Consorci
Administració Oberta
de Catalunya

Declaració de Pràctiques de Certificació
Entitat de Certificació del Consorci AOC

Referència:	D1111_E0650_N-DPC Consorci AOC
Versió:	6.6
Data:	20/07/2021

La versió original en vigor d'aquest document es troba en format electrònic publicada en el lloc web del Consorci AOC i pot ser accessible a través de la següent URL: https://www.aoc.cat/catcert/regulacio

Historial de versions

Versió	Resum dels canvis	Data
5.0	Adaptació a EIDAS	9/5/2018
6.0	Creació de nova declaració de pràctiques de certificació unificada. Es numera com a versió 6.0 a l'efecte de gestió documental.	26/07/2018
6.1	• Revisió anual de la documentació, post auditoria eIDAS. • Alineat document amb RFC 3647. • "*1.1. Presentació*": indicada prevalença de les guies del CA/Browser Forum sobre la propia DPC. • "*1.5.5. Freqüència de revisió*": creat apartat. • "*4.4.3. Publicació del certificat*": indicada possibilitat de publicació de certificats si es disposa del consentiment exprés. • "*4.10.7. Freqüència d'emissió de llistes de revocació de certificats (LRCs)*": afegida freqüència de publicació de la CRL. • "*5.2.2. Número de persones per tasca*": especificada la redundancia de rols per certes tasques. • "*6.5.3. Freqüència de revisió de les configuracions dels sistemes de confiança*": creat apartat. • "*9.4. Protecció de dades personals*": ajustades descripcions i actualitzada legislació aplicable, incloent RGPD i la LOPDGDD. • "*9.12.1. Procediment per a les modificacions*": reformulat apartat • Eliminades referències a signatura de codi. • Realitzats petits ajustos de congruència als textos.	24/07/2019
6.2	• Adaptació a requeriments del CAB-Forum: alineat amb tots els apartats de la RFC 3647: • Inclusió de 1.6 "Definicions i acrònims" • Inclusió de 7.3: "Perfils d'OCSP"	31/03/2020
6.3	• Introducció de la identificació per videoconferència en l'apartat 3.2.3 • Altres canvis menors	21/05/2020
6.4	• Inclusió de certificats d'autenticació i signatura de treballador públic de nivell mitjà i de nivell alt. • Procediment de generació de l'última CRL en cas de compromís de claus o finalització del servei. Secció 4.10.9	03/08/2020

6.5	• Adequació a la llei 6/2020, d'11 de novembre, reguladora de determinats aspectes dels serveis electrònics de confiança.	27/01/2021
6.6	• Apartat 3.2.5: S'afegeix informació verificada per a certificats SSL. • Apartat 4.10.1: noves causes de revocació. • Apartat 4.10.12: adaptació dels requeriments per compromís de clau. • Apartat 5.3.1: qualificació de l'especialista de validació. • Apartat 5.7.3: adaptació compromís de clau privada • Apartat 6.1.9: adaptació de propòsits d'ús clau • Apartat 6.2.1.1: cas de pèrdua de qualificació del dispositu segur de creació de signatura. • Apartat 7.1: perfil de certificat. Aclaració d'entropia mínima del número de sèrie • Apartat 9.5.2: Propietat intel·lectual de la DPC i PCs • Apartat 9.14: es relaciona tota la normativa aplicable.	20/07/2021

Índex

1. Introducció

1.1. Presentació

Aquest document és la Declaració de Pràctiques de Certificació (DPC) del Consorci Administració Oberta de Catalunya (Consorci AOC), Prestador dels serveis de confiança (PSC) o Trust Service Provider (TSP) que opera a l'empara del previst en el Reglament (UE) núm. 910/2014 del Parlament Europeu i del Consell de 23 de juliol de 2014, relatiu a la identificació electrònica i els serveis de confiança per a les transaccions electròniques al mercat interior i pel qual es deroga la Directiva 1999/93/CE (Reglament (UE) núm. 910/2014)

En aquesta DPC es detallen el conjunt de pràctiques adoptades pel Consorci AOC com a Prestador de Serveis de Confiança per a l'emissió de certificats electrònics i serveis de confiança basats en els següents estàndards:

- ETSI EN 319 401 (General Policy Requirements for Trust Service Providers).
- ETSI EN 319 411-1 (Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements)
- ETSI EN 319 411-2 (Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates)
- ETSI EN 319 412-1 (Certificate Profiles; Part 1: Overview and common data structures)
- ETSI EN 319 412-2 (Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons)
- ETSI EN 319 412-3 (Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons)
- ETSI EN 319 412-4 (Certificate Profiles; Part 4: Certificate profile for web site certificates)
- ETSI EN 319 422 (Certificate profiles for time-stamping protocol and time-stamp token profiles)
- ETSI EN 319 412-5 (Certificate Profiles; Part 5: QCStatements)

L'estructura d'aquest document està basada en l'especificació de l'estàndard “RFC3647 - Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework “, creat pel grup de treball PKIX del IETF.

La present DPC es correlaciona amb les diferents Polítiques de Certificació (PC) desenvolupades per a cada tipologia de certificats electrònics emesos sota el control del Consorci AOC, els quals són descrits a l'apartat 1.1.1 del present document. En cas de contradicció entre la present DPC i correspondents PC prevaldrà el que es disposa en aquest document.

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 gestió de certificats de validació estesa (extended validation), i amb les pautes de Baseline Requirements d'aquest mateix organisme per a l'emissió de certificats de dispositiu servidor (CDS), publicades en: http://www.cabforum.org. Les indicacions de les guies del CA/Browser Fòrum prevaldran a la DPC.

1.1.1. Tipus i classes de certificats

El Consorci AOC presta els seus serveis de certificació amb la finalitat d'emetre certificats electrònics per a diversos usos i diferents usuaris finals. Tots els certificats que emet el Consorci AOC s'adeqüen als requeriments del Reglament UE núm. 910/2014.

1.1.1.1. Certificats de ciutadania

- **Certificat qualificat de ciutadà (idCAT):** El certificat idCAT és un certificat qualificat d'identificació i signatura electrònica avançada destinat a ciutadans i ciutadanes amb veïnatge administratiu català, i per a altres persones (col·lectivament denominats "subscriptors") que necessiten relacionar-se amb les Administracions públiques i altres institucions de Catalunya.

1.1.1.2. Certificats Personals del Sector Públic

- **Certificat d'autenticació d'empleat públic de nivell alt (T-CAT autenticació).** Permet la identificació d'un empleat públic en l'exercici de les seves funcions, com a instrument per a l'actuació en l'àmbit electrònic d'una Administració Pública, òrgan, organisme públic o entitat de dret públic català conforme al previst en la regulació aplicable. Els certificats T-CAT d'Autenticació i T-CAT de Signatura s'emeten i emmagatzemen conjuntament en un únic dispositiu criptogràfic.

- **Certificat qualificat de signatura d'empleat públic de nivell alt (T-CAT signatura).** Permet la signatura electrònica per part d'un empleat públic en l'exercici de les seves funcions, com a instrument per a l'actuació en l'àmbit electrònic d'una Administració Pública, òrgan, organisme públic o entitat de dret públic català conforme al previst en la regulació aplicable. Els certificats T-CAT d'Autenticació i T-CAT de Signatura s'emeten i emmagatzemen conjuntament en un únic dispositiu criptogràfic.

- **Certificat qualificat d'autenticació i signatura de empleat públic de nivell mig/substancial (T-CATP).** Aquest tipus de certificats d'autenticació i signatura s'emeten per al seu ús en software per part de empleats públics catalans en l'exercici de les seves funcions en actuacions que no requereixin un nivell alt de

seguretat, segons la regulació aplicable.

- **Certificat d'autenticació de empleat públic amb pseudònim de nivell alt (T-CAT pseudònim autenticació).** L'emissió d'aquests certificats es farà sota la valoració prèvia de l'acreditació legal del pseudònim que haurà d'acompanyar la sol·licitud. S'acceptaran molt específicament per a usos justificats dels quals no es puguin mostrar les dades del titular i per persones que, dins de la seva organització, ja disposin de pseudònim regulat, cas dels funcionaris de presons, Mossos d'esquadra, serveis socials, etc. Exceptuant allò que té a veure amb l'ús de pseudònim, les seves característiques són iguals a les del certificat T-CAT d'Autenticació. Els certificats T-CAT amb Pseudònim i d'Autenticació i T-CAT amb Pseudònim i de Signatura s'emeten i emmagatzemen conjuntament en un únic dispositiu criptogràfic.

- **Certificat qualificat de signatura de empleat públic amb pseudònim de nivell alt (T-CAT pseudònim signatura).** Per a l'emissió d'aquests certificats es tindran en compte les mateixes circumstàncies que en el cas dels certificats T-CAT amb Pseudònim i d'Autenticació. Excepte en el que respecta a l'ús de pseudònim, les seves característiques són iguals a les del certificat T-CAT de Signatura. Els certificats T-CAT amb Pseudònim i d'Autenticació i T-CAT amb Pseudònim i de Signatura s'emeten i emmagatzemen conjuntament en un únic dispositiu criptogràfic.

- **Certificat qualificat d'autenticació i signatura de persona vinculada de nivell alt (T-CAT persona vinculada):** Certificat personal d'identificació i signatura electrònica qualificada, amb càrrec opcional. Aquests certificats s'emeten i emmagatzemen en un dispositiu criptogràfic. Aquests certificats estan destinats a aquelles persones amb relació funcional o de servei amb una institució pública, però sense relació laboral amb aquesta institució. Com per exemple externalització de serveis públics.

- **Certificat qualificat d'autenticació i signatura de persona vinculada de nivell mig/substancial (T-CATP Persona vinculada):** Certificat personal d'identificació i signatura electrònica qualificada, amb càrrec opcional. Aquests certificats s'emeten i emmagatzemen en software.

- **Certificat qualificat d'autenticació i signatura de representant davant les Administracions Públiques (T-CAT Representant)**: Certificat personal d'identificació i signatura electrònica qualificada, amb càrrec opcional. Aquest certificat s'emet en dispositiu criptogràfic. Va dirigit a persones físiques, disposa d'informació referent al titular i permet la seva identificació i la de la seva organització. Se subministra als empleats públics d'ens del sector públic de Catalunya com a element identificatiu en les comunicacions electròniques, permetent signar documents en format electrònic per fer possible els tràmits i les

consultes en línia. Aquest certificat permet identificar-se com persona posseïdora d'un determinat càrrec en la seva organització.

- **Certificat qualificat d'autenticació i signatura de treballador públic de nivell alt (T-CAT treballador públic)**. Certificat personal d'identificació i signatura electrònica qualificada, emesos i emmagatzemats en dispositiu criptogràfic. Aquests certificats estan destinats a aquelles persones que mantenen una relació laboral o d'alta direcció en una entitat que integra el sector públic de Catalunya.

- **Certificat qualificat d'autenticació i signatura de treballador públic de nivell mig/substancial (T-CATP treballador públic)**. Aquest tipus de certificats d'autenticació i signatura s'emeten per al seu ús en programari per part de treballadors públics d'ens del sector públic de Catalunya en l'exercici de les seves funcions en actuacions que no requereixin un nivell alt de seguretat, conforme al que es preveu en la regulació aplicable.

1.1.1.3. Certificats de Dispositius i Infraestructures

- **Certificat d'Aplicació (Dispositiu aplicació):** Aquest certificat s'emmagatzema en un servidor (preferiblement en un dispositiu criptogràfic) i és requerit per una aplicació per segellar documents, fitxers o missatges amb l'objectiu d'assegurar la seva autenticitat i integritat. Jurídicament opera com un segell electrònic avançat de l'ens o departament de l'Administració Pública a nom de qui s'emet, segons el que preveu el Reglament (UE) núm.910/2014, encara que el seu ús queda limitat a l'intercanvi de dades entre aplicacions.

- **Certificat de Segell Electrònic Avançat (Segell nivell mig/substancial)**: Serveix per a la identificació i l'autenticació de documents, fitxers o missatges en l'exercici de les competències en l'actuació administrativa automatitzada per a la prestació de serveis públics segons el que preveu l'article 37 del Reglament (UE) núm. 910/2014. Aquest certificat pot ser utilitzat per a l'intercanvi de dades (entre administracions, administracions i ciutadans i entre administracions i empreses), la identificació i autenticació d'un sistema, servei web o aplicació, l'arxiu electrònic automatitzat, les compulses i còpies electròniques, entre uns altres. Aquests certificats s'emeten i emmagatzemen en software.

- **Certificat de Seu Electrònica (Seu-e nivell mig/substancial)**: Serveix per identificar i garantir la integritat i autenticitat de la seu electrònica d'un ens, entenent seu electrònica en els termes descrits en l'article 38 de la Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic i l'establiment de comunicacions segures.

  Aquest certificat pot utilitzar-se per a la connexió segura dels ciutadans a pàgines web oficials, l'autenticació d'un lloc web, l'allotjament de registres electrònics, la consulta i autorització de registres de representació, etc.

Des de 2011, el Consorci AOC emet el certificat de Seu seguint el Standard Extended Validation SSL Certificate, la qual cosa garanteix el màxim nivell de seguretat en les transaccions através del lloc web que pugui utilitzar.

- **Certificat de Servidor Segur (Dispositiu SSL):** Aquest tipus de certificats garanteixen la identitat d'un domini davant els usuaris que es connecten, acreditant que el lloc web és l'original, el domini està oficialment registrat, és vàlid i no ha estat suplantat, i que ningú ha pogut alterar la informació publicada ni manipular les dades registrades en el servidor de manera no autoritzada.

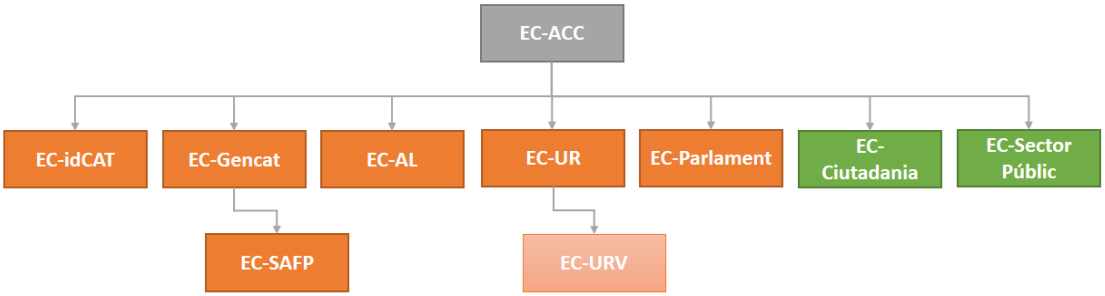
- **Certificat de Servidor Segur *Extended Validation* (Dispositiu SSL EV):** Els certificats de dispositiu servidor EV (CDS EV) no són estructuralment o funcionalment diferents dels certificat de dispositiu servidor (CDS), però es diferencien d'aquests en què han estat emesos per Entitats de Certificació que, com el Consorci AOC, han superat els estrictes requisits de seguretat establerts en el Standard Extended Validation SSL Certificate.

