# DECLARACIÓ DE PRÀCTIQUES DE CERTIFICACIÓ PKI A L'ADMINISTRACIÓ PÚBLICA ANDORRANA


Govern d'Andorra

Versió 2.2.0

Idioma: **Català**

# Índex de contingut

# 1. INTRODUCCIÓ

## *1.1. Visió general*

La infraestructura de clau pública (PKI) de l'Administració pública andorrana ha estat creada per permetre l'autenticació fiable i segura de la identitat, a més de facilitar la confidencialitat i integritat de les transaccions electròniques a les instal·lacions de Camerfirma, AC. Aquest document identifica les pràctiques i els procediments que empra l'Oficina de Serveis de Confiança Electrònica del Principat d'Andorra, "Oscepa" des d'ara, en l'emissió de certificats digitals dins d'aquesta infraestructura com les de Camefirma, AC en la seva relació contractual amb l'OSCEPA.

Aquestes pràctiques estan alineades amb els requisits marcats en els Baseline Requirements for the Resolucions and Management of Publicly-Trusted Certificates, elaborats pel CA / B Forum, http://www.cabforum.org, en la seva versió 1.6.6.

En el cas que hi hagi alguna inconsistència entre aquest document i els Baseline Requirements, aquests últims tindran prioritat sobre aquest document.

## *1.2. Identificació i nom del document*

Aquest document és la Declaració de pràctiques de certificació de l'Oscepa.

Tots els certificats que emeti l'Oscepa contindran un identificador de política corresponent al tipus de certificat aplicable.

L'Oscepa emet els tipus de certificats següents, que poden identificar-se mitjançant l'identificador d'objectes de política de certificats continguda en l'extensió *certificatePolicy* d'un certificat. A continuació s'identifiquen els tipus de certificat emesos per l'Oscepa.

- Certificats corporatius públics, adquirits pel sector públic per cobrir les seves necessitats de seguretat.
- Certificats de la ciutadania, emesos per l'Entitat de Certificació de l'Administració Pública Andorrana o per altres prestadors de serveis de certificació, quan hagin estat objecte d'admissió per part de l'Administració pública.

Complementàriament, es defineix la tipologia de certificats següent:

- Certificats individuals de persona física.
- Certificats individuals de persona física amb professió regulada.
- Certificats corporatius de persona física al servei d'una administració pública.
- Certificats corporatius de persona física al servei d'una organització privada.
- Certificat de representant de persona jurídica privada, pública o entitat sense personalitat jurídica.
- Segell d'òrgan, Administració pública o entitat de dret públic.
- Segell d'empresa.

## *1.3. Participants en la PKI*

### 1.3.1 Autoritats de certificació

És el component d'una PKI responsable de l'emissió i gestió dels certificats digitals. Actua com a tercera part de confiança, entre el signant (subscriptor) i el tercer que confia, en les relacions electròniques, vinculant una determinada clau pública amb una persona.

Una autoritat de certificació (AC) utilitza autoritats de registre (AR) per dur a terme les tasques de comprovació i emmagatzematge de la documentació dels continguts incorporats en el certificat digital.

Una AC pertany a una entitat jurídica indicada en el camp "organització" (O) del certificat digital associat.

La informació relativa a l'AC gestionada per l'Administració pública andorrana pot trobar-se en aquest document o a l'adreça web https://www.signaturaelectronica.ad/jerarquia-politiques-i-practiques-de-certificacio.

### 1.3.2 Autoritats de registre

Una autoritat de registre (AR) pot ser una persona física o jurídica que actua d'acord amb aquesta CPS i, si escau, mitjançant un acord subscrit amb una AC concreta, exercint les funcions de gestió de les sol·licituds i identificació i registre dels sol·licitants del certificat, i les que es disposin en les polítiques de certificació concretes. Les AR són autoritats delegades de l'AC, encara que l'AC és l'última responsable del servei en darrera instància.

A l'efecte d'aquesta CPS podran actuar com a AR:

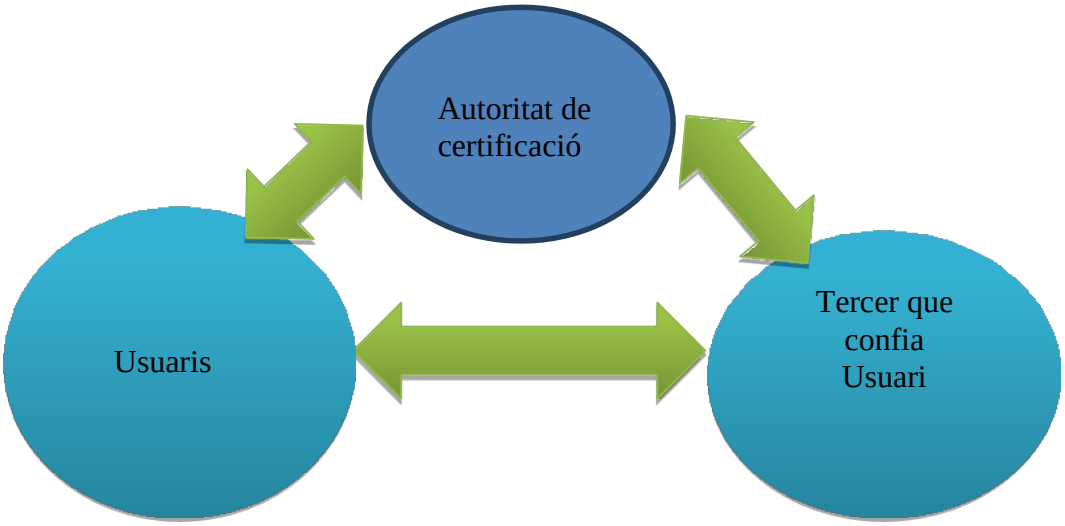
- La mateixa autoritat de certificació.
- Qualsevol agent nacional o internacional que mantingui una relació contractual amb l'AC i superi els processos d'alta i les auditories que demostren que se segueixen els requisits exigits en aquest document.

### 1.3.3 Signant/subscriptor

Entenem per signant/subscriptor el titular del certificat quan sigui una persona física o jurídica i està descrita en el camp CN del certificat. Quan s'emeti a nom d'un dispositiu maquinari o aplicació informàtica, es considerarà signant/subscriptor la persona física o jurídica sol·licitant del certificat emès.

### 1.3.4 Part que confia

En aquesta CPS s'entén per *tercer que confia* o *usuari* la persona que rep una transacció electrònica efectuada amb un certificat emès per l'AC gestionada per l'Oscepa i que voluntàriament confia en el certificat emès per aquesta última.




### 1.3.5 Altres participants

No és aplicable.

## *1.4. Àmbit d'aplicació i usos*

### 1.4.1 Usos apropiats dels certificats

Els certificats de l'Oscepa podran usar-se en els termes que estableix aquest document. En

termes generals, admeten els certificats per als usos següents:

- Autenticació basada en certificats X.509v3.
- Signatura electrònica, avançada o reconeguda, basada en certificats X.509v3.
- Xifratge asimètric o mixt, basat en certificats X.509v3.

### 1.4.2 Usos prohibits dels certificats

Els certificats només podran ser emprats amb els límits i per als usos per als quals hagin estat emesos en cada cas, i que estan descrits en aquest document.

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

La utilització dels certificats digitals en operacions que contravenen la CPS o els contractes de l'AC amb les AR o amb els seus signants/subscriptors tindrà la consideració d'ús indegut, als efectes legals oportuns, i per tant s'eximirà l'AC, en funció de la legislació vigent, de qualsevol responsabilitat per aquest ús indegut dels certificats que faci el signant o qualsevol tercer.

L'Oscepa no té accés a les dades sobre les quals es pot aplicar l'ús d'un certificat. Així doncs, i com a conseqüència d'aquesta impossibilitat tècnica d'accedir al contingut del missatge, no és possible que l'Oscepa emeti cap valoració sobre aquest contingut, i per tant el signatari assumeix qualsevol responsabilitat que provingui del contingut aparellat a l'ús d'un certificat. Així mateix, serà imputable al signatari qualsevol responsabilitat que pogués derivar-se de la utilització del certificat fora dels límits i les condicions d'ús recollides en la CPS i els contractes de l'AC amb els seus signants, així com qualsevol altre ús indegut del certificat derivat d'aquest apartat o que pugui ser interpretat com a tal en funció de la legislació vigent.

L'Oscepa incorpora en el certificat informació sobre la limitació d'ús, bé en camps estandarditzats en els atributs "ús de la clau" (*key usage*), "restriccions bàsiques" (*basic constrains*) i/o "restriccions de nom" (*name constrains*) marcats com a crítics en el certificat i per tant de compliment obligatori per les aplicacions que l'utilitzin, o bé limitacions en atributs com "ús estès de clau" (*extended key usage*) i/o mitjançant textos incorporats al camp "declaració de l'emissor" (*user notice*) marcats com a "no crític" però d'obligat compliment pel titular i l'usuari del certificat.

## *1.5. Autoritat de polítiques*

Aquesta CPS defineix la forma en què l'autoritat de certificació dona resposta a tots els requisits i nivells de seguretat imposats per les polítiques de certificació corresponents.

L'activitat de l'autoritat de certificació podrà ser sotmesa a la inspecció de l'autoritat de les polítiques (PA) o per personal delegat per aquesta última.

Per a les jerarquies descrites en aquest document, l'autoritat de les polítiques correspon a la direcció tècnica de l'Oscepa.

### 1.5.1 Organització que administra el document

La redacció i el control d'aquesta CPS són gestionats per la direcció tècnica de l'Oscepa.

### 1.5.2 Dades de contacte de l'organització

| | |
|---|---|
| **Adreça:** | Carrer de la Grau, Edifici Prat del Rull, Andorra la Vella |
| **Telèfon:** | +376 875 700 |
| **A/e:** | oficina.certificacio@govern.ad |

Per reportar incidents de seguretat relacionats amb els certificats podeu posar-vos en contacte amb l'Administració pública andorrana mitjançant una comunicació dirigida al compte de correu electrònic oficina.certificacio@govern.ad.

### 1.5.3 Persona que determina la idoneïtat de la CPS per a la política

La direcció tècnica de l'Oscepa es constitueix per tant en l'autoritat de les polítiques (PA) de les jerarquies i autoritats de certificació descrites anteriorment i és responsable de l'administració de la CPS.

### 1.5.4 Procediments de gestió del document

La publicació de les revisions d'aquesta CPS ha d'estar aprovada per la direcció tècnica de l'Oscepa.

L'Administració pública andorrana publica a la seva pàgina web cada nova versió. La CPS està publicada en format PDF signat electrònicament amb un certificat digital.

## *1.6. Acrònims i definicions*

### 1.6.1 Acrònims

AC Autoritat de certificació

RA Autoritat de registre

CPS *Certification Practice Statement*. Declaració de pràctiques de certificació CRL *Certificate Revocation List.* Llista de certificats revocats

CSR *Certificate Signing Request.* Petició de signatura de certificat DES *Data Encryption Standard*. Estàndard de xifratge de dades

DN *Distinguished Name.* Nom distintiu dins del certificat digital

DSA *Digital Signature Algorithm.* Estàndard d'algoritme de signatura

DSCF Dispositiu segur de creació de signatura

DSADCF Dispositiu segur de magatzem de dades de creació de signatura

FIPS *Federal Information Processing Standard Publication*

IETF *Internet Engineering Task Force*

ISO I*nternational Organization for Standardization.* Organisme Internacional d'Estandardització

ITU *International Telecommunications Union.* Unió Internacional de Telecomunicacions

| | |
|---|---|
| LDAP | Lightweight Directory Access Protocol. Protocol d'accés a directoris |
| OCSP | *Online Certificate Status Protocol.* Protocol d'accés a l'estat dels certificats |
| OID | *Object Identifier*. Identificador d'objecte |
| PA | *Policy Authority.* Autoritat de polítiques |
| PC | *Política de certificació* |
| PIN | *Personal Identification Number*. Número d'identificació personal |
| PKI | *Public Key Infrastructure*. Infraestructura de clau pública |
| RSA | Rivest-Shamir-Adleman. Tipus d'algorisme de xifratge |
| SHA | *Secure Hash Algorithm.* Algorisme segur de Hash |
| SSL | *Secure Sockets Layer*. Protocol dissenyat per Netscape i convertit en estàndard de la xarxa. Permet la transmissió d'informació xifrada entre un navegador d'Internet i un servidor. |
| TCP / IP | *Transmission Control. Protocol / Internet Protocol*. Sistema de protocols, definits en el marc de la IEFT. El protocol TCP s'usa per dividir en origen la informació en paquets, per després recompondre-la en destinació. El protocol IP s'encarrega d'adreçar adequadament la informació cap al seu destinatari. |

### 1.6.2 Definicions

| | |
|---|---|
| Autoritat de certificacions | L'entitat responsable de l'emissió i gestió dels certificats digitals. Actua com a tercera part de confiança entre el subjecte/signant i la part usuària, vinculant una determinada clau pública amb una persona. |
| Autoritat de polítiques | Persona o conjunt de persones responsables de totes les decisions relatives a la creació, administració, manteniment i supressió de les polítiques de certificació i CPS. |
| Autoritat de Registre | Entitat responsable de la gestió de les sol·licituds i la identificació i registre dels sol·licitants d'un certificat. |
| Certificació encreuada | L'establiment d'una relació de confiança entre dos AC, mitjançant l'intercanvi de certificats entre les dos en virtut de nivells de seguretat semblants. |
| Certificat | Arxiu que associa la clau pública amb algunes dades identificatives del subjecte/signant i és signada per l'AC. |
| Clau pública | Valor matemàtic conegut públicament i usat per a la verificació d'una signatura digital o el xifratge de dades. També anomenada *dades de verificació de signatura*. |
| Clau privada | Valor matemàtic conegut únicament pel |

| | |
|---|---|
| | subjecte/signant i usat per a la creació d'una signatura digital o el desxifratge de dades. També anomenada *dades de creació de signatura*.<br><br>La clau privada de l'AC s'usarà per a signatura de certificats i signatura de CRL. |
| CPS | Conjunt de pràctiques adoptades per una autoritat de certificació per emetre certificats de conformitat amb una política de certificació concreta. |
| CRL Arxiu | Que conté una llista dels certificats que han estat revocats en un període de temps determinat i que és signada per l'AC. |
| Dades d'activació de dades | Privades, com PIN o contrasenyes emprades per activar la clau privada. |
| DSADCF | Dispositiu segur de magatzem de les dades de creació de signatura. Element programari o maquinari emprat per custodiar la clau privada del subjecte/signant de manera que només ell en tingui el control. |
| DSCF | Dispositiu segur de creació de signatura. Element programari o maquinari emprat pel subjecte/signant per generar signatures electròniques, de manera que es duguin a terme les operacions criptogràfiques dins el dispositiu i se'n garanteixi el control únicament per part del subjecte/signant. |
| Entitat | Dins del context d'aquestes polítiques de certificació, l'empresa o organització de qualsevol mena amb la qual el sol·licitant té algun tipus de vinculació. |
| Signatura digital | El resultat de la transformació d'un missatge, o qualsevol tipus de dada, per l'aplicació de la clau privada en conjunció amb uns algoritmes coneguts, per garantir d'aquesta manera:<br>a) Que les dades no han estat modificades (integritat)<br><br>b) Que la persona que signa les dades és qui diu ser (identificació)<br><br>c) Que la persona que signa les dades no pot negar haver-ho fet (no repudi en origen) |
| OID | Identificador numèric únic registrat sota l'estandardització ISO i referit a un objecte o classe d'objecte determinat. |
| Parell de claus | Conjunt format per la clau pública i privada, ambdós relacionades entre si matemàticament. |

| | |
|---|---|
| PKI | Conjunt d'elements maquinari, programari, recursos humans, procediments, etc., que componen un sistema basat en la creació i gestió de certificats de clau pública. |
| Política de certificació | Conjunt de regles que defineixen l'aplicabilitat d'un certificat en una comunitat i/o en alguna aplicació, amb requisits de seguretat i d'utilització comuns. |
| Sol·licitant | Dins del context d'aquesta política de certificació, el sol·licitant serà una persona física apoderada amb un poder especial per fer determinats tràmits en nom i representació de l'entitat. |
| Subjecte/firmant | Dins del context d'aquesta Declaració de pràctiques de certificació, la persona física la clau pública de la qual és certificada per l'AC i que disposa d'una de privada vàlida per generar signatures digitals. |
| Part usuària | Dins del context d'aquesta política de certificació, persona que voluntàriament confia en el certificat digital i l'utilitza com a mitjà d'acreditació de l'autenticitat i integritat del document signat. |

# 2. RESPONSABILITAT DE PUBLICACIÓ I DIPÒSITS

## *2.1. Repositoris*

L'Oscepa fa públic el seu certificat d'AC, l'estat de validesa dels certificats digitals emesos i la CPS.

El repositori es troba a https://www.signaturaelectronica.ad/ajuda.

Els serveis de consulta estan dissenyats per garantir una disponibilitat de 24 hores per dia set dies a la setmana.

L'Oscepa sol·licita prèviament l'autorització del titular abans de publicar el certificat.

## *2.2. Publicació d'informació de certificats*

L'Oscepa publica les CRL i l'accés al servei OCSP a:

http://crl.govern.ad/GovernAndorra.crl
http://crl1.govern.ad/GovernAndorra.crl
http://ocsp.govern.ad
http://ocsp1.govern.ad

## *2.3. Freqüència de publicació*

L'Oscepa emet i publica llistes de revocats de forma periòdica seguint la taula marcada en l'apartat d'aquestes pràctiques "Freqüència d'emissió de CRL".

L'Oscepa publica de forma immediata al seu lloc web https://www.signaturaelectronica.ad/jerarquia-politiques-i-practiques-de-certificacio qualsevol modificació en les polítiques i la CPS, i manté un històric de versions.

Aquesta informació es publicarà quan es trobi disponible i, en especial, de forma immediata quan s'emeten les mencions relatives a la vigència dels certificats.

Els canvis en la CPS es regiran pel que estableix la secció corresponent de la CPS.

