau pública

Es realitzarà d'acord els requisits i recomanacions de la normativa que indiqui la qualitat dels algoritmes de signatura electrònica.

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

El parell de claus de les Entitats de Certificació (tant del Consorci AOC, com de les Entitats de Certificació Vinculades) hauran d'estar generades utilitzant mòdul criptogràfic que compleixi els requisits establerts en un perfil de protecció de protecció, d'acord amb ITSEC, Common Criteria EAL 4+o FIPS 140-2 Nivell 3 o superior nivell de seguretat.

El parell de claus dels subscriptors de certificats de signatura i de certificats de nivell alt hauran de generar-se en targetes intel·ligents o en dispositius criptogràfics que compleixin els requisits establerts en un perfil de protecció de dispositiu qualificat de creació de signatura electrònica.

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

6.1.9. Propòsits d'ús de claus

L'Entitat de Certificació haurà d'incloure 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 de mòduls criptogràfics

Les claus privades de les Entitats de Certificació (tant del Consorci AOC com de les Entitats de Certificació Vinculades) hauran de protegir-se utilitzant *mòdul* criptogràfic que compleixi els requisits establerts en un perfil de protecció t, d'acord amb Common Criteria EAL 4+ o FIPS 140-2 Nivell 3 o superior nivell de seguretat.

Els parells de claus dels subscriptors de certificats de signatura qualificada i de certificats de nivell alt seran protegits mitjançant targetes intel·ligents o en dispositius criptogràfics que compleixin els requisits establerts en un perfil de protecció de dispositiu qualificat de creació de signatura electrònica.

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

6.2.1.2. Cicle de vida de les targetes amb circuit integrat

Les targetes amb circuit integrat (també targetes intel·ligents) s'entreguen en cada emissió de nou certificat per l'Entitat de Registre Col·laboradora o Interna, o bé directament pel Consorci AOC quan actua com a Entitat de Registre Virtual.

Per cada nova emissió o renovació dels certificats s'entrega una targeta nova, és a dir, no es carreguen certificats en targetes usades.

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

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

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

Cadascun d'aquests dispositius és responsabilitat d'una persona concreta, única coneixedora de la clau d'activació del mateix. La clau d'activació serà coneguda únicament per la persona responsable d'aquest dispositiu;cap d'elles coneixerà més que una de les claus d'accés. També es diposita davant Notari un sobre tancat en què el responsable de cada dispositiu ha escrit la clau d'activació del dispositiu del qual és responsable. Aquests sobres només poden ser retirats de la custòdia del Notari pel propi responsable o per altra persona degudament autoritzada per aquest (presentant autorització signada per ell).

Els dispositius criptogràfics quedaran emmagatzemats en les dependències de l'Entitat de Certificació Vinculada.

6.2.3. Dipòsit de la clau privada

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

6.2.4. Backup de la clau privada

Haurà d'existir backup en dependència independent d'aquella on s'emmagatzema habitualment, de la clau privada de l'Entitat de Certificació Vinculada, així com dels mitjans necessaris pera accedir a ella.

6.2.5. Arxiu de la clau privada

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

Hauran de mantenir-se i utilitzar-se protegides per un dispositiu criptogràfic que compleixi els requisits establerts en un perfil de protecció t, d'acord amb Common Criteria EAL 4+, o FIPS 140-2 Nivell 3 o superior nivell de seguretat.

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

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

Quan les claus s'emmagatzemin en un mòdul criptogràfic de procés dedicat, hauran de proveir-se els controls oportuns per a que aquestes mai puguin abandonar el dispositiu.

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

6.2.6. Introducció de la clau privada en el mòdul criptogràfic

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

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

6.2.7. Emmagatzematge de la clau privada en el mòdul criptogràfic

Les claus privades es generaran directament en els mòduls criptogràfics.

6.2.8. Mètode d'activació de la clau privada

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

Per a certificats personals, la clau privada del subscriptor s'activarà mitjançant la introducció del PIN en la targeta intel·ligent o de les dades d'activació exigides per al dispositiu criptogràfic o sistema d'emmagatzematge.

6.2.9. Mètode de desactivació de la clau privada

Per a certificats personals que incloguin la política bàsica de signatura qualificada (CPSQ) , quan la targeta intel·ligent es retiri del dispositiu lector, o l'aplicació que la utilitzi finalitzi la sessió, serà necessari introduir novament les dades d'activació anteriorment indicades.

Per a certificats personals que incloguin la política bàsica de signatura avançada (CPSA), quan l'aplicació que utilitzi el certificat finalitzi la sessió, serà necessari introduir novament les dades d'activació de signatura (PIN).

6.2.10. Mètode de destrucció de la clau privada

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

6.2.11. Classificació dels mòduls criptogràfics

Els mòduls de l'Entitat de Certificació Vinculada han de trobar-se certificats amb el nivell i els augments previstos en un perfil de protecció , d'acord amb Common Criteria EAL 4+, o FIPS 140-2 Nivell 3.

Els mòduls dels subscriptors de certificats de signatura electrònica reconeguda i de certificats de nivell alt han de trobar-se certificats amb el nivell i augments previstos en un perfil de protecció de dispositiu qualificat de creació de signatura electrònica..

6.3. Altres aspectes de gestió del parell de claus

6.3.1. Arxiu de la clau pública

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

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

Els períodes d'utilització de les claus seran els determinats per la durada del certificat i un cop transcorregut no es podran continuar utilitzant.

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

6.4. Dades d'activació

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

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

6.4.2. Protecció de dades d'activació

Si l'Entitat de Certificació facilita al subscriptor un dispositiu qualificat de creació de signatura, les dades d'activació del dispositiu hauran de ser distribuïdes separadament del dispositiu de creació de signatura (per exemple, entregant-se en moments diferents, o per rutes o canals diferents).

Com a excepció, quan el posseïdor de claus rebi presencialment un dispositiu d'una Entitat de Registre, podrà seleccionar i introduir les dades d'activació, de forma que els conegui únicament ell.

6.4.3. Altres aspectes de les dades d'activació

Sense estipulació.

6.5. Controls de seguretat informàtica

6.5.1. Requisits tècnics específics de seguretat informàtica

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

- L'Entitat de Certificació ha de garantir una administració efectiva del nivell d'accés dels usuaris (operadors, administradors, així com de qualsevol usuari amb accés directe al sistema) pera mantenir la seguretat del sistema, incloent la gestió de comptes d'usuari, auditoria i modificacions o denegacions d'accés oportunes.
- L'Entitat de Certificació ha de garantir que l'accés als sistemes d'informació i aplicacions es restringeix d'acord amb allò establert en la política de control d'accés, així com que els sistemes proporcionen els controls de seguretat suficients pera

implementar la segregació de funcions identificada en les pràctiques de l'Entitat, incloent la separació de funcions d'administració dels sistemes de seguretat i dels operadors. En concret, l'ús de programes d'utilitats del sistema estarà restringit i estretament controlat.