  El principal avantatge és que els nous navegadors web els acceptaran immediatament i mostraran una confirmació de seguretat que permetrà als usuaris identificar ràpidament un lloc segur i de confiança, ja que estan dissenyats per mostrar senyals visuals únics que indiquen la presència d'un certificat EV.

- **Certificat de Segell Qualificat de Temps (Segell de temps):** Permet garantir la integritat d'un arxiu o una comunicació electrònica en una hora i data determinades, per tant, la referència del temps és de confiança. Els Certificats de Segell Qualificat de temps emesos pel Consorci AOC compleixen amb els requisits establerts en l'article 42 del Reglament UE 910/2014.

1.1.2. Jerarquies

Segons es detalla en el gràfic següent, a partir de 2015, la jerarquia actual de certificació del Consorci AOC s'ha vist reduïda a dues Entitats de Certificació subordinades (marcades en verd) i una Entitat de Certificació arrel:



L'EC-SectorPúblic: que concentra l'emissió de certificats per al Sector Públic de Catalunya, en substitució de les antigues EC-SAFP, EC-AL, EC-UR i EC-Parlament. Aquestes Entitats de Certificació han deixat d'emetre certificats però alguns d'ells encara es troben en vigor.

Els certificats emesos sota les antigues Entitats de Certificació EC-SAFP, EC-AL, EC-UR i EC-Parlament no es regeixen per aquesta versió de la DPC. Als mateixos els resultarà d'aplicació el previst en les DPC AI, GENCAT, SAFP, PARLAMENT, UR i URV en la seva versió 5.0, 2.0, 5.0, 2.0, 7.0, 4.0, corresponent a l'última actualització de l'esmentat document abans del cessament en l'emissió de certificats a l'empara de les citades Entitats de Certificació.

L'EC-Ciutadania: que emet certificats electrònics a ciutadans en substitució de l'antiga EC-idCAT, la qual també ha deixat d'emetre certificats encara que alguns d'ells es troben vigents. Els certificats emesos sota l'antiga Entitat de Certificació EC-idCAT no es regeixen tampoc per aquesta versió de la DPC. Als mateixos els resultarà d'aplicació el previst en la DPC [idCAT] en la seva versió [4.0], corresponent a l'última actualització del citat document abans del cessament en l'emissió de certificats a l'empara de la citada Entitat de Certificació.

1.1.3. Emissió de certificats de proves

El Consorci AOC pot emetre certificats de proves signats per una EC real però amb contingut fictici perquè els organismes supervisors i les entitats de validació i els desenvolupadors d'aplicacions puguin dur a terme els seus processos d'integració i/o avaluació per a la seva acceptació. El Consorci AOC incorpora en aquests certificats la següent informació de manera que qualsevol usuari pugui conèixer clarament que es tracta d'un certificat de proves sense responsabilitat:

Nom de l'organització	Organització de prova
NIF de l'organització	VATES-Q0000000J
Domicili	Barcelona
Codi Postal	08008
Correu electrònic	scd@aoc.cat
Primer Cognom	de la Peça
Segon Cognom	de Proves
DNI/NIE	00000000T

1.2. Nom del document i identificació

1.2.1. Identificació d'aquest document

Nom:	Declaració de Pràctiques de Certificació (DPC)
Versió:	6.6
Descripció	Declaració de Pràctiques de Certificació del Consorci AOC
Data d'emissió:	20/07/2021
OID:	1.3.6.1.4.1.15096.1.2.2
Localització:	https://www.aoc.cat/catcert/regulacio

1.2.2. Identificació de polítiques de certificació cobertes per aquesta DPC

Tipus de Certificat	OID	Política
Certificats de ciutadania		
Certificat de ciutadà (idCAT)	1.3.6.1.4.1.15096.1.3.2.86.2	PC Ciutadà
Certificats personals del sector públic		
Certificat d'autenticació de empleat públic de nivell alt (T-CAT autenticació)	1.3.6.1.4.1.15096.1.3.2.7.1.2	PC Certificats Personals Sector Públic
Certificat qualificat de signatura de empleat públic de nivell alt (T-CAT signatura)	1. 3.6.1.4.1.15096.1.3.2.7.1.1	PC Certificats Personals Sector Públic
Certificat qualificat d'autenticació i signatura de empleat públic de nivell mig/substancial (T-CATP)	1.3.6.1.4.1.15096.1.3.2.7.3.1	PC Certificats Personals Sector Públic

Certificat d'autenticació de empleat públic amb pseudònim de nivell alt (T-CAT pseudònim autenticació)	1.3.6.1.4.1.15096.1.3.2.4.1.2	PC Certificats Personals Sector Públic
Certificat qualificat de signatura de empleat públic amb pseudònim de nivell alt (T-CAT pseudònim signatura)	1.3.6.1.4.1.15096.1.3.2.4.1.1	PC Certificats Personals Sector Públic
Certificat qualificat d'autenticació i signatura de persona vinculada de nivell alt (T-CAT persona vinculada)	1.3.6.1.4.1.15096.1.3.2.82.1	PC Certificats Personals Sector Públic
Certificat qualificat d'autenticació i signatura de persona vinculada de nivell mitjà (T-CATP persona vinculada)	1.3.6.1.4.1.15096.1.3.2.86.1	PC Certificats Personals Sector Públic
Certificat qualificat d'autenticació i signatura de representant davant les Administracions Públiques (T-CAT representant)	1.3.6.1.4.1.15096.1.3.2.8.1.1	PC Certificats Personals Sector Públic
Certificat qualificat d'autenticació i signatura de treballador públic de nivell alt (T-CAT treballador públic)	1.3.6.1.4.1.15096.1.3.2.82.2	PC Certificats Personals Sector Públic
Certificat qualificat d'autenticació i signatura de treballador públic de nivell mitjà (T-CATP treballador públic)	1.3.6.1.4.1.15096.1.3.2.86.3	PC Certificats Personals Sector Públic
Certificats de Dispositius i Infraestructures		
Certificat d'Aplicació (Dispositiu aplicació)	1.3.6.1.4.1.15096.1.3.2.91.1	PC Dispositius i Infraestructures
Certificat de Segell Electrònic Avançat (Segell nivell mig/substancial)	1.3.6.1.4.1.15096.1.3.2.6.2	PC Dispositius i Infraestructures
Certificat de Seu Electrònic (Seu-e nivell mig/substancial)	1.3.6.1.4.1.15096.1.3.2.5.2	PC Dispositius i Infraestructures
Certificat de Servidor Segur (Dispositiu SSL)	1.3.6.1.4.1.15096.1.3.2.51.1	PC Dispositius i Infraestructures
Certificat de Servidor Segur Extended Validation (Dispositiu SSL EV)	1.3.6.1.4.1.15096.1.3.2.51.2	PC Dispositius i Infraestructures
Certificat de Segell Qualificat de Temps (segell de temps)	1.3.6.1.4.1.15096.1.3.2.111	PC Dispositius i Infraestructures

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

1.3. Entitats participants

1.3.1. Prestador de serveis de confiança

D'acord amb la terminologia del Reglament 910/2014 (UE) núm. relatiu a la identificació electrònica i els serveis de confiança per a les transaccions electròniques al mercat interior, el Consorci AOC actua en el marc d'aquesta DPC com a prestador de serveis de confiança o TSP, sent responsable de l'emissió i gestió dels certificats electrònics generats dins de la jerarquia de certificació (PKI) esmentada anteriorment en aquest document.

1.3.2. Entitat de Certificació Arrel

L'Entitat de Certificació Arrel és l'entitat dins de l'esmentada jerarquia de certificació que emet certificats a altres entitats de certificació i la clau pública de la qual ha estat autofirmada. La seva funció és signar el certificat d'altres Entitats de Certificació pertanyents a aquesta jerarquia de certificació.

Les dades d'identificació del Certificat Arrel de la jerarquia de certificació del Consorci AOC són els següents:

Root CA EC-ACC

CN:	EC-ACC
Hash:	88:49:7F:01:60:2F:31:54:24:6A:E2:8C:4D:5A:EF:10:F1:D8:7E:BB:76:62:6F:4A:E0:B7:F9:5B:A7:96:87:99
Vigència:	07/01/2031
Tipus de clau:	RSA 2048

1.3.3. Entitats de Certificació subordinades

Es denominen Entitats de Certificació Delegades o Subordinades a les entitats dins la jerarquia de certificació que emeten certificats d'entitat final, el certificat de clau pública d'aquests ha estat signat digitalment per l'Entitat de Certificació Arrel.

Les dades d'identificació de les Entitats de Certificació subordinades operades pel Consorci AOC a l'empara d'aquesta DPC són els següents:

CA EC-CIUTADANIA

CN:	EC-Ciutadania
Hash:	0F:D9:9A:AE:1F:FC:D5:D9:F0:AD:76:ED:DD:CB:EF:6B:88:4C:C8:5C:16:BF:CF:A4:B5:24:61:55:D6:59:7E:D6
Vigència:	18/9/2030
Tipus de clau:	RSA 2048

CA EC-SECTORPUBLIC

CN:	EC-SectorPublic
Hash:	35:6A:5F:4D:99:4E:9E:FA:7C:AE:FC:49:17:68:91:1D:65:EC:25:97:74:65:B6:10:E2:F2:9A:A4:47:26:31:C3
Vigència:	18/9/2030
Tipus de clau:	RSA 2048

1.3.4. Entitats de Registre

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

1.3.5. Usuaris finals

Els usuaris finals són les persones que obtenen i utilitzen els certificats electrònics. En concret, es poden distingir els usuaris finals següents:

- Els sol·licitants de certificats.
- Els subscriptors de certificats.
- Els signants o posseïdors de claus.
- Tercer que confia en els certificats.

1.3.5.1. Sol·licitants de certificats

Sol·licitant és la persona física que, en nom propi o en representació d'un tercer, sol·licita l'emissió d'un certificat electrònic.

Els requisits que ha de reunir un sol·licitant dependran del tipus de certificat sol·licitat i estan recollits en la PC aplicable a cada tipus de certificat concret.

1.3.5.2. Subscriptors de certificats

El Subscriptor és la persona física o jurídica que contracta amb el Consorci AOC la prestació dels seus serveis.

En alguns casos, el Subscriptor podrà actuar com a Punt de Verificació Presencial, assumint part de les funcions de registre i responsabilitzant-se, en tal cas, enfront del Consorci AOC, a les seves Entitats de Registre i als Usuaris finals de:

- La correcta identificació dels Sol·licitants de certificats i Signataris respecte els quals actuï com a Punt de Verificació Presencial.
- La veracitat i exactitud de tota la documentació requerida formalment per a cada classe de certificat.
- La compulsa de còpies pel que fa a la presentació de documents originals.
- La custòdia d'aquesta documentació i el lliurament de la mateixa al Consorci AOC en cas de ser requerit per fer-ho.
- Del lliurament de certificats als signants o posseïdors de claus.

1.3.5.3. Posseïdors de claus o signatàries

Els posseïdors de claus o signatàries són les persones físiques que posseeixen de forma exclusiva les claus de signatura o autenticació electròniques dels certificats, ja sigui actuant en el seu propi nom i dret, o bé, en representació d'una organització o mitjançant algun altre tipus de vinculació.
Aquestes persones físiques hauran d'estar degudament identificades en el certificat mitjançant el seu nom i cognoms o mitjançant un pseudònim, havent de també identificar-se, si escau, l'organització corresponent de forma unívoca.
Correspon al signatari o posseïdor de claus la custòdia de les dades de creació de signatura associats al certificat electrònic.

1.3.5.4. Tercer que confia en els certificats

S'entén per tercer que confia en els certificats (en anglès, relying party) a tota persona o organització que voluntàriament confia en un certificat emès sota alguna de les jerarquies de certificació del Consorci AOC.

Les obligacions i responsabilitats del Consorci AOC amb tercers que voluntàriament confiïn en els certificats es limitaran a les recollides en aquesta DPC, en el Reglament (UE) núm. 910/2014 i en la resta de normativa que resulti d'aplicació.

Els tercers que confiïn en aquests certificats han de tenir present les limitacions en el seu ús.

1.4. Ús dels certificats

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

1.4.1. Ús típic dels certificats

Els certificats del Consorci AOC podran usar-se en els termes establerts per les PC.

1.4.2. Usos prohibits

Els certificats només es podran utilitzar dins dels límits d'ús recollits d'una manera expressa en aquesta DPC i en la corresponent PC. Qualsevol altre ús fora dels descrits en els esmentats documents, queda exclòs expressament de l'àmbit contractual i prohibits formalment. Queda expressament prohibit qualsevol ús que sigui contrari a la Llei.

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

Els certificats d'usuari final no poden emprar-se per signar certificats de clau pública de cap tipus, ni signar llistes de revocació de certificats.

1.5. Administració de la Declaració de Pràctiques

1.5.1. Organització que administra l'especificació

Consorci Administració Oberta de Catalunya – Consorci AOC

1.5.2. Dades de contacte de l'organització

Consorci Administració Oberta de Catalunya – Consorci AOC

Domicil social: Via Laietana, 26 – 08003 Barcelona

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

Web del Consorci AOC: www.aoc.cat

Web del servei de certificació digital del Consorci AOC: www.aoc.cat/catcert

Servei d'Atenció a l'Usuari: 900 90 50 90, o +34 93 272 25 01 per trucades des de l'exterior de l'estat, en horari 24x7 per a la gestió de suspensions de certificats.

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

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

1.5.4. Procediment d'aprovació

El sistema documental i d'organització del Consorci AOC garanteix, mitjançant l'existència i l'aplicació dels corresponents procediments, el correcte manteniment de la DPC i de les especificacions del procediment de publicació d'especificacions de servei.

La versió inicial d'aquesta DPC és aprovada per la Comissió Executiva del Consorci AOC, que és l'òrgan col·legiat de direcció executiva del Consorci AOC. El Director Gerent del Consorci AOC és competent per aprovar les successives modificacions d'aquesta DPC.

1.5.5. Freqüència de revisió

La DPC, les diferents PC i els textos divulgatius (en anglès PDS: PKI Disclosure Statements), seran revisades i, si escau, actualitzades anualment. Els documents esmentats seran revisats i modificats quan es produeixi qualsevol canvi que pugui afectar al seu contingut, com poden ser modificacions legislatives, canvis en infraestructura o canvis en l'operativa dels serveis, entre d'altres.

1.6 DEFINICIONS i ACRÒNIMS

1.6.1 Definicions

- Prestador de Serveis de Certificació: persona física o jurídica que expedeix certificats electrònics o presta altres serveis en relació amb la signatura electrònica.
- Prestador de Serveis de Confiança (PSC) : persona física o jurídica que presta un o més serveis de confiança, bé como prestador qualificat o com a prestador no qualificat de serveis de confiança;
- Certificat Electrònic: un document signat electrònicament per un prestador de serveis de confiança que vincula unes dades de verificació de signatura a un signant i confirma la seva identitat.
- Certificat Qualificat: Certificat expedit per un PSC i que compleix els requisits establerts en l'Annex I del RD (UE) núm. 910/2014 en l'article 7 de la llei 6/2020, d'11 de novembre, en quant a la comprovació de la identitat i altres circumstàncies dels sol·licitants i a la fiabilitat i les garanties dels serveis de confiança que presten, de conformmitat amb el Titol III de l'esmentada Llei 6/2020 d'11 de novembre

- Clau Pública i Clau Privada: la criptografia asimètrica en la que es basa la PKI utilitza un parell de claus en la qual el que queda xifrat amb una d'elles només es pot desxifrar amb l'altra i viceversa. A una d'aquestes claus se la denomina pública i queda inclosa en el certificat electrònic, mentres que l'altra es denominada privada i únicament és coneguda pel titular del certificat.