La informació d'estat de revocació de certificats es publicarà d'acord amb el que estableix la secció corresponent d'aquesta CPS.

Al cap de 15 (quinze) dies des de la publicació de la nova versió, podrà retirar-se la referència al canvi de la pàgina principal i inserir-se en el dipòsit. Les versions antigues de la documentació seran conservades per un període de 15 (quinze) anys per l'entitat de certificació i podran ser consultades, per causa raonada, pels interessats.

## *2.4. Controls d'accés als repositoris*

L'accés al repositori de l'Oscepa és lliure.

Es mantenen controls físics i lògics per impedir modificacions o esborrament d'informació no autoritzat en aquest repositori.

# 3. IDENTIFICACIÓ I AUTENTICACIÓ

## *3.1. Denominació*

### 3.1.1 Tipus de noms

El signant/subscriptor es descriu en els certificats mitjançant un nom distintiu (DN, *distinguished name*, *Subject*) d'acord amb l'estàndard X.501. Les descripcions de camp DN estan reflectides en cadascuna de les fitxes de perfil dels certificats. Així mateix, inclou un component *Common Name* (CN =).

Les fitxes de perfil es poden sol·licitar a través del suport a client a oficina.certificacio@govern.ad i en https://www.signaturaelectronica.ad/ajuda

En certificats corresponents a persones físiques, la identificació del signatari estarà formada pel seu nom i cognoms més el seu NIA.

En certificats corresponents a persones jurídiques, aquesta identificació es durà a terme per mitjà de la seva denominació o raó social i el seu NRT.

### 3.1.2 Significat dels noms

Tots els noms distingits han de ser significatius, i la identificació dels atributs associats al subscriptor ha de ser en una forma llegible per humans. Vegeu 7.1.4.

### 3.1.3 Anonimat o pseudònims de subscriptors

No és aplicable.

### 3.1.4 Regles utilitzades per interpretar diversos formats de noms

L'Oscepa atén en tot cas el que marca l'estàndard X.500 de referència en l'ISO / IEC 9594.

### 3.1.5 Unicitat dels noms

Dins de la mateixa AC no es pot tornar a assignar un nom de subscriptor que ja hagi estat ocupat a un subscriptor diferent. Això s'aconsegueix incorporant l'identificador fiscal únic a la cadena del nom que distingeix el titular del certificat.

#### *3.1.5.1 Emissió de diversos certificats de persona física per a un mateix titular*

Sota aquesta CPS el subscriptor pot demanar més d'un certificat sempre que la combinació dels valors següents que hi hagi en la sol·licitud sigui diferent d'un certificat vàlid:

- Número d'identificació administrativa (NIA) de la persona física
- Número de registre tributari (NRT) de l'empresa
- Tipus de certificat (camp Descripció del certificat)

Com a excepció, aquesta CPS permet la validació d'una sol·licitud d'un certificat quan coincideixin el NIA, l'NRT i el tipus amb un certificat vàlid, sempre que hi hagi algun element diferenciador entre tots dos en els camps Title i/o Departament.

### 3.1.6 Reconeixement, autenticació i funció de marques registrades i altres signes distintius

L'Oscepa no assumeix compromisos en l'emissió de certificats respecte a l'ús de marques i altres signes distintius. L'Oscepa no permet deliberadament l'ús d'un signe distintiu sobre el subjecte/signant que no tingui drets d'ús. No obstant això, l'OSCEPA no està obligada a buscar proves sobre els drets d'ús sobre marques registrades o altres signes distintius amb anterioritat a l'emissió dels certificats, així que pot negar-se a generar o sol·licitar la revocació de qualsevol certificat involucrat en una disputa.

### 3.1.7 Procediment de resolució de disputes de noms

L'Oscepa no té responsabilitat en el cas de resolució de disputes de noms. En tot cas, l'assignació de noms es durà a terme basant-se en el seu ordre d'entrada.

L'Administració pública andorrana no arbitra aquest tipus de disputes, que hauran de ser resoltes directament per les parts.

## *3.2. Validació inicial de la identitat*

### 3.2.1 Mètodes de prova de la possessió de la clau privada

L'Oscepa empra diversos circuits per emetre certificats en què la clau privada es gestiona de diferent manera. La clau privada pot ser generada tant per l'usuari com per l'Oscepa.

a) Generació de claus per part de l'Oscepa.
   En programari: es lliuren al subjecte/signant en mà o mitjançant correu a través de fitxers protegits utilitzant l'Standard PKCS # 12. La seguretat del procés queda garantida pel fet que el codi d'accés a l'arxiu PKCS # 12 que possibilita que s'instal·li en les aplicacions es lliura per un mitjà diferent de l'utilitzat en la recepció de l'arxiu.

   En maquinari: les claus poden ser lliurades per l'Oscepa al subjecte/signant, directament o a través d'una autoritat de registre en un dispositiu segur de creació de signatura.

b) Generació de les claus pel subscriptor.
   El signant disposa d'un mecanisme de generació de claus, ja sigui programari o maquinari, La prova de possessió de la clau privada en aquests casos és la petició rebuda per l'Oscepa en format PKCS # 10 o un de criptogràficament equivalent.

## 3.2.2 Identificació de l'entitat

### *3.2.2.1 Identitat*

Amb caràcter previ a l'emissió i el lliurament d'un certificat emès a una persona jurídica o a una persona física amb atribut de vinculació a una entitat, cal autenticar les dades relatives a la constitució i la personalitat jurídica de l'entitat.

Per a aquests certificats, s'exigeix en tots els casos la identificació de l'entitat, per a la qual cosa la RA requerirà la documentació pertinent en funció del tipus d'entitat.

A més, es comprova:

- Que les dades o documents aportats no tinguin una antiguitat superior a 1 any.

En administracions públiques: no s'exigeix la documentació acreditativa de l'existència de l'Administració pública, organisme o entitat de dret públic, atès que aquesta identitat forma part de l'àmbit corporatiu de les AAPP de l'Estat.

### *3.2.2.2 Marques registrades*

Vegeu el punt 3.1.6.

### *3.2.2.3 Verificació de país*

Vegeu el punt 3.2.2.1.

### *3.2.2.4 Validació de l'autorització o control de domini*

Vegeu el punt 3.2.5.1.

### *3.2.2.5 Autenticació d'una adreça IP*

No aplicable.

### *3.2.2.6 Validació del domini Wildcard*

No aplicable.

### *3.2.2.7 Exactitud de les fonts de dades*

Vegeu el punt 3.2.2.1.

### *3.2.2.8 Registres CAA*

No aplicable.

## 3.2.3 Identificació de la identitat d'un individu

Amb caràcter previ a l'emissió i el lliurament d'un certificat, s'exigeix la presència física del subjecte/titular o signant quan sigui una persona física o del sol·licitant quan el subjecte/titular és una entitat jurídica, amb la presentació d'un document oficial que acrediti de forma fefaent la seva identitat (document oficial d'identitat, targeta de residència, passaport o qualsevol altre document admès en dret), d'acord amb el que disposa l'article 26 de la Llei 35/2014, del 27 de novembre, de serveis de confiança electrònica, sempre que contingui, almenys, la informació següent:

- Nom i cognoms de la persona
- Lloc i data de naixement
- Número d’identitat reconegut legalment
- Altres atributs de la persona que hagin de constar en el certificat

En el cas de documents d’identitat estrangers, es podrà demanar la traducció jurada en català amb la postil·la de la Haia si es considera necessari.

### 3.2.4 Informació de subscriptor no verificada

No està permès sota aquestes pràctiques de certificació incloure informació no verificada en el "*subject"* d’un certificat.

## 3.2.5 Validació de l'autoritat

### *3.2.5.1 Identificació de la vinculació*

| Tipus de certificat | Documentació |
|---|---|
| Certificats individuals de persona física<br><br>Certificats individuals de persona física amb professió regulada<br><br>Certificats corporatius de persona física al servei d'una Administració pública<br><br>Certificats corporatius de persona física al servei d'una organització privada<br><br>Certificat de representant de persona jurídica privada, pública o entitat sense personalitat jurídica | L'article 26.2 de la Llei 35/2014, del 27 de novembre, de serveis de confiança electrònica estableix el següent: "El prestador de serveis de confiança electrònica qualificat haurà de verificar fefaentment la identitat i, si escau, qualsevol altra atribució específica de la persona natural a qui expedeix el certificat electrònic qualificat, mitjançant l'exhibició dels documents públics o privats que acrediti suficientment. Aquesta informació ha de ser verificada pel proveïdor de serveis qualificat o per un tercer que actuï sota la responsabilitat del proveïdor de serveis qualificat:<br>i. A través de la presència física d'aquesta persona, o<br>ii. A distància, utilitzant altres certificats electrònics reconeguts emesos per un proveïdor de serveis qualificat."<br>D'altra banda, l'article 26.3 de la Llei 35/2014, del 27 de novembre, de serveis de confiança electrònica, estableix que en el cas de "certificats electrònics expedits a persones físiques però vinculades a una organització, entitat, institució, empresa o una altra persona jurídica, el prestador de serveis de confiança ha d'acreditar, a més de la identitat de la persona sol·licitant i de la persona identificada en el certificat electrònic, les dades relatives a la constitució i personalitat jurídica de l'entitat, o l'extensió i validesa de les facultats o poders de representació de la persona sol·licitant, mitjançant els documents públics que acrediti de forma específica o mitjançant la consulta del registre públic corresponent, que és el resultat de les dades que hagin de figurar-hi". |
| Segell d'òrgan, Administració pública o entitat de dret públic<br><br>Segell d'empresa (persona jurídica) | L'article 26.2 de la Llei 35/2014, del 27 de novembre, de serveis de confiança electrònica, estableix el següent: "El prestador de serveis de confiança electrònica qualificat ha de verificar la identitat i, si escau, qualsevol altra atribució específica de la persona jurídica a la qual s'expedeixi el certificat electrònic qualificat, mitjançant l'exhibició de documents públics o privats que acrediti suficientment. Aquesta informació ha de ser verificada pel proveïdor de serveis qualificat o per un tercer que actuï sota la responsabilitat del proveïdor de serveis qualificat:<br>i. Mitjançant la presència física d'un representant autoritzat de la persona jurídica, o<br>ii. A distància, utilitzant altres certificats electrònics reconeguts emesos per un proveïdor de serveis qualificat." |

### 3.2.6 Criteris per a la interoperació

L'Oscepa pot proporcionar serveis que permetin que una altra CA operi dins, o interoperi amb, la seva PKI. Aquesta interoperació pot incloure certificació encreuada, certificació unilateral o altres formes d'operació. L'Oscepa es reserva el dret de proporcionar serveis d'interoperació i interoperar amb altres CA, els termes i criteris dels quals s'han d'establir contractualment.

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

### 3.3.1 Validació per a la renovació rutinària de certificats

La identificació d'una sol·licitud de renovació es fa a través del certificat que s'ha de renovar. No es renovarà si el certificat per renovar ha superat els cinc anys des de l'última verificació física o procés equivalent.

### 3.3.2 Identificació i autenticació de la sol·licitud de renovació després d'una revocació

La política d'identificació i autenticació per renovar el certificat després d'una revocació serà la mateixa que per al registre inicial.

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

La forma de fer les sol·licituds de revocació s'estableix en l'apartat 4.9.3 d'aquest document.

L'Oscepa pot sol·licitar, per iniciativa pròpia, la revocació d'un certificat si sap o sospita que la clau privada del subscriptor s'ha vist compromesa, o si sap o sospita de qualsevol altre esdeveniment que aconselli prendre aquesta mesura.

# 4. REQUISITS D'OPERACIÓ DEL CICLE DE VIDA DELS CERTIFICATS

L'Oscepa empra, per a la gestió del cicle de vida dels certificats, una plataforma que permet la sol·licitud, el registre, la publicació i la revocació de tots els certificats emesos.

## *4.1. Sol·licitud de certificats*

### 4.1.1 Qui pot fer la sol·licitud d'un certificat

Una sol·licitud de certificat pot ser presentada pel subjecte del certificat o per un representant autoritzat d'aquest últim, en el cas del segell d'empresa.

### 4.1.2 Procediment d'alta i responsabilitats

#### *4.1.2.1 Formularis web*

Les sol·licituds dels certificats es fan de forma general mitjançant l'accés als formularis de sol·licitud a l'adreça o mitjançant l'enviament al sol·licitant d'un enllaç a un formulari concret, o presencialment a qualsevol entitat de registre.

https://www.signaturaelectronica.ad

Al lloc web es troben els formularis necessaris per fer la sol·licitud de cada tipus de certificat distribuït per l'Oscepa en diferents formats i els dispositius de generació de signatura, si fossin necessaris.

El formulari permetrà la incorporació d'un CSR (PKCS # 11) en el cas que l'usuari hagi creat les claus.

L'usuari rep, després de la confirmació de les dades de la sol·licitud, un correu electrònic en el compte associat a la sol·licitud del certificat amb un enllaç per confirmar la sol·licitud i acceptar les condicions d'ús.

Un cop confirmada la sol·licitud, el subscriptor és informat de la documentació que ha de presentar en una oficina de registre habilitada i ha de complir el requisit d'identificació presencial si és pertinent.

#### *4.1.2.2 Sol·licituds via capa de serveis web (WS)*

A fi d'incorporar la integració d'aplicacions de tercers amb la plataforma de gestió de certificats Status propietat de l'AC Camerfirma, s'ha desenvolupat una capa de serveis web (WS) que ofereixen processos d'emissió i revocació de certificats. Les trucades a aquests WS estan signades amb un certificat reconegut per la plataforma.

L'emissió "cega" d'aquest tipus de certificats fa que el procés sigui revisat en detall. Abans d'iniciar l'emissió mitjançant aquest sistema s'ha de comptar amb un informe tècnic favorable de l'AC Camerfirma, un contracte en què l'autoritat de registre es compromet a mantenir el sistema en condicions de seguretat òptimes i a notificar a l'Oscepa qualsevol modificació o

incidència. Addicionalment el sistema haurà de ser sotmès a auditories anuals en què es comprova:

1. Els expedients documentals dels certificats emesos.
2. Que els certificats són emesos sota les directrius marcades per les polítiques de certificació sota la qual es regeixen.

#### *4.1.2.3 Lots*

La plataforma Status permet igualment circuits de sol·licitud mitjançant lots. En aquest cas, el sol·licitant enviarà a l'AR un fitxer estructurat segons un disseny prefixat per l'Oscepa amb les dades dels sol·licitants. L'AR carregarà les peticions en l'aplicació de gestió.

## *4.2. Processament de les sol·licituds de certificats*

### 4.2.1 Execució de les funcions d'identificació i autenticació

Un cop hagi tingut lloc una petició de certificat, l'operador de l'RA, mitjançant l'accés a la plataforma de gestió PKI (Status o Siaval SafeCert), verifica que la informació proporcionada és conforme.

L'operador de la plataforma posseeix un certificat de gestió interna emès per dur a terme aquestes operacions i que s'obté després d'un procés de formació i avaluació.

El certificat utilitzat per l'operador de registre és considerat un accés multifactor usat no només per a l'accés a la plataforma de gestió PKI (Status o Siaval SafeCert), sinó per aprovar cada petició d'emissió d'un certificat fent una signatura electrònica.

### 4.2.2 Aprovació o refús de la sol·licitud

**Per als certificats d'entitat final:**

L'operador de registre visualitza les peticions pendents de tramitar i que li han estat assignades.

L'operador de l'RA queda en espera que el subjecte/signant lliuri la documentació corresponent.

Si la informació no és correcta, l'RA denega la petició. En el cas que les dades es verifiquin correctament l'entitat de registre ha d'aprovar l'emissió del certificat mitjançant la signatura electrònica amb el seu certificat d'operador.

### 4.2.3 Termini per resoldre la sol·licitud

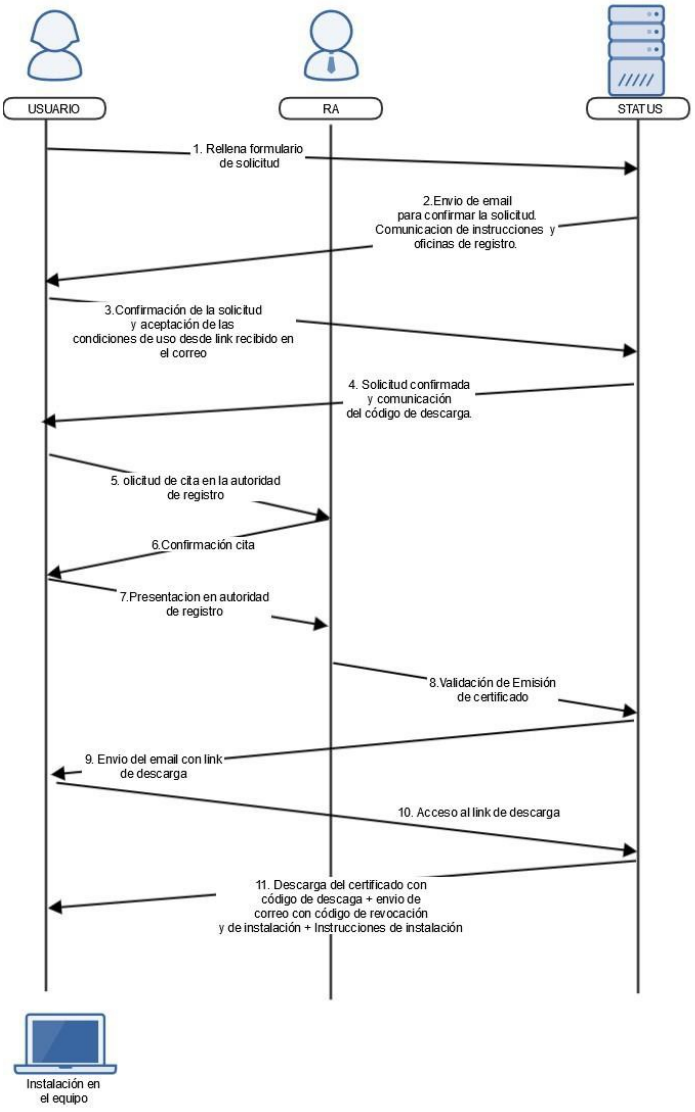
Les sol·licituds presentades per la plataforma PKI Status es validen un cop comprovada la documentació acreditativa associada al perfil del certificat. Sempre que sigui viable, l'Oscepa eliminarà les sol·licituds amb més d'un any d'antiguitat.