- El personal de l'Entitat haurà d'estar identificat i reconegut abans d'utilitzar aplicacions crítiques relacionades amb el cicle de vida del certificat.
- El personal de l'Entitat serà responsable i haurà de poder justificar les seves activitats, per exemple mitjançant un arxiu d'esdeveniments.
- Haurà d'evitar-se la possibilitat de revelació de dades sensibles mitjançant la reutilització d'objectes d'emmagatzematge (per exemple fitxers esborrats) que queden accessibles a usuaris no autoritzats.
- Els sistemes de seguretat i monitorització han de permetre una ràpida detecció, registre i actuació davant intents irregulars d'accés o no autoritzats als seus recursos (per exemple, mitjançant un sistema de detecció d'intrusions, monitorització i alarma).
- L'accés als dipòsits públics de la informació de l'Entitat (per exemple, certificats o informació d'estat de revocació) haurà de comptar amb un control d'accés pera modificacions o esborrat de dades.

6.5.2. Evaluació del nivell de seguretat informàtica

Els sistemes hauran de ser fiables, d'acord amb la norma EN 319 411-2.

6.6. Controls tècnics del cicle de vida

6.6.1. Controls de desenvolupament de sistemes

S'haurà de realitzar una anàlisi de requisits de seguretat durant les fases de dissenyi especificació de requisits de qualsevol component utilitzada en les aplicacions d'Autoritat (tècnica) de certificació i d'Autoritat (tècnica) de Registre, pera garantir que els sistemes són segurs.

S'utilitzaran procediments de control de canvis pera les noves versions, actualitzacions i pedaços d'emergència, d'aquests components.

6.6.2. Controls de gestió de seguretat

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

La configuració dels sistemes s'auditarà de forma periòdica, d'acord amb allò establert en la secció corresponent d'aquesta política.

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

6.6.3. Avaluació del nivell de seguretat del cicle de vida

Sense estipulació.

6.7. Controls de seguretat de xarxa

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

- Han d'implementar-se controls (com per exemple,tallafocs) pera protegir la xarxa interna de dominis externs accessibles per terceres parts. Els talla focs hauran de configurar-se de forma que s'impedeixin accessos i protocols que no siguin necessaris pera l'operació de l'Entitat de Certificació.
- Les dades sensibles hauran de protegir-se quan s'intercanvien a través de xarxes no segures (incloent les dades de registre del subscriptor).
- S'ha de garantir que els components locals de xarxa (com direccionadors) es trobin ubicats en entorns segurs, així com l'auditoria periòdica de les seves configuracions.

6.8. Segell de temps

Sense estipulació addicional.

7. Perfils de certificats i llistes de certificats revocats

7.1. Perfil de certificat

Els certificats emesos pel Consorci AOC i les Entitats de Certificació adscrites a la jerarquia pública de certificació de Catalunya tindran el contingut i els camps descrits en el document "perfil de certificat" corresponent, que el Consorci AOC publica en el seu web.

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

a. Número de sèrie, que serà un codi únic respecte al nom distingit de l'emissor
b. Algoritme de signatura, amb algun dels algoritmes identificats en la secció corresponent d'aquesta política
c. El nom distingit de l'emissor, d'acord amb la secció corresponent d'aquesta política
d. Inici de validesa del certificat, en Temps Coordinat Universal, codificat conforme a l'RFC 6818
e. Fi de validesa del certificat, en Temps Coordinat Universal, codificat conforme a l'RFC 6818
f. Nom distingit del subjecte, d'acord amb la secció corresponent d'aquesta política
g. Clau pública del subjecte, codificada d'acord amb l'RFC 6818
h. Signatura generada i codificada, d'acord amb l'RFC 6818

Els certificats seran conformes amb les següents normes:

1. RFC 6818: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008
2. ITU-T Recommendation X.509 (1997): Information Technology – Open Systems Interconnection - The Directory: Authentication Framework, June 1997
3. L'especificació "*Perfiles de Certificados Electrónicos*" elaborada per la *Dirección de Tecnologías de la Información y las Comunicaciones* (DTIC) del *Ministerio de Hacienda y Administraciones Públicas* (MINHAP)

Addicionalment, els certificats de signatura qualificada seran conformes amb les següents normes:

1. ETSI EN 319 412, parts 1, 2 i 5, a la seva versió vigent en el moment de la publicació d'aquesta política.
2. L'especificació "*Perfiles de Certificados Electrónicos*" elaborada per la *Dirección de Tecnologías de la Información y las Comunicaciones* (DTIC) del *Ministerio de Hacienda y Administraciones Públicas* (MINHAP)
3. RFC 3739: Internet X.509 Public Key Infrastructure – Qualified Certificate Profile, 2001 (sempre que no entri en conflicte amb les anteriors TS 101 862)

Així mateix,els certificats qualificats hauran de contenir els següents camps:

a. La indicació que s'expedeixen com a certificats qualificats
b. El codi identificatiu únic del certificat

c. La identificació del prestador de serveis de certificació que expedeix el certificat, indicant el nom o raó social, domicili, direcció electrònica i número d'identificació fiscal

d. La signatura electrònica avançada del prestador de serveis de certificació que expedeix el certificat

e. La identificació del signant (el subscriptor, en cas de certificats individuals, o del posseïdor de claus, en cas de certificats d'organització), pel seu nom i cognoms i DNI o equivalent, o a través d'un pseudònim que consti de manera inequívoca

f. Les dades de verificació de signatura que corresponguin a les dades de creació de signatura que es trobin sota el control del signant

g. L'inici i el final del període de validesa del certificat

h. Els límits d'ús del certificat, si es preveuen

i. Els límits del valor de les transaccions pera les quals pot utilitzar-se el certificat, si s'estableixen

7.1.1. Número de versió

Tots els certificats contindran un camp amb el número de versió, indicant que es tracta de certificats de versió 3.

7.1.2. Extensions de certificat

Les extensions de cada certificat, així com el seu significat semàntic,es troba descrit en el document "perfil de certificat" corresponent, que el Consorci AOC publica en el seu web.

7.1.3. Identificadors d'objecte d'algoritmes

L'Entitat de Certificació podrà utilitzar el següent algoritme de signatura:

- sha256WithRSAEncryption OID = {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}

7.1.4. Formats de noms

L'Entitat de Certificació emplenarà els camps de noms dels certificats amb les informacions establertes en el perfil corresponent de certificat, publicat en el web.

7.1.5. Restriccions de noms

Sense estipulació.

7.1.6. Identificador d'objecte de política de certificat

L'Entitat de Certificació emplenarà l'extensió política de certificat amb els identificadors d'objecte establerts en la secció corresponent d'aquesta política, quan s'adhereixen directament a ella mateixa.

En cas de crear la seva pròpia política, en els casos permesos per aquesta política de certificats, inclourà l'identificador d'objecte específicament definit a l'efecte.

7.1.7. Ús de l'extensió restriccions de política

Sense estipulació addicional.

7.1.8. Sintaxi i semàntica dels qualificadors de política

L'Entitat de certificació inclourà en els certificats un qualificador de política, amb els següents elements:

- CPS Pointer
- Explicit Text

CPS Pointer haurà d'incloure una referència URI a les condicions generals de verificació dels certificats emesos per l'Entitat de Certificació.

Explicit Text haurà de contenir una declaració concisa relativa al certificat.

7.1.9. Semàntica del procés de l'extensió crítica de la política de certificat

Sense estipulació addicional.

7.1.10. Especificacions tècniques pera totes les Entitats de Certificació

Les Entitats de Certificació han de respectar els usos tecnològics generalment acceptats i han d'adaptar-se a les bones pràctiques i als requisits tècnics més avançats.