- Conformity Assessment Body: Organismes acreditats pels estats membres per a poder emetre informes de conformitat segons requeriments del Reglament (UE) núm. 910/2014.

- Dades de Creació de Signatura (Clau Privada): Són dades úniques, com codis o claus criptogràfiques privades, que el signant utilitza per a crear la signatura electrònica.

- Dades de Verificació de Signatura (Clau Pública): són les dades, com codis o claus criptogràfiques públique, que s'utilitzen per a verificar la signatura electrònica

- Dispositiu Qualificat de Creació de Signatura / de Segell electrònic (DCCF): Dispositiu de creació de signatures electròniques que compleix els requisits enumerats en l'annex II del Reglament (UE) núm. 910/2014.

- Signatura electrònica: és el conjunt de dades en forma electrònica, consignats junt amb altres o associats amb ells, que poden ser utilitzats com a mitjà d'identificació personal.

- Signatura Electrònica Avançada: és la signatura electrònica que permet establir la identitat personal del signant respecte de les dades signades i comprovar la integritat de les mateixes, per estar vinculada de manera exclusiva tant al signador, com a les dades a les quals fa referència i per haver estat creada per mitjans que manté sota el seu control exclusiu.

- Signatura Electrònica Qualificada: és aquella signatura electrònica avançada basada en un certificat qualificat i generada mitjançant un dispositiu qualificat de creació de signatura.

- Funció Hash: és una operació que es realitza sobre un conjunt de dades de qualsevol mida, de manera que el resultat obtingut és altre conjunt de dades de mida fixa, independentment de la mida original i que té la propietat d'estar associat unívocament a les dades inicials.

- Llistes de Certificats Revocats (LCR o CRL): llista a on figuren les relacions de certificats revocats o suspesos.

- Mòdul Criptogràfic Hardware (HSM): mòdul hardware utilitzat per a realitzar funcions criptogràfique i emmagatzemar claus d'un mode segur.

- Segell de Temps Electrònic: és un tipus especial de signatura electrònica emesa per un tercer de confiança que permet garantir la integritat d'un document en una data i hora determinades.

- Segell Qualificat de Temps Electrònic: és un segell de temps electrònic que compleix els requisits establerts en l'article 42 del Reglament (UE) núm. 910/2014.
- Autoritat de Segellat de Temps (TSA): Entitat de confiança que emet segells de temps.
- Autoritat de Validació (VA): Entitat de confiança de proporciona informació sobre la validesa dels certificats electrònics i de les signatures electròniques.

1.6.2. Acrònims

AOC:	Administració Oberta de Catalunya
CA:	Autoritat de Certificació (Certification Authority)
PC :	Política de Certificació (Certificate Policy)
DPC:	Declaració de Pràctiques de Certificació (Certification Practices Statement)
ETSI:	European Telecommunications Standard Institute
HSM:	Mòdul de seguretat criptogràfic (Hardware Security Module)
IETF:	Internet Engineering Task Force
LDAP:	Lightweight Directory Access Protocol
LRC:	Llista de Certificats Revocats (Certificate Revocation List)
OCSP:	Online Certificate Status Protocol
OID:	Identificador d'objecte únic (Object identifier)
PDS	Text de Divulgació (PKI Disclosure Statement)
PKI:	Infraestructura de Clau Pública (Public Key Infrastructure)
PSC:	Prestador de Serveis de Confiança

2. Publicació d'informació i directori de certificats

2.1. Directori de certificats

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

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

L'Entitat de Certificació publica les informacions següents al seu web (http://www.aoc.cat/catcert/regulacio):

- Les llistes de revocació de certificats (LRC) i altres informacions d'estat de revocació dels certificats.
- Els perfils dels certificats i de les llistes de revocació dels certificats.
- La DPC.
- Les PC aplicables a cada tipus de certificat.
- El text divulgatiu per a certificats electrònics.

Qualsevol canvi en les especificacions o en les condicions del servei es comunica als usuaris per l'Entitat de Certificació a través del directori.

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

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

2.3. Freqüència de publicació

La informació de l'Entitat de Certificació es publica quan es troba disponible i especialment, de forma immediata quan s'emeten les mencions relatives a la vigència dels certificats.

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

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

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

La informació d'estat de revocació de certificats es publica d'acord amb l'establert en la secció 4.10.7.

2.4. Control d'accés

La DPC, les PC, els Textos divulgatius (en anglès PDS: PKI Disclosure Statements), els certificats d'EC i les LRC es publiquen en repositoris d'accés públic sense control d'accés.

3. Identificació i autenticació

3.1. Gestió de nom

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

3.1.1. Tipus de noms

3.1.1.1. Estructura sintàctica

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

L'estructura sintàctica i el contingut dels camps de cada certificat, així com el seu significat semàntic, es troben descrits en el document “perfil de certificat” corresponent que el Consorci AOC publica al seu web (http://www.aoc.cat/catcert/regulacio).

3.1.1.2. Perfils dels certificats

Els perfils dels certificats emesos es publiquen al web del Consorci AOC (http://www.aoc.cat/catcert/regulacio).

3.1.2. Significat dels noms

Sense estipulació.

3.1.3. Utilització de pseudònims

El possible ús de pseudònims es regularà en la corresponent PC.

3.1.4. Interpretació de formats de noms

El Consorci AOC aten en tot cas al marcat per l'estàndard X.500 de referència en la ISO/IEC 9594, així com per la RFC 5280 i pels Requeriments de CA/Browser-Forum (Baseline Requirements i EV Guidelines).

3.1.5. Unicitat dels noms

L'Entitat de Certificació emet diferents tipus de certificats. Els noms dels subscriptors de certificats són únics per a cada servei de generació de certificats operat per l'Entitat de Certificació i per a cada tipus de certificat, és a dir, una mateixa persona només pot tenir al seu nom certificats de tipus diferents emesos per l'Entitat de Certificació. L'atribut de CIF o NIF s'usa per distingir entre dues identitats quan existeixi algun problema de duplicitat de noms.

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

Tot el personal vinculat a l'Entitat de Registre té com a requisit imprescindible l'assistència al curs de formació d'Entitats de Registre impartit per l'Entitat de Certificació.

3.1.6. Seqüència i freqüència de rotació laboral

Sense estipulació.

3.1.7. Resolució de conflictes relatius a noms

El Consorci AOC no arbitrarà davant possibles disputes de noms, ni tindrà responsabilitat sobre aquest tema. L'assignació de noms es realitzarà basant-se en l'ordre d'entrada. Referent al tractament de marques registrades, veure l'apartat 9.5.3.

3.2. Validació inicial de la identitat

3.2.1. Prova de possessió de clau privada

Quan s'expedeix un certificat en un dispositiu hardware, la clau privada es crea en l'instant previ a la generació del certificat, mitjançant un procediment que garanteix la seva confidencialitat i la seva vinculació amb la identitat del sol·licitant.

Cada Entitat de Registre és responsable de garantir el lliurament o l'accés al dispositiu al sol·licitant de forma segura. En els altres casos, el mètode de prova de la possessió de la clau privada pel subscriptor serà el lliurament de PKCS#10 o una prova criptogràfica equivalent o un altre mètode aprovat pel Consorci AOC.

3.2.2. Autenticació de la identitat d'una organització

L'Entitat de Registre haurà de verificar les següents dades per poder autenticar la identitat de l'organització:

- Les dades relatives a la denominació o raó social de l'organització.
- Les dades relatives a la constitució, i personalitat jurídica del subscriptor.
- Les dades relatives a l'extensió i vigència de les facultats de representació del sol·licitant.
- Les dades relatives al codi d'identificació fiscal de l'organització o codi equivalent.

El Consorci AOC es reserva el dret de no emetre el certificat si considera que la documentació aportada no és suficient o adequada per a la comprovació de les dades anteriorment citades.

3.2.2.1. Entitats de Registre

L'Entitat de Certificació autentica, prèviament a l'emissió i al lliurament d'un certificat certificat, per a qualsevol dels components d'una Entitat de Registre, la identitat de l'Entitat de Registre i de l'operador conforme a la secció corresponent d'aquesta DPC.

3.2.3. Autenticació de la identitat d'una persona física

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

3.2.3.1. Elements d'identificació

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

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

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

3.2.3.2. Validació dels elements d'identificació

Sense estipulació addicional.

3.2.3.3. Necessitat de presència personal

La identificació de la persona física que hagi d'obtenir un certificat qualificat (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.
- Es podrà emprar el mètode d'identificació per videoconferència només en aquells casos permesos per la legislació espanyola i conforme a l'article article 24.1.d) del Reglament (UE) núm. 910/2014 La vigència dels certificat emesos a través d'aquest mètode d'identificació i l'ús dels mateixos quedarà limitat segons el que s'estableix per la legislació vigent a cada moment.

Abans de l'emissió i lliurament 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 de lliurament i acceptació del certificat, aprofitant per validar la identitat de la persona que serà posseïdora de la clau privada corresponent al certificat que es lliura.

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 hagi transcorregut més de cinc anys des de la identificació amb presència personal.

En el cas dels certificats per a la ciutadania es pot prescindir de la personació si la signatura continguda en la sol·licitud d'expedició d'un certificat ha estat legitimada notarialment i en els casos previstos en l'article 24 del Reglament (UE) núm. 910/2014. Però aquesta DPC no dóna suport a aquest mecanisme a causa de la inexistència d'un procediment a aquest efecte per part dels notaris.

3.2.3.4. Vinculació de la persona física amb l'organització

Es regula de manera diferenciada en cadascuna de les Polítiques de Certificació vigents per a cada tipus de Certificat.

3.2.4. Validació del domini

Per garantir que una entitat sol·licitant té control sobre el domini (URL) que sol·licita incloure en un certificat es realitzen els següents tipus de comprovacions:

- **Organitzacionals**: se sol·licita la titularitat del nom de domini, certificada per un representant legal de l'organització, a més del nom de la persona jurídica a la qual s'expedeixi el certificat i, quan escaigui, el nombre de registre, tal com es recullin en els registres oficials.

- **Tècniques**: es consulten els següents serveis whois autenticats:
    - Per a dominis "*.es": https://www.nic.es/sgnd/dominio/publicInformacionDominios.action
    - Per a la resta de dominis:

      Consultar en http://www.iana.org/domains/root/db/ quin és el servidor WHOIS autoritzat per buscar informació sobre el domini, depenent del domini d'alt nivell (TLD), és a dir, depenent de si el domini acaba en .com, .org, .net, ...
- **Validació del registre del domini**: s'envia un correu electrònic a l'adreça del registrant del domini i/o a una adreça construïda per "admin", "administrator", "webmaster", "hostmaster" o "postmaster" seguit de @ i el nom de domini d'autorització, amb un número aleatori únic al que han de contestar en un termini màxim de 30 dies.

3.2.5. Informació no verificada

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

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

Tota la informació dels certificats SSL està verificada prèviament a l'emissió dels mateixos contrastant amb fonts d'iformació independents.

3.2.6 Criteris d'interoperabilitat

Sense estipulació.

3.3. Identificació i autenticació de sol·licituds de renovació

3.3.1. Validació per a la renovació de certificats

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

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

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

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

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

4.1. Sol·licitud d'emissió de certificat

4.1.1. Legitimació per sol·licitar l'emissió

Els requisits que ha de reunir un sol·licitant dependran del tipus de certificat sol·licitat i es recolliran en la PC de cada tipus de certificat concret.

4.1.2. Procediment d'alta; Responsabilitats

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

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

4.2. Processament de la sol·licitud de certificació

Els requisits que ha de reunir una sol·licitud de certificació dependran del tipus de certificat sol·licitat i es recolliran en la PC de cada tipus de certificat concret.

4.3. Emissió de certificat

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

Per a cada sol·licitud de certificat tramitada, l'Entitat de Certificació:

- Utilitza un procediment de generació de certificats X.509 v3 que vincula de forma segura el certificat amb la informació de registre, incloent la clau pública certificada, mitjançant la signatura electrònica de l'Entitat de Certificació.
- Protegeix la confidencialitat i la integritat de les dades de registre.
- Inclou als certificats personals les informacions establertes a la legislació aplicable que es descriu en 9.15 Conformitat amb la llei aplicable.

- Compleix les obligacions establertes a la legislació corresponent, en la generació de certificats qualificats.
- Compleix els controls establerts per aquesta DPC.

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

4.3.2. Comunicació de l'emissió al subscriptor

L'Entitat de Certificació comunica al subscriptor l'emissió del certificat, o la incidència corresponent. Així mateix, s'indicarà la disponibilitat del certificat i la forma d'obtenir-lo.

4.4. Acceptació del certificat

4.4.1. Responsabilitats del Prestador de Serveis de Confiança

L'Entitat de Certificació (o PSC):

- Si no ho ha fet abans, i quan resulti necessari, acreditarà la identitat del subscriptor.
- Proporcionarà al subscriptor accés al certificat.
- Lliurarà, si escau, el dispositiu criptogràfic de signatura, verificació de signatura, xifrat i desxifrat.
- Proporcionarà la informació següent:
    - Informació bàsica sobre la política i l'ús del certificat, incloent especialment informació sobre l'Entitat de Certificació Vinculada i la DPC aplicable, així com les seves obligacions, facultats i responsabilitats.
    - Informació sobre el certificat i el dispositiu criptogràfic.
    - Reconeixement del posseïdor de rebre el certificat i, si escau, el dispositiu criptogràfic, i acceptació dels esmentats elements.
    - Obligacions del posseïdor de claus.
    - Responsabilitat de posseïdor de claus.
    - Mètode d'imputació exclusiva al posseïdor de la seva clau privada i de les seves dades d'activació del certificat i, si escau, del dispositiu criptogràfic, d'acord amb l'establert a les seccions corresponents d'aquesta política.
    - La data de l'acte de lliurament i acceptació.

4.4.2. Conducta que constitueix acceptació del certificat

El certificat es pot acceptar mitjançant la signatura del full de posseïdor o responsable de la custòdia de claus.

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

4.4.3. Publicació del certificat

Els certificats es poden publicar si es disposa del consentiment exprés de les persones físiques, les dades de les quals constin en els citats certificats.

4.4.4. Notificació de l'emissió a tercers

Sense estipulació.

4.5. Ús del parell de claus i del certificat

4.5.1. Ús per part dels posseïdors de claus

Sense estipulació.

4.5.2. Ús pel tercer que confia en certificats

Sense estipulació.

4.6. Renovació de certificats sense renovació de claus

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

4.7. Renovació de certificats amb renovació de claus

La renovació d'un certificat s'inicia 2 (dos) mesos abans de la data d'expiració del certificat, quan el subscriptor rep un correu electrònic on se li informa dels passos a seguir per executar la renovació del certificat. Aquest correu es torna a enviar 30 (trenta) dies abans de l'expiració.