## *4.3. Emissió de certificats*

### 4.3.1 Accions de la CA durant el procés d'emissió

#### *4.3.1.1 Certificats en programari*

Un cop aprovada la sol·licitud, el subscriptor rep un correu electrònic amb la notificació d'aquest fet i a partir d'aquí es pot generar i descarregar el certificat. Per a la instal·lació necessita el codi de producte que li ha estat lliurat i un codi d'instal·lació que s'haurà lliurat en un correu electrònic independent conjuntament amb un codi de revocació.



#### *4.3.1.2 Certificats en HW (dispositiu segur de creació de signatura)*

La clau privada la genera el titular mitjançant el procés d'emissió proveït pel prestador, un cop ha estat personat i validat per l'AR.

Els parells de claus es generen en un dispositiu qualificat de creació de signatura electrònica o QSCD Siaval SafeCert Server Signing System. Les claus són protegides sota el control exclusiu del signant i, per tant, no hi ha cap lliurament de la clau privada al titular, la protecció es fa amb el PIN o la contrasenya i un segon factor d'autenticació basat en un missatge SMS enviat al telèfon mòbil de l'usuari.

El sistema informarà el titular que se li emetrà el certificat de signatura centralitzada i generarà en aquest moment la seva clau privada i l'emmagatzemarà en el sistema de manera protegida, de manera que se'n garanteixi l'ús sota el control exclusiu del seu titular.

La clau pública és generada juntament amb la clau privada sobre el dispositiu qualificat de creació de signatura electrònica Siaval SafeCert Server Signing System i és lliurada a l'autoritat de certificació mitjançant l'enviament d'una sol·licitud de certificació en format PKCS # 10.

### 4.3.2 Notificació de l'emissió al subscriptor

L'Oscepa notifica al sol·licitant, mitjançant un correu electrònic, l'aprovació o denegació de la sol·licitud.

## *4.4. Acceptació de certificats*

### 4.4.1 Conducta que constitueix acceptació del certificat

Un cop emès l'usuari disposa d'un període de set dies per comprovar-ne l'emissió correcta.

Si el certificat no ha estat emès correctament per causes tècniques, es revocarà i se n'emetrà un de nou.

### 4.4.2 Publicació del certificat per l'AC

L'Oscepa ofereix un sistema de consulta de l'estat dels certificats emesos al seu lloc web: https://secure.camerfirma.com/solicitudes_status/estado_certificado.php. L'accés a aquesta pàgina és lliure i gratuït.

### 4.4.3 Notificació d'emissió de certificat per l'AC a altres entitats

L'Oscepa ofereix un sistema de consulta de l'estat dels certificats emesos al seu lloc web: https://secure.camerfirma.com/solicitudes_status/estado_certificado.php. L'accés a aquesta pàgina és lliure i gratuït.

## *4.5. Ús del parell de claus i els certificats*

### 4.5.1 Ús del certificat i la clau privada del subscriptor

La limitació d'ús de la clau ve definida en el contingut del certificat en les extensions: keyUsage, extendedKeyUsage i basicConstraints.

| CA | Key Usage | Extended Key Usage | Basic Constraints |
|---|---|---|---|
| **Entitat de certificació de l'Administració pública andorrana** | critical, cRLSign, keyCertSign | - | critical, CA: true |
| PERSONA FÍSICA en DSCF - Signatura | critical, nonRepudiation | clientAuth, emailProtection | critical, CA: false |
| PERSONA FÍSICA en DSCF - IDENTITAT | critical, digitalSignature | clientAuth, emailProtection | critical, CA: false |
| PERSONA FÍSICA AMB professió regulada en DSCF - Signatura | critical, nonRepudiation | clientAuth, emailProtection | critical, CA: false |
| PERSONA FÍSICA AMB professió regulada en DSCF - IDENTITAT | critical, digitalSignature | clientAuth, emailProtection | critical, CA: false |
| PERSONA FÍSICA AMB professió regulada en DSCF – XIFRATGE | critical, keyEncipherment, dataEncipherment | clientAuth, emailProtection | critical, CA: false |
| PERSONA FÍSICA al servei d'una ORGANITZACIÓ en DSCF - Signatura | critical, nonRepudiation | clientAuth, emailProtection | critical, CA: false |
| PERSONA FÍSICA al servei d'una ORGANITZACIÓ en DSCF - IDENTITAT | critical, digitalSignature | clientAuth, emailProtection | critical, CA: false |
| PERSONA FÍSICA al servei de l'ADMINISTRACIÓ a DSCF - Signatura | critical, nonRepudiation | clientAuth, emailProtection | critical, CA: false |
| PERSONA FÍSICA al servei de l'ADMINISTRACIÓ a DSCF - IDENTITAT | critical, digitalSignature | clientAuth, emailProtection | critical, CA: false |
| PERSONA FÍSICA al servei de l'ADMINISTRACIÓ a DSCF – XIFRA | critical, keyEncipherment, dataEncipherment | clientAuth, emailProtection | critical, CA: false |
| SEGELL D'EMPRESA (persona jurídica) a HSM - Segell electrònic | critical, nonRepudiation | clientAuth, emailProtection | critical, CA: false |
| SEGELL D'EMPRESA (persona jurídica) a HSM – IDENTITAT | critical, digitalSignature | clientAuth, emailProtection | critical, CA: false |
| SEGELL D'EMPRESA (persona jurídica) en programari | critical, digitalSignature, keyEncipherment, dataEncipherment, nonRepudiation | clientAuth, emailProtection | critical, CA: false |
| SEGELL DE REGISTRE, ADMINISTRACIÓ PÚBLICA O ENTITAT DE DRET PÚBLIC a HSM – signatura | critical, nonRepudiation | clientAuth, emailProtection | critical, CA: false |
| SEGELL DE REGISTRE, ADMINISTRACIÓ PÚBLICA O ENTITAT DE DRET PÚBLIC a HSM – IDENTITAT | critical, digitalSignature | clientAuth, emailProtection | critical, CA: false |
| SEGELL DE REGISTRE, ADMINISTRACIÓ PÚBLICA O ENTITAT DE DRET PÚBLIC a programari | critical, digitalSignature, keyEncipherment, dataEncipherment, nonRepudiation | clientAuth, emailProtection | critical, CA: false |
| REPRESENTANT DE PERSONA JURÍDICA en HSM - Segell electrònic | critical, nonRepudiation | clientAuth, emailProtection | critical, CA: false |
| REPRESENTANT DE PERSONA JURÍDICA en HSM - IDENTITAT | critical, digitalSignature | clientAuth, emailProtection | critical, CA: false |

*Malgrat eu el xifrat de les dades es possible amb els certificats, l'OScepa no es responsabilitza dels danys causats per la pèrdua de control per part del titular de la clau privada necessària per des-xifrar la informació..*

### 4.5.2 Ús de la clau pública i del certificat per la part que confia

Les parts que confien han d'accedir i utilitzar la clau pública i el certificat los segons el que estipula aquesta CPS i segons el que indiquen les "Condicions d'ús", bé en un document físic o mitjançant l'acceptació en el procés d'emissió.

## *4.6. Renovació del certificat*

### 4.6.1 Circumstància per a la renovació del certificat

Un certificat s'ha de renovar abans de la data de caducitat del certificat. Un cop renovat, l'Oscepa emet el certificat renovat amb data d'inici igual a la data de caducitat del certificat que s'ha de renovar.

Els certificats OCSP s'emeten periòdicament i no s'estableixen processos de renovació.

### 4.6.2 Qui pot sol·licitar la renovació

En els certificats en què es permet la renovació, l'autenticació del posseïdor es fa sobre la base del seu certificat que s'ha de renovar.

### 4.6.3 Processament de sol·licituds de renovació de certificats

Abans de renovar un certificat, l'Oscepa comprova que la informació utilitzada per verificar la identitat i altres dades del signant i del posseïdor de la clau segueix sent vàlida.

En el cas de renovació dels certificats d'entitat final de persona física, es permet l'emissió d'un certificat sense presència física fins a un període de cinc anys des de l'últim registre presencial. Un cop superat el termini marcat, el signant haurà de fer un procés d'emissió presencial igual al realitzat en la primera emissió. Sota aquestes pràctiques, si en el moment de la renovació del certificat no han transcorregut més de cinc anys, la presència física del titular no serà requerida.

Sota aquestes pràctiques, si qualsevol informació del signant o del posseïdor de la clau ha canviat, s'ha de fer un nou registre i emissió, d'acord amb el que estableixen les seccions corresponents en aquest document.

*L'Oscepa duu a terme les renovacions de certificats emetent sempre noves claus i, per tant, el procés tècnic d'emissió és igual al que se segueix quan es fa una nova petició.*

L'Oscepa fa quatre avisos (30 dies, 15 dies, 7 dies, 1 dia) via correu electrònic al signant en què li notifica que el certificat caduca.

El procés de renovació s'inicia a partir del correu d'avís de caducitat o directament a través del lloc web de l'Oscepa, https://www.signaturaelectronica.ad.

Aquest procés requereix disposar del certificat vàlid que s'ha de renovar.

- Un cop identificat amb el certificat que s'ha de renovar, l'aplicació presenta al signant les dades del certificat antic i li demana la confirmació d'aquestes dades. L'aplicació permet al signant modificar l'adreça electrònica assignada al certificat. Si hi ha altres dades incorporades en el certificat que han canviat, el certificat s'ha de revocar i s'ha de fer una emissió nova.
- La petició s'incorpora a l'aplicació de l'RA en què l'operador, un cop revisades les dades, demana l'emissió del certificat a l'AC.
- L'Oscepa, com a norma general, emet un nou certificat prenent com a inici de validesa la finalització del certificat que s'ha de renovar. En algun cas es permet en els processos d'emissió, a través dels serveis web, la renovació del certificat amb data en el mateix moment de la renovació, i posteriorment es revoca el certificat que s'ha de renovar.

### 4.6.4 Notificació de nova emissió de certificat al subscriptor

La notificació de l'emissió d'un certificat renovat es produirà tal com es descriu a la secció 4.3.2 d'aquest document.

### 4.6.5 Conducta que constitueix l'acceptació d'un certificat de renovació

Segons l'apartat 4.4.1 d'aquest document.

### 4.6.6 Publicació del certificat de renovació per la CA

Segons l'apartat 4.4.2 d'aquest document.

### 4.6.7 Notificació d'emissió de certificat per la CA a altres entitats

En alguns casos s'envien certificats d'entitat final als supervisors nacionals que regulen les activitats de les autoritats de certificació.

Els certificats OCSP es comuniquen a diferents organismes governamentals que disposen de plataforma de validació de certificats.

Els certificats d'autoritat de certificació arrel i d'autoritat de certificació intermèdia es notifiquen al supervisor nacional per incorporar-los en el seu TSL, i addicionalment a un repositori d'informació gestionat per Mozilla, que incorpora informació sobre autoritats de certificació (CCADB). Aquesta base de dades és utilitzada per diversos programes comercials per gestionar els seus magatzems de confiança.

## *4.7. Renovació de claus*

Aquest és el procediment habitual de la renovació dels certificats de l'Oscepa, de manera que tots els processos descrits a la secció 4.6 es refereixen a aquest mètode de renovació.

L'Oscepa no permet la renovació de certificats sense la renovació de claus.

### 4.7.1 Circumstància per a la renovació de claus (*re-key*) del certificat

La renovació de certificats normalment tindrà lloc com a part de la renovació d'un certificat.

### 4.7.2 Qui pot sol·licitar la certificació d'una nova clau pública

Segons el que està estipulat en 4.6.2.

### 4.7.3 Processament de sol·licituds de canvi de claus del certificat

Segons el que està estipulat en 4.6.3.

### 4.7.4 Notificació de nova emissió de certificat al subscriptor

Segons el que està estipulat en 4.6.4.

### 4.7.5 Conducta que constitueix l'acceptació d'un certificat amb noves claus (*re-keyed*)

Segons el que està estipulat en 4.6.5.

### 4.7.6 Publicació del certificat amb renovació de claus (*re-keyed*) per l'AC

Segons el que està estipulat en 4.6.6.

### 4.7.7 Notificació d'emissió de certificat per l'AC a altres entitats

Segons el que està estipulat en 4.6.7.

## *4.8. Modificació de certificats*

Qualsevol necessitat de modificació de certificats implicarà una nova sol·licitud. Es farà una revocació del certificat i una nova emissió amb les dades corregides.

En el cas de tractar-se d'un procés de substitució de certificats, es considerarà una renovació i així computa a l'hora de calcular els anys de renovació sense presència física tal com marca la llei.

Es podran modificar certificats i renovar quan els atributs del subscriptor o del posseïdor de claus que formin part del control d'unicitat previst per aquesta política no hagin variat.

Si la sol·licitud de modificació es fa dins del període ordinari previst per renovar el certificat, es durà a terme aquesta renovació.

### 4.8.1 Circumstància per modificar el certificat

No és aplicable.

### 4.8.2 Qui pot sol·licitar la modificació del certificat

No és aplicable.

### 4.8.3 Processament de sol·licituds de modificació de certificats

No és aplicable.

### 4.8.4 Notificació de l'emissió d'un nou certificat al subscriptor

No és aplicable.

### 4.8.5 Conducta que constitueix l'acceptació del certificat modificat

No és aplicable.

### 4.8.6 Publicació del certificat modificat per la CA

No és aplicable.

### 4.8.7 Notificació d'emissió de certificat per la CA a altres entitats

No és aplicable.

## *4.9. Revocació i suspensió de certificats*

S'entén per *revocació* aquell canvi en l'estat d'un certificat motivat per la seva pèrdua de validesa en funció d'alguna circumstància diferent de la de la seva caducitat.

La suspensió, per la seva banda, suposa una revocació amb causa de suspensió (això és, un cas particular de revocació), és a dir, es revoca un certificat temporalment fins que es decideixi sobre l'oportunitat o no de fer una revocació definitiva o la seva activació.

El període màxim de suspensió d'un certificat és de set dies naturals. En cas que s'arribi al període màxim de suspensió i el certificat no hagi estat activat, el sistema automàticament revoca definitivament el certificat amb causa "sense especificar".

L'extinció de la vigència d'un certificat electrònic per causa de revocació o suspensió produirà efectes davant de tercers des que la indicació d'aquesta extinció s'inclogui en el servei de consulta sobre la vigència dels certificats del prestador de serveis de certificació (publicació de la llista de certificats revocats o consulta al servei OCSP).

L'Oscepa manté els certificats a la llista de revocació fins a la fi de la seva validesa. Quan aquesta situació es produeix, s'eliminen de la llista de certificats revocats. L'Oscepa només eliminarà de la Llista de revocació un certificat quan es produeixi alguna de les dos situacions següents.

- Caducitat del certificat.
- Certificat revocat per causa de suspensió del qual, un cop revisat, s'ha conclòs que no es troben causes per revocar-lo definitivament.

No obstant, l'Oscepa mantindrà la informació sobre l'estat d'un certificat caducat en les seves bases de dades i accessible a través del servei OCSP.

No es permet en cap cas sota aquestes pràctiques la utilització d'un certificat revocat.

La resposta OCSP per a un certificat revocat quan caduca manté l'estat de revocat i la seva causa.

A causa de les diferents naturaleses dels serveis OCSP i CRL, en cas d'obtenir respostes diferents per a un certificat caducat es mantindrà com a resposta vàlida la que ofereix l'OCSP.

Per a l'Oscepa el servei de consulta de l'estat d'un certificat primari és l'ofert per l'OCSP.

### 4.9.1 Causes de revocació

Com a norma general es revocarà un certificat per:

- Modificació d'alguna de les dades contingudes al certificat.
- Descobriment que alguna de les dades aportades en la sol·licitud de certificat és incorrecta o incompleta, així com l'alteració o modificació de les circumstàncies verificades per expedir el certificat.
- Manca de pagament del certificat.

Per circumstàncies que afecten la seguretat de la clau o del certificat:

- Compromís de la clau privada o de la infraestructura o sistemes de l'entitat de certificació que va emetre el certificat, sempre que afecti la fiabilitat dels certificats emesos a partir d'aquest incident.
- Infracció, per l'entitat de certificació, dels requisits previstos en els procediments de gestió de certificats, establerts en aquesta CPS.
- Compromís o sospita de compromís de la seguretat de la clau o del certificat del signant o del responsable del certificat.
- Accés o utilització no autoritzats, per un tercer, de la clau privada del signant o del responsable de certificat.
- L'ús irregular del certificat pel signant o del responsable del certificat, o falta de diligència en la custòdia de la clau privada.

Per circumstàncies que afecten la seguretat del dispositiu criptogràfic:

- Compromís o sospita de compromís de la seguretat del dispositiu criptogràfic.
- Pèrdua o inutilització per danys del dispositiu criptogràfic.
- Accés no autoritzat, per un tercer, a les dades d'activació del signant o del responsable de certificat.

Per circumstàncies que afecten el signant o el responsable del certificat.

- Finalització de la relació entre entitat de certificació i signant o responsable del certificat.
- Modificació o extinció de la relació jurídica subjacent o causa que va provocar l'emissió del certificat al signant o responsable del certificat.
- Infracció pel sol·licitant del certificat dels requisits preestablerts per sol·licitar-lo.
- Infracció pel signant o responsable del certificat de les seves obligacions, responsabilitat i garanties, establertes en l'instrument jurídic corresponent o en aquesta Declaració de pràctiques de certificació.
- La incapacitat sobrevinguda o la mort del signant o responsable del certificat.
- L'extinció de la persona jurídica signant del certificat, així com la finalitat de l'autorització del signant al responsable del certificat o la finalització de la relació entre signant i responsable del certificat.
- Sol·licitud del signant de revocació del certificat, d'acord amb el que estableix aquesta CPS.
- Resolució ferma de l'autoritat administrativa o judicial competent.