Addicionalment, la renovació de les Entitats de Certificació immediatament posterior a la present versió de la Política General respectarà les següents especificacions tècniques:

- L'algoritme utilitzat ha de ser renovat quan existeixi un risc de desencriptació advertit per la comunitat. Les Entitats de Certificació incorporaran, posteriorment a l'emissió d'aquesta Política General, l'algoritme SHA-256
- Els números de sèrie dels certificats sempre seran enters i, en tot cas, positius
- S'utilitzarà la codificació UTF-8
- Se simplificarà l'extensió "authorityKeyIdentifier"
- Es restringiran els *OIDs* generats per les entitats de certificació intermèdies

8. Auditoria de conformitat

L'Entitat de Certificació Vinculada ha de realitzar periòdicament una auditoria de conformitat pera provar que compleix, un cop ha començat a funcionar, els requisits de seguretat i d'operació necessaris pera formar part de la jerarquia pública de certificació de Catalunya.

Amés de l'auditoria de conformitat, l'Entitat de Certificació Vinculada ha d'estar preparada pera passar altres revisions, no periòdiques, que demostrin la seva confiança:

- Abans d'acceptar una nova Entitat de Certificació subordinada a la jerarquia, el Consorci AOC ha de realitzar una revisió dels seus documents de seguretat i DPC i PdC per a assegurar que compleix els requisits de seguretat i d'operació necessaris pera formar part de la Jerarquia d'Entitats de Certificació del Consorci AOC.

- Si en qualsevol moment se sospita que l'Entitat de Certificació Vinculada, un cop ha començat a funcionar, no compleix algun dels requisits de seguretat, o si s'ha detectat un compromís de claus -ja sigui una sospita o compromís real - o qualsevol esdeveniment que pugui suposar un perill pera la seguretat o integritat de l'Entitat de Certificació Vinculada, es portarà a terme una auditoria interna.

L'Entitat de Certificació Vinculada pot delegar l'execució de les auditories a una tercera entitat, i ha de cooperar completament amb el personal que porti a terme la investigació.

8.1. Freqüència de l'auditoria de conformitat

L'Entitat de Certificació Vinculada ha de portar a terme una auditoria de conformitat anualment, amés de les auditories internes que puguin portar a terme sota el seu propi criteri o en qualsevol moment, a causa d'una sospita d'incompliment d'alguna mesura de seguretat o per un compromís de claus.

8.2. Identificació i qualificació de l'auditor

Si l'Entitat de Certificació Vinculada disposa d'un departament d'auditoria interna, aquest podrà encarregar-se de portar a terme l'auditoria de conformitat.

En el cas de no posseir aquest departament, l'Entitat de Certificació Vinculada podrà recórrer a un auditor independent extern, el qual ha de demostrar experiència en seguretat informàtica, en seguretat de Sistemes d'Informació i en auditories de conformitat d'Autoritats de certificació i els elements relacionats.

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

Les auditories de conformitat executades per tercers han de ser portades a terme per una entitat independent de l'Entitat de Certificació Vinculada auditada. En cas d'auditoria interna, l'auditor no ha de tenir cap conflicte d'interessos que afecti negativament a la seva capacitat de portar a terme serveis d'auditoria.

8.4. Relació d'elements objecte d'auditoria

Els elements objecte d'auditoria seran els següents:

- Procés d'Autoritats de certificació i elements relacionats
- Sistemes d'informació
- Protecció del centre de procés
- Documents

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

Un cop s'obté l'informe de l'auditoria de compliment portada a terme, l'Entitat de Certificació Vinculada ha de discutir amb l'entitat que ha executat l'auditoria i amb el Consorci AOC, les deficiències trobades i desenvolupar i executar un pla correctiu que solucioni aquestes deficiències.

Si l'Entitat de Certificació Vinculada auditada és incapaç de desenvolupar i/o executar aquest pla o si les deficiències trobades suposen una amenaça immediata pera la seguretat o la integritat del sistema, haurà de realitzar-se una de les següents accions:

- Revocar la clau de l'Entitat de Certificació Vinculada, de la manera com es descriu en les seccions corresponents d'aquesta política.
- Acabar el servei de l'Entitat de Certificació Vinculada, de la manera com es descriu en la secció corresponent d'aquesta política.

8.6. Tractament dels informes d'auditoria

Els informes de resultats de les auditories seran entregats al Consorci AOC en un termini màxim de 15 dies després de l'execució de l'auditoria, en tant que és el Prestador de Serveis de Certificació.

9. Requisits comercials i legals

9.1. Tarifes

9.1.1. Tarifa d'emissió o renovació de certificats

El Consorci AOC establirà les tarifes que aplicaran totes les Entitats de Certificació Vinculades a la prestació dels seus serveis.

Aquestes tarifes poden trobar-se en la web del Consorci AOC.

9.1.2. Tarifa d'accés a certificats

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

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

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

9.1.4. Tarifes d'altres serveis

Sense estipulació addicional.

9.1.5. Política de reintegrament

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

9.2. Capacitat financera

9.2.1. Assegurança de responsabilitat civil

El Consorci AOC, com aprestador de serveis de certificació, disposa d'una garantia suficient de cobertura de la seva responsabilitat civil, en els termes previstos a l'article 20.2 de la Llei 59/2003, de 19 de desembre, excepte quan es trobi eximida per Llei d'aquesta obligació.

En cas d'ús incorrecte o no autoritzat dels certificats, el Consorci AOC (o l'Entitat de Certificació Vinculada corresponent) 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'Entitat de Certificació Vinculada corresponent).

9.2.2. Altres actius

Sense estipulació addicional.

9.2.3. Cobertura d'assegurament pera subscriptors i tercers que confien en certificats

Sense estipulació addicional.

9.3. Confidencialitat

9.3.1. Informacions confidencials

Les següents informacions seran mantingudes com a confidencials per l'Entitat de Certificació:

a. Informació de negoci subministrada pels seus proveïdors i altres persones amb les quals el Consorci AOC o l'Entitat de Certificació Vinculada tingui una obligació de guardar secret, establerta legal o convencionalment
b. Registres de transaccions, incloent els registres complets i els registres d'auditoria de les transaccions
c. Registres d'auditoria interna i externa, creats i/o mantinguts per l'Entitat de Certificació Vinculada i els seus auditors
d. Plans de continuïtat de negoci i d'emergència
e. Política i plans de seguretat
f. Documentació d'operacions i restants plans d'operació, com ara arxiu, monitorització i altres d'anàlogues
g. Tota altra informació identificada com a "Confidencial"

9.3.2. Informacions no confidencials

Les següents informacions no tindran caràcter confidencial:

a. Les Declaracions de Pràctiques de Certificació de totes les Entitats de Certificació
b. Tota altra informació identificada com a "Pública"

9.3.3. Responsabilitat pera la protecció d'informació confidencial

L'Entitat de Certificació Vinculada serà responsable de l'establiment de les mesures apropiades de protecció de la informació confidencial.

Aquestes mesures inclouran les apropiades clàusules d'informació confidencials en els instruments jurídics amb totes les persones.

9.4. Protecció de dades personals

9.4.1. Política de Protecció de Dades Personals

El Consorci AOC desenvolupa una política de protecció de dades personals, d'acord amb la Llei Orgànica 15/1999, de 13 de desembre, de Protecció de Dades de Caràcter Personal (LOPD) i la normativa reglamentària d'aplicació en matèria de protecció de dades de caràcter personal.