El procés per a la renovació d'un certificat és el mateix que se segueix per a 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 continuïn sent vàlides i, si ha canviat alguna dada, aquest haurà de ser verificat, 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 DPC.

En qualsevol cas, si han passat més de cinc anys des de l'última vegada que el subscriptor es va identificar presencialment en una oficina d'Entitat de Registre, haurà de personar-se de nou per dur 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.

Per a 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

L'Entitat de Certificació permet la renovació telemàtica de certificats digitals - a partir d'una autenticació segura i la corresponent signatura electrònica del full de lliurament 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 últims mesos de vigència - sempre que no hagin transcorregut més de cinc anys des de l'última 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. Amb caràcter general, 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.ej 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 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

4.10.1. Causes de revocació de certificats

L'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 per a l'expedició del certificat.
    - Descobriment que alguna de les dades contingudes en el certificat és incorrecte.
2. Circumstàncies que afecten a la seguretat de la clau o del certificat
    - Compromís de la clau privada o de la infraestructura o sistema de l'Entitat de Certificació que va emetre el certificat, sempre que afecti a 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 PC 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.
- La CA coneix un mètode comprovat que pot calcular fàcilment la clau privada del subscriptor en funció de la clau pública en el certificat.

3. Circumstàncies que afectin a 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 al 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 per a la seva sol·licitud.
    - Infracció, per part del posseïdor de claus, de les seves obligacions, responsabilitat i garanties, establertes en l'instrument jurídic corresponent o a la Declaració de Pràctiques de Certificació de l'Entitat de Certificació Vinculada que li va emetre el certificat o a les seves Polítiques de Certificació associades.
    - 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 l'establert en la secció 3.4 d'aquesta declaració.
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 del Text Divulgatiu per a certificats electrònics o d'altres especificacions establertes en la documentació jurídica operativa.
- L'Entitat de Certificació cessa activitats que donen suport a la revocació de certificats Extended Validation. Si l'Entitat de Certificació pot garantir el manteniment dels serveis de validació LRC i OCSP (protocol de comprovació de l'estat d'un certificat en línia, en anglès Online Certificate Status Protocol), 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 per a víctimes de phishing o “activitats d'enginyeria inversa”)

6. Altres circumstàncies
    - La suspensió del certificat electrònic per un període superior a 120 dies.
    - La finalització del servei de l'Entitat de Certificació Vinculada.
    - La finalització de la prestació de servei per part de l'Entitat de Certificació.
    - Resolució judicial o administrativa que ho ordeni.
    - Compliment del que es preveu en les disposicions legals vigents.
    - En cas de certificats SSL, per qualsevol de les causes establertes en els Requerimentos Bàsics del CA Browser Forum (Baseline Requirements) i en les Guies dels certificats EV (EV Guidelines) del CAB-Forum i en els temps establerts per cada causa.
    - Qualsevol circumstància establerta en les Política de certificat de Mozilla (Mozilla Root Store Policy)

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 per determinar la revocació d'un certificat, però té indicis del seu compromís, pot decidir la suspensió.

4.10.2. Legitimació per sol·licitar la revocació

Podran sol·licitar la revocació d'un certificat:

- En cas de certificats individuals, el subscriptor a nom de qui es va emetre el certificat.
- En cas de certificats corporatius, la persona autoritzada a aquest efecte per a l'entitat subscriptora; en ocasions, a instàncies 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 sol·licitud de revocació ha de ser enviada telemàticament. Excepcionalment, en cas d'indisponibilitat del canal telemàtic, es podrà enviar per correu electrònic signat o per correu certificat convencional. S'ha d'incloure la informació suficient per poder identificar raonablement, en criteri de l'Entitat de Certificació, d'una banda, el certificat que se sol·licita revocar i, per una altra, l'autenticitat i autoritat del sol·licitant. El procediment detallat es troba al web del Consorci AOC.

Aquesta informació suficient ha d'estar formada per les dades de contacte del posseïdor de claus, inclòs el seu DNI o equivalent i de l'entitat que demana la revocació, la data i la raó de la petició, així com el nombre de sèrie del certificat.
Qui faci la sol·licitud de revocació pot demanar a l'Entitat de Registre més informació sobre aquest procediment.

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

Les Entitats de Registre atenen les sol·licituds de revocació dins 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 Servei d'Atenció a l'Usuari de l'Entitat de Certificació, l'horari d'atenció és 24x365. Les dades de contacte del Servei d'Atenció a l'Usuari es desciuren al punt "1.5.2. Dades de contacte de l'organització" d'aquest document.

L'acció de revocació la duu a terme un dels operadors de l'Entitat de Registre, qui accedeix a l'aplicació web a aquest efecte, autenticant-se mitjançant un certificat digital emès per l'Entitat de Certificació.

Una vegada registrat el canvi d'estat del certificat en el sistema de l'Entitat de Certificació, de forma automàtica i com més aviat millor, es genera i publica una nova LRC en la qual constarà la referència d'aquest certificat.

S'informa al subscriptor i, si escau, al posseïdor de claus, sobre el canvi d'estat del certificat, d'acord amb la legislació aplicable.

4.10.4. Termini temporal de sol·licitud de revocació

Les sol·licituds de revocació s'han de remetre en 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 de l'Entitat de Certificació d'acord amb el procediment definit al web 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 DPC.

Quan la sol·licitud de revocació hagi estat remesa a una Entitat de Registre, aquesta podrà, una vegada 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 també. Quan es tracti de certificats corporatius, al subscriptor.

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

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

Per verificar l'estat dels certificats ha de consultar-se LRC 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 qual 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 LRC i serveis OCSP) s'indiquen en el contingut dels certificats que emeten.

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

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

L'Entitat de Certificació Arrel emetrà una Llista d'Entitats de Certificació Revocades (en anglès Authority Revocation List, ARL) com a mínim cada sis mesos, o extraordinàriament, quan es produeixi la revocació d'un certificat d'autoritat.

Cada Entitat de Certificació Subordinada emetrà una LRC L diàriament, i de forma extraordinària, cada vegada que se suspengui o es revoqui un certificat.

4.10.8. Període màxim de publicació de LRCs

Una vegada generades, les noves versions de les LRCs 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 electrònics poden consultar el servei en línia que respongui sobre l'estat de certificats (servei *OCSP Responder*, de consulta d'estat de certificats en línia, o altres serveis de validació de certificats) operat per un prestador de serveis de validació en el qual es confia.

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

La URL en la 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 en http://www.aoc.cat/catcert/regulacio.

En cas de cessament de l'activitat i/o compromís de claus de l'EC, es generarà una última LRC que es mantindrà íntegra i disponible per a la seva consulta garantint la disponibilitat del servei d'informació sobre l'estat dels certificats, durant almenys 15 anys des de la seva publicació.

La provisió de la informació sobre l'estat de revocació dels Certificats, en cas de cessament d'activitat del Consorci AOC com a PSC, queda garantida mitjançant la transferència, a l'organisme supervisor o a un altre Prestador amb el qual s'arribi al corresponent acord, de tota la informació relativa als Certificats i, especialment, de les dades del seu estat de revocació.

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 quals desitgin confiar, encara que no s'estipula obligació alguna referent al mecanisme utilitzat per a la comprovació d'aquest estat.

4.10.11. Altres formes d'informació de revocació de certificats

Sense estipulació.

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, el més aviat possible, a tots els participants en la jerarquia pública de certificació de Catalunya, com a mínim mitjançant la inclusió en la LRC corresponent de la referència al certificat electrònic d'aquesta Entitat de Certificació.

Addicionalment, les Terceres parts poden utilitzar els següents mètodes per a demostra un possible compromís de claus:

- Enviar un CSR signat, la clau privada que ha estat comprometida o altra resposta de desafiament signada per la Clau Privada esmentada i verificable per la clau pública.
- Proporcionar referències a fonts d'incidents de seguretat i o vulnerabilitat per les quals el compromís sigui verificable.
- Enviar binaris que contenen una clau privada compromesa, inclós el mètode per a extraure la clau privada.

Les terceres parts notificaran l'esmentat compromís a la CA a través del correo electrònic per a notificació d'incidències: **incident_pki@aoc.cat**

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 la normativa sobre signatura electrònica i serveis de confiança digital que resulti d'aplicació i, en tot cas, quan 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 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 per confirmar el seu compromís.

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

- Certificat de Servidor Segur (Dispositiu SSL)
- Certificat de Servidor Segur *Extended Validation* (Dispositiu SSL EV)
- Certificat de Seu Electrònica (Seu-e nivell mig/substancial)

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 ha sol·licitat la posterior habilitació, passarà automàticament a estat revocat.

Per dur 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, perquè 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 personals del sector públic, 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 el seu nom.
- 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. Procediments 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 de l'Entitat de Certificació.
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 de l'Entitat de Certificació.
3. La suspensió pot ser sol·licitada per l'Entitat de Registre. En cas que l'Entitat de Registre disposi de l'autorització de l'Entitat de Certificació, pot realitzar ella mateixa el procés de suspensió. En cas contrari, realitza la tramitació de la suspensió a través de l'Entitat de Certificació.

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 a de suspendre el certificat electrònic.
- Document identificatiu del posseïdor de claus a qui se li ha de suspendre el certificat electrònic.

- Número de sèrie (*serialNumber*) del certificat electrònic que se sol·licita suspendre.
- Raó detallada per a la petició de suspensió.
- Codi de suspensió associat al certificat o, per defecte, pregunta i resposta secreta escollida al moment d'activar el certificat.
- Quan es tracta 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 sol·licita la suspensió.
    - Organisme i departament al que està vinculat el posseïdor de claus.

Una vegada suspesa la vigència d'un certificat, s'informarà al subscriptor i, si escau, al posseïdor de claus, sobre el canvi d'estat de suspensió i també que el termini màxim serà de 120 (cent vint) dies naturals.

4.10.17. Període màxim de suspensió

El termini màxim de suspensió serà de 120 (cent vint) dies naturals.

4.10.18. Habilitació d'un certificat suspès

Per 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 per deixar constància que s'ha extingit el motiu que va provocar la suspensió.

4.10.19. Període de validesa dels certificats

El període de validesa serà el que s'indiqui en el propi certificat, amb un màxim de 5 anys.

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.

4.11.2. Disponibilitat dels serveis

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

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

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

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 per assegurar que aquest servei es manté inactiu el mínim temps possible.

4.11.3. Altres funcions dels serveis

Sense estipulació.

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

La possibilitat que l'Entitat de Certificació o PSC ofereixi el servei de dipòsit i recuperació de claus pel que fa a una o diverses categories de certificats haurà de constar, en cas que aquesta opció sigui possible, en la corresponent PC . En la mateixa serà necessari detallar, almenys, els següents aspectes:

a. Qui pot sol·licitar el dipòsit i la recuperació de claus

b. Com es tramitarà la sol·licitud

c. Els requisits de confirmació de sol·licituds

d. Els mecanismes utilitzats per dipositar i recuperar claus

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

Sense estipulació.

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

L'Entitat de Certificació s'assegura de l'aplicació dels procediments administratius i de gestió adequats conformes amb els estàndards reconeguts i, en particular:

a. Es realitza una anàlisi de gestió de risc per avaluar les mesures necessàries de seguretat.

b. S'és responsable per la provisió dels serveis de forma segura, fins i tot quan una part dels mateixos sigui subcontractada. Les responsabilitats de tercers es defineixen i s'han d'implantar els controls jurídics necessaris per garantir que els tercers compleixen les seves obligacions amb un nivell de seguretat equivalent.

c. S'estableixen les normes principals en matèria de seguretat mitjançant un òrgan d'alt nivell que defineix la política de seguretat de la informació de l'Entitat i dóna la publicitat necessària mitjançant accions de comunicació interna.

d. Es manté a tot moment la infraestructura necessària per gestionar la seguretat de les operacions. Qualsevol canvi que tingui impacte en el nivell de seguretat ha de ser aprovat per l'òrgan referit al punt anterior.

e. Es documenten, implanten i mantenen els controls de seguretat i procediments d'operació de les instal·lacions, els sistemes i els actius d'informació en què es sustenta la prestació dels serveis.

f. En cas de subcontractació total dels serveis, es garanteix el manteniment del nivell necessari de seguretat de la informació.

5.1. Controls de seguretat física

5.1.1. Àrees segures

L'Entitat de Certificació disposa d'instal·lacions que protegeixen 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'aconsegueix mitjançant la creació de perímetres de seguretat clarament definits entorn dels serveis de generació de certificats, de dispositius criptogràfics i de gestió de revocació. La part de les instal·lacions compartida amb altres organitzacions es troba fora d'aquests perímetres.

5.1.2. Controls de seguretat física

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

- Controls d'accés físic.

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

5.1.3. Localització i construcció de les instal·lacions

La localització de les instal·lacions permet la presència de forces de seguretat en un termini de temps raonablement immediat des del moment en què els hi notifica una incidència.

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

5.1.4. Accés físic

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

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

Aquesta identificació, davant el sistema de control d'accessos, es realitza mitjançant reconeixement d'algun paràmetre biomètric de l'individu, excepte en cas de visites escortades.

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

5.1.5. Electricitat i aire condicionat

Els equips informàtics de l'Entitat de Certificació estan protegits convenientment davant fluctuacions o talls de subministrament elèctric que puguin danyar-los o interrompre el servei.
Les instal·lacions compten amb un sistema d'estabilització del corrent, així com d'un sistema de generació propi amb autonomia suficient per mantenir el subministrament durant el temps que requereixi el tancament ordenat i complet de tots els sistemes informàtics.

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

5.1.6. Exposició a l'aigua

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

5.1.7. Advertiment i protecció d'incendis

Totes les instal·lacions i actius de l'Entitat de Certificació compten 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 a la resta de la instal·lació per a la protecció davant el foc.

5.1.8. Emmagatzematge de suports

L'ús de suports extraïbles està minimitzat i restringit únicament a moviment d'arxius entre sistemes mitjançant dispositius pendrive USB. Per garantir tant la integritat com la confidencialitat els suports extraïbles es guardaran en una caixa forta a la mateixa sala.

5.1.9. Tractament de residus

L'eliminació de suports, tant paper com magnètics, es realitza mitjançant mecanismes que garanteixen la impossibilitat de recuperació de la informació.
En el cas de suports magnètics, es procedeix al format, esborrat permanent o destrucció física del suport.
En el cas de documentació en paper, aquest se sotmet a un tractament físic de destrucció.

5.1.10. Còpia de seguretat fora de les instal·lacions

Es realitzen còpies de seguretat dels sistemes d'informació en dependències físicament separades d'aquelles en les quals es troben els equips.
Les còpies de seguretat es faran online en el sistema de contingència, un CPD alternatiu, a través de comunicacions xifrades.

5.2. Controls de procediments

L'Entitat de Certificació garanteix que els seus sistemes s'operen de forma segura i, per això, estableix i implanta procediments per a les funcions que afecten la provisió dels seus serveis.
El personal al servei de l'Entitat de Certificació realitza els procediments administratius i de gestió d'acord amb la política de seguretat de l'Entitat de Certificació.