Altres circumstàncies:

- La suspensió del certificat digital per un període superior al que està establert en aquesta CPS.
- Per l'emissió d'un certificat que no compleixi els requisits establerts en aquesta Declaració de pràctiques de certificació.
- La finalització del servei de l'entitat de certificació, d'acord amb el que estableix la secció corresponent en aquesta CPS.

Per justificar la necessitat de revocació que s'al·lega s'hauran de presentar davant l'RA o l'AC els documents corresponents, en funció de la causa que motiva la sol·licitud.

- Si sol·licita la revocació el titular del certificat o la persona física sol·licitant d'un certificat de persona jurídica, haurà de presentar una declaració signada per ell en què indiqui el certificat que s'ha de revocar i la causa d'aquesta sol·licitud, i s'haurà d'identificar davant l'RA.

- Si la revocació la demana un tercer, haurà de presentar una autorització bé del titular persona física bé del representant legal de la persona jurídica titular en què s'indiquin a més les causes per les quals se sol·licita la revocació del certificat i s'haurà d'identificar davant l'RA.

- Si sol·licita la revocació l'entitat vinculada al titular per causa de la terminació de la relació amb aquest últim, ha d'acreditar aquesta circumstància (revocació de poders, fi de contracte...) i la persona s'ha d'identificar davant l'RA com a facultada per representar l'entitat.

Els signants disposen dels codis de revocació que poden fer servir en els serveis de revocació via web o mitjançant una trucada telefònica als serveis de suport.

### 4.9.2 Qui pot sol·licitar la revocació

La revocació d'un certificat la pot sol·licitar:

- El subjecte/signant.
- El sol·licitant responsable.
- L'entitat (a través d'un representant seu).
- L'AR o l'AC.
- També es preveu la possibilitat que tercers o parts interessades puguin comunicar fraus, mals usos, conductes inadequades o dades errònies. En aquest cas, l'AR o l'AC podrà revocar el certificat després de comprovar la veracitat d'aquestes causes de revocació.

### 4.9.3 Procediment de sol·licitud de revocació

Totes les sol·licituds s'han de fer:

- Mitjançant el Servei de Revocació en línia, a través de l'accés al servei de revocació local situat al lloc web de l'Oscepa i introduint-hi el PIN de revocació pels certificats de persona jurídica.

  https://www.signaturaelectronica.ad

- A través de la presència física en l'AR, en horari d'atenció al públic, mostrant un document d'identificatció vàlid del signant/subscriptor o sol·licitant. Aquest darrer omplirà la sol·licitud de revocació del/s certificats/s.
- Enviant a l'Oscepa un document signat per un representant amb capacitat de representació suficient de l'entitat en què se sol·liciti la revocació del certificat.

  L'Oscepa manté al seu lloc web tota la informació relativa als processos de revocació dels certificats.

*Tant el servei de gestió de les revocacions com el servei de consulta són considerats serveis crítics, i així consten en el Pla de contingències i el pla de continuïtat de negoci de l'Oscepa. Aquests serveis estaran disponibles les 24 hores del dia, els set dies de la setmana. En cas de fallada de sistema, o qualsevol altre factor que no estigui sota el control de l'Oscepa, l'Oscepa farà els màxims esforços per assegurar que aquests serveis no es troben inaccessibles durant un període màxim de 24 hores.*

### 4.9.4 Període de gràcia de la sol·licitud de revocació

El príode de revocació des que l'Oscepa o un AR té coneixement autenticat de la revocació d'un certificat es produeix de forma immediata o en un termini màxim de 24 hores, i s'incorpora en la pròxima CRL que s'ha d'emetre i en la base de dades de la plataforma de gestió on s'alimenta el transponedor OCSP.

### 4.9.5 Temps dins el qual CA ha de processar la sol·licitud de revocació

L'Oscepa processarà una sol·licitud de revocació de manera immediata a partir del procediment descrit en el punt 4.9.3.

En les revocacions produïdes per una mala emissió del certificat, es notificarà prèviament al titular per acordar els terminis de la substitució.

En tot cas, i sota aquestes pràctiques de certificació, l'Oscepa pot revocar un certificat de forma unilateral i immediata per motius de seguretat, sense que el titular pugui reclamar cap mena d'indemnització per aquest fet.

### 4.9.6 Requisits de comprovació de la revocació per les parts que confien en els certificats

Els tercers que confien en els certificats han de comprovar, prèviament al seu ús, el seu estat. Hauran de comprovar en tot cas l'última CRL emesa, que podrà descarregar-se en l'URL que apareix en l'extensió Punt de Distribució de CRL (CRL Distribution Point) de cada certificat.

L'Oscepa emet sempre CRL signades per l'AC que ha emès el certificat. La CRL conté un camp (NextUpdate) amb la data de la seva pròxima actualització.

### 4.9.7 Freqüència d'emissió de CRL

| CA | Freqüència d'emissió | Durada |
|---|---|---|
| Entitat de Certificació de l'Administració pública andorrana | 24 hores | 48 hores |

### 4.9.8 Màxima latència de CRL

Les CRL es publiquen cada 24 hores i tenen una validesa de 48 hores.

### 4.9.9 Disponibilitat de comprovació en línia de la revocació

L'AC proporciona un servei en línia de comprovació de revocació via HTTPS a https://www.camerfirma.com/area-de-usuario/consulta-de-certificados/.

També mitjançant consultes OCSP

a: https://www.signaturaelectronica.ad/consulta-l-estat-del-certificat-

csp

Les adreces d'accés a aquests serveis venen referenciades en el certificat digital. Per a les CRL i ARL en l'extensió Punts de Distribució de CRL, CRL Distribution Point, i l'adreça de l'OCSP en l'extensió Accés a la Informació de l'Autoritat (Authority Information Access).

En els certificats pot aparèixer més d'una adreça d'accés a les CRL per garantir-ne la disponibilitat.

El servei OCSP s'alimenta de les CRL emeses per les diferents autoritats de certificació (CA) o per accessos a la BD de la plataforma (EE). Les dades tècniques d'accés, així com els certificats de validació de les respostes OCSP, es troben publicades al web de l'Oscepa: https://www.signaturaelectronica.ad/consulta-l-estat- de l'-Certificat-OCSP.

Aquests serveis estaran disponibles les 24 hores del dia, els 7 dies de la setmana, 365 dies a l'any.

L'Oscepa farà tots els esforços necessaris perquè el servei mai no es trobi inaccessible de forma contínua més de 24 hores, i serà aquest un servei crític en les activitats de l'Oscepa i per tant es tractarà de forma adequada en el Pla de contingències i de continuïtat de negoci.
La latència de publicació en el servei OCSP d'una revocació és d'1 hora.

### 4.9.10 Requisits de la comprovació en línia de la revocació

Per comprovar una revocació el tercer que confia en el certificat ha de conèixer l'adreça electrònica associada al certificat que es vol consultar si es fa mitjançant accés web o el número de sèrie si es comprova mitjançant el servei OCSP.

Les respostes OCSP van signades per les AC que emeten el certificat que s'ha de consultar, així que és necessari el certificat per validar la resposta. Els certificats actualitzats es poden

trobar a l'enllaç https://www.signaturaelectronica.ad/consulta-l-estat-del-certificat-ocsp.

### 4.9.11 Altres formes de divulgació d'informació de revocació disponibles

Els mecanismes que l'Oscepa posa a disposició dels usuaris de sistema estaran publicats al seu lloc web: https://www.camerfirma.com/area-de-usuario/consulta-de- certificats /.

### 4.9.12 Requisits especials de revocació per compromís de les claus

No estipulat.

### 4.9.13 Circumstàncies per a la suspensió

Quan es produeix una suspensió, l'Oscepa tindrà una setmana per decidir l'estat definitiu del certificat: revocat o actiu. En cas de no tenir en aquest termini tota la informació necessària per verificar el seu estat definitiu, l'Oscepa el revocarà.

En el cas de produir-se una suspensió del certificat, s'envia un comunicat mitjançant correu electrònic al signant/subscriptor en què es comunica l'hora de suspensió i la seva causa.

Si finalment la suspensió no dona lloc a la revocació definitiva i el certificat ha de tornar-se a activar, el signant/subscriptor rebrà un correu en què se li indicarà el nou estat del certificat.

El procés de suspensió no s'aplica a certificats
- D'operador d'AR
- D'OCSP

### 4.9.14 Qui pot sol·licitar la suspensió

Vegeu la secció 4.9.2.

### 4.9.15 Procediment de sol·licitud de suspensió

La sol·licitud de suspensió es farà mitjançant una comunicació oral o escrita prèviament autenticada. En el cas dels certificats de persona jurídica el subscriptor ha de tenir el codi de revocació per suspendre el certificat.

### 4.9.16 Límits del període de suspensió

Un certificat no romandrà suspès més de set dies.

L'Oscepa supervisarà, mitjançant un sistema d'alertes de la plataforma de gestió de certificats, que no se sobrepassa el període de suspensió marcat per aquesta CPS.

## *4.10. Serveis de comprovació de l'estat dels certificats*

### 4.10.1 Característiques operacionals

L'Oscepa disposa d'un servei de consulta de certificats emesos i llistes de revocació. Aquests serveis estan disponibles públicament al seu lloc web, https://www.camerfirma.com/area-de-usuario/consulta-de-certificados/.

### 4.10.2 Disponibilitat del servei

Els serveis de consulta estan dissenyats per garantir una disponibilitat de 24 hores per dia 7 dies a la setmana.

### 4.10.3 Característiques opcionals

No estipulat.

## *4.11. Finalització de la subscripció*

Transcorregut el període de vigència del certificat, finalitzarà la subscripció al servei. Com a excepció, el subscriptor pot mantenir el servei vigent sol·licitant la renovació del certificat, amb l'antelació que determina aquesta Declaració de pràctiques de certificació.

## *4.12. Custòdia i recuperació de claus*

### 4.12.1 Política i pràctiques de custòdia i recuperació de claus

Les claus dels usuaris es generen i custodien en un dispositiu qualificat de creació de signatura electrònica, de manera que el prestador de serveis de certificació no podrà en cap moment recuperar la clau dels usuaris ni podrà fer-ne una recuperació. En cas de pèrdua, s'haurà de revocar el certificat i emetre'n un de nou generant un altre parell de claus.

### 4.12.2 Política i pràctiques d'encapsulació i recuperació de claus de sessió

No estipulat.

# 5. CONTROLS DE LES INSTAL·LACIONS, DE GESTIÓ I OPERACIONALS

## *5.1. Controls de seguretat física*

L'Oscepa està subjecta a les validacions anuals de la norma UNE-ISO / IEC 27001: 2007, que regula l'establiment de processos adequats per garantir una correcta gestió de la seguretat en els sistemes d'informació.

L'Oscepa té establerts 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 emprats per a les operacions.

La política de seguretat física i ambiental aplicable als serveis de generació de certificats ofereix protecció davant:

- Accessos físics no autoritzats
- Desastres naturals
- Incendis
- Fallada dels sistemes de suport (energia electrònica, telecomunicacions, etc.)
- Esfondrament de l'estructura
- Inundacions
- Robatori
- Sortida no autoritzada d'equipaments, informacions, suports i aplicacions relatius a components emprats per als serveis del prestador de serveis de certificació

Les instal·lacions compten amb sistemes de manteniment preventiu i correctiu amb assistència 24 hores, 365 dies a l'any, amb assistència en les 24 hores següents a l'avís.

### 5.1.1 Ubicació i construcció

Les instal·lacions en què es troba l'Oscepa estan construïdes amb materials que garanteixen la protecció davant atacs per força bruta, estan situades en una zona de baix risc de desastres i permeten un accés ràpid.

En concret, la sala on es duen a terme les operacions criptogràfiques és una caixa de Faraday amb protecció de radiacions externes, doble vall, detecció i extinció d'incendis, sistemes contra la humitat, doble sistema de refrigeració i sistema doble de subministrament elèctric.

### 5.1.2 Accés físic

L'accés físic a les dependències de les instal·lacions en què es troba l'Oscepa on es duen a terme processos de certificació està limitat i protegit mitjançant una combinació de mesures físiques i procedimentals.

Està limitat a personal expressament autoritzat, amb identificació en el moment de l'accés i registre del personal, incloent-hi filmació per circuit tancat de televisió i el seu arxivament.

Qualsevol persona externa ha d'estar acompanyada per un responsable de l'organització quan es trobi per qualsevol motiu dins d'àrees restringides.

Les instal·lacions compten amb detectors de presència en tots els punts vulnerables, així com amb sistemes d'alarma per detectar intrusisme amb avís per canals alternatius.

L'accés a les sales es fa amb lectors de targeta d'identificació i és gestionat per un sistema informàtic que manté un registre d'auditoria d'entrades i sortides automàtic.

L'accés a les sales es fa amb lectors de targeta d'identificació i és gestionat per un sistema informàtic que manté un registre d'entrades i sortides automàtic.

L'accés als sistemes de certificació està protegit amb quatre nivells d'accés: Edifici, Oficines, CPD i Sala criptogràfica.

### 5.1.3 Alimentació elèctrica i aire condicionat

Les instal·lacions en què es troba l'Oscepa disposen d'equips estabilitzadors de corrent i un sistema d'alimentació elèctrica d'equips duplicat amb un grup electrogen.

Les sales que alberguen equips informàtics disposen de sistemes de control de temperatura amb equips d'aire condicionat duplicat.

### 5.1.4 Exposició a l'aigua

Les instal·lacions en què es troba l'Oscepa estan ubicades en una zona de baix risc d'inundació i en una primera planta. Les sales on s'alberguen equips informàtics disposen d'un sistema de detecció d'humitat.

### 5.1.5 Prevenció i protecció d'incendis

Les sales on s'alberguen equips informàtics disposen de sistemes de detecció i extinció d'incendis automàtics.

Els dispositius criptogràfics i suports que emmagatzemen claus de les entitats de certificació compten amb un sistema específic i addicional a la resta de la instal·lació, per a la protecció davant el foc.

### 5.1.6 Sistema d'emmagatzematge

Cada mitjà d'emmagatzematge desmuntable (cintes, cartutxos, CD, discs, etc.) roman solament a l'abast del personal autoritzat.

La informació amb classificació de confidencial, sense importar el dispositiu d'emmagatzematge, es guarda en armaris ignífugs o tancats amb una clau permanentment.

### 5.1.7 Eliminació de residus

Quan hagi deixat de ser útil, la informació sensible és destruïda de la forma més adequada segons el suport que la conté.

Impresos i paper: mitjançant trituradores o en papereres disposades a aquest efecte per posteriorment ser destruïts, sota control.

Mitjans d'emmagatzematge: abans de ser refusats o reutilitzats han de ser processats per esborrar, destruir físicament o fer il·legible la informació continguda.

### 5.1.8 Sistema de seguretat (*backup*) extern

L'Oscepa utilitza un magatzem extern segur per custodiar documents i dispositius magnètics i electrònics que són independents del centre operacional.

Es requereix almenys dues persones autoritzades expressament per a l'accés, el dipòsit o la retirada de dispositius.

## *5.2. Controls procedimentals*

### 5.2.1 Rols de confiança

Els rols de confiança garanteixen una segregació de funcions que dissemina el control i limita el frau intern, i no permet que una sola persona controli de principi a fi totes les funcions de certificació, amb una concessió de mínim privilegi, quan sigui possible.

Per determinar la sensibilitat de la funció, es tenen en compte els elements següents:

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

**Auditor intern:**
Responsable de l'acompliment dels procediments operatius. És una persona externa al Departament de Sistemes d'Informació.

Les tasques d'auditor intern són incompatibles en el temps amb les tasques de certificació i incompatibles amb sistemes. Aquestes funcions estaran subordinades a la prefectura d'operacions, i es reportarà tant a aquesta última com a la direcció tècnica.

**Administrador de sistemes:**
Responsable del funcionament correcte del maquinari i programari de suport de la plataforma de certificació.

Les tasques de l'administrador de sistemes són incompatibles amb les tasques de certificació i no pot dur a terme tasques dels auditors d'operacions.

**Administrador d'AC:**
Responsable de les accions que s'han d'executar amb el material criptogràfic, o amb la realització d'alguna funció que impliqui l'activació de les claus privades de les autoritats de certificació descrites en aquest document, o de qualsevol dels seus elements.

Les tasques de l'administrador d'AC són incompatibles amb les tasques de certificació i sistemes.

**Operador d'AC:**
Responsable necessari, conjuntament amb l'administrador d'AC, de la custòdia de material d'activació de les claus criptogràfiques. També és responsable de les operacions de còpia de seguretat i manteniment de l'AC.

Les tasques de l'operador d'AC són incompatibles amb les d'administrador d'AC i no pot dur a terme tasques d'auditor ni auditor intern.

**Operador d'RA:**
Persona responsable d'aprovar les peticions de certificació efectuades pel signant.

Les operacions d'operador d'RA són incompatibles amb les d'administrador d'RA i tampoc no pot dur a terme tasques d'auditoria interna ni externa.

**Operador de revocació:**
Les tasques de l'operador de revocació són incompatibles amb les tasques d'auditoria.

**Responsable de seguretat:**
Encarregat de coordinar, controlar i fer complir les mesures de seguretat definides per les polítiques de seguretat de l'Oscepa. S'ha d'encarregar dels aspectes relacionats amb la seguretat de la informació: lògica, física, xarxes, organitzativa, etc.

### 5.2.2 Nombre de persones requerides per tasca

L'Oscepa garanteix almenys dues persones per dur a terme les tasques classificades com a sensibles, principalment en la manipulació del dispositiu de custòdia de les claus de l'autoritat de certificació.

### 5.2.3 Identificació i autenticació per a cada rol

Les persones assignades per a cada rol són identificades per l'auditor intern, que s'assegura que cada persona duu a terme les operacions per a les quals està assignada.

Cada persona només controla els actius necessaris per al seu paper, i s'assegura així que cap persona no accedeix a recursos no assignats.

L'accés a recursos es fa en funció de l'actiu mitjançant targetes criptogràfiques i codis d'activació.