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

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

SUBSCRIPTORS DE CERTIFICATS:

- Dades identificatives del col·lectiu subscriptor: nom de l'entitat o de l'organisme que sol·licita els certificats, NIF, Adreça postal completa, Adreça electrònica, pàgina web.

- Dades identificatives de la persona que assumeix el rol de responsable del servei: nom, cognoms, DNI o equivalent, telèfon, fax, adreça postal, adreça electrònica.

PERSONES FÍSIQUES CERTIFICADES:

- Dades identificatives: nom, cognoms i DNI, o equivalent, de la persona física certificada. Opcionalment, altres dades personals, la inclusió de les quals sigui sol·licitada perla persona autoritzada, com el codi CIP de la Targeta Individual Sanitària, així com el codi identificatiu o usuari en el cas de certificats amb pseudònim.

- Dades de contacte: adreça postal completa a efectes de notificacions, així com l'adreça electrònica.

- Dades de l'entitat a la que presten els seus serveis .

- Denominació de l'entitat,NIF, àrea d'adscripció política, orgànica, laboral o professional.

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

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

El Consorci AOC estableix les mesures de seguretat de caràcter tècnic i organitzatiu necessàries pera donar compliment a les mesures de seguretat aplicables a fitxers automatitzats del RLOPD. Amb caràcter merament informatiu,es detallen a continuació les mesures aplicades, el precepte del RLOPD i la secció d'aquest document i de la Política General de Certificació on es desenvolupen:

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

9.4.2. Dades de caràcter personal no disponibles a tercers

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

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

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

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

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

9.4.3. Dades de caràcter personal disponibles a tercers

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

Aquesta informació, proporcionada en la sol·licitud de certificats en els termes previstos a l'article 17.2 de la Llei 59/2003, de 19 de desembre, de signatura electrònica, s'inclou en els seus certificats i en el mecanisme de comprovació de l'estat dels certificats.

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

En tot cas, es considera no confidencial la següent informació:

a. Els certificats emesos o en tràmit d'emissió
b. La subjecció de subscriptor a un certificat emès per l'Entitat de Certificació
c. El nom i cognoms del subscriptor del certificat, així com qualsevol altra circumstància o dada personal del titular en el supòsit que siguin significatius en funció de la finalitat del certificat, d'acord amb aquest document
d. L'adreça electrònica del subscriptor del certificat
e. Els usos i límits econòmics ressenyats en el certificat
f. El període de validesa del certificat, així com la data d'emissió del certificat i la data de caducitat
g. El número de sèrie del certificat
h. Els diferents estats o situacions del certificat i la data d'inici de cadascun d'ells, en concret: pendent de generació i/o entrega, vàlid, revocat, suspès o caducat i el motiu que va provocar el canvi d'estat
i. Les llistes de revocació de certificats (LRCs), així com la resta d'informacions d'estat de revocació
j. La informació continguda en la part pública del Registre de l'Entitat de Certificació

9.4.4. Responsabilitat corresponent a la protecció de dades personals

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

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

El Consorci AOC inclou en aquest document el seu procediment de comunicació, gestió i resposta davant de les incidències relacionades amb les dades personals.

Aquest procediment de comunicació s'inicia quan l'administrador dels sistemes de l'Entitat de Certificació, en les seves instal·lacions, comunica immediatament per telèfon amb el

Responsable de l'Àrea Tècnica de l'Entitat de Certificació, descrivint el tipus d'incidència i els efectes que s'observen.

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

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

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

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

- Quin recurs té la incidència
- El seu codi i descripció
- El dia i l'hora
- El tipus d'incidència
- Els efectes
- El comunicant i el destinatari
- La resposta
- Els procediments previstos a realitzar
- La persona que els realitzarà
- El procediment pera la recuperació
- La persona (i autorització) pera la recuperació
- Les dades restaurades.

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

Pera la prestació del servei, el Consorci AOC necessita recollir i emmagatzemar certes informacions que comporten tractament de dades personals.

En l'expedició de certificats a LES INSTITUCIONS, aquestes dades són comunicades pels subscriptors, sense necessitat de consentiment dels afectats posseïdors de claus, d'acord amb allò establert per la normativa reguladora de la relació del personal al servei del subscriptor del certificat o altra normativa que resulti aplicable.

El Consorci AOC informa als posseïdors de claus de l'obtenció de les seves dades personals.

9.4.7. Comunicació de dades personals

El Consorci AOC només comunica les dades de caràcter personal a tercers en els casos legalment previstos.

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

El Consorci AOC dona compliment a totes les prescripcions legals, de Conformitat amb la política de protecció de dades prevista en la secció 9.4.1.

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

9.5. Drets de propietat intel·lectual

9.5.1. Propietat dels certificats i informació de revocació

L'Entitat de Certificació Vinculada serà la única entitat que gaudirà dels drets de propietat intel·lectual sobre els certificats que emeti.

L'Entitat de Certificació Vinculada haurà de concedir llicència no exclusiva per a reproduir, distribuir, verificar i utilitzar els certificats, sense cap cost, en relació amb signatures digitals i/o sistemes de xifrat dintre de l'àmbit d'aplicació d'aquesta política, d'acord amb el corresponent instrument vinculant entre l'Entitat de Certificació Vinculada i la part que reprodueixi i/o distribueixi el certificat.

Les anteriors normes figuraran en els instruments jurídics que existeixin entre l'Entitat de Certificació Vinculada i els subscriptors i els verificadors.

Addicionalment, els certificats emesos per l'Entitat de Certificació Vinculada han de contenir un avís legal relatiu a la propietat d'aquests.

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

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

El Consorci AOC serà la única entitat que gaudirà dels drets de propietat intel·lectual sobre la política de certificació de la jerarquia pública de certificació de Catalunya.

Cada Entitat de Certificació Vinculada serà propietària de la seva Declaració de Pràctiques de Certificació.

9.5.3. Propietat de la informació relativa a noms

El subscriptor i, en el seu cas, el posseïdor de claus, conservarà qualsevol dret, d'existir aquest, relatiu a la marca, producte o nom comercial contingut en el certificat.

El subscriptor, o en el seu cas, el posseïdor de claus, serà el propietari del nom distingit del certificat, format per les informacions especificades en la secció corresponent d'aquesta política.

9.5.4. Propietat de claus

Els parells de claus seran propietat dels subscriptors dels certificats.

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

9.6. Obligacions i responsabilitat civil

9.6.1. Entitats de Certificació

9.6.1.1. Obligacions i altres compromisos

9.6.1.1.1. Obligacions del Consorci AOC

El Consorci AOC té les següents obligacions

a. Operar l'Entitat de Certificació arrel diligentment, d'acord amb les polítiques, pràctiques i normativa de la jerarquia pública de certificació de Catalunya.
b. Operar les seves Entitats de Certificació Vinculades, pròpies o que donin servei a les Entitats de Certificació Virtuals, d'acord amb allò disposat per l'apartat 9.6.1.1.2.
c. Garantir l'equivalència de la seguretat de l'operació de les Entitats de Certificació Vinculades de tercers prestadors de serveis de certificació, i especialment, vetllar per a que aquestes compleixin les obligacions previstes per l'apartat 9.6.1.1.2.