5.2.1. Funcions fiables

Les persones que ocupen aquests llocs són nomenades formalment per l'alta direcció de l'Entitat de Certificació.

Les funcions fiables inclouen:

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

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

- Responsable de seguretat (Security Officer): Manté la responsabilitat global sobre l'administració i la implementació de les polítiques i procediments de seguretat.
- 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.
- Responsable de revocació (Revocation Officers): Responsable de realitzar els canvis en l'estat d'un certificat.
- Administradors del sistema de certificació (System Administrator): Autoritzat per realitzar canvis en la configuració del sistema, però sense accés a les dades del mateix.
- Operadors de sistemes (System Operators): Responsables de la gestió del dia a dia del sistema (Monitoreig, backup, recovery…)
- Auditor intern (System Auditors): Autoritzat a accedir als logs del sistema i verificar els procediments que es realitzen sobre el mateix.
- Operador d'EC - Operador de Certificació: Responsables d'activar les claus de l'EC en l'entorn Online, o dels processos de signatura de certificats i LRC's en l'entorn Root Offline.

5.2.2. Número de persones per tasca

L'Entitat de Certificació garanteix almenys dues persones per a fer les tasques que requereixen control multipersona i que es detallen a continuació:

- La generació de la clau de les EC's.
- La recuperació i back-up de la clau privada de les EC's.
- L'emissió de certificats de les EC's.
- Activació de la clau privada de les EC's.
- Qualsevol activitat realitzada sobre els recursos maquinari i programari que donen suport a la root EC.

5.2.3. Identificació i autenticació per a cada funció

L'Entitat de Certificació identifica i autentica al personal abans d'accedir a la corresponent funció fiable.

5.2.4. Rols que requereixen separació de tasques

L'Entitat de Certificació identifica, a la seva política de seguretat, funcions o rols fiables.

Les funcions fiables inclouen:

a. Oficial de Seguretat
b. Operador de registre
c. Administradors del sistema
d. Operadors del sistema
e. Auditors del sistema
f. Qualsevol altra persona amb accés a dades de caràcter personal

Les esmentades restriccions s'apliquen en tot cas a:

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

Les descripcions de rols 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. Per determinar la sensibilitat de la funció, es tindran en compte els següents elements:

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

Les esmentades restriccions s'apliquen en tot cas a:

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

5.3. Controls de personal

L'Entitat de Certificació té en compte els aspectes següents:

- Es manté confidencialitat de la informació, posant els mitjans necessaris i mantenint una actitud adequada en el desenvolupament de les seves funcions i, fora de l'àmbit laboral, en allò referent a la seguretat de les infraestructures.

- S'és diligent i responsable en el tractament, el manteniment i la custòdia dels actius de la infraestructura identificats en la política, en els plans de seguretat o en aquesta DPC.
- No es revela informació no pública fora de l'àmbit de la infraestructura, ni s'extreuen suports d'informació a nivells de seguretat inferiors.
- Es reporta al Responsable de Seguretat, el més aviat possible, qualsevol incident que es consideri que afecta la seguretat de la infraestructura o limita la qualitat del servei.
- S'utilitzen els actius de la infraestructura per a les finalitats per les quals han estat encomanades.
- S'exigeixen manuals o guies d'usuari dels sistemes que utilitza, que permetin desenvolupar la seva funció correctament.
- S'exigeix documentació escrita que marqui les seves funcions i les mesures de seguretat al fet que està sotmès.
- El responsable de seguretat vetlla perquè el punt anterior sigui executat i proveeix als responsables d'àrea de tota la informació que sigui necessària.
- No s'instal·la, en cap dels sistemes de la infraestructura, software o hardware que no sigui expressament autoritzat per escrit pel responsable de sistemes d'informació.
- No s'accedeix voluntàriament ni s'elimina o altera informació no destinada a la seva persona o perfil professional.

El personal afectat per aquesta normativa és:

- El Responsable del Servei.
- El Responsable de l'Entitat de Certificació.
- El Responsable de Seguretat.
- El Responsable d'Operacions.
- L'Equip tècnic d'administració, operació explotació.
- Els Administradors de la Xarxa.
- Els Usuaris de l'Entitat de Certificació.

L'Entitat de Certificació, a més, es veu afectada pel següent personal:

- qui fa les peticions dels certificats.
- qui fa l'aprovació i la validació de les peticions de certificats.
- qui fa la generació / personalització de certificats.
- qui custodia les claus o els tokens criptogràfics.
- qui custodia les claus o les combinacions de seguretat d'accés a la sala d'operacions.

- qui accedeix a informació classificada.
- el personal de comunicacions i d'operacions.
- el personal de seguretat (física i lògica) involucrat en l'operació.
- el responsable del servei.

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

L'Entitat de Certificació és ocupada per personal qualificat i amb l'experiència necessària per a la prestació dels serveis oferts, en l'àmbit de la signatura electrònica i els procediments de seguretat i de gestió adequada.

Aquest requisit s'aplicarà al personal de gestió de l'Entitat de Certificació, especialment en relació amb procediments de personal de seguretat.
La qualificació i l'experiència es poden suplir mitjançant una formació i un entrenament apropiats.
El personal en rols de confiança es troba lliure d'interessos personals que entrin en conflicte amb el desenvolupament de la funció que tingui encomanada.

Els especialistes de validació per a emissió de certificats d'autenticació web hauran de complir els requisits previs de formació i qualificació establerts en l'apartat 14.1.2 dels EV Guidelines i l'apartat 5.3.3 dels Baseline Requirements del CA/Browser Forum

5.3.2. Requisits de formació

L'Entitat de Certificació forma el personal en rols de confiança i de gestió fins que aconsegueixen la qualificació necessària.

La formació inclou els continguts següents:

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

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

5.3.3. Requisits i freqüència d'actualització formativa

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

Es realitzaran actualitzacions amb una freqüència anual, excepte per modificacions en la DPC, que seran notificades a mesura que siguin aprovades.

5.3.4. Sancions per accions no autoritzades

L'Entitat de Certificació disposa d'un sistema sancionador per depurar les responsabilitats derivades d'accions no autoritzades.
Les accions disciplinàries inclouen la suspensió i l'acomiadament de la persona responsable de l'acció danyosa.

5.3.5. Requisits de contractació de professionals

L'Entitat de Certificació contracta professionals per a qualsevol funció, fins i tot per a un rol de confiança. En aquest cas, se sotmet als mateixos controls que els empleats restants.
En cas que el professional no hagi de sotmetre's a aquests controls, estarà constantment acompanyat per un empleat de confiança.
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 d'aquesta DPC, són aplicats i completats pel tercer que realitza les funcions d'operació dels serveis de certificació. El Consorci AOC és responsable, en tot cas, de l'efectiva execució.
Aquests aspectes queden concretats en l'instrument jurídic utilitzat per acordar la prestació dels serveis de certificació pel tercer diferent del l'Entitat de Certificació.

5.3.6. Subministrament de documentació al personal

L'Entitat de Certificació subministrarà la documentació que necessita estrictament el seu personal en cada moment, amb la finalitat que pugui desenvolupar de forma competent les seves funcions.

5.4. Procediments d'auditoria de seguretat

5.4.1. Tipus d'esdeveniments registrats

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

- L'encesa i l'apagat dels sistemes.
- L'inici i la finalització de l'aplicació d'Entitat (tècnica) de certificació.
- Els intents de crear, esborrar, canviar contrasenyes o permisos dels usuaris dins del sistema.
- Els canvis en les claus de l'Entitat (tècnica) de certificat.

- Els canvis en les polítiques d'emissió de certificats.
- Els intents d'entrada i de sortida del sistema.
- Els intents no autoritzats d'entrada a la xarxa de l'Entitat de Certificació.
- Els intents no autoritzats d'accés als fitxers del sistema
- La generació de les claus de l'Entitat de Certificació.
- Els 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, una emissió, una revocació i una renovació d'un certificat.
- Esdeveniments relacionats amb el cicle de vida del mòdul criptogràfic, com a recepció, ús i desinstal·lació d'aquest.

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

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

5.4.2. Freqüència de tractament de registres d'auditoria

Els registres d'auditoria s'examinen almenys una vegada a la setmana per buscar 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 recerca més profunda de qualsevol alerta o irregularitat en els registres. Les accions realitzades a partir de la revisió d'auditoria també estan documentades.

5.4.3. Període de conservació de registres d'auditoria

Els registres d'auditoria es retenen durant almenys 2 (dos) mesos després de processar-los i a partir d'aquell moment s'arxiven d'acord amb la secció 5.5 d'aquesta DPC.

5.4.4. Protecció dels registres d'auditoria

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

5.4.5. Procediments de còpia de seguretat

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

Per conservar correctament les còpies de seguretat realitzades, l'Entitat de Certificació té adoptades, com a mínim, les mesures de seguretat següents:

- S'emmagatzemen en armaris ignífugs.
- Només persones autoritzades disposen d'accés a les còpies de seguretat.
- Les còpies estan identificades.
- Si un material ha contingut còpies de seguretat (disquets, DVD's...) i es volen reutilitzar s'assegura que les dades que ha contingut estiguin completament esborrats fent impossible la seva recuperació.
- S'autoritza expressament l'extracció de les còpies de seguretat fora de l'Entitat de Registre, omplint una fitxa al respecte i anotant el corresponent detall en un llibre de registre.
- Es procura anar dipositant còpies de seguretat periòdicament fora de l'Entitat de Registre.

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

El sistema d'acumulació de registres d'auditoria és, almenys, un sistema intern de l'Entitat de Certificació, compost pels registres de l'aplicació, pels registres de xarxa, pels registres del sistema operatiu i per les dades manualment generades, que emmagatzemarà el personal degudament autoritzat.

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

Quan el sistema d'acumulació de registres d'auditoria registra un esdeveniment, no és necessari enviar una notificació a l'individu, organització, dispositiu o aplicació que va causar l'esdeveniment.
Es comunica si el resultat de la seva acció ha tingut èxit o no, però no que s'ha auditat l'acció.

5.4.8. Anàlisi de vulnerabilitats

Els esdeveniments en el procés d'auditoria es guarden, entre d'altres raons, per monitoritzar les vulnerabilitats del sistema.

Es realitzen anàlisi de vulnerabilitats internes almenys trimestralment i externes almenys anualment.

5.5. Arxiu d'informacions

L'Entitat de Certificació garanteix que tota la informació relativa als certificats es guarda durant un període de temps apropiat, segons l'establert en la secció 5.5.2 d'aquesta DPC.

5.5.1. Tipus d'esdeveniments registrats

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

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

Així mateix, haurà de conservar els següents documents originals:

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

5.5.2. Període de conservació de registres

L'Entitat de Certificació guardarà els registres especificats a la secció 5.5.1 d'aquesta DPC durant, almenys, 15 (quinze) anys, des de l'extinció del certificat o la finalització del servei prestat.

Tota la informació relativa als Certificats d'Infraestructura es guarda de forma permanent.

5.5.3. Protecció de l'arxiu

L'Entitat de Certificació assegura la correcta protecció dels arxius mitjançant l'assignació de personal qualificat per al seu tractament i l'emmagatzematge en caixes de seguretat ignífugues i instal·lacions externes en els casos en què així es requereixi. L'Entitat de Certificació posarà tots els mitjans al seu abast per garantir la confidencialitat enfront de tercers, durant el procés de generació, de les claus privades de signatura digital que proporciona.

5.5.4. Procediments de còpia de seguretat

Un tècnic de comunicacions de l'Entitat de Certificació s'encarrega de fer i de verificar la realització de les còpies de seguretat dels logs d'accés lògic al sistema operatiu de la Entitat de Registre.

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

També es realitzen còpies de seguretat de l'aplicació KeyOne personalitzada per a l'Entitat de Certificació. Aquestes còpies les guarda l'Entitat de Certificació a les seves instal·lacions.

5.5.5. Requisits de segell de cautela de data i hora

L'Entitat de Certificació emet els certificats i les LRC amb informació de temps i hora.

5.5.6. Localització del sistema d'arxiu

L'Entitat de Certificació té un sistema de manteniment de dades d'arxiu fora de les seves pròpies instal·lacions.

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

Només les persones autoritzades per l'Entitat de Certificació tenen accés a les dades d'arxiu, ja sigui a les mateixes instal·lacions de l'Entitat de Certificació com als arxius de les Entitats de Registre.

5.6. Renovació de claus

Els certificats de l'Entitat de Certificació que s'hagin renovat, es comuniquen als usuaris finals, mitjançant la seva publicació en el directori del Consorci AOC.

5.7. Compromís de claus i recuperació de desastre

5.7.1. Procediment de gestió d'incidències i compromisos

L'Entitat de Certificació estableix els procediments que aplica a la gestió de les incidències que afecten les seves claus i, molt especialment, als 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 inicia les gestions necessàries, segons els documents Pla de Seguretat, Pla d'Emergència i Pla d'Auditoria, per fer que el sistema torni al seu estat normal de funcionament.

5.7.3. Compromís de la clau privada de l'Entitat

El pla de continuïtat de negoci de l'Entitat de Certificació (o pla de recuperació de desastres) considera 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, com a mínim:

- Informar a tots els subscriptors i verificadors del compromís.
- Indicar que els certificats i la informació de l'estat de revocació lliurats usant la clau de l'Entitat de Certificació ja no són vàlids.
- Revocar, en el termini que es pacti amb el supervisor nacional, els certificats emesos per aquesta EC, aplicant, si escau, algun dels procediments previstos en el Pla de Cessament o en el Pla de Continuïtat.
- Notificar a l'Òrgan de Supervisió nacional en el termini màxim de 24 hores un cop s'hagi tingut coneixement del compromís de la clau privada.
- Notificar als fabricants de software que confien en els certificats, en els terminis establerts en les seves respectives polítiques d'admissió de CAs

5.7.4. Desastre sobre les instal·lacions

L'Entitat de Certificació desenvolupa, manté, prova i, si és necessari, executa un pla d'emergència en el cas de desastre, ja sigui per causes naturals o causat per l'home, sobre les instal·lacions, que indica com es restauren els serveis dels Sistemes d'Informació. La ubicació dels sistemes de recuperació de desastres disposa de les proteccions físiques de seguretat detallades en el Pla de Seguretat.
L'Entitat de Certificació és capaç de restaurar l'operació normal de la PKI durant les 24 hores següents al desastre i es poden executar, com a mínim, les accions següents:

- Revocació de certificats
- Publicació d'informació de revocació

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

5.8. Finalització del servei

5.8.1. L'Entitat de Certificació

L'Entitat de Certificació assegura 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, assegura un manteniment continu dels registres requerits per proporcionar evidència de certificació en procediments legals.

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

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

L'Entitat de Certificació declara en el seu Pla de Cessament les previsions que ha d'adoptar en cas de finalització del servei. Aquestes inclouen:

- Notificació a les entitats afectades amb una antelació mínima de 2 (dos) mesos a la finalització efectiva del servei.
- Com es tracta l'estat de revocació dels certificats emesos que encara no han expirat.

L'Entitat de Certificació transferirà els certificats, en els termes previstos en la legislació aplicable de signatura electrònica i serveis electrònics de confiança.