### 5.2.4 Rols que requereixen separació de tasques

Taula de segregació de rols.

| | Responsable de seguretat | Administració de sistemes | Operació de sistemes | Auditor de plataforma CA | Especialista en validació SSL | Operador RA |
|---|---|---|---|---|---|---|
| Responsable de seguretat | | SÍ | NO | SÍ | SÍ | SÍ |
| Administració de sistemes | NO | | NO | NO | NO | NO |
| Operació de sistemes | NO | NO | | NO | NO | NO |
| Auditor de plataformes CA | NO | NO | NO | | SÍ | SÍ |
| Especialista en validació SSL | NO | NO | NO | SÍ | | SÍ |
| Operador RA | NO | NO | NO | NO | SÍ | |

### 5.2.5 Arrencada i parada del sistema de gestió PKI

El sistema de PKI es compon dels mòduls següents:

Mòdul de gestió d'AR; per a això s'activaran o desactivaran els serveis del gestor de pàgines específic.

Mòdul de gestió de sol·licituds; per a això s'activaran o desactivaran els serveis del gestor de pàgines específic.

Mòdul de gestió de claus, ubicat en l'equip HSM. S'activa o desactiva mitjançant encesa física.

Mòdul de BD, gestió centralitzada dels certificats i CRL gestionats, OCSP i TSA. Arrencada i parada del servei específic del gestor de BD.

Mòdul OCSP. Servidor de respostes d'estat dels certificats en línia. Arrencada i parada del servei de sistema encarregat d'aquesta tasca.

El procés d'apagada de mòduls seguiria la seqüència:

- Mòdul de sol·licitud
- Mòdul d'AR
- Mòdul OCSP
- Mòdul BD
- Mòdul de gestió de claus

Es durà a terme l'encesa en procés invers.

## *5.3. Controls del personal*

### 5.3.1 Qualificacions, experiència i requisits d'autorització

Tot el personal està qualificat i ha estat instruït convenientment per executar les operacions que li han estat assignades.

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

L'Oscepa s'assegura que el personal de registre o els administradors d'AR són fiables i pertanyen a un organisme delegat per dur a terme les tasques de registre.

L'administrador d'AR haurà assistit a un curs de preparació per dur a terme les tasques de validació de les peticions.

En general, l'Oscepa retirarà de les seves funcions de confiança un empleat quan es tingui coneixement de l'existència de la comissió d'algun fet delictiu que pugui afectar l'acompliment de les seves funcions.

L'Oscepa no assignarà a un lloc fiable o de gestió una persona que no sigui idònia per al lloc, especialment per haver estat condemnada per un delicte o una falta que afecti la seva idoneïtat per al lloc. Per aquest motiu, prèviament es duu a terme una investigació, fins on permeti la legislació aplicable, relativa als aspectes següents:

- Estudis, incloent-hi la titulació al·legada.
- Treballs anteriors, fins a cinc anys, incloent-hi referències professionals i comprovació que realment es va dur a terme el treball al·legat.
- Morositat.

### 5.3.2 Procediments de comprovació d'antecedents

L'Oscepa, dins dels seus procediments de RRHH, fa les investigacions pertinents abans de contractar qualsevol persona i en el Govern d'Andorra se segueixen els procediments segons la Llei 1/2019, del 17 de gener, de la funció pública.

L'Oscepa, en la sol·licitud per al lloc de treball en determinats rols, informa sobre la necessitat de la investigació prèvia i adverteix que la negativa a sotmetre's a la investigació implicarà el refús de la sol·licitud. Així mateix, demana el consentiment inequívoc de l'afectat per a la investigació prèvia i processar i protegir totes les seves dades personals d'acord amb la legislació de protecció de dades de caràcter personal.

### 5.3.3 Requisits de formació

El personal encarregat de tasques de confiança ha estat format en els termes que estableixen les polítiques de certificació. Hi ha un pla de formació que forma part dels controls UNE-ISO / IEC 27001: 2007.

La formació inclou els continguts següents:

- Principis i mecanismes de seguretat de la jerarquia pública de certificació.
- Versions de maquinari i aplicacions en ús.
- Tasques que ha de dur a terme 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.

### 5.3.4 Requisits i freqüència de l'actualització de la formació

L'Oscepa duu a terme els cursos d'actualització necessaris per assegurar-se la correcta execució de les tasques de certificació, especialment quan s'hi facin modificacions substancials.

### 5.3.5 Freqüència i seqüència de rotació de tasques

No està estipulat.

### 5.3.6 Sancions per accions no autoritzades

L'Oscepa, per mitjà de la Secretaria de Funció Pública, disposa d'un règim sancionador intern, descrit en la seva política d'RH, per aplicar- lo quan un empleat dugui a terme accions no autoritzades, i es podrà arribar a fer-lo cessar.

### 5.3.7 Requisits de contractació de personal

Els empleats contractats per dur a terme tasques de confiança signen anteriorment les clàusules de confidencialitat i els requisits operacionals emprats pel Govern d'Andorra. Qualsevol acció que comprometi la seguretat dels processos acceptats podria, un cop avaluada, donar lloc al cessament del contracte laboral.

En el cas que tots o una part dels serveis de certificació siguin operats per un tercer, els controls i les previsions efectuades en aquesta secció, o en altres parts de la CPS, seran aplicats i complerts pel tercer que dugui a terme les funcions d'operació dels serveis de certificació. L'entitat de certificació serà responsable en tot cas de l'execució efectiva.

### 5.3.8 Documentació proporcionada al personal

L'Oscepa posa a disposició de tot el personal la documentació en què es detallen les funcions encomanades, en particular la normativa de seguretat i la CPS.

Aquesta documentació es troba en un repositori intern accessible per qualsevol empleat de l'Oscepa. Al repositori hi ha una llista de documents d'obligat coneixement i compliment.

A més se subministrarà la documentació que necessiti el personal en cada moment, a fi que pugui desenvolupar de forma competent les seves funcions.

## *5.4. Procediments de registre d'esdeveniments*

L'Oscepa està subjecta a les validacions anuals de la norma UNE-ISO / IEC 27001: 2007, que regula l'establiment de processos adequats per garantir una correcta gestió de la seguretat en els sistemes d'informació.

### 5.4.1 Tipus d'esdeveniments registrats

L'Oscepa registra i guarda els registres d'auditoria de tots els esdeveniments relatius al sistema de seguretat de l'AC.

S'han de registrar els esdeveniments següents:

- Encesa i apagada del sistema.
- Intents de creació, esborrament, establiment de contrasenyes o canvi de privilegis.
- Intents d'inici i fi de sessió.
- Intents d'accessos no autoritzats al sistema de l'AC a través de la xarxa.
- Intents d'accessos no autoritzats al sistema d'arxius.
- Accés físic als registres d'auditoria.
- Canvis en la configuració i el manteniment del sistema.
- Registres de les aplicacions de l'AC.
- Encesa i apagada de l'aplicació de l'AC.
- Canvis en els detalls de l'AC i/o les seves claus.
- Canvis en la creació de polítiques de certificats.
- Generació de claus pròpies.
- Creació i revocació de certificats.
- Registres de la destrucció dels mitjans que contenen les claus, dades d'activació.
- Esdeveniments relacionats amb el cicle de vida del mòdul criptogràfic, com recepció, ús i desinstal·lació del mòdul.

L'Oscepa també conserva, 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 signant, en cas de certificats individuals, o del posseïdor de claus, en cas de certificats d'organització.
- Possessió de dades d'activació, per a operacions amb la clau privada de l'entitat de certificació.
- Informes complets dels intents d'intrusió física i vulnerabilitats en les infraestructures que donen suport a l'emissió i gestió de certificats.

L'Oscepa manté un sistema que permet garantir:

- Espai suficient per a l'emmagatzematge de registres d'auditoria.
- Que els fitxers de registres d'auditoria no es reescriguin.

- Que la informació que es guarda inclou com a mínim: tipus d'esdeveniment, data i hora, usuari que executa l'esdeveniment i resultat de l'operació.
- Els fitxers de registres d'auditoria es guardaran en fitxers estructurats susceptibles d'incorporar-se en una BD per a l'exploració posterior.

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

L'Oscepa revisa els seus registres d'auditoria quan es produeix un avís de sistema motivat per l'existència d'algun incident.

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

### 5.4.3 Períodes de retenció per als diaris (*logs*) d'auditoria

L'Oscepa emmagatzema la informació dels registres d'auditoria almenys durant cinc anys.

### 5.4.4 Protecció dels registres d'auditoria

Els registres d'auditoria dels sistemes són protegits de la manipulació mitjançant la signatura dels fitxers que els contenen.

Són emmagatzemats en dispositius tancats en clau i en repositoris degudament protegits

Se'n protegeix la disponibilitat mitjançant l'emmagatzematge en instal·lacions externes al centre on s'ubica l'AC.

L'accés als fitxers de registres d'auditoria està reservat només a les persones autoritzades. Els

dispositius són manejats en tot moment per personal autoritzat.

Hi ha un procediment intern en què es detallen els processos de gestió dels dispositius que contenen dades de registres d'auditoria.

### 5.4.5 Procediments de còpia de seguretat dels registres d'auditoria

L'Oscepa, a través del Departament de Sistemes d'Informació, disposa d'un procediment adequat de còpia de seguretat de manera que, en cas de pèrdua o destrucció d'arxius rellevants, estiguin disponibles en un període curt de temps les corresponents còpies de còpia de seguretat dels registres d'auditoria.

L'Oscepa té implantat un procediment de sistema de seguretat (*backup*) dels diaris (*logs*) d'auditoria, i cada setmana fa una còpia de tots els registres d'auditoria en un mitjà extern.

A més es manté una còpia en un centre de custòdia extern.

### 5.4.6 Sistema de recollida d'informació d'auditoria

La informació de l'auditoria d'esdeveniments és recollida internament i de forma automatitzada pel sistema operatiu, la xarxa i el programari de gestió de certificats, i també per les dades generades manualment, que seran emmagatzemades pel personal degudament autoritzat. Tot això compon el sistema d'acumulació de registres d'auditoria.

### *5.4.7* Notificació al subjecte causa de l'esdeveniment

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

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

### 5.4.8 Anàlisi de vulnerabilitats

L'anàlisi de vulnerabilitats queda coberta pels processos d'auditoria de l'Oscepa. Anualment es revisen els processos de gestió de riscos i vulnerabilitats dins del marc de revisió de la certificació UNE-ISO / IEC 27001.

Les dades d'auditoria dels sistemes són emmagatzemades per utilitzar-les en la investigació de qualsevol incidència i localitzar vulnerabilitats.

Mensualment el Departament de Sistemes d'Informació del Govern d'Andorra executa una anàlisi dels sistemes de l'Oscepa amb objectiu de detectar activitats sospitoses. Aquest informe és executat per una empresa externa i incorpora:

- Detecció d'intrusió - IDS (HIDS)
- Sistema de control d'integritat OSSEC
- Splunk. Intel·ligència operacional
- Informe de correlació d'esdeveniments

L'Oscepa corregeix qualsevol problema reportat i és registrat pel departament de sistemes.

## *5.5. Arxiu de registres*

### 5.5.1 Tipus d'arxius registrats

Els documents següents implicats en el cicle de vida del certificat són emmagatzemats per l'AC o per les RA:

- Totes les dades d'auditoria de sistema. PKI i OCSP incorporen els esdeveniments de signatura realitzats.
- Totes les dades relatives als certificats, incloent-hi els contractes amb els signants i RA. Les dades relatives a la identificació i la ubicació dels certificats.
- Sol·licituds d'emissió i revocació de certificats.

- Tipus de document presentat en la sol·licitud del certificat.
- Identitat de l'entitat de registre que accepta la sol·licitud de certificat.
- Número d'identificació únic proporcionat pel document anterior.
- Tots els certificats emesos o publicats.
- CRL emeses o registres de l'estat dels certificats generats.
- L'historial de claus generades.
- Les comunicacions entre els elements de la PKI.
- Polítiques i pràctiques de certificació.

L'Oscepa és el responsable de l'arxivament correcte de tot aquest material.

### 5.5.2 Període de retenció per a l'arxivament

Els certificats, els contractes amb els subjectes/signants i qualsevol informació relativa a la identificació i autenticació del subjecte/signant es conservaran durant almenys quinze anys.

Les versions antigues de la documentació també són conservades, per un període de quinze anys, per l'Oscepa, i podran ser consultades, per causa raonada, pels interessats.

### 5.5.3 Protecció de l'arxiu

L'Oscepa assegura la correcta protecció dels arxius mitjançant l'assignació de personal qualificat per tractar-los i emmagatzemar-los en armaris tancats amb clau.

### 5.5.4 Procediments de còpia de seguretat de l'arxiu

L'Oscepa disposa d'un centre d'emmagatzematge extern per garantir la disponibilitat de les còpies de l'arxiu de fitxers electrònics. Els documents físics es troben emmagatzemats en llocs segurs d'accés restringit només a personal autoritzat.

L'Oscepa com a mínim fa còpies de seguretat incrementals diàries de tots els seus documents electrònics i fa còpies de seguretat completes mensualment per a casos de recuperació de dades.

### 5.5.5 Requisits per al segellament de temps dels registres

Els registres estan datats amb una font fiable via NTP, GPS i sistemes de sincronització via ràdio.

L'Oscepa disposa d'un document de seguretat informàtica en què descriu la configuració dels paràmetres de data i hora dels equips utilitzats en l'emissió de certificats.

### 5.5.6 Sistema de recollida d'informació d'auditoria

L'Oscepa disposa d'un sistema centralitzat de recollida d'informació de l'activitat dels equips implicats en el servei de gestió de certificats.

### 5.5.7 Procediments per obtenir i verificar informació arxivada

L'Oscepa disposa d'un document de seguretat informàtica en què es descriu el procés per verificar que la informació arxivada és correcta i accessible.

## *5.6. Canvi de claus*

El canvi de claus importants final es duu a terme mitjançant un nou procés d'emissió (vegeu l'apartat corresponent d'aquesta CPS).

Abans que el certificat de l'AC caduqui es farà un canvi de claus. El certificat que s'ha d'actualitzar de l'AC i la seva clau privada només es faran servir per signar CRL mentre hi hagi certificats actius emesos per aquesta AC. Es generarà un nou certificat d'AC amb una clau privada nova i un CN (*common name*) diferent del certificat de l'AC que s'ha de substituir.

També es farà el canvi de certificat d'una AC quan l'estat de l'art criptogràfic (algoritmes, mida de claus, etc.) ho requereixi.

## *5.7. Recuperació en cas de compromís de la clau o desastre*

El cas de compromís de la clau arrel es pren com un cas particular en el document de contingència i continuïtat de negoci. Aquesta incidència afecta, en cas de substitució de les claus, els reconeixements per diverses aplicacions del sector privat i públic. Una recuperació de l'efectivitat de les claus en termes de negoci dependrà principalment de la durada d'aquests processos de reconeixement. El document de contingència i continuïtat de negoci incorpora aquests termes purament tècnics i operatius perquè les noves claus estiguin disponibles, però no així el seu reconeixement per tercers.

El compromís dels algoritmes o els paràmetres associats utilitzats en la generació de certificats digitals o serveis associats s'incorpora també en el Pla de contingències i continuïtat de negoci.

### 5.7.1 Procediments de gestió d'incidències i compromisos

L'Oscepa ha desenvolupat un pla de contingències per recuperar els sistemes crítics, si fos necessari un centre de dades alternatiu com a part del certificat UNE-ISO / IEC 27001: 2007.

### 5.7.2 Corrupció de recursos, aplicacions o dades

Si algun equip es fa malbé o deixa de funcionar però les claus privades no es destrueixen, l'operació s'ha de restablir el més ràpid possible donant prioritat a la capacitat de generar informació de l'estat del certificat segons el pla de recuperació de desastres de l'Oscepa.

### 5.7.3 Compromís de clau privada de l'entitat

El Pla de contingències emmarcat en el certificat UNE-ISO / IEC 27001: 2007 de l'Oscepa tracta el compromís de la clau privada de l'AC com una situació de desastre.

En cas de compromís d'una clau arrel:

- Informarà del compromís tots els signants/subscriptors, el tercer que confia i altres AC amb els quals tingui acords o un altre tipus de relació.
- Indicarà que els certificats i la informació relativa a l'estat de la revocació signats usant aquesta clau no són vàlids.

### 5.7.4 Continuïtat del negoci després d'un desastre

L'Oscepa restablirà els serveis crítics (revocació i publicació de revocats) d'acord amb el Pla de contingències i continuïtat de negoci emmarcat en el certificat UNE-ISO / IEC 27001: 2007, indicant un restabliment en les 24 hores següents.

L'Oscepa disposa d'un centre alternatiu en cas de ser necessari per posar en funcionament els sistemes de certificació, descrit en el Pla de continuïtat de negoci.

## *5.8. Cessament de l'AC o AR*

Abans del cessament de la seva activitat, l'Oscepa durà a terme les actuacions següents:

- Proveirà dels fons necessaris (mitjançant una assegurança de responsabilitat civil) per continuar la finalització de les activitats de revocació.
- Informarà de la cessació tots els signants/subscriptors, el tercer que confia i altres AC amb els quals tingui acords o un altre tipus de relació, amb una anticipació mínima de sis mesos.
- Revocarà tota autorització a entitats subcontractades per actuar en nom de l'AC en el procediment d'emissió de certificats.
- Transferirà les seves obligacions relatives al manteniment de la informació del registre i dels diaris (*logs*) durant el període de temps indicat als subscriptors i usuaris.
- Les claus privades de l'AC seran destruïdes o desactivades per a l'ús.
- L'Oscepa mantindrà els certificats actius i el sistema de verificació i revocació fins a l'extinció de tots els certificats emesos.

# 6. CONTROLS DE SEGURETAT TÈCNICA

## *6.1. Generació i instal·lació del parell de claus*

### 6.1.1 Generació del parell de claus

Els equips usats per l'Oscepa són nCipher. Aquests dispositius alberguen claus arrel i estan certificats FIPS 140-2, si nivell 3.

Les claus arrel es generen i gestionen en un equip fora de línia, en una sala criptogràfica.