9.6.1.1.2. Obligacions de les Entitats de Certificació Vinculades

Les Entitats de Certificació Vinculades s'obligaran a complir el següent:

a. L'Entitat de Certificació Vinculada ha de garantir sota la seva plena responsabilitat, que compleix amb tots els requisits establerts en aquesta política de certificació.
b. L'Entitat de Certificació Vinculada serà la única entitat responsable del compliment dels procediments descrits en aquesta política, inclús quan una part o la totalitat de les operacions siguin subcontractades externament.
c. L'Entitat de Certificació Vinculada ha de prestar els seus serveis de certificació d'acord amb la seva Declaració de Pràctiques de Certificació vigent, en la qual es detallaran al menys els continguts previstos a l'article 19 de la Llei 59/2003.
d. Abans de l'emissió i entrega del certificat al subscriptor, l'Entitat de Certificació Vinculada haurà d'informar-lo dels aspectes previstos a l'article 18.b) de la Llei 59/2003, i dels següents aspectes:
    a) Indicació de la política aplicable, amb indicació de si els certificats s'expedeixen al públic i de la necessitat d'utilització de dispositiu qualificat de creació de signatura
    b) Forma en què es garanteix la responsabilitat patrimonial de l'Entitat de Certificació
    c) Si l'Entitat de Certificació ha sigut declarada conforme amb la política de certificació i, en el seu cas, d'acord amb quin sistema. En concret, la

certificació del prestador de serveis de certificació i la certificació dels productes de signatura electrònica utilitzats

e. Aquest requisit es complirà mitjançant un “Text divulgatiu de la política de certificat” aplicable, que podrà ser transmesa electrònicament, utilitzant un mitjà de comunicació que duri en el temps, i llenguatge comprensible.

f. L’Entitat de Certificació Vinculada ha d’obligar als subscriptors, als posseïdors de claus i als verificadors mitjançant instruments jurídics apropiats en cada situació.

g. Aquests instruments jurídics podran ser transmesos electrònicament, hauran d’estar en llenguatge escrit i comprensible i han de tenir els següents continguts mínims:

    a) Prescripcions pera donar compliment a allò establert en la present política de certificació

    b) Indicació de la política aplicable, amb indicació de si els certificats s’expedeixen al públic i de la necessitat d’ús del dispositiu segur de creació de signatura

    c) Manifestació que la informació continguda en el certificat és correcta, excepte notificació en contra pel subscriptor

    d) Consentiment per a la publicació del certificat en el directori i accés per a tercers al mateix

    e) Consentiment per a l’emmagatzematge de la informació utilitzada per al registre del subscriptor i del posseïdor de claus, pera la provisió del dispositiu qualificat de creació de signatura i pera la cessió d’aquesta informació a tercers, en cas de finalització d’operacions de l’Entitat de Certificació Vinculada sense revocació de certificats vàlids

    f) Límits d’ús del certificat, incloent els establerts en la secció 4.5 d’aquesta política

    g) Informació sobre com validar un certificat, incloent el requisit de comprovar l’estat del certificat i les condicions en les que es pot confiar raonablement en el certificat, que resulta aplicable quan el subscriptor actua com a verificador

    h) Limitacions de responsabilitat aplicables, incloent els usos pels que l’Entitat de Certificació Vinculada accepta o exclou la seva responsabilitat

    i) Procediments aplicables de resolució de disputes

    j) Llei aplicable i jurisdicció competent

h. L’Entitat de Certificació Vinculada ha d’identificar al subscriptor del certificat, d’acord amb els articles 12 i 13 de la Llei 59/2003 i la present política de certificat i, en concret:

    a) L’Entitat de Certificació Vinculada ha de comprovar per sí mateixa o per mitjà d’una Entitat de Registre, la identitat i qualsevol altra circumstància personal dels sol·licitants dels certificats, d’acord amb allò establerta l’article 13 de la Llei 59/2003

    b) En cas que el subscriptor del certificat de persona física sigui una persona jurídica, l’Entitat de Certificació Vinculada ha de comprovar que el posseïdor de la clau es troba degudament autoritzat pel subscriptor

i. L'Entitat de Certificació Vinculada ha de complir la resta d'obligacions contingudes en l'article 12 de la Llei 59/2003

9.6.1.1.2.1. Requisits específics per als certificats personals i d'entitat

L'Entitat de Certificació ha d'assumir altres obligacions incorporades directament en el certificat o incorporades per referència.

Nota: La incorporació per referència s'aconsegueix incloent en el certificat un identificador d'objecte o altra forma d'enllaç a un document, que es considera inclòs de forma íntegra en la present política de certificat.

Addicionalment a allò establert en la secció corresponent, l'instrument jurídic que vincula l'Entitat de Certificació Vinculada i el subscriptor haurà d'estar en llenguatge escrit i comprensible i ha de tenir els següents continguts mínims:

a. Indicació de la política aplicable, amb indicació de si els certificats s'expedeixen al públic o a una comunitat tancada d'usuaris i de la necessitat d'ús de dispositiu qualificat de creació de signatura
b. Certificació de serveis de l'Entitat de Certificació Vinculada
c. Forma en què es garanteix la responsabilitat patrimonial de l'Entitat de Certificació Vinculada

9.6.1.1.2.2. Requisits específics per al CDS i CDS-1 de Seu electrònica

L'Entitat de Certificació ha de comprovar el nom de domini i altres dades tècniques, com la IP, que hagin de figurar en el certificat.

9.6.1.1.3. Obligacions de l'Entitat de Certificació Virtual

Les Entitats de Certificació Virtual s'obligaran a complir el següent:

a. Determinar la comunitat de subscriptors i verificadors de l'Entitat de Certificació Vinculada
b. Aprovar les polítiques de certificació i, si és necessari, les polítiques específiques de certificació
c. Aprovar, si és necessari, la Declaració de Pràctiques de Certificació
d. Aprovar la documentació contractual i reguladora dels serveis de certificació en la comunitat d'usuaris de l'Entitat de Certificació Vinculada
e. Notificar puntualment a l'Entitat de Certificació Vinculada de totes les informacions relatives als canvis a realitzar, incidències en el servei, reclamacions, denúncies i inspeccions del servei

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

9.6.1.2. Garanties ofertes a subscriptors i verificadors

L'Entitat de Certificació Vinculada, com a mínim, garantirà al subscriptor:

a. El compliment de les seves obligacions legals com aprestador de serveis de certificació, d'acord amb la Llei 59/2003, de 19 de desembre

b. Que no hi hagi errors de fet en les informacions contingudes en els certificats, coneguts o realitzats per l'Entitat de Certificació Vinculada i, en el seu cas, per l'Entitat de Registre

c. Que no hagi errors de fet en les informacions contingudes en els certificats, deguts a falta de diligència en la gestió de la sol·licitud de certificat o a la creació d'aquest

d. Que els certificats compleixin tots els requisits materials establerts en la DPC

e. Que els serveis de revocació i l'ús del directori compleixin tots els requisits materials establerts en la DPC