5.8.2. Entitat de Registre

Sense estipulació.

6. Controls de seguretat tècnica

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

6.1. Generació i instal·lació del parell de claus

6.1.1. Generació del parell de claus

6.1.1.1. Requisits per a tots els certificats

Les claus pública i privada podran ser generades pel futur posseïdor de claus o per l'Entitat de Certificació.

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 lliurada 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 bé, emmagatzemada segons els termes de la secció 3.2.1. de la present DPC. Addicionalment, s'hauran 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

El mètode d'enviament de la clau pública a l'Entitat de Certificació és PKCS #10, una altra prova equivalent o qualsevol un altre mètode aprovat pel Consorci AOC.

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

La clau de l'Entitat de Certificació i les claus de les Entitats de Certificació anteriors en la jerarquia pública de certificació de Catalunya es comuniquen als verificadors, i així s'assegura la integritat de la clau i s'autentica l'origen.

La clau pública de l'Entitat de Certificació, que és l'arrel de la jerarquia, es publica en el directori de l'Entitat de Certificació en forma de certificat autosignat juntament amb una declaració que fa referència al fet que la clau permet autenticar a l'Entitat de Certificació.

S'estableixen mesures addicionals per confiar en el certificat autosignat, com per exemple la comprovació de l'empremta digital del certificat.

La clau pública de l'Entitat de Certificació es publica al seu web del Consorci AOC: https://www.aoc.cat/catcert/regulacio.

Els usuaris accedeixen al directori per obtenir les claus públiques de l'Entitat de Certificació.

6.1.5. Mesures de claus

Les claus de l'Entitat de Certificació són de 2.048 bits.

Les claus de tots els certificats emesos per l'Entitat de Certificació són de 2.048 bits.

6.1.6. Generació de paràmetres de clau pública

Sense estipulació.

6.1.7. Comprovació de qualitat de paràmetres de clau pública

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

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

Els parells de claus de l'Entitat de Certificació són generats utilitzant hardware criptogràfic que compleix els requisits establerts per l'especificació tècnica CEN CWA 14167 o equivalent i d'acord amb ITSEC, Common Criteria EAL 4+o FIPS 140-2 Nivell 3 o superior nivell de seguretat.

Els parells de claus dels subscriptors de certificats T-CAT de signatura qualificada s'han de generar en targetes intel·ligents o en dispositius criptogràfics que compleixen els requisits establerts per les especificacions tècniques CEN CWA 14169 i CWA 14170 o equivalent.

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 per a la resta de certificats es pot realitzar mitjançant aplicacions informàtiques.

6.1.9. Propòsits d'ús de claus

El Consorci AOC inclou l'extensió KeyUsage en tots els certificats, indicant els usos permesos de les corresponents claus privades i limitant tècnicament la funcionalitat del certificat en el software compatible amb X.509v3

6.2. Protecció de la clau privada

6.2.1. Mòduls de protecció de la clau privada

6.2.1.1. Estàndards dels mòduls criptogràfics

Les claus privades de les Entitats de Certificació hauran de protegir-se utilitzant mòdul criptogràfic que compleixi els requisits establerts en un perfil de protecció, 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.

En el cas que s'hagi de produir una pèrdua de qualificació d'alguns dels dispositius utilitzats pel Consorci AOC com QSCD, es procedirà a la recerca de proveïdors substitutius dels esmentats dispositius, es deixarà d'utilitzar el dispositiu abans de la pèrdua de la qualificació i es notificarà als clients la futura pèrdua de qualificació per a poder prendre les mesures oportunes. En qualsevol cas, el Consorci AOC revocarà tots els certificats vigents que haguessin estat emesos en aquells dispositius que hagin perdut la qualificació.

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) es lliuren 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 es lliura 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, es substituirà la targeta afectada, prèvia revocació del certificat i s'emetrà un nou certificat que es lliurarà en una targeta nova, sense cost addicional per al subscriptor.

6.2.2. Control per més d'una persona 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.

Cadascun d'aquests dispositius és responsabilitat d'una persona concreta, única coneixedora de la clau d'accés al mateix. La clau d'accés és coneguda únicament per una persona responsable d'aquest dispositiu. Cap persona coneix més d'una de les claus d'accés. També es diposita davant Notari un sobre tancat en el que 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 una altra persona degudament autoritzada per aquest (presentant autorització signada per ell).

Els dispositius criptogràfics queden emmagatzemats en les dependències de l'Entitat de Certificació i per al seu accés és necessària una persona addicional.

6.2.3. Dipòsit de la clau privada

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

6.2.4. Còpia de seguretat de la clau privada

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

6.2.5. Arxiu de la clau privada

La clau privada de l'Entitat de Certificació haurà de comptar amb una còpia de seguretat realitzada, emmagatzemada i recuperada si escau per personal subjecte a la política de confiança del personal. Aquest personal ha d'estar expressament autoritzat per a aquestes finalitats.

Haurà de mantenir-se i utilitzar-se protegida per un dispositiu criptogràfic que compleixi els requisits establerts en un perfil de protecció, 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 en les còpies de suport de l'Entitat de Certificació hauran de ser d'igual o superior nivell a les quals 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 perquè aquestes mai puguin abandonar el dispositiu.

No s'emmagatzemaran còpies de claus privades dels certificats, excepte en casos de certificats sobre els quals es prevegi aquesta possibilitat conforme a l'establert en la corresponent PC. Aquesta clau privada podrà estar emmagatzemada per garantir la recuperació de dades.

6.2.6. Introducció de la clau privada en el mòdul criptogràfic

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

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

6.2.7. Emmagatzematge de la clau privada en el mòdul criptogràfic

Les claus privades es generen directament en els mòduls criptogràfics.

6.2.8. Mètode d'activació de la clau privada

Es requereixen almenys dues persones per activar les claus privades de l'Entitat de Certificació.

Per a certificats T-CAT en targeta, la clau privada del subscriptor s'activa mitjançant la introducció del PIN en la targeta intel·ligent o dispositiu criptogràfic.

Per a certificats T-CAT en targeta, quan la targeta intel·ligent o dispositiu criptogràfic es retiri del dispositiu lector, serà necessària novament la introducció del PIN.

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 T-CAT en targeta, quan la targeta intel·ligent o dispositiu criptogràfic es retiri del dispositiu lector, serà necessària novament la introducció del PIN.

Per a certificats personals que incloguin la política bàsica de signatura qualificada, 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, 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 són destruïdes de manera que impedeixi el seu robatori, modificació, divulgació o ús no autoritzat.

6.2.11. Classificació dels mòduls criptogràfics

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

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 T-CAT en targeta obtenen o superen el nivell EAL 4 de Common Criteria (ISO 15408) amb els augments que es determinen a l'especificació tècnica CEN CWA 14169.

Els mòduls dels subscriptors de certificats de signatura electrònica qualificada 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 arxiva les seves claus públiques, d'acord amb l'establert a la secció 5.5.

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

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

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

6.4. Dades d'activació

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

Per protegir al màxim les dades d'activació l'Entitat de Certificació s'encarrega de distribuir els elements dels certificats per dos canals diferents.

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

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

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

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

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

6.5.2. Avaluació del nivell de seguretat informàtica

Les aplicacions informàtiques de l'Entitat de Certificació i de l'Entitat de Registre són fiables, d'acord amb les especificacions tècniques CEN CWA 14167-1 i EN 319 411-2., i s'avalua el grau de compliment mitjançant una auditoria de seguretat informàtica conforme a l'especificació tècnica CWA 14172-2 i un perfil de protecció adequada, d'acord amb la norma ISO 15408 o equivalent.

6.5.3. Freqüència de revisió de les configuracions dels sistemes de confiança

El màxim interval de revisió interval màxim de revisió entre 2 versions de les configuracions dels sistemes de confiança serà d'1 (un) any.

6.6. Controls tècnics del cicle de vida

6.6.1. Controls de desenvolupament de sistemes

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

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

6.6.2. Controls de gestió de seguretat

L'Entitat de Certificació garanteix que les seves funcions de gestió de les operacions dels mòduls criptogràfics són suficientment segures; en particular, existeixen instruccions per:

a. Operar els mòduls de forma correcta i segura
b. Instal·lar els mòduls minimitzant el risc de fallida dels sistemes
c. Protegir els mòduls contra virus i software maliciós per garantir la integritat i validesa de la informació que processen

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 per garantir suficient disponibilitat electrònica i d'emmagatzematge per als actius informatius.

6.6.3. Avaluació del nivell de seguretat del cicle de vida

Sense estipulació addicional.

6.7. Controls de seguretat de xarxa

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

- S'implementen controls (com per exemple tallafocs) per protegir la xarxa interna de dominis externs accessibles per terceres parts. Els tallafocs es configuren de manera que s'impedeixin accessos i protocols que no siguin necessaris per a l'operació de les Entitats de Certificació.
- Les dades sensibles (incloent les dades de registre del subscriptor) es protegeixen quan s'intercanvien a través de xarxes no segures.

- Es garanteix que els components locals de xarxa (com enrutadores/routers) es troben situats en entorns segurs; també es garanteix l'auditoria periòdica de les seves configuracions.

6.8. Segell de temps

Sense estipulació.

7. Perfils de certificats i llistes de revocació de certificats

7.1. Perfil de certificat

Els documents descriptius dels diferents perfils de certificats digitals que expedeix l'Entitat de Certificació es publiquen a la web del Consorci AOC.

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 al 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 amb una entropia superior a 64 bits
b. Algorisme de signatura, amb algun dels algorismes 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 al RFC 6818
e. Fi de validesa del certificat, en Temps Coordinat Universal, codificat conforme al 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 el RFC 6818
h. Signatura generada i codificada, d'acord amb la 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 *Direcció de Tecnologies de la Informació i les Comunicacions* (DTIC) del *Ministeri d'Hisenda i Administracions Públiques* (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 al moment de la publicació d'aquesta política.
2. L'especificació *"Perfiles de Certificados Electrónicos"* elaborada per la Direcció de Tecnologies de la Informació i les Comunicacions (DTIC) del Ministeri d'Hisenda i Administracions Públiques (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, adreça electrònica i nombre d'identificació fiscal
d. La signatura electrònica avançada del prestador de serveis de certificació que expedeix el certificat
e. La identificació del signatari (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 signatari
g. Els límits d'ús del certificat, si es preveuen
h. Els límits del valor de les transaccions per 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 al seu web.

7.1.3. Identificadors d'objecte d'algorismes

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

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

7.1.4. Formats de nom

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

7.1.7. Ús de l'extensió restriccions de política

Sense estipulació.

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 en 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.

7.1.10. Especificacions tècniques per a totes les Entitat 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 DPC respectarà les següents especificacions tècniques:

- L'algorisme utilitzat ha de ser renovat quan existeixi un risc de desencriptació advertit per la comunitat. Les Entitats de Certificació incorporaran, a partir de l'emissió d'aquesta DPC, l'algorisme SHA-256
- Els números de sèrie dels certificats sempre seran sencers i, en tot cas, positius
- S'utilitzarà la codificació UTF-8
- Es simplificarà l'extensió “authorityKeyIdentifier”
- Es restringiran els OIDs generats per les Entitats de Certificació intermèdies

7.2. Perfil de la llista de revocació de certificats

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

7.3 Perfil de OCSP

Els serveis d'OCSP compleixen amb la norma IETF RFC 6960.

8. Auditoria de conformitat

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

L'Entitat de Certificació pot delegar l'execució de les auditories en una tercera entitat contractada pel Consorci AOC. En aquests casos l'Entitat de Certificació coopera completament amb el personal que duu a terme la recerca.

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

L'Entitat de Certificació Vinculada ha d'estar preparada per passar altres revisions, no periòdiques, que demostrin la seva confiança:

- Abans d'acceptar una nova Entitat de Certificació subordinada a la jerarquia, el Consorci AOC ha de realitzar una revisió dels seus documents de seguretat i DPC i PCs per assegurar que compleix els requisits de seguretat i d'operació necessaris per formar part de la Jerarquia d'Entitats de Certificació del Consorci AOC.
- Si en qualsevol moment se sospita que l'Entitat de Certificació Vinculada, una vegada 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 per a la seguretat o integritat de l'Entitat de Certificació Vinculada, es durà a terme una auditoria interna.

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

8.1. Freqüència de l'auditoria de conformitat

L'Entitat de Certificació ha de dur a terme una auditoria de conformitat anualment, a més de les auditories internes que puguin dur a terme sota el seu propi criteri o a 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

L'Entitat de Certificació haurà d'acudir a auditors independents externs per a la realització de les auditories anuals de conformitat. Aquests han de demostrar experiència en seguretat informàtica, en seguretat de sistemes d'informació i en auditories de conformitat d'Entitats de Certificació i dels elements relacionats.

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

Les auditories externes de conformitat executades per tercers són realitzades per entitats independents de l'Entitat de Certificació.

8.4. Relació d'elements objecte d'auditoria

Els elements objecte d'auditoria seran els següents:

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

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

Una vegada rebut l'informe de l'auditoria de compliment dut a terme, l'Entitat de Certificació discuteix, amb l'entitat que ha executat l'auditoria i amb el Consorci AOC, les deficiències oposades i desenvolupa i executa un pla correctiu que les soluciona.

Si l'Entitat de Certificació, una vegada auditat, és incapaç de desenvolupar i/o executar l'esmentat pla o si les deficiències oposades suposen una amenaça immediata per a la seguretat o la integritat del sistema, s'ha de realitzar una de les accions següents:

- Revocar la clau de l'Entitat de Certificació, tal com es descriu en la secció 4.9 d'aquesta DPC.
- Acabar el servei de l'Entitat de Certificació, tal com es descriu en la secció 5.8 d'aquesta DPC.

8.6. Tractament dels informes d'auditoria

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

9. Requisits comercials i legals

9.1. Imports

9.1.1. Import d'emissió i renovació de certificats

El Consorci AOC estableix els imports que aplica l'Entitat de Certificació en la prestació dels seus serveis. Els imports es poden consultar a la web del servei de certificació digital del Consorci AOC.

9.1.2. Import d'accés a certificats

No es pot establir un import per l'accés als certificats.

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

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

9.1.4. Imports d'altres serveis

Sense estipulació addicional.

9.1.5. Política de reintegrament

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

9.2. Capacitat financera

9.2.1. Segur de responsabilitat civil

El Consorci AOC disposa d'una garantia de cobertura de la seva responsabilitat civil suficient, en els termes previstos en la normativa aplicable de signatura electrònica i serveis de confiança. Aquesta assegurança cobreix les actuacions del Consorci AOC com a PSC.

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 de dirigir-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.

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

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

9.3. Confidencialitat

9.3.1. Informacions confidencials

Les informacions següents es mantenen de forma confidencial per l'Entitat de Certificació:

a. Informació de negoci subministrada pels seus proveïdors i altres persones amb els qui el Consorci AOC o l'Entitat de Certificació tenen una obligació de guardar secret, establerta legalment o convencionalment.

b. Registres de transaccions, incloent els registres complets i els registres d'auditoria de les transaccions.

c. Registres d'auditoria interna i externa, creats i/o mantinguts per l'Entitat de Certificació i els seus auditors.

d. Plans de continuïtat de negoci i d'emergència.

e. Política i plans de seguretat.

f. Documentació d'operacions, com per exemple, l'arxiu, el monitoratge i altres operacions anàlogues.

g. Qualsevol altra informació identificada com a "Confidencial".