Les claus de l'autoritat de certificació intermèdia es generen en equips HSM, on s'albergaran per a l'ús corresponent. El certificat emès per la clau arrel es fa en una sala criptogràfica segura.

#### *6.1.1.1 Generació del parell de claus de subscriptor*

Les claus del subjecte/signant poden ser creades per ell mateix mitjançant dispositius maquinari (SSCD) o programari autoritzats per l'Oscepa o poden ser creades per l'Oscepa en format programari PKCS # 12.

La plataforma de gestió Status genera amb els seus propis recursos una contrasenya aleatòria robusta i una clau privada protegida amb aquesta contrasenya usant l'algoritme 3DES. A partir d'aquesta clau privada genera una petició de signatura de certificat en format PKCS # 10. Amb aquesta petició l'AC fa la signatura del certificat del signant. El certificat és lliurat a l'usuari en un fitxer PKCS # 12, en el qual s'inclouen el mateix certificat i la clau privada que hi està associada. La contrasenya de la clau privada i del fitxer PKCS # 12 mai no està clara en el sistema.

Les claus són generades usant l'algoritme de clau pública RSA.

Les claus també poden ser creades en un sistema remot usant la capa de serveis web per generar una sol·licitud PKCS # 10 i la recollida del PKCS # 7 corresponent.

Les claus tenen una longitud mínima de 2.048 bits.

#### *6.1.1.2 Maquinari/programari de generació de claus*

Les claus dels signants/subscriptors poden ser generades per ells mateixos en un dispositiu autoritzat per l'Oscepa (vegeu 6.1.1.1.).

Per a les claus de l'autoritat de certificació intermèdia s'utilitza un dispositiu criptogràfic que compleix les especificacions FIPS 140-2 *level 2* i *level 3.*

### 6.1.2 Lliurament de la clau privada al signant

Vegeu el 3.2.1.

### 6.1.3 Lliurament de la clau pública a l'emissor del certificat

L'enviament de la clau pública a l'Oscepa per generar el certificat quan el circuit així ho requereixi, es duu a terme mitjançant un format estàndard, preferiblement en format PKCS # 10.

### 6.1.4 Lliurament de la clau pública de l'AC als usuaris

El certificat de l'AC i la seva empremta digital (f*ingerprint*) estaran a disposició dels usuaris al lloc web https://www.signaturaelectronica.ad/descarrega-claus-publiques.

### 6.1.5 Mida de les claus

Les claus privades del signant/subscriptor estan basades en l'algoritme RSA, amb una longitud mínima de 2.048 bits.

El període d'ús de la clau pública i privada varia en funció del tipus de certificat. Vegeu l'apartat 6.1.1.

### 6.1.6 Paràmetres de generació de la clau pública i control de qualitat

La clau pública de l'autoritat de certificació intermèdia i dels certificats dels subscriptors està codificada d'acord amb RFC 3280 i PKCS # 1. L'algoritme de generació de claus és l'RSA.

- Mida de les claus = mínim 2.048 bits
- Algorisme de generació de claus: rsagen1
- Mètode de farciment: EMSA-pkcs1-v1_5
- Funcions criptogràfiques de resum: SHA-256

### 6.1.7 Propòsits d'ús de claus

Tots els certificats emesos contenen els atributs "Key Usage" i "Extended Key Usage", tal com es defineix en l'estàndard X.509v3. Més informació disponible a la secció 7.1.2.

## *6.2. Protecció de la clau privada i estàndards per als mòduls criptogràfics*

### 6.2.1 Controls i estàndards de mòduls criptogràfics

#### *6.2.1.1 Clau privada de l'AC*

La clau privada de signatura de l'autoritat de certificació intermèdia és mantinguda en un dispositiu criptogràfic que compleix les especificacions FIPS 140-2, nivell 3.

Quan la clau privada de l'AC és fora del dispositiu, es manté xifrada.

Hi ha una còpia de seguretat (*backup*) de la clau privada de signatura de l'AC que és emmagatzemada i recuperada només pel personal autoritzat segons els rols de confiança fent servir, almenys, un control dual en un mitjà físic segur.

Les còpies de seguretat de la clau privada de signatura de l'AC estan emmagatzemades de forma segura. Aquest procediment es descriu en detall en les polítiques de seguretat de l'Oscepa.

#### *6.2.1.2* Clau privada del subscriptor

La clau privada del subscriptor es pot emmagatzemar en un dispositiu programari o maquinari.

Quan s'emmagatzemi en format programari, l'Oscepa oferirà les instruccions de configuració adequada per a un ús segur.

Pel que fa als dispositius criptogràfics distribuïts per l'Oscepa per albergar certificats qualificats, compleixen tots els requisits de dispositius qualificats de creació de signatura qualificada, i per tant són aptes per generar aquesta classe de signatura.

La informació respecte al procés de creació i custòdia de claus que utilitza l'Oscepa s'incorpora en el mateix certificat digital, mitjançant l'OID corresponent que permet a la part usuària actuar en conseqüència.

### 6.2.2 Control multipersonal (n d'entre m) de la clau privada

Es requereix un control multipersonal per activar la clau privada de l'AC. En el cas d'aquesta CPS, en concret hi ha una política de dos a quatre persones per a l'activació de les claus.

### 6.2.3 Dipòsit de clau privada

L'Oscepa no emmagatzema ni copia les claus privades dels titulars.

Excepcions:

- En cas de certificats per a xifratge d'informació, l'Oscepa pot guardar una còpia de la clau.

### 6.2.4 Còpia de seguretat de la clau privada

L'Oscepa fa una còpia de seguretat de les claus privades de l'AC que fa possible recuperar-les en cas de desastre, pèrdua o deteriorament. Tant la generació de la còpia com la recuperació necessiten almenys la participació de dos persones.

Aquests fitxers de recuperació s'emmagatzemen en armaris ignífugs i al centre de custòdia extern.

Les claus del signant en programari poden ser emmagatzemades per a la possible recuperació en cas de contingència, en un dispositiu d'emmagatzematge extern separat de la clau d'instal·lació tal com s'indica en el manual d'instal·lació de claus en programari.

Les claus del signant en maquinari no es poden copiar, ja que no poden sortir del dispositiu criptogràfic.

L’Oscepa guarda actes dels processos de gestió de les claus privades d’AC.

### 6.2.5 Arxiu de la clau privada

Les claus privades de les ACS són arxivades per un període de deu anys després de l’emissió de l’últim certificat. S’emmagatzemaran en arxius ignífugs segurs i en el centre de custòdia extern. Almenys serà necessària la col·laboració de dos persones per recuperar la clau privada de les AC al dispositiu criptogràfic inicial.

El signant podrà emmagatzemar les claus lliurades en programari en el període de durada del certificat. Posteriorment les haurà destruir assegurant abans que no té cap informació xifrada amb la clau pública.

Només en cas de certificats de xifratge el signant podrà emmagatzemar la clau privada el temps que cregui oportú. En aquest cas l’Oscepa podrà guardar una còpia de la clau privada associada al certificat de xifratge.

L’Oscepa posa a disposició dels titulars de certificats la clau privada dels quals sigui generada pel prestador des del moment del lliurament del certificat la descàrrega de l’arxiu PKCS # 12, que conté la clau privada i el certificat associat, durant tres dies hàbils.

L’Oscepa guarda actes dels processos de gestió de les claus privades d’AC.

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

Les claus de l’autoritat de certificació intermèdia s’emmagatzemen en equips HSM de xarxa en línia, de manera que s’hi pugui accedir des de les aplicacions de PKI per a la generació de certificats.

### 6.2.7 Emmagatzematge de clau privada en el mòdul criptogràfic

Les claus de l’autoritat de certificació intermèdia s’emmagatzemen en equips HSM de xarxa en línia, de manera que s’hi pugui accedir des de les aplicacions de PKI per a la generació de certificats.

### 6.2.8 Mètode d’activació de la clau privada

L’accés a la clau privada del subscriptor es fa per mitjà d’una clau d’activació que coneixerà només el subscriptor, que evitarà tenir-la per escrit.

L’activació de la clau privada de l’autoritat de certificació intermèdia és gestionada per l’aplicació de gestió de l’HSM.

L’Oscepa guarda actes dels processos de gestió de les claus privades d’AC.

### 6.2.9 Mètode de desactivació de la clau privada

Quan la clau estigui en suport programari, pot ser desactivada mitjançant l’esborrament d’aquestes claus de l’aplicació corresponent en què estiguin instal·lades.

Per a la desactivació de la clau privada de l'AC se seguiran els passos descrits en el manual d'administrador de l'equip criptogràfic corresponent.

Per a claus d'AC es durà a terme una cerimònia criptogràfica en la qual s'elaborarà l'acta corresponent.

### 6.2.10 Mètode de destrucció de la clau privada

Amb anterioritat a la destrucció de les claus s'emetrà una revocació del certificat de la clau pública que hi està associada.

Es destruiran físicament o reiniciaran a baix nivell els dispositius que tinguin emmagatzemades arreu les claus privades de l'AC. Per a l'eliminació se seguiran els passos descrits en el manual d'administrador de l'equip criptogràfic.

Finalment es destruiran de forma segura les còpies de seguretat.

Les claus del signant en programari es podran destruir esborrant-les, seguint les instruccions de l'aplicació que les alberga.

Les claus del signant en maquinari podran ser destruïdes mitjançant un programari especial en els punts de registre o a l'AC.

L'Oscepa guarda actes dels processos de gestió de les claus privades d'AC.

### 6.2.11 Qualificació del mòdul criptogràfic

Els mòduls criptogràfics que estan certificats FIPS-140-2 nivell 3 són manejats per almenys dos operadors en un model d'HSM. Els equips estan albergats en entorns segurs. El mòdul criptogràfic que emmagatzema les claus de Root es gestiona dins d'una sala criptogràfica aïllada i desconnectada. Els mòduls criptogràfics que emmagatzemen les claus de l'autoritat de certificació intermèdia s'emmagatzemen en entorns segurs dins d'un CPD seguint la normativa ISO27001.

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

### 6.3.1 Arxiu de la clau pública

L'Oscepa, en compliment del que estableix l'article 26 de la Llei 35/2014, del 27 de novembre, de serveis de confiança electrònica, mantindrà els seus arxius per un període mínim de quinze (15) anys sempre que la tecnologia de cada moment ho permeti. Dins de la documentació que s'ha de custodiar es troben els certificats de clau pública emesos als seus subscriptors i els certificats de clau pública propis.

### 6.3.2 Període d'ús per a les claus públiques i privades

La clau privada no hauria de ser usada després del període de validesa del certificat de clau pública associada.

La clau pública o el seu certificat de clau pública poden usar-se com a mecanisme de verificació de dades xifrades amb la clau pública fora de l'àmbit temporal per a tasques de validació.

Una clau privada podrà usar-se fora del període marcat pel certificat digital corresponent, únicament per a la recuperació de dades xifrades.

## *6.4. Dades d'activació*

### 6.4.1 Generació i activació de les dades d'activació

Les dades d'activació de la clau privada d'usuari es generen de diferent manera segons el tipus de certificat.

En programari. El certificat el genera el prestador i es lliura en un fitxer estandarditzat PKCS # 12 protegit per una contrasenya generada per l'aplicació de gestió i lliurada al subjecte mitjançant l'adreça associada al certificat digital.

En dispositiu maquinari. Les targetes utilitzades per l'Oscepa es generen en el lloc de registre protegides amb un PIN i PUK calculat de fàbrica. Aquesta informació és enviada per la plataforma de gestió al subjecte mitjançant l'adreça associada al certificat digital. El subjecte disposa d'un programari per canviar el PIN i PUK de la targeta.

En dispositiu maquinari (HSM) de tercer. L'Oscepa homologa dispositius de tercers, encara que disposin d'una gestió independent. Les claus es generen en una cerimònia independent i es lliura a l'Oscepa una sol·licitud d'emissió de certificat conjuntament amb l'acta de la cerimònia.

### 6.4.2 Protecció de les dades d'activació

Les dades d'activació són comunicades al subjecte per un canal independent a la plataforma de gestió PKI. L'Oscepa no emmagatzema aquesta informació custodiada a la base de dades quan parlem de certificats en format programari o maquinari. A la plataforma centralitzada no els emmagatzemem sent coneguts i custodiats pel titular. Les dades poden enviar-se de nou al subjecte. Cal demanar-ho a l'adreça associada al certificat, i seran eficaces sempre que l'usuari no hi hagi fet un canvi prèviament.

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

No estipulats.

## *6.5. Controls de seguretat informàtica*

L'Oscepa empra sistemes fiables per oferir els seus serveis de certificació. L'Oscepa ha fet controls i auditories informàtics per tal d'establir una gestió dels seus actius informàtics adequats amb el nivell de seguretat requerit en la gestió de sistemes de certificació electrònica.

Respecte a la seguretat de la informació, se segueix l'esquema de certificació sobre sistemes de gestió de la informació ISO 270001.

Els equips usats són inicialment configurats amb els perfils de seguretat adequats per part de personal de sistemes de l'Oscepa, en els aspectes següents:

1. Configuració de seguretat de sistema operatiu.
2. Configuració de seguretat de les aplicacions.
3. Dimensionament correcte del sistema.
4. Configuració d'usuaris i permisos.
5. Configuració d'esdeveniments de diari (*log*).
6. Pla de còpia de seguretat (*backup*) i recuperació.
7. Configuració de l'antivirus.
8. Requisits de trànsit de xarxa.

### 6.5.1 Requisits tècnics de seguretat informàtica específics

Cada servidor de l'Oscepa inclou les funcionalitats següents:

- Control d'accés als serveis d'AC i gestió de privilegis.
- Imposició de separació de tasques per a la gestió de privilegis.
- Identificació i autenticació de rols associats a identitats.
- Arxiu de l'historial de subscriptor i l'AC i dades d'auditoria.
- Auditoria d'esdeveniments relatius a la seguretat.
- Acte-diagnòstic de seguretat relacionat amb els serveis de l'AC.
- Mecanismes de recuperació de claus i del sistema d'AC.

Les funcionalitats exposades es duen a terme mitjançant una combinació de sistema operatiu, programari de PKI, protecció física i procediments.

### 6.5.2 Valoració de la seguretat informàtica

La seguretat dels equips està reflectida en una anàlisi de riscos inicials de tal manera que les mesures de seguretat implantades són resposta a la probabilitat i l'impacte produït quan un grup d'amenaces definides pugui aprofitar bretxes de seguretat.

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

Quan les claus criptogràfiques associades a un certificat s'emmagatzemen en un dispositiu maquinari, aquest és sempre un dispositiu qualificat de creació de signatura, en compliment de l'annex II d'eIDAS. El dispositiu maquinari pot ser una targeta criptogràfica, testimoni (*token*) USB o HSM.

Pel que fa als dispositius maquinari:

a) Els dispositius maquinari són preparats i estampats per un proveïdor extern.
b) La gestió de distribució del suport la fa el proveïdor extern, que el distribueix a les autoritats de registre per lliurar-lo al signant.

c) El signant o l'RA utilitza el dispositiu per generar el parell de claus i enviar la clau pública a l'AC.
d) L'AC envia un certificat de clau pública al signant o l'RA que és introduït en el dispositiu.
e) El dispositiu és reutilitzable i pot mantenir de forma segura diversos parells de claus.
f) El dispositiu queda en propietat del subjecte/signant.

Pel que fa als dispositius utilitzats en la plataforma de gestió centralitzada de claus: el dispositiu que emmagatzema aquestes claus està certificat FIPS-104-2 nivell 3 o EAL4 + i autoritzat pel supervisor europeu per als serveis catalogats com a QSCDManagedOnBehalf.

### 6.6.1 Controls de desenvolupament de sistema

L'Oscepa posseeix un procediment de control de canvis en les versions de sistemes operatius i aplicacions que impliquin una millora en les seves funcions de seguretat o que corregeixin qualsevol vulnerabilitat detectada.

Com a resposta a les anàlisis d'intrusió i vulnerabilitats, es fan les adaptacions dels sistemes i aplicacions que poden tenir problemes de seguretat i a les alertes de seguretat rebudes des dels serveis de seguretat gestionades contractats amb tercers, s'executen els RFC (*Request for Changes*) corresponents per a la incorporació dels pegats de seguretat o l'actualització de les versions amb problemes.

En l'RFC s'incorporen i es documenten les mesures preses per a l'acceptació, l'execució o la denegació d'aquest canvi.

En els casos que l'execució de l'actualització o correcció d'un problema incorpori una situació de vulnerabilitat o un risc important, s'incorpora en l'anàlisi de riscos i s'executen controls alternatius fins que el nivell de risc sigui assumible.

### 6.6.2 Controls de gestió de la seguretat

#### *6.6.2.1 Gestió de seguretat*

El Departament de la Funció Pública desenvolupa les activitats necessàries per formar i conscienciar els empleats en matèria de seguretat. Els materials emprats per a la formació i els documents descriptius dels processos són actualitzats després de ser aprovats per un grup per a la gestió de la seguretat.

Per dur a terme aquesta funció disposa d'un pla de formació anual.

L'Oscepa exigeix, mitjançant contracte, les mesures de seguretat equivalents a qualsevol proveïdor extern implicat en les tasques de certificació.

#### *6.6.2.2 Classificació i gestió d'informació i béns*

El Departament de Sistemes d'Informació (DSI) manté un inventari d'actius i documentació i un procediment per a la gestió d'aquest material per garantir-ne l'ús.

La política de seguretat de Govern detalla els procediments de gestió de la informació, en què es classifica segons el seu nivell de confidencialitat.

Els documents estan catalogats en tres nivells: públic, ús intern i confidencial.

### 6.6.2.3 *Operacions de gestió*

El Departament de Sistemes d'Informació (DSI) disposa d'un procediment de gestió i resposta d'incidències adequat, mitjançant la implementació d'un sistema d'alertes i la generació d'informes periòdics. En el document de seguretat de l'Oscepa es desenvolupa en detall el procés de gestió d'incidències.

L'Oscepa té documentat tot el procediment relatiu a les funcions i responsabilitats del personal implicat en el control i la manipulació d'elements continguts en el procés de certificació.