L'Entitat de Certificació Vinculada, com a mínim, garantirà al verificador:

a. El compliment de les seves obligacions legals com aprestador de serveis de certificació, d'acord amb la Llei 59/2003, de 19 de desembre

b. Que la informació continguda o incorporada per referència al certificat és correcta, excepte quan s'indiqui el contrari

c. En cas de certificats publicats en el directori, que el certificat ha sigut emès al subscriptor identificat en aquest i que el certificat ha sigut acceptat, d'acord amb la secció corresponent de la present política de certificació

d. Que en l'aprovació de la sol·licitud de certificat i en l'emissió del certificat s'han complert tots els requisits materials establerts en la DPC

e. La rapidesa i seguretat en la prestació dels serveis, en especial dels serveis de revocació

Addicionalment, l'Entitat de Certificació garantirà al subscriptor i al verificador:

a. Que el certificat conté les informacions que ha de contenir un certificat qualificat, d'acord amb la legislació aplicable, descrita a l'apartat 9.15 Conformitat amb la Llei aplicable

b. Que, en el cas que generi les claus privades del subscriptor o, en el seu cas, el posseïdor de claus, es manté la seva confidencialitat durant el procés

c. La responsabilitat de l'Entitat de Certificació, amb els límits que s'estableixin

9.6.2. Entitats de Registre

9.6.2.1. Obligacions i altres compromisos

9.6.2.1.1. Obligacions de les Entitats de Registre Internes

L'Entitat de Registre Interna s'obligarà a complir el següent:

a. Actuar exclusivament en relació amb persones vinculades a l'Entitat de Registre Interna

b. Nomenar com a operadors de l'autoritat (tècnica) de registre a dos o més dels seus treballadors (depenent de l'EC, generalment quatre o més) i comunicar al Consorci AOC les dades corresponents a aquestes persones pera l'emissió dels certificats d'operador corresponents. Quan un operador deixi de tenir capacitat pera actuar com el que és, sota el control i l'autoritat de l'Entitat de Registre Interna, aquesta

Entitat de Registre Interna ha de sol·licitar de forma immediata a l'Entitat de Certificació Vinculada la revocació del certificat d'operador corresponent

c. Validar i aprovar les sol·licituds de certificats i generar els certificats per als posseïdors de claus, d'acord amb els procediments i instruments tècnics establerts per l'Entitat de Certificació Vinculada, d'acord amb la DPC i la documentació d'operacions de l'Entitat de Certificació Vinculada

d. Si l'Entitat de Registre Interna no disposés d'informació actualitzada del posseïdor de claus, comprovar la identitat personalment o d'acord amb allò establert a la legislació aplicable, descrita a l'apartat 9.15 Conformitat amb la Llei aplicable, i registrar un justificant acreditatiu del nom complet, lloc i data de naixement, DNI i/o qualsevol altra informació que pogués ser utilitzada pera diferenciar una persona respecte altra en l'àmbit de l'Entitat de Registre Interna

e. Verificar, quan sigui necessari, qualsevol atribut específic del posseïdor de claus i registrar un justificant acreditatiu de la informació

f. Realitzar o tramitar les sol·licituds de suspensió, habilitació, revocació i renovació de certificats, d'acord amb els procediments i els instruments tècnics establerts per l'Entitat de Certificació Vinculada, d'acord amb la Declaració de Pràctiques de certificació i la documentació d'operacions de l'Entitat de Certificació Vinculada

g. Emmagatzemar els registres, ja sigui en paper, ja sigui de forma electrònica, amb les adequades mesures de seguretat, autenticitat, integritat i conservació, relatius a la informació continguda en el certificat, durant un període de 15 anys. Aquests registres han d'estar a disposició de l'Entitat de Certificació Vinculada

h. Emmagatzemar els fulls d'entrega de certificat durant un període de 15 anys. Aquests registres han d'estar a disposició de l'Entitat de Certificació Vinculada

9.6.2.1.2. Entitat de Registre Virtual

L'Entitat de Registre Virtual s'obligarà a complir el següent:

a. Aportar la justificació documental necessària per al registre d'usuaris i pera la posterior emissió de certificats per part de l'Entitat de Certificació Vinculada o l'Entitat de Registre Col·laboradora

b. La justificació documental haurà de ser realitzada per una unitat orgànica de l'Entitat de Registre Virtual facultada legalment pera donar fe de les dades a certificar, que s'indicarà al Consorci AOC

9.6.2.1.3. Entitat de Registre Col·laboradora

L'Entitat de Certificació podrà delegar algunes funcions a Entitats de Registre Col·laboradores, que en aquest cas quedaran obligades al seu compliment, en les mateixes condicions que l'Entitat de Certificació.

L'Entitat de Registre Col·laboradora assistirà als subscriptors de certificats emesos a LES INSTITUCIONS amb Entitat de Registre Virtual, i a tots els subscriptors de la resta de certificats .

L'Entitat de Registre Col·laboradora actuarà en el seu propi nom, sense perjudici de la responsabilitat de l'Entitat de Certificació Vinculada.

L'Entitat de Registre Col·laboradora queda obligada a registrar les dades del certificat i la seva aprovació en cas de ser correctes, així com al registre de les dades d'aquest certificat, pel qual es realitzaran les comprovacions que consideri necessàries al respecte de la identitat i la resta de dades personals i complementàries dels subscriptors i, si fos necessari, dels posseïdors de claus.

Aquestes comprovacions han d'incloure la justificació documental aportada pel sol·licitant i, si l'Entitat de Registre Col·laboradora ho considerés necessari, qualsevol altre document i informació rellevant, facilitats pel subscriptor, pel posseïdor de claus o per terceres persones.

Si l'Entitat de Registre Col·laboradora detectés errors en les dades que han de ser incloses en els certificats, o en els documents que justifiquessin aquestes dades, estarà obligada a realitzar els canvis que consideri necessaris abans de l'emissió del certificat, o a la paralització del procés d'emissió i a gestionar amb el subscriptor la incidència corresponent.

En el cas que l'Entitat de Registre Col·laboradora corregeixi les dades sense gestió prèvia de la incidència corresponent amb el subscriptor, quedarà obligada a notificar les dades que finalment se certifiquin al subscriptor en el moment de l'entrega.

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

9.6.2.2. Garanties ofertes a subscriptor i verificadors

9.6.2.2.1. Garantia del Consorci AOC per als serveis de certificació digital

El Consorci AOC garanteix que la clau privada de l'entitat de certificació utilitzada pera emetre certificats no ha sigut compromesa, a excepció que el Consorci AOC no hagués comunicat el contrari,mitjançant el registre de certificació del Consorci AOC, de Conformitat amb la Declaració de pràctiques de certificació.

El Consorci AOC únicament garanteix que:

a. Els certificats de signatura electrònica contenen tota la informació exigida per la Llei desembre aplicable, que es descriu a l'apartat 9.15 Conformitat amb la Llei aplicable.
b. No ha originat ni ha introduït declaracions falses o errònies en la informació de cap certificat, ni ha deixat d'incloure informació necessària aportada pel subscriptor i validada pel Consorci AOC o per l'entitat de registre col·laboradora, en el moment de l'emissió del certificat.
c. Tots els certificats compleixen els requisits formals i de contingut de la seva Declaració de pràctiques de certificació.
d. Queda vinculada pels procediments operatius, de seguretat i d'arxiu descrits en la Declaració de pràctiques de certificació

9.6.2.2.2. Exclusió de la garantia

El Consorci AOC no garanteix cap programari utilitzat pel subscriptor o per qualsevol altra persona, pera generar, verificar o no utilitzar de forma distinta cap signatura digital o certificat digital emès pel Consorci AOC, a excepció dels casos en què existeixi una declaració escrita del Consorci AOC en sentit contrari.