9.3.2. Informacions no confidencials

Les informacions següents no tenen caràcter confidencial:

- Aquesta DPC i les PC del Consorci AOC.
- La informació continguda en els certificats
- Qualsevol informació la publicitat de la qual sigui imposada normativament
- Qualsevol altra informació identificada com a "Pública".

9.3.3. Responsabilitat per a la protecció d'informació confidencial

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

Aquestes mesures inclouen les clàusules apropiades d'informació confidencial a les quals estaran sotmeses totes les persones involucrades en els processos de certificació que corresponguin.

9.4. Protecció de dades personals

9.4.1. Política de Protecció de Dades Personals

El Consorci AOC desenvolupa una política de protecció de les dades personals, d'acord amb la normativa aplicable de protecció de dades.

En particular, i en compliment de les obligacions imposades pel Reglament (UE) 2016/679 del Parlament Europeu i del Consell,de 27 d'abril de 2016 relatiu a la protecció de les persones físiques en el que respecta al tractament de dades personals i la lliura circulació d'aquestes dades i pel que es deroga la Directiva 95/46/CE- Reglament general de protecció de dades- (en endavant, RGPD) i la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals (en endavant, LOPDGDD), disposa d'un Registre d'Activitats de Tractament de dades de caràcter personal, en el qual estan recollits els següents fitxers:

1. Subscriptors De Certificats: https://www.seu-e.cat/documents/31307/0/RAT_SubscriptorsColectiusCertificats/f70ee619-882e-40ab-b926-4e300d160da3

2. Persones Físiques Certificades: https://www.seu-e.cat/documents/31307/0/RAT+-+Persones+f%C3%ADsiques+certificades/a943e588-6744-43e5-8ae4-1e87d570591f

El Consorci AOC desenvolupa els procediments indicats en aquest document, que aplica en la prestació dels seus serveis, en els quals, en compliment dels requisits establerts per les polítiques de certificats que gestiona, es detallen els requisits i obligacions en relació amb l'obtenció i gestió de les dades personals.

El Consorci AOC estableix les mesures de seguretat de caire tècnic i organitzatiu necessàries per donar compliment a les mesures de seguretat aplicables a fitxers i tractaments automatitzats.

9.4.2. Dades de caràcter personal no disponibles a tercers

De conformitat amb el que s'estableix en l'article 4 RGPD es consideren dades personals qualsevol informació relativa a persones físiques identificades o identificables.

La informació personal que no hagi de ser inclosa en els certificats i en el mecanisme indicat de comprovació de l'estat dels certificats, és considerada informació personal de caràcter privat.

Les següents dades són considerades en tot cas com a informació privada:

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

9.4.3. Dades de caràcter personal disponibles a tercers

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

L'esmentada informació, proporcionada durant la sol·licitud de certificats en els termes que es preveuen a la legislació aplicable, és inclosa en els seus certificats i el mecanisme de comprovació de l'estat dels certificats.

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

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

a. Els certificats emesos o en tràmit d'emissió.
b. La subjecció del subscriptor a un certificat emès per l'Entitat de Certificació.
c. El nom i els cognoms del subscriptor del certificat, així com qualsevol altra circumstància o dades personals del titular, en el supòsit que siguin significatives en funció de la finalitat del certificat, d'acord amb aquest document.
d. L'adreça electrònica del subscriptor del certificat.
e. Els usos i límits econòmics ressenyats al certificat.
f. El període de validesa del certificat, així com la data d'emissió del certificat i la data de caducitat.
g. El número de sèrie del certificat.
h. Els diferents estats o situacions del certificat i la data de l'inici de cadascun d'ells, en concret: pendent de generació i/o lliurament, vàlid, revocat, suspès o caducat i el motiu que va provocar el canvi d'estat.
i. Les 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

La informació confidencial és protegida, d'acord amb el RGPD, de la seva pèrdua, destrucció, mal, falsificació i processament il·lícit o no autoritzat.

Davant qualsevol violació de la seguretat o pèrdua de la integritat que tingui un impacte significatiu en el servei de confiança prestat o en les dades personals corresponents, el

Consorci AOC notificarà al supervisor nacional competent en matèria de seguretat de la informació o a l'Autoritat de protecció de dades corresponent, en un termini de 72 hores després de tenir coneixement dels fets.

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

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

Aquest procediment de notificació 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'Entitat de Certificació, descrivint el tipus d'incidència i els efectes que s'observen.

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

Una vegada fetes les actuacions necessàries i restablit el normal funcionament dels sistemes, l'administrador dels sistemes envia per correu electrònic dirigit al Responsable de l'Entitat de Certificació 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'Entitat de Certificació manté còpia dels formularis corresponents a les incidències registrades durant els 12 últims mesos sobre els fitxers que contenen dades de caràcter personal. Aquests es guarden en un directori dedicat dins del servidor que comparteixen els usuaris de l'Entitat de Certificació, protegit convenientment perquè només pot accedir el personal autoritzat; així queda garantit que es fan còpies de seguretat del seu contingut.

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

- Quin recurs té la incidència
- El seu codi i descripció
- El dia i l'hora
- El tipus d'incidència
- Els efectes
- El comunicant i el destinatari
- La resposta
- Els procediments previstos a realitzar
- La persona que els realitzarà

- El procediment per a la recuperació
- La persona (i autorització) per a la recuperació
- Les dades restaurades.

9.4.6. Tractament de dades de caràcter personal

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

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

La informació personal recollida dels usuaris registrats és emmagatzemada en la base de dades propietat de Consorci AOC que assumeix les mesures d'índole tècnica, organitzativa i de seguretat que garanteixin la confidencialitat i integritat de la informació d'acord amb el que s'estableix en el RGPD, i altra legislació aplicable.

L'usuari respondrà, en qualsevol cas, de la veracitat de les dades facilitades, reservant-se Consorci AOC el dret a excloure dels serveis registrats a tot usuari que hagi facilitat dades falses, sense perjudici de les altres accions legals.

Qualsevol usuari registrat pot en qualsevol moment exercir el dret d'accés, rectificació o supressió, oposició, limitació al tractament i portabilitat, mitjançant sol·licitud a l'adreça del Consorci AOC C/Tànger 98, 22@- 08018 Barcelona o bé mitjançant formulari electrònic (https://www.seu-e.cat/web/consorciaoc/govern-obert-i-transparencia/serveis-i-tramits/tramits/tramits-associats-a-la-lopd-193)

No obstant això, si l'usuari considera que el seu dret a la protecció de dades personals ha pogut ser vulnerat, pot reclamar davant l'Autoritat Catalana de Protecció de Dades.

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 obligada a revelar la identitat dels signants quan ho sol·licitin els òrgans judicials en l'exercici de les funcions que tinguin atribuïdes i en la resta

de supòsits previstos en la normativa aplicable de protecció de dades de caràcter personal.

El Consorci AOC dóna compliment a totes les prescripcions legals de conformitat amb el RGPD i la LOPDGDD.

Excepcionalment, en cas de cessament de la seva activitat per part 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

9.5.1. Propietat dels certificats i informació de revocació

El Consorci AOC és l'única entitat que gaudeix dels drets de propietat sobre els certificats que emet.

El Consorci AOC concedeix llicència no exclusiva per reproduir, distribuir, verificar i utilitzar els certificats, sense cap cost, en relació a signatures digitals i/o sistemes de xifrat dins de l'àmbit d'aplicació d'aquesta DPC, d'acord amb el corresponent instrument vinculant entre el Consorci AOC i la part que reprodueixi i/o distribueixi el certificat.

Les normes anteriors figuren als instruments jurídics que existeixen entre el Consorci AOC i els subscriptors i els verificadors.

Addicionalment, els certificats emesos pel Consorci AOC contenen un avís legal relatiu a la propietat d'aquests certificats. Aquesta normativa resulta igualment d'aplicació en l'ús d'informació de revocació de certificats.

9.5.2. Propietat de la Declaració de Pràctiques de Certificació i les Polítiques de Certificació

El Consorci AOC és l'única entitat que gaudeix dels drets de propietat sobre les PC de la jerarquia pública de certificació de Catalunya.

El Consorci AOC és propietària d'aquesta DPC. El Consorci AOC no cobra una tarifa per l'excés a aquesta DPC ni a les diferents PC. Qualsevol ús que es faci amb finalitats diferents a la visualització dels documents, com reproducció, redistribució, modificació o creació d'un derivat de les mateixes, estaran subjectes a un acord de llicència amb l'enitat titular dels drets d'autor del document.

9.5.3. Propietat de la informació relativa a noms

El subscriptor (o el posseïdor de claus, si escau) conserva qualsevol dret, d'existir aquest, relatiu en la marca, producte o nom comercial contingut al certificat.

El subscriptor (o el posseïdor de claus, si escau) és el propietari del nom distingit del certificat, format per les informacions especificades a la secció 3.1 d'aquesta DPC.

9.5.4. Propietat de claus

Els parells de claus són propietat dels subscriptors dels certificats.

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

9.6. Obligacions i responsabilitat civil

9.6.1. L'Entitat de Certificació

9.6.1.1. Obligacions i altres compromisos

L'Entitat de Certificació s'obliga a complir el següent:

- Determina la comunitat de subscriptors i verificadors de l'Entitat de Certificació.
- Aprova les polítiques de certificació i, si escau, les polítiques específiques de certificació.
- Aprova, si escau, la documentació contractual i reguladora dels serveis de certificació en la comunitat d'usuaris de l'Entitat de Certificació, d'acord amb el procediment previst en aquesta DPC.
- Informa puntualment al Consorci AOC de totes les informacions relatives als canvis a realitzar, incidències en el servei, reclamacions, denúncies i inspeccions del servei.
- Garanteix, sota la seva plena responsabilitat, que compleix amb tots els requisits establerts en aquesta DPC.
- És l'única entitat responsable del compliment dels procediments descrits en aquesta DPC, fins i tot quan una part o la totalitat de les operacions siguin subcontractades externament.
- Presta els seus serveis de certificació d'acord amb aquesta DPC, on es detallen, almenys, els continguts previstos en la legislació aplicable, descrita a 9.15
- De conformitat amb la llei aplicable, abans de l'emissió i lliurament del certificat, l'Entitat de Certificació informa dels aspectes previstos a la legislació aplicable, així com dels següents aspectes:
    - Indicació de la política aplicable, amb indicació que els certificats no s'expedeixen al públic i la necessitat d'utilització de dispositiu qualificat de creació de signatura.
    - Forma en què es garanteix la responsabilitat patrimonial de l'Entitat de Certificació.
    - L'Entitat de Certificació es declara d'acord amb la política de certificació, la certificació del Prestador de serveis de certificació i la certificació dels productes de signatura electrònica utilitzats.

Aquest requisit es compleix mitjançant un “Text divulgatiu de la política de certificat” aplicable que es transmet electrònicament utilitzant un mitjà de comunicació durador en el temps i en llenguatge comprensible.

- L'Entitat de Certificació obliga als subscriptors, posseïdors de claus i als verificadors mitjançant instruments jurídics apropiats en cada situació, els quals es transmeten electrònicament, en llenguatge escrit i comprensible, a tenir en compte els continguts mínims següents:
    - Prescripcions per donar compliment a l'establert en aquesta DPC.
    - Indicació de la política aplicable, amb indicació de si els certificats s'expedeixen al públic i de la necessitat d'ús del dispositiu qualificat de creació de signatura.
    - Manifestació que la informació continguda en el certificat és correcta, excepte notificació en contra pel subscriptor.
    - Consentiment per a la publicació del certificat al directori i accés per tercers al mateix.
    - Consentiment per a l'emmagatzematge de la informació utilitzada per al registre del subscriptor i del posseïdor de claus, per a la provisió del dispositiu qualificat de creació de signatura i per a la cessió de l'esmentada informació en tercers, en cas de final d'operacions de l'Entitat de Certificació sense revocació de certificats vàlids.
    - Límits d'ús del certificat, incloent els establerts en la secció 4.5 d'aquesta DPC.
    - Informació sobre com validar un certificat, incloent el requisit de comprovar l'estat del certificat, i les condicions en les quals es pot confiar raonablement en el certificat, que resulta aplicable quan el subscriptor actua com a verificador.
    - Limitacions de responsabilitat aplicables, incloent els usos pels quals l'Entitat de Certificació accepta o exclou la seva responsabilitat.
    - Procediments aplicables de resolució de disputes.
    - Llei aplicable i jurisdicció competent.

L'Entitat de Certificació identifica al posseïdor de claus, d'acord amb la legislació aplicable i aquesta DPC. Especialment, l'Entitat de Certificació, comprova per si mateixa la identitat i altres circumstàncies personals dels sol·licitants dels certificats.

9.6.1.2. Garanties ofertes

9.6.1.2.1. Garanties ofertes als subscriptors

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

a. El compliment de les seves obligacions legals com a PSC, d'acord amb la legislació aplicable.

b. Que no hi ha errors en les informacions contingudes als certificats, coneguts o realitzats per aquesta, ni deguts a la manca de diligència en la gestió de la sol·licitud de certificat o en la creació d'aquest.

c. Que els certificats compleixen tots els requisits materials establerts en la DPC.

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

e. Que, en cas que hagi generat les claus privades, es manté la confidencialitat durant el procés.

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

9.6.1.2.2. Garanties ofertes als verificadors

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

a. El compliment de les seves obligacions legals com a PSC d'acord amb la legislació aplicable.

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

c. En cas de certificats publicats al directori, que el certificat ha estat emès al subscriptor identificat en aquest i que el certificat ha estat acceptat, d'acord amb la secció 4.4 d'aquesta DPC.

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 aquesta DPC.

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

f. Que els certificats compleixin tots els requisits materials establerts en aquesta DPC.

g. Que, en cas que hagi generat les claus privades, es manté la confidencialitat durant el procés.

h. Que els serveis de revocació i l'ús del directori compleixen tots els requisits materials establerts en aquesta DPC.

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. Nomenar com a operadors de l'entitat (tècnica) de registre a dos o més dels seus treballadors (depenent del EC, generalment quatre o més) i comunicar al Consorci AOC les dades corresponents a aquestes persones per a l'emissió dels certificats

d'operador corresponents. Quan un operador deixi de tenir capacitat per actuar com el qual 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.

b. 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.

c. 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 de 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 per diferenciar una persona respecte una altra en l'àmbit de l'Entitat de Registre Interna.

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

e. 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 DPC i la documentació d'operacions de l'Entitat de Certificació Vinculada.

f. 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 (quinze) anys des de l'extinció del certificat o la finalització del servei prestat i en tot cas el període que estableix la legislació vigent. Aquests registres han d'estar a la disposició de l'Entitat de Certificació Vinculada.

g. Emmagatzemar els fulls de lliurament de certificat durant un període de 15 (quinze) anys. Aquests registres han d'estar a la 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 per a la posterior emissió de certificats per part de l'Entitat de Certificació Vinculada o l'Entitat de Registre Col·laboradora.

b. La justificació documental haurà de ser realitzada per una unitat orgànica de l'Entitat de Registre Virtual facultada legalment per donar fe de les dades a certificar, que s'indicarà 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 referent a 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 un 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/o 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 al moment del lliurament.