Tractament dels suports i seguretat.
Tots els suports són tractats de manera segura d'acord amb els requisits de la classificació de la informació. Els suports que continguin dades sensibles són destruïts de manera segura si no han de tornar a ser requerits.

Planificació del sistema
El Departament de Sistemes d'Informació (DSI) manté un registre de les capacitats dels equips. Conjuntament amb l'aplicació de control de recursos de cada sistema es pot preveure un possible redimensionament.

Informes d'incidències i resposta
El Departament de Sistemes d'Informació (DSI) disposa d'un procediment per al seguiment d'incidències i la seva resolució en què es registren les respostes i una avaluació econòmica que suposa la resolució de la incidència.

Procediments operacionals i responsabilitats.
L'Oscepa defineix activitats, assignades a persones amb un paper de confiança, diferents de les persones encarregades de dur a terme les operacions quotidianes que no tenen caràcter de confidencialitat.

### 6.6.2.4 *Gestió de sistema d'accés*

L'Oscepa fa tots els esforços que raonablement estan al seu abast per confirmar que el sistema d'accés està limitat a les persones autoritzades.
En particular:

AC General

a) Es disposa de controls basats en tallafocs, antivirus i IDS en alta disponibilitat.

b) Les dades sensibles són protegides mitjançant tècniques criptogràfiques o controls d'accés amb identificació forta.

c) L'Oscepa disposa d'un procediment documentat de gestió d'altes i baixes d'usuaris i política d'accés detallat en la seva política de seguretat.

d) L'Oscepa disposa de procediments per assegurar que les operacions s'efectuen respectant la política de rols.

e) Cada persona té associat un paper per dur a terme les operacions de certificació.

f) El personal de l'Oscepa és responsable dels seus actes mitjançant el compromís de confidencialitat signat amb l'empresa.

Generació del certificat
L'autenticació per al procés d'emissió es duu a terme mitjançant un sistema m de n operadors per a l'activació de la clau privada de l'AC.

Gestió de la revocació
La revocació s'efectuarà mitjançant autenticació forta a les aplicacions d'un administrador autoritzat. Els sistemes de diaris (logs) generaran les proves que garanteixen el no repudi de l'acció efectuada per l'administrador d'AC.

Estat de la revocació
L'aplicació de l'estat de la revocació disposa d'un control d'accés basat en l'autenticació per certificats per evitar l'intent de modificació de la informació de l'estat de la revocació.

### *6.6.2.5 Gestió del cicle de vida del programari criptogràfic*

L'Oscepa s'assegura que el maquinari criptogràfic usat per a la signatura de certificats no es manipula mentre es transporta mitjançant la inspecció del material lliurat.

El maquinari criptogràfic es trasllada sobre suports preparats per evitar qualsevol manipulació.

L'Oscepa registra tota la informació pertinent del dispositiu per afegir-la al catàleg d'actius.

L'ús del maquinari criptogràfic de signatura de certificats requereix almenys l'ús de dos empleats de confiança.

L'Oscepa fa el test de proves periòdiques per assegurar el funcionament correcte de l'aparell.

El dispositiu maquinari criptogràfic només és manipulat per personal fiable.

La clau privada de signatura de l'AC emmagatzemada en el maquinari criptogràfic s'eliminarà un cop s'ha retirat el dispositiu.

La configuració de sistema de l'AC, així com les seves modificacions i actualitzacions, és documentada i controlada.

L'Oscepa té un contracte de manteniment de l'aparell. Els canvis o actualitzacions són autoritzats pel responsable de seguretat i queden reflectits en les actes de treball corresponents. Aquestes configuracions les faran almenys dos persones de confiança.

## 6.6.3 Avaluació de la seguretat del cicle de vida

No estipulat.

## *6.7. Controls de seguretat de la xarxa*

L'Oscepa protegeix l'accés físic als dispositius de gestió de xarxa i disposa d'una arquitectura que ordena el trànsit generat basant-se en les seves característiques de seguretat creant seccions de xarxa clarament definides. Aquesta divisió es duu a terme mitjançant l'ús de tallafocs.

La informació confidencial que es transfereix per xarxes no segures es realitza de forma xifrada mitjançant l'ús de protocols SSL.

La política emprada per a la configuració dels sistemes i elements de seguretat és partir d'un estat inicial de bloqueig total i anar obrint serveis i ports necessaris per a l'execució dels serveis. Com a part de les tasques que s'han de dur a terme en el departament de sistemes s'incorpora la revisió dels accessos.

Els sistemes d'administració i els sistemes de producció estan en entorns separats.

## *6.8. Fonts de temps*

L'Oscepa té un procediment de sincronització de temps coordinat amb el ROA Reial Institut i l'Observatori de l'Armada Espanyola a San Fernando via NTP. També obté una font segura via GPS i sincronització via ràdio.

# 7. PERFILS DE CERTIFICAT, CRL I OCSP

## *7.1. Perfil de certificat*

Els perfils de certificats compleixen l'RFC 5280.

Tots els certificats qualificats o reconeguts emesos sota aquesta política són conformes a l'estàndard X.509, versió 3, i a l'RFC 3739 i ETSE 101.867 "Qualified Certificate Profile".

Els perfils d'aquests certificats es poden sol·licitar a l'adreça gestion_soporte@camerfirma.com o al telèfon +34 902 361 207

### 7.1.1 Nombre de versió

L'Oscepa emet certificats X.509, versió 3

### 7.1.2 Extensions del certificat

Els documents de les extensions dels certificats es troben detallats en les fitxes de perfils. Els perfils d'aquests certificats es poden sol·licitar a l'adreça gestion_soporte@camerfirma.com o al telèfon +34 902 361 207.

### 7.1.3 Identificadors d'objecte (OID) dels algoritmes

L'identificador d'objecte de l'algoritme de signatura és
- 1.2.840.113549.1.1.5 – sha1 con RSAEncryption
- 1.2.840.113549.1.1.11 – sha256 con RSAEncryption

El camp Subject Public Key Informació (1.2.840.113549.1.1.1) incorpora el valor rsaEncryption.

### 7.1.4 Format de noms

Els certificats hauran de contenir les informacions que siguin necessàries per usar-los, segons determini la corresponent política d'autenticació, signatura electrònica, xifratge o evidència electrònica.

En general, els certificats d'ús en el sector públic han de contenir la identitat de la persona que els rep, preferiblement en els camps *Subject Name* o *Subject Alternative Name*, incloent-hi les dades següents:

- Nom i cognoms de la persona signant, posseïdora o representada, en camps separats, o amb indicació de l'algoritme que permet la separació de forma automàtica.
- Denominació social de la persona jurídica, quan correspongui.
- Números de documents d'identificació corresponents, d'acord amb la legislació aplicable a la persona signant, posseïdora o representada, sigui física o jurídica.

La semàntica exacta dels noms es descriu en les fitxes dels perfils. Els perfils d'aquests certificats es poden trobar https://www.signaturaelectronica.ad/jerarquia-politiques-i-practiques-de-certificacio.

### 7.1.5 Restr**iccions dels noms**

L'Oscepa pot utilitzar restriccions de nom (utilitzant l'extensió del certificat *name constraints*) en els certificats d'AC subordinada emesos a terceres parts de manera que només es pugui emetre per l'AC subordinada al conjunt de certificats permès en aquesta extensió.

### 7.1.6 Identificador d'objecte (OID) de la política de certificació

Tots els certificats Camerfirma tenen un identificador de política que comença des de la base 1.3.6.1.4.1.17326.

Govern d'Andorra (OSCEPA) = 2.16.20.2.1.3.1

### 7.1.7 Ús de l'extensió Policy Constraints

L'Oscepa pot utilitzar restriccions de política (utilitzant l'extensió del certificat *Policy Constraints*) en els certificats d'AC subordinada emesos a terceres parts de manera que només es pugui emetre per l'AC subordinada al conjunt de certificats permès en aquesta extensió.

### 7.1.8 Sintaxi i semàntica dels qualificadors de política

No estipulat.

### 7.1.9 Tractament semàntic per a l'extensió crítica Certificate Policy

L'extensió *Certificate Policy* identifica la política que defineix les pràctiques que l'Oscepa associa explícitament amb el certificat. L'extensió pot contenir un qualificador de la política. Vegeu el 7.1.6.

## *7.2. Perfil de CRL*

El perfil de les CRL es correspon amb el proposat en les polítiques de certificació corresponents. Les CRL són signades per l'AC que ha emès els certificats.

El perfil detallat de la CRN es pot sol·licitar a https://www.camerfirma.com/ayuda/soporte/ o al telèfon 902 361 207.

### 7.2.1 Nombre de versió

Les CRL emeses per l'Oscepa són de la versió 2.

### 7.2.2 CRL i extensions

Les imposades per les polítiques de certificació corresponents. El perfil detallat de la CRN i les seves extensions es pot sol·licitar a https://www.camerfirma.com/ayuda/soporte/ o al telèfon 902 361 207.

## *7.3. Perfil d'OCSP*

### 7.3.1 Nombre de versió

Els certificats de contestador OCSP són versió 3. Aquests certificats són emesos per l'AC gestionada per l'Oscepa segons l'estàndard RFC 6960.

### 7.3.2 Extensions OCSP

Es pot obtenir el perfil dels certificats transponedors d'OCSP a l'adreça següent gestion_soporte@camerfirma.com o al telèfon 902 361 207.

Es pot obtenir una llista actualitzada dels certificats OCSP a https://www.signaturaelectronica.ad/consulta-l-estat-del-certificat-ocsp.

# 8. AUDITORIES DE CONFORMITAT

L'Oscepa és una organització compromesa amb la seguretat i la qualitat dels seus serveis.

Els objectius de l'Oscepa pel que fa a la seguretat i la qualitat han estat fonamentalment l'obtenció dels certificats ISO / IEC 27001 i ISO / IEC 20000 i la realització d'auditories internes biennals al sistema de certificació de l'Oscepa, i fonamentalment a les autoritats de registre, per garantir el compliment dels procediments interns.

L'Oscepa està subjecta a unes auditories periòdiques amb el segell WebTrust for CA, que assegura que els documents de polítiques i CPS tenen un format i abast adequats, a la vegada que estan completament alineades amb les seves polítiques i pràctiques de certificació.

L'Oscepa està també subjecta als controls que duu a terme l'organisme regulador nacional respecte a la seva activitat, d'aquesta manera la Comissió Nacional d'Acreditació (CNAC).

Les autoritats de registres pertanyents a ambdós jerarquies estan subjectes a un procés d'auditoria interna. Aquestes auditories es duen a terme periòdicament de manera discrecional sobre la base d'una valoració de risc pel nombre de certificats emesos i el nombre d'operadors de registre, fet que determinarà també que es dugui a terme l'auditoria de forma presencial o remota. Les auditories es descriuen en un pla anual d'auditories.

L'Oscepa està subjecta a una auditoria biennal sobre protecció de dades.

L'Oscepa duu a terme una auditoria interna. En aquesta auditoria l'Oscepa comprova de forma aleatòria un nombre de certificats emesos per aquesta autoritat de registre, assegurant-se que les proves recollides siguin correctes i suficients per emetre el certificat.

## *8.1. Freqüència o circumstàncies de les auditories*

Com s'ha indicat en l'apartat 2.7, l'Oscepa porta a terme una auditoria de conformitat anualment, a més de les auditories internes que efectua de forma discrecional.

- Auditoria ISO 27001, ISO20000 i ISO 9001, cicle de tres anys amb revisions anuals.
- WebTrust for CA de forma anual.
- Avaluació de conformitat eIDAS, biennal amb revisió anual.
- Una anàlisi de vulnerabilitats trimestral.
- Una anàlisi d'intrusió anual.
- Auditories d'RA de manera discrecional.

### 8.1.1 Auditoria en les autoritats de registre

Totes les AR són auditades. Aquestes auditories es duen a terme almenys cada dos anys de forma discrecional i sobre la base d'una anàlisi de riscos. Les auditories comproven el compliment dels requisits exigits per aquestes CPS per al desenvolupament de les tasques de registre exposades en el contracte de servei signat.

Dins de l'auditoria interna efectuada es prenen mostrejos sobre certificats emesos, verificant-ne el processament correcte.

## 8.2. Identificació i qualificació de l'auditor

Les auditories les duen a terme les companyies independents externes següents d'ampli reconeixement en seguretat informàtica, en seguretat de sistemes d'informació i en auditories de conformitat d'autoritats de certificació:

- Per a l'auditoria WebTrust: AUREN (http://www.auren.com)
- Per a les auditories ISO27001 / 20000 ISO 9001: AENOR (http://www.aenor.es)
- Per a les auditories internes: / A - AUREN (http://www.auren.com/)

## 8.3. Relació entre l'auditor i l'AC

Les empreses d'auditoria són independents i de prestigi reconegut, i compten amb departaments especialitzats en auditories informàtiques i en la gestió de certificats digitals i serveis de confiança, de manera que no hi ha cap conflicte d'interessos que pugui desvirtuar la seva actuació en relació amb l'AC.

No hi ha vinculació ni dependència financera ni orgànica entre les empreses auditores i l'AC Oscepa.

## 8.4. Tòpics coberts per l'auditoria

En línies generals, les auditories verifiquen:

a) Que l'Oscepa té un sistema que garanteix la qualitat del servei prestat.
b) Que la CPS s'ajusta al que estableixen les polítiques, al que està acordat per l'autoritat aprovadora de la política i al que estableix la normativa vigent.
c) Que l'Oscepa gestiona de forma adequada la seguretat dels seus sistemes d'informació.
d) En els certificats l'auditora comprova l'alienació amb les polítiques marcades per CA / B Forum en els seus *Baseline Requirements*.

En línies generals, els elements objecte d'auditoria seran els següents:

- Processos de l'Oscepa, AR i elements relacionats amb l'emissió de certificats i serveis de validació en línia OCSP.
- Sistemes d'informació.
- Protecció de centre de procés de dades.
- Documentació requerida per a cada tipus de certificat.
- Verificació que els operadors d'RA coneixen la CPS de l'Oscepa.

## 8.5. Accions preses com a resultat de les deficiències

Un cop rebut l'informe de l'auditoria de compliment portada a terme, l'Oscepa discutirà, amb l'entitat que ha executat l'auditoria, les deficiències trobades i desenvoluparà i executarà un pla correctiu a fi de solucionar-les.

Si l'entitat auditada és incapaç de desenvolupar i/o executar aquest pla en el termini de temps sol·licitat, o si les deficiències trobades suposen una amenaça immediata per a la seguretat o integritat de sistema, ho ha de comunicar immediatament a l'autoritat de polítiques, que podrà executar les accions següents:

- Fer cessar les operacions transitòriament.
- Revocar el certificat corresponent i regenerar la infraestructura.
- Acabar el servei a l'entitat.

- Altres accions complementàries que siguin necessàries.

## *8.6. Comunicació de resultats*

Els resultats els comuniquen al responsable de seguretat i compliment normatiu els auditors que han dut a terme l'avaluació. Es fan saber en un acte amb la presència de la direcció corporativa. El certificat d'auditoria es publica al web de l'Oscepa.

# 9. ASPECTES LEGALS I ALTRES ASSUMPTES

## *9.1. Tarifes*

### 9.1.1 Tarifes d'emissió de certificats i renovació

Els preus dels serveis de certificació o qualsevol altre servei relacionat estan disponibles i actualitzats al lloc web del *Butlletí Oficial del Principat d'Andorra*: https://www.bopa.ad.

Cada tipus de certificat té publicat el seu preu concret, excepte els que estan subjectes a una negociació comercial prèvia.

### 9.1.2 Tarifes d'accés als certificats

L'accés als certificats emesos és gratuït. L'Oscepa implanta controls per evitar els casos de descàrrega massiva de certificats. Qualsevol altra circumstància que segons el parer de l'Oscepa hagi de ser considerada a aquest efecte es publica al lloc web de l'Oscepa: https://www.signaturaelectronica.ad.

### 9.1.3 Tarifes d'accés a la informació relativa a l'estat dels certificats o els certificats revocats

L'Oscepa proveeix un accés a la informació relativa a l'estat dels certificats o dels certificats revocats gratuït a través de llistes de certificats revocats o mitjançant accés via web a l'adreça Internet de l'Oscepa: https://www.signaturaelectronica.ad/consulta- l-estat-de el-Certificat-OCSP.
L'Oscepa ofereix el servei OCSP de forma gratuïta: https://ocsp.govern.ad.

### 9.1.4 Tarifes per a l'accés al contingut d'aquestes pràctiques de certificació

L'accés al contingut d'aquesta CPS és gratuït, al lloc web de l'Oscepa:
https://www.signaturaelectronica.ad/jerarquia-politiques-i-practiques-de-certificacio.

### 9.1.5 Política de reintegraments

L'Oscepa no té una política de reintegraments específica, i s'acull a la normativa general vigent.

## *9.2. Responsabilitat financera*

### 9.2.1 Cobertura de l'assegurança

L'Oscepa, en la seva activitat com a PSC, disposa d'una assegurança de responsabilitat civil que té en compte les seves responsabilitats, per indemnitzar per danys i perjudicis que es puguin ocasionar als usuaris dels seus serveis: el subjecte/signant i la part usuària i tercers, d'un import conjunt de 600.000 d'euros.

### 9.2.2 Altres actius

No estipulat.

### 9.2.3 Assegurança de cobertura o garantia per a entitats finals

Vegeu l'apartat 9.2.1.

## *9.3. Confidencialitat de la informació del negoci*

### 9.3.1 Tipus d'informació que s'ha de mantenir confidencial

L'Oscepa considera confidencial tota la informació que no estigui catalogada expressament com a pública. No es difon informació confidencial sense el consentiment exprés per escrit de l'entitat o organització que hagi atorgat el caràcter confidencial a aquesta informació, tret que hi hagi una imposició legal.

L'Oscepa disposa d'una adequada política de tractament de la informació i dels models d'acord de confidencialitat, que hauran de signar totes les persones que tinguin accés a informació confidencial.

### 9.3.2 Tipus d'informació considerada no confidencial

L'Oscepa considera com a informació no confidencial:

a) La continguda en aquesta CPS i en les polítiques de certificació.
b) La informació continguda en els certificats.
c) Qualsevol informació l'accessibilitat a la qual no sigui prohibida per la normativa vigent.