9.6.3. Subscriptors

9.6.3.1. Obligacions i altres compromisos

9.6.3.1.1. Requisits pera tots els tipus de certificats

L'Entitat de Certificació Vinculada obligarà al subscriptor a:

a. Facilitar a l'Entitat de Certificació Vinculada informació completa i adequada, conforme als requeriments d'aquesta política de certificació, en especial pel que respecta al procediment de registre

b. Manifestar el seu consentiment previ a l'emissió i entrega d'un certificat

c. Complir les obligacions que s'estableixen per al subscriptor en la present política de certificació i a la legislació aplicable, descrita a l'apartat 9.15 Conformitat amb la Llei aplicable.

d. Utilitzar el certificat d'acord amb allò establert en la secció corresponent

e. Notificar a l'Entitat de Certificació Vinculada, sense retards injustificables, la pèrdua, l'alteració, l'ús no autoritzat, el robatori o el compromís del seu dispositiu qualificat de creació de signatura

f. Notificar a l'Entitat de Certificació Vinculada i qualsevol persona que el subscriptor cregui que pugui confiar en el certificat, sense retards injustificables:

    a) La pèrdua, el robatori o el compromís potencial de la seva clau privada

    b) La pèrdua de control sobre la seva clau privada, a causa del compromís de les dades d'activació (per exemple, el codi PIN del dispositiu qualificat de creació de signatura) o per qualsevol altra causa

    c) Les inexactituds o canvis en el contingut del certificat que conegui o pogués conèixer el subscriptor

g. Deixar d'utilitzar la clau privada transcorregut el període indicat en la secció corresponent

h. Transferir als posseïdors de claus les obligacions específiques d'aquests

i. No monitoritzar, manipular o realitzar actes d'enginyeria inversa sobre la implantació tècnica de la jerarquia, sense permís previ per escrit

j. No comprometre intencionadament la seguretat de la jerarquia pública de certificació de Catalunya

9.6.3.1.2. Requisits específics per als certificats de signatura electrònica reconeguda

L'Entitat de Certificació Vinculada obligarà al subscriptor a:

a. Utilitzar el parell de claus exclusivament pera signatures electròniques i conforme a qualsevol altra limitació que li sigui notificada

b. Reconèixer que aquestes signatures electròniques són signatures electròniques equivalents a signatures manuscrites, d'acord amb l'article 3.4 de la Llei 59/2003, de 19 de desembre

c. Ser especialment diligent en la custòdia de la seva clau privada i del seu dispositiu qualificat de creació de signatura, amb la finalitat d'evitar usos no autoritzats

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

   1. Generar les seves claus de subscriptor utilitzant un algoritme reconegut com acceptable pera la signatura electrònica reconeguda

   2. Crear les claus dintre del dispositiu qualificat de creació de signatura

   3. Utilitzar longituds i algoritmes de clau reconeguts com acceptables per a la signatura electrònica reconeguda

e. Notificar a l'EC, sense retards injustificables, la pèrdua, l'alteració, l'ús no autoritzat, el robatori o el compromís del seu dispositiu qualificat de creació de signatura

9.6.3.2. Garanties ofertes pel subscriptor

L'Entitat de Certificació Vinculada haurà d'obligar al subscriptor, mitjançant el corresponent instrument jurídic, a garantir:

a. En cas que el subscriptor sigui el sol·licitant del certificat, que totes les manifestacions realitzades en la sol·licitud són correctes

b. Que totes les informacions subministrades pel subscriptor que es trobin contingudes en el certificat són correctes

c. Que el certificat s'utilitza exclusivament pera usos legals i autoritzats, d'acord amb la DPC de l'Entitat de Certificació Vinculada

d. Que cada signatura digital creada amb la clau privada corresponent a la clau pública llistada en el certificat és la signatura digital del subscriptor o posseïdor de claus i que el certificat ha sigut acceptat i es troba operatiu (no ha expirat ni ha sigut revocat) en el moment de creació de la signatura

e. Que el subscriptor és una entitat final i no una Entitat de Certificació, i no utilitzarà la clau privada corresponent a la clau pública llistada en el certificat pera signar cap certificat (o qualsevol altre format de clau pública certificada), ni LRC

f. Que cap persona no autoritzada ha tingut mai accés a la clau privada del subscriptor

9.6.3.3. Protecció de la clau privada

L'Entitat de Certificació Vinculada haurà d'obligar al subscriptor, mitjançant el corresponent instrument jurídic, a garantir que el subscriptor és l'únic responsable dels danys causats pel seu incompliment del deure de protegir la clau privada.

9.6.4. Verificadors

9.6.4.1. Obligacions i altres compromisos

L'Entitat de Certificació Vinculada ha d'obligar a l'usuari de certificats a:

a. Assessorar-se sobre el fet que el certificat és apropiat pera l'ús que es pretén
b. Verificar la validesa, suspensió o revocació dels certificats emesos, cosa per a la qual utilitzarà informació sobre l'estat dels certificats
c. Verificar tots els certificats de la jerarquia de certificats, abans de confiar en la signatura digital o en algun dels certificats de la jerarquia
d. Tenir present qualsevol limitació en l'ús del certificat, amb independència que es trobi en el mateix certificat o en el contracte de verificador
e. Tenir present qualsevol precaució establerta en un contracte o en altre instrument, amb independència de la seva naturalesa jurídica
f. No monitoritzar, manipular o realitzar actes d'enginyeria inversa sobre la implantació tècnica de la jerarquia pública de certificació de Catalunya, sense permís previ per escrit
g. No comprometre intencionadament la seguretat de la jerarquia pública de certificació de Catalunya
h. Reconèixer que les signatures electròniques produïdes per certificats qualificats de signatura qualificada, són signatures electròniques equivalents a signatures escrites, d'acord amb l'article 3.4 de la Llei 59/2003, de 19 de desembre.

9.6.4.2. Garanties ofertes pel verificador

L'Entitat de Certificació haurà d'obligar al verificador, mitjançant el corresponent instrument jurídic, a manifestar:

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

9.6.5. Altres Participants

9.6.5.1. Obligacions i garanties del directori

L'Entitat de Certificació Vinculada podrà delegar algunes funcions en el directori, que en aquest cas estarà obligat al seu compliment, en les mateixes condicions que l'Entitat de Certificació.

Les funcions, obligacions i deures del directori s'establiran detalladament en la Declaració de Pràctiques de Certificació de l'Entitat de Certificació Vinculada, així com en la documentació jurídica auxiliar, especialment l'entregada a subscriptors, posseïdors de claus i verificadors.

9.6.5.2. Garanties ofertes pel directori

L'Entitat de Certificació Vinculada ha d'establir en la seva DPC la responsabilitat civil del directori, quan sigui operat per una tercera entitat.

9.7. Renúncia de garanties

9.7.1. Renúncia de garanties de l'Entitat de Certificació

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

9.8. Limitacions de responsabilitat

9.8.1. Limitacions de responsabilitat de l'Entitat de Certificació

L'Entitat de Certificació Vinculada limitarà la seva responsabilitat restringint el servei a l'emissió i la 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) subministrat per l'Entitat de Certificació.