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 per a la correcta identificació i/o autenticació del subscriptor, i si fos necessari, del posseïdor de claus.

9.6.2.2. Garanties ofertes a subscriptor i verificadors

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 per emetre certificats no ha estat compromesa, tret que el Consorci AOC hagués comunicat el contrari, de conformitat amb aquesta DPC.

El Consorci AOC únicament garanteix que:

a. Els certificats de signatura electrònica contenen tota la informació exigida per la Llei 6/2020 d'11 de novembre, el Reglament (UE) 910/2014 i altra normativa d'aplicació , que es descriu en la secció 9.15.

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, al moment de l'emissió del certificat.

c. Tots els certificats compleixen els requisits formals i de contingut de la seva Política de certificació i Perfil de Certificat corresponent.

d. Queda vinculada pels procediments operatius, de seguretat i d'arxiu descrits a la DPC.

9.6.2.2.2. Exclusió de la garantia

El Consorci AOC no garanteix cap software utilitzat pel subscriptor o per qualsevol altra persona, per generar, verificar o no utilitzar de forma diferent cap signatura digital o certificat electrònic 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 per a tots els tipus de certificats

L'Entitat de Certificació obliga al subscriptor dels certificats a:

a. Facilitar a l'Entitat de Certificació la informació completa i adequada conforme als requisits d'aquesta DPC, especialment, en allò referent al procediment de registre.

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

c. Complir les obligacions que s'estableixen per al subscriptor en aquesta DPC i amb la legislació vigent descrita en la secció 9.15 d'aquesta DPC.

d. Utilitzar el certificat d'acord amb l'establert en la secció 1.4 d'aquesta DPC.

e. Notificar a l'Entitat de Certificació, 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 i a qualsevol persona que el subscriptor crea 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 una vegada transcorregut el període indicat a la secció corresponent.

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

i. No monitorizar, manipular o realitzar actes d'enginyeria reversa sobre la implantació tècnica de la jerarquia pública de certificació de Catalunya 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 qualificada

L'Entitat de Certificació Vinculada obligarà al subscriptor a:

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

b. 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

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

    1. Generar les seves claus de subscriptor utilitzant un algorisme reconegut com a acceptable per a la signatura electrònica qualificada

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

    3. Utilitzar longituds i algorismes de clau reconeguts com a acceptables per a la signatura electrònica qualificada

e. Notificar a l'Entitat de Certificació, 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 obliga, mitjançant el corresponent instrument jurídic, al subscriptor a garantir que:

a. Totes les manifestacions realitzades a la sol·licitud són correctes.

b. Totes les informacions subministrades pel subscriptor que es trobin contingudes al certificat són correctes.

c. El certificat s'utilitza exclusivament per a usos legals i autoritzats, d'acord amb aquesta DPC.

d. Cada signatura digital creada amb la clau privada corresponent a la clau pública inclosa en el certificat és la signatura digital del subscriptor i que el certificat ha estat acceptat i es troba operatiu (no ha expirat ni ha estat revocat) al moment de creació de la signatura.

e. El subscriptor és una entitat final i no una Entitat de Certificació i no utilitza la clau privada corresponent a la clau pública inclosa en el certificat per signar cap certificat (o qualsevol un altre format de clau pública certificada) ni LRC.

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

9.6.3.3. Protecció de la clau privada

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

9.6.4. Verificadors

9.6.4.1. Obligacions i altres compromisos

L'Entitat de Certificació obliga a l'usuari de certificats a:

a. Assessorar-se sobre el fet que el certificat és apropiat per a l'ús que es pretén.

b. Verificar la validesa, suspensió o revocació dels certificats emesos, per a això 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 un altre instrument, amb independència de la seva naturalesa jurídica.

f. No monitorizar, 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 dispositius qualificats de signatura electrònica són signatures electròniques equivalents a signatures manuscrites, d'acord amb l'article 25.2 del Reglament (UE) 910/2014.

9.6.4.2. Garanties ofertes pel verificador

L'Entitat de Certificació obliga al verificador, mitjançant el corresponent instrument jurídic, a manifestar que:

a. Disposa de suficient informació per prendre una decisió informada per confiar o no en el certificat.

b. És l'únic responsable de confiar o no en la informació continguda al certificat.

c. Serà l'únic responsable si incompleix les seves obligacions com a verificador.

9.6.5. Consorci AOC

9.6.5.1. Obligacions i compromisos

El Consorci AOC s'obliga a operar les Entitats de Certificació al seu càrrec, incloent l'Entitat de Certificació arrel de la jerarquia pública de certificació de Catalunya, de manera diligent, de conformitat amb les polítiques, pràctiques i normativa de l'esmentada jerarquia.

9.6.5.2. Garanties ofertes als subscriptors

El Consorci AOC garanteix que la clau privada de les Entitats de Certificació al seu càrrec no ha estat compromesa, tret que així ho indiqui expressament mitjançant el directori del Consorci AOC.

El Consorci AOC únicament garanteix:

a. Que els certificats contenen tota la informació exigida per la legislació aplicable, descrita en la secció 9.15 d'aquesta DPC. Que no ha originat ni introduït declaracions falses o errònies en la informació dels certificats, ni tampoc ha deixat d'incloure informació necessària aportada per l'Entitat de Certificació i validada pel Consorci AOC o l'Entitat de Registre, al moment d'emissió dels certificats.
b. Que tots els certificats emesos compleixen els requisits formals i de contingut.

El Consorci AOC està vinculat als procediments operatius i de seguretat descrits en aquesta DPC.

9.6.5.3. Garanties ofertes als verificadors

La responsabilitat del Consorci AOC, que deriva d'una relació indirecta, és la prevista en la legislació aplicable, descrita a la secció 9.15 d'aquesta DPC.

9.6.5.4. Exclusió de garanties

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

9.6.6. Directori

9.6.6.1. Obligacions i compromisos

L'Entitat de Certificació pot delegar algunes funcions al directori, que en aquest cas està obligat al seu compliment, en les mateixes condicions que aquesta.

Les funcions, obligacions i deures del directori s'estableixen detalladament en aquesta

DPC, així com en la documentació jurídica auxiliar, especialment la lliurada a subscriptors, posseïdors de claus i verificadors.

9.6.6.2. Garanties

L'Entitat de Certificació estableix en aquesta DPC la responsabilitat civil del directori quan sigui operat per una tercera entitat.

9.7. Renúncies de garanties

9.7.1. Rebuig de garanties de l'Entitat de Certificació

L'Entitat de Certificació pot rebutjar totes les garanties del servei que no es trobin vinculades a obligacions establertes per la legislació aplicable, descrita a la secció 9.15 d'aquesta DPC, incloent especialment la garantia d'adaptació per a un propòsit particular o garantia d'ús mercantil del certificat.

9.8. Limitacions de responsabilitat

9.8.1. Limitacions de responsabilitat de l'Entitat de Certificació

L'Entitat de Certificació limita la seva responsabilitat restringint el servei a l'emissió i gestió de certificats i, si escau, de parells de claus de subscriptors i dipòsits criptogràfics (de signatura i verificació de signatura, així com de xifrat o desxifrat) subministrats per aquesta.

L'Autoritat de Certificació pot limitar la seva responsabilitat mitjançant la inclusió de límits d'ús del certificat límits de valor de les transaccions per les quals es pot utilitzar el certificat.

9.8.2. Cas fortuït i força major

L'Autoritat de Certificació inclou clàusules per limitar la seva responsabilitat en cas fortuït i en cas de força major, als instruments jurídics amb que vinculi subscriptors i verificadors.

9.9. Indemnitzacions

9.9.1. Clàusula d'indemnització de subscriptor

No s'establirà clàusula d'indemnització del subscriptor.

9.9.2. Clàusula d’indemnitat de verificador

No s'establirà clàusula d'indemnització del verificador.

9.10. Termini i finalització

9.10.1. Termini i finalització

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

9.10.2. Supervivència

L'Entitat de Certificació estableix, en els seus instruments jurídics amb els subscriptors i els verificadors, clàusules de supervivència, en virtut de les quals s'estableix com certes obligacions continuen vigents després de la finalització de la relació jurídica reguladora del servei entre les parts.

A aquest efecte, l'Entitat de Certificació vetlla perquè, almenys els requisits continguts a 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 vinculin l'Entitat de Certificació amb subscriptors i verificadors.

El Consorci AOC determinarà un Pla de Cessament de Negoci. Aquest Pla de Cessament de Negoci establirà les obligacions que assumeix el Consorci AOC en cas de cessament d'activitats, dirigides a mantenir en vigència dels certificats emesos fins a la seva expiració i l'ús i 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 que hagin estat generats o emmagatzemats. A aquest efecte, el Consorci AOC s'assegura que es genera una còpia de seguretat amb periodicitat, com a previsió complementària de l'activitat corrent i igualment de l'assegurament de la continuïtat de negoci.

9.11. Notificacions

L'Entitat de Certificació estableix, en els seus instruments jurídics vinculants amb subscriptors i verificadors, clàusules de notificació, en les quals s'estableix el procediment pel qual les parts es notifiquen fets mútuament.

9.12. Modificacions

9.12.1. Procediment per a les modificacions

El Consorci AOC pot modificar, de forma unilateral, la documentació reguladora del servei, sempre que procedeixi segons el procediment següent:

- La modificació ha d'estar justificada des del punt de vista tècnic, legal o comercial.
- S'estableix un control de modificacions per garantir, en tot cas, que les especificacions resultants compleixen els requisits que s'intenten complir i que van donar motiu al canvi.

- S'estableixen les implicacions que el canvi d'especificacions té sobre l'usuari, i es preveu la necessitat de notificar-li les esmentades modificacions.
- Els canvis han de ser aprovats pel Consorci AOC.

9.12.2. Període i mecanismes per a notificacions

Les modificacions d'aquesta DPC es notifiquen al Consorci AOC, per a la seva posterior aprovació.

9.13. Resolució de conflictes

9.13.1. Resolució extrajudicial de conflictes

L'Entitat de Certificació estableix, en els seus instruments jurídics amb subscriptors i verificadors, els procediments de mediació i resolució de conflictes aplicables, amb aquesta finalitat, es té en compte la consideració com a Administració Pública de l'Entitat de Certificació.

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

9.13.2. Jurisdicció competent

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

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

Així mateix, es té en compte la legislació administrativa que resulti aplicable.

9.14. Llei aplicable

L'Entitat de Certificació estableix, en els seus instruments jurídics amb subscriptors i verificadors, que la llei aplicable a la prestació dels serveis, incloent la DPC i les PC , és la següent:

- Reglament (UE) núm. 910/2014 del Parlament Europeu i del Consell, de 23 de juliol de 2014, relatiu a la identificació electrònica y els serveis de confiança per a les transaccions electròniques en el mercat interior i por la qual es deroga la Directiva 1999/93/CE.
- Llei 6/2020, d'11 de novembre, reguladora de determinats aspectes dels serveis electrònics de confiança.

- Llei 39/2015, d'1 d'octubre, del Procediment Administratiu Comú de las Administracions Públiques.
- Llei 40/2015, d'1 d'octubre, de Règim Jurídic del Sector Públic.
- Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques en el que respecta al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE (RGPD).
- Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals (LOPDGDD).
- Directiva (UE) 2015/2366 del Parlament Europeu i del Consell de 25 de novembre de 2015 sobre serveis de pagament en el mercat interior i per la qual es modifiquen les Directives 2002/65/CE, 2009/110/CE y 2013/36/UE i el Reglament (UE) núm. 1093/2010 i es deroga la Directiva 2007/64/CE.
- Reglament d'Execució (UE) 2015/1502 de la Comissió de 8 de setembre de 2015 sobre la fixació d'especificacions i procediments tècnics mínims per als nivells de seguretat de mitjans d'identificació electrònica segons el disposat en l'article 8, apartat 3, del Reglament (UE) núm.910/2014 del Parlament Europeu i del Consell, relatiu a la identificació electrònica i els serveis de confiança per a les transaccions electròniques en el mercat interior.
- Decisió d'Execució (UE) 2016/650 de la Comissió, de 25 d'abril de 2016, per la qual es fixen les normes per a l'avaluació de la seguretat dels dispositius qualificats de creació de firmes i segells segons l'article 30, apartat 3, i a l'article 39, apartat 2, del Reglament (UE) núm. 910/2014 del Parlament Europeu i del Consell, relatiu a la identificació electrònica i els serveis de confiança per a les transaccions electròniques en el mercat interior.
- Reglament Delegat (UE) 2018/389 de la Comissió de 27 de novembre de 2017 pel qual es complementa la Directiva (UE) 2015/2366 del Parlament Europeu i del Consell en lo relatiu a les normes tècniques de regulació per l'autenticació reforçada de clients i uns estàndards de comunicació oberts comuns i segurs.
- Última versió dels "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" publicats en http://www.cabforum.org pel CA/Browser Forum. En cas de qualsevol inconsistència entre aquesta Declaració de Pràctiques de Certificació i els esmentats requisits, prevaldran els esmentats requisits.
- Guidelines For The Issuance And Management Of Extended Validation Certificates, publicats en http://www.cabforum.org pel CA/Browser Forum. En cas de qualsevol inconsistència entre aquest document i aquelles Directrius, aquelles Directrius prevaldran sobre aquest document.

En cas d'inconsistència entre la llei nacional aplicable i els requeriments del CA/Browser Forum, aquesta DPC s'ajustarà per a alinear-se amb els requisits de la llei nacional, però el Consorci AOC notificarà al CA/Browser Forum de l'esmentat ajust.

9.15. Conformitat amb la llei aplicable

El Consorci AOC serà responsable dels danys i perjudicis ocasionats als usuaris pels seus serveis i a altres tercers en els termes establerts en la legislació vigent i en la present DPC.

9.16. Clàusules diverses

9.16.1. Acord íntegre

L'Entitat de Certificació estableix, en els seus instruments jurídics vinculants amb subscriptors i verificadors, clàusules d'acord íntegre, en virtut de les quals s'entén 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 no poden ser objecte de cessió a tercers de cap tipus, ni cap tercera entitat es pot subrogar en la posició jurídica d'una Entitat de Certificació.

En cas que es produeixi una cessió o subrogació, es procedeix a la finalització de l'esmentada Entitat de Certificació.

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

9.16.3. Divisibilitat

L'Entitat de Certificació estableix clàusules de divisibilidad, en els seus instruments jurídics vinculants amb subscriptors i verificadors, en virtut de les quals la invalidesa d'una clàusula no afecta la resta del contracte.

Encas que, com a causa als articles 7 i 8 de la Llei 7/1998 de 13 d'abril sobre condicions generals de la contractació, es considerarien no incorporades al contracte, o nul·les algunes o qualsevol de les clàusules indicades, la referida no incorporació o nul·litat no determina la ineficàcia total del contracte, si aquest pogués subsistir sense les clàusules indicades.

9.16.4. Aplicacions

Sense estipulació.

9.16.5. Altres clàusules

Sense estipulació.