L'Entitat de Certificació Vinculada podrà limitar la seva responsabilitat mitjançant la inclusió de límits d'ús del certificat i límits de valor de les transaccions pera les que pot utilitzar-se el certificat.

9.8.2. Cas fortuït i força major

L'Entitat de Certificació Vinculada inclourà clàusules pera limitar la seva responsabilitat en cas fortuït i en casos 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'Entitat de Certificació Vinculada haurà d'establir, en els seus instruments jurídics amb els subscriptors, una clàusula que determini el període de vigència de la relació jurídica en virtut de la qual els subministra certificats.

9.10.2. Finalització

L'Entitat de Certificació Vinculada haurà d'establir, en els seus instruments jurídics amb els subscriptors, una clàusula que determini les conseqüències de la finalització de la relació jurídica en virtut de la qual els subministra certificats.

9.10.3. Supervivència

L'Entitat de Certificació Vinculada haurà d'establir, en els seus instruments jurídics amb els subscriptors, clàusules de supervivència, en virtut de la qual certes regles continuaran vigents després de la finalització de la relació jurídica reguladora del servei entre les parts.

A aquest efecte, l'Entitat de Certificació Vinculada vetllarà perquè, al menys els requisits continguts en les seccions Obligacions, Responsabilitat civil, Auditoria de conformitat i Confidencialitat, continuïn vigents després de la finalització de la política de certificació i dels instruments jurídics que vinculen l'Entitat de Certificació amb subscriptors.

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

9.11. Notificacions

L'Entitat de Certificació Vinculada haurà d'establir clàusules de notificació en els seus instruments jurídics vinculants amb subscriptors i verificadors.

En virtut d'aquestes clàusules, s'establirà el procediment pel qual les parts es notifiquen fets mútuament.

9.12. Modificacions

9.12.1. Procediment pera les modificacions

Les Entitats de Certificació Vinculades podran modificar, de forma unilateral, la política de certificació, sempre que procedeixin segons el següent procediment:

- La modificació haurà d'estar justificada des del punt de vista tècnic, legal o comercial
- La modificació proposada per una Entitat de Certificació Vinculada no podrà anar en contra de la política de certificació establerta pel Consorci AOC
- S'establirà un control de modificacions pera garantir, en tot cas, que les especificacions resultants compleixen els requisits que s'intentaven complir i que van donar peu al canvi

- S'establiran les implicacions que el canvi d'especificacions té sobre l'usuari i es preveurà la necessitat de notificar-li aquestes modificacions
- La nova política haurà de ser aprovada pel Consorci AOC

9.12.2. Període i mecanismes per a notificacions

Les modificacions de la política es notificaran al Consorci AOC pera la seva posterior aprovació.

9.12.3. Circumstàncies en què un OID ha de ser canviat

Sense estipulació addicional.

9.13. Resolució de conflictes

9.13.1. Resolució extrajudicial de conflictes

L'Entitat de Certificació Vinculada haurà d'establir, en els seus instruments jurídics amb subscriptors i verificadors, els procediments de mediació i resolució de conflictes aplicables.

Amb aquesta finalitat, es tindrà en compte la consideració com Administració Pública de l'Entitat de Certificació Vinculada.

Les situacions de discrepància que es derivin de l'ús dels certificats emesos per l'Entitat de Certificació Vinculada, es resoldran aplicant els mateixos criteris de competència que en els casos dels documents signats per escrit.

9.13.2. Jurisdicció competent

L'Entitat de Certificació Vinculada haurà d'establir, en els seus instruments jurídics vinculants amb subscriptors i verificadors, una clàusula de jurisdicció competent, indicant que la competència judicial internacional correspon als jutges espanyols.

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

Quan l'Entitat de Certificació Vinculada tingui la consideració d'Administració Pública es tindrà en compte la legislació administrativa que resulti aplicable.

9.14. Llei aplicable

L'Entitat de Certificació Vinculada haurà d'establir en els seus instruments jurídics amb subscriptors i verificadors, que la Llei aplicable a la prestació dels serveis, incloent la política i pràctiques de certificació,és la següent:

- En general, la Llei espanyola, sempre i quan l'Entitat de Certificació Vinculada estigui establerta a l'Estat Espanyol, i/o els seus serveis de Certificació es prestin per mitjà d'un establiment permanent situat a l'Estat Espanyol

- Per a les Entitats de Certificació Vinculades a la jerarquia amb la consideració d'Administració Pública, la normativa administrativa corresponent, estatal i autonòmica.

9.15. Conformitat amb la Llei aplicable

L'Entitat de Certificació Vinculada haurà de manifestar, en aquest document i en els instruments jurídics amb subscriptors, el compliment de:

1. el REGLAMENT (UE) No 910/2014 DEL PARLAMENT EUROPEU I DEL CONSELL, de 23 juliol 2014, relatiu a la identificació electrònica i els serveis de confiança per a les transaccions electròniques en el mercat interior i per la qual es deroga la Directiva 1999/93 / CE, i la normativa tècnica associada.
2. la Llei 59/2003, , de 19 de desembre, de firma electrònica,
3. la Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques,
4. la Llei 40/2015, d'1 d'octubre, de règim jurídic del Sector Públic i
5. la Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i comerç electrònic,

en la seva DPC i amb els instruments jurídics amb subscriptors i verificadors.

9.16. Clàusules diverses

9.16.1. Acord íntegre

L'Entitat de Certificació haurà d'establir, en els seus instruments jurídics vinculants amb subscriptors i verificadors, clàusules d'acord íntegre.

En virtut de la clàusula d'acord íntegre s'entendrà que l'instrument jurídic regulador del servei conté la voluntat completa i tots els acords entre les parts.

9.16.2. Subrogació

Els drets i els deures associats a la condició d'Entitat de Certificació Vinculada no podran ser objecte de cessió a tercers de cap tipus, ni cap tercera entitat podrà subrogar-se en la posició jurídica d'una Entitat de Certificació.

En cas de produir-se una cessió o subrogació, es procedirà a la finalització de l'Entitat de Certificació Vinculada.

Els drets i els deures associats a la condició d'Entitat de Certificació Virtual podran ser objecte, en canvi, de cessió i subrogació, però aquestes incidències hauran de ser notificades al Consorci AOC.

9.16.3. Divisibilitat

L'Entitat de Certificació haurà d'establir,als seus instruments jurídics vinculants amb subscriptors i verificadors, clàusules de divisibilitat.

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

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

9.16.4. Aplicacions

Sense estipulació addicional.

9.16.5. Altres clàusules

Sense estipulació addicional.

10. ANNEX – Control documental

Projecte:	**Informe modificació del document PGdC**
Entitat de destí:	**Consorci AOC**
Codi de referència:	**Revisió 1er semestre 2018**
Versió:	**Canvis de la v4.1 a la v4.2 en català i en castellà**
Data d'edició:	**09/05/2018**

Versió	Parts que canvien	Descripció del canvi	Autor del canvi	Data del canvi
4.2	Tot el document	Revisió global 1er semestre 2016.	Servei de Certificació Digital – Consorci AOC	09/12/20166
5.0	Tot el document	Adaptació eIDAS. Eliminació diferenciació entre certificats de classe 1 i classe 2. Simplificació de les referències.	Servei de Certificació Digital – Consorci AOC	09/05/2018