### 9.3.3 Responsabilitat de protegir la informació confidencial

L'Oscepa és responsable de la protecció de la informació confidencial generada o comunicada durant totes les operacions. Les parts delegades, com les entitats que administren les CA emissores subordinades o les autoritats de registre, són responsables de protegir la informació confidencial que s'ha generat o emmagatzemat pels seus propis mitjans. Per a les entitats finals, els subscriptors del certificat són responsables de protegir la seva pròpia clau privada i tota la informació d'activació (és a dir, contrasenyes o PIN) necessària per accedir a la clau privada o utilitzar-la.

#### *9.3.3.1 Divulgació d'informació de revocació/suspensió de certificats*

L'Oscepa difon la informació relativa a la suspensió o revocació d'un certificat mitjançant la publicació periòdica de les corresponents CRL.

L'Oscepa disposa d'un servei de consulta de CRL i certificats en el lloc d'Internet https://crl.govern.ad.

L'Oscepa disposa d'un servei de consulta en línia d'estat dels certificats basat en l'estàndard OCSP, a l'adreça http://ocsp.govern.ad. El servei OCSP ofereix respostes estandarditzades sota l'RFC 2560 sobre l'estat d'un certificat digital, és a dir, si el certificat consultat està actiu o revocat, o si ha estat emès o no per l'autoritat de certificació.

#### *9.3.3.2 Enviament a l'autoritat competent*

L'Oscepa proporcionarà la informació sol·licitada per l'autoritat competent o a l'organisme regulador corresponent, en els casos i la forma que estableix la legislació vigent.

## *9.4. Privacitat de la informació personal*

### 9.4.1 Pla de privacitat

L'Oscepa compleix en tot cas la normativa vigent en cada moment en matèria de protecció de dades, en particular ha adaptat els seus procediments al general de protecció de dades (RGPD).

### 9.4.2 Informació tractada com a privada

La informació personal sobre un individu que no està públicament disponible en els continguts d'un certificat o CRL es considera privada.

### 9.4.3 Informació no considerada privada

La informació personal sobre un individu disponible en els continguts d'un certificat o CRL, es considera no privada en ésser necessària per prestar el servei contractat, sense perjudici dels drets corresponents al titular de les dades personals en virtut de la legislació RGPD.

### 9.4.4 Responsabilitat de protegir la informació privada

És responsabilitat del responsable del tractament protegir adequadament la informació privada.

### 9.4.5 Avís i consentiment per utilitzar informació privada

Abans d'establir una relació contractual, l'Oscepa oferirà als interessats la informació prèvia sobre el tractament de les seves dades personals i exercici de drets, i, si escau, ha de demanar el consentiment preceptiu per al tractament diferenciat del tractament principal per prestar els serveis contractats.

### 9.4.6 Divulgació de conformitat amb un procés judicial o administratiu

Les dades personals que siguin considerades privades o no, només podran divulgar-se en cas que sigui necessari per a la formulació, l'exercici o la defensa de reclamacions, ja sigui per un procediment judicial o un procediment administratiu o extrajudicial.

### 9.4.7 Altres circumstàncies de divulgació d'informació

No se cediran dades personals a tercers excepte si és obligació legal.

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

L'Oscepa és titular dels drets de propietat intel·lectual sobre aquesta CPS.

## *9.6. Obligacions i responsabilitat civil*

### 9.6.1 Obligació i responsabilitat de la CA

#### *9.6.1.1 AC*

L'Oscepa s'obliga segons el que disposa aquesta CPS, així com el que disposa la normativa vigent sobre prestació de serveis de certificació, a:

- Respectar el que disposa l'abast d'aquesta CPS.
- Protegir les seves claus privades de forma segura.
- Emetre certificats d'acord amb aquesta CPS, les polítiques de certificació i els estàndards tècnics aplicables.
- Emetre certificats segons la informació que està en el seu poder i lliures d'errors d'entrada de dades.
- Emetre certificats el contingut mínim dels quals sigui el definit per la normativa vigent per als certificats qualificats o reconeguts.
- Publicar els certificats emesos en un directori, respectant en tot cas el que disposa en matèria de protecció de dades la normativa vigent.
- Suspendre i revocar els certificats segons el que disposa aquesta política i publicar les revocacions esmentades a la CRL.
- Informar els subjectes/signants de la revocació o suspensió dels seus certificats, en temps i forma d'acord amb la legislació vigent.
- Publicar aquesta CPS i les polítiques de certificació corresponents al seu lloc web.
- Informar sobre les modificacions d'aquesta CPS i de les polítiques de certificació els subjectes/signants i les RA que estiguin vinculades.
- No emmagatzemar ni copiar les dades de creació de signatura del subjecte/signant excepte per als certificats de xifratge i per als casos en què legalment es prevegi o permeti el dit

emmagatzematge o còpia.
- Protegir, amb la deguda cura, les dades de creació de signatura mentre estiguin sota la seva custòdia, si escau.
- Establir els mecanismes de generació i custòdia de la informació rellevant en les activitats descrites, protegint-les de pèrdua o destrucció o falsificació.
- Conservar la informació sobre el certificat emès pel període mínim exigit per la normativa vigent.

L'Oscepa serà responsable dels danys i perjudicis ocasionats als usuaris pels seus serveis, ja sigui al signant/subscriptor o al tercer que confia, i a altres tercers en els termes que s'estableix en la legislació vigent i en les polítiques de certificació.

En aquest sentit l'Oscepa és l'única responsable (i) d'emetre els certificats, (ii) de gestionar-los durant tot el seu cicle de vida i (iii) en particular, si cal, de suspendre'ls i revocar-los. En concret, l'Oscepa fonamentalment serà responsable de:

- L'exactitud de tota la informació continguda en el certificat en la data de l'emissió, mitjançant la confirmació de les dades de sol·licitant i les pràctiques d'AR.
- La garantia que, en el moment del lliurament del certificat, està en poder del signant/subscriptor la clau privada corresponent a la clau pública donada o la identificació en el certificat quan el procés així ho requereixi, mitjançant la utilització de peticions estandarditzades en format PKCS # 10.
- La garantia que la clau pública i la privada funcionen conjuntament i complementàriament, utilitzant dispositius i mecanismes criptogràfics certificats.
- La correspondència entre el certificat sol·licitat i el certificat lliurat.
- Qualsevol responsabilitat que s'estableixi en la legislació vigent.

En compliment de la legislació vigent l'Oscepa disposa d'una assegurança de responsabilitat civil que cobreix els requisits marcats per les polítiques de certificació afectades per aquestes pràctiques de certificació.

### 9.6.2 Obligació i responsabilitat de l'AR

Les AR són les entitats delegades per l'AC per dur a terme les tasques de registre i aprovació de les sol·licituds de certificats; per tant, l'AR també s'obliga en els termes definits en les pràctiques de certificació per emetre certificats, principalment, a:

- Respectar el que disposa aquesta CPS.
- Protegir les seves claus secretes, que els serviran per a l'exercici de les seves funcions.
- Comprovar la identitat dels subjectes/signants i sol·licitants dels certificats quan sigui necessari, acreditant definitivament la identitat del signant, en cas de certificats individuals, o del posseïdor de claus, en cas de certificats d'organització, d'acord amb el que estableixen les seccions corresponents d'aquest document.
- Verificar l'exactitud i l'autenticitat de la informació subministrada pel sol·licitant.
- Proporcionar al signant, en cas de certificats individuals, o al futur posseïdor de claus, en cas de certificats d'organització, accés al certificat.
- Lliurar, si escau, el dispositiu criptogràfic corresponent.
- Arxivar, pel període que disposa la legislació vigent, els documents subministrats pel sol·licitant o signant.

- Respectar el que disposen els contractes signats amb l'Oscepa i amb el subjecte/signant.
- Informar l'Oscepa de les causes de la revocació, sempre que en prenguin coneixement.
- Oferir informació bàsica sobre la política i l'ús del certificat, incloent-hi especialment informació sobre l'Oscepa i la Declaració de pràctiques de certificació aplicable, així com de les seves obligacions, facultats i responsabilitats.
- Oferir informació sobre el certificat i el dispositiu criptogràfic.
- Recopilar informació i proves del posseïdor de rebre el certificat i, si escau, el dispositiu criptogràfic, i acceptació d'aquests elements.
- Informar del mètode d'imputació exclusiva al posseïdor de la clau privada i de les seves dades d'activació del certificat i, si escau, del dispositiu criptogràfic, d'acord amb el que estableixen les seccions corresponents d'aquest document.

La informació sobre l'ús i les responsabilitats del subscriptor se subministra mitjançant l'acceptació de les clàusules d'ús prèviament a la confirmació de la sol·licitud del certificat i mitjançant correu electrònic.

La responsabilitat de les AR

Les AR subscriuen un contracte de prestació de servei amb l'Oscepa mitjançant el qual aquesta última delega les funcions de registre en les AR, consistent fonamentalment a:

1. Obligacions prèvies a l'expedició d'un certificat:
   a) Informar adequadament els sol·licitants de la signatura de les seves obligacions i responsabilitats.
   b) Identificar adequadament els sol·licitants, que han de ser persones capacitades o autoritzades per sol·licitar un certificat digital.
   c) Comprovar correctament la validesa i vigència d'aquestes dades dels sol·licitants i de l'entitat, en el cas que hi hagi una relació de vinculació o representació.
   d) Accedir a l'aplicació de l'autoritat de registre per gestionar les sol·licituds i els certificats emesos.

2. Obligacions un cop expedit el certificat:
   a) Subscriure els contractes de prestació de serveis de certificació digital amb els sol·licitants. En la majoria dels processos d'emissions aquest contracte és formalitzat mitjançant l'acceptació de condicions en les pàgines web que formen part del procés d'emissió del certificat, i no es pot fer l'emissió sense haver acceptat abans les condicions d'ús.
   b) El manteniment dels certificats durant la seva vigència (extinció, suspensió, revocació).
   c) Arxivar les còpies de la documentació presentada i els contractes degudament signats pels sol·licitants de conformitat amb les polítiques de certificació publicades per l'Oscepa i la legislació vigent.

Així doncs, les AR es responsabilitzen de les conseqüències en cas d'incompliment de les seves tasques de registre, i es comprometen a respectar a més les normes reguladores internes de l'Oscepa (CPS), les quals hauran de ser perfectament controlades per les AR i que hauran de servir-los de manual de referència.

En cas de reclamació per un subjecte, una entitat o un usuari, l'AC haurà d'aportar la prova de l'actuació diligent i si es constata que l'origen de la reclamació radica en un error en la validació o comprovació de les dades, l'AC podrà, en virtut dels acords signats amb les AR, fer suportar a l'AR responsable l'assumpció de les conseqüències. Perquè, encara que legalment sigui l'AC la persona jurídica responsable davant del subjecte, una entitat o part usuària, per a la qual cosa

disposa d'una assegurança de responsabilitat civil, segons l'acord vigent i les polítiques vinculants, l'AR té com a obligació contractual "identificar i autenticar correctament el sol·licitant i, si escau, l'entitat que correspongui", i en virtut d'això haurà de respondre davant de l'Oscepa dels seus incompliments.

Per descomptat, no és intenció de l'Oscepa descarregar tot el pes de l'assumpció de responsabilitat a les AR pel que fa als possibles danys l'origen dels quals vindria d'un incompliment de les tasques delegades a les AR. Per aquesta raó, igual que el que està previst per a l'AC, l'AR es veu sotmesa a un règim de control que serà exercit per l'Oscepa, no

només a través dels controls d'arxius i procediments de conservació dels arxius assumits per l'AR mitjançant la realització d'auditories per avaluar, entre altres aspectes, els recursos emprats i el coneixement i control dels procediments operatius per oferir els serveis d'AR.

Les mateixes responsabilitats les hauran d'assumir les AR en virtut d'incompliments de les entitats delegades com ara els punts de verificació presencial (PVP), sense perjudici del seu dret a repercutir-los contra elles.

### 9.6.3 Obligació i responsabilitat del subscriptor

#### *9.6.3.1 Signant/subscriptor*

El signant/subscriptor estarà obligat a complir el que disposa la normativa vigent i a més a:

- Utilitzar el certificat segons el que estableixen aquesta CPS i les polítiques de certificació aplicables.
- Respectar el que disposen els documents signats amb l'Oscepa i l'AR.
- Informar com més aviat millor de l'existència d'alguna causa de suspensió/revocació.
- Notificar qualsevol inexactitud o canvi en les dades aportades per crear el certificat durant el seu període de validesa.
- No utilitzar la clau privada ni el certificat des del moment en què se sol·licita o és advertit per l'Oscepa o l'AR de la suspensió o revocació de la clau, o un cop expirat el termini de validesa del certificat.
- Fer ús del certificat digital amb el caràcter de personal i intransferible i, per tant, assumir la responsabilitat per qualsevol actuació que es dugui a terme en contravenció d'aquesta obligació, així com complir les obligacions que siguin específiques de la normativa aplicable als dits certificats digitals.
- Autoritzar l'Oscepa a tractar les dades personals contingudes en els certificats, en connexió amb les finalitats de la relació electrònica i, en tot cas, per complir les obligacions legals de verificació de certificats.
- Responsabilitzar-se que tota la informació inclosa, per qualsevol mitjà, en la sol·licitud del certificat i en el mateix certificat sigui exacta i completa per a la finalitat del certificat, i estigui actualitzada en tot moment.
- Informar immediatament el prestador de serveis de certificació corresponent de qualsevol inexactitud en el certificat detectada un cop s'hagi emès, així com dels canvis que es produeixin en la informació aportada per a l'emissió del certificat.
- Si es tracta de certificats en un dispositiu material, en cas que en perdi la possessió, posar-ho en coneixement fefaent de l'entitat que els hagi emès en el termini més breu possible i, en tot cas, dins de les 24 hores següents a la producció de la circumstància esmentada, amb independència del fet concret que l'hagi originat o de les accions que eventualment pugui exercir.

- No utilitzar la clau privada, el certificat electrònic o qualsevol altre suport tècnic lliurat pel prestador de serveis de certificació corresponent per efectuar cap transacció prohibida per la llei aplicable.

En el cas de certificats qualificats, el subscriptor o el posseïdor de certificats ha d'utilitzar el parell de claus exclusivament per crear signatures o segells electrònics i d'acord amb qualssevol altres limitacions que li siguin notificades.

**Així mateix, ha de ser especialment diligent en la custòdia de la seva clau privada i del seu dispositiu segur de creació de signatura, amb la finalitat d'evitar usos no autoritzats. Serà l'únic responsable davant de tercers o davant de l'entitat que representa, si no està autoritzat per a això, de les conseqüències que un ús indegut o no controlat correctament pugui generar.**

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

- Generar les seves claus de subscriptor utilitzant un algoritme reconegut com a acceptable per a la signatura electrònica, si escau qualificada, o el segell electrònic, si escau qualificat.
- Crear les claus dins del dispositiu de creació de signatura o de segell, utilitzant un dispositiu segur quan sigui procedent.
- Utilitzar longituds i algoritmes de clau reconeguts com a acceptables per a la signatura electrònica, si escau qualificada, o el segell electrònic, si escau qualificat.

### *9.6.3.2 Sol·licitant del certificat*

El sol·licitant (bé directament o a través d'un tercer autoritzat) d'un certificat estarà obligat a complir el que disposa la normativa i a més a:

- Subministrar a l'AR la informació necessària per fer una identificació correcta.
- Garantir l'exactitud i veracitat de la informació subministrada.
- Notificar qualsevol canvi en les dades aportades per a la creació del certificat durant el seu període de validesa.
- Custodiar la seva clau privada de manera diligent.

### *9.6.3.3 Entitat*

En el cas dels certificats que impliquin vinculació a una entitat, l'entitat està obligada a sol·licitar a l'AR la suspensió/revocació del certificat quan el subjecte/signant cessin aquesta vinculació respecte a l'organització.

### 9.6.4 Obligació i responsabilitat de terceres parts

Serà obligació de la part usuària complir el que disposa la normativa vigent i, a més:

- Verificar la validesa dels certificats abans de fer qualsevol operació que hi estigui basada. L'Oscepa disposa de diversos mecanismes per dur a terme aquesta comprovació, com l'accés a llistes de revocats o serveis de consulta en línia com OCSP. Tots aquests mecanismes estan descrits en el lloc web de l'Oscepa. En particular, per assegurar-se que és davant d'un certificat qualificat haurà de fer la validació contra la TSL vigent en cada moment.
- Conèixer i subjectar-se a les garanties, límits i responsabilitats aplicables en l'acceptació i l'ús dels certificats en què confia, i acceptar subjectar-s'hi. En els certificats de representant de persona jurídica, que impliquen una relació de representació basada en un poder especial notarial o un document privat amb facultats limitades, les terceres parts han de comprovar els límits d'aquestes facultats.
- Comprovar la validesa de la qualificació d'una firma associada a un certificat emès per l'Oscepa comprovant que l'autoritat de certificació que ha emès el certificat es troba publicada a la llista de confiança del supervisor nacional corresponent.

### 9.6.5 Obligació i responsabilitat d'altres participants

No estipulat.

## *9.7. Exoneració de responsabilitat*

Segons la legislació vigent, la responsabilitat de l'Oscepa i de l'AR no s'estén als supòsits en què la utilització indeguda del certificat té el seu origen en conductes imputables al subjecte i la part usuària per:

- No haver proporcionat informació adequada, inicialment o posteriorment, com a conseqüència de modificacions de les circumstàncies reflectides en el certificat electrònic, quan la seva inexactitud no hagi pogut ser detectada pel prestador de serveis de certificació.
- Haver incorregut en negligència pel que fa a la conservació de les dades de creació de signatura i a la seva confidencialitat.
- No haver sol·licitat la suspensió o revocació de les dades del certificat electrònic en cas de dubte sobre el manteniment de la confidencialitat.
- Haver utilitzat la signatura després d'haver expirat el període de validesa del certificat electrònic.
- Superar els límits que figuren en el certificat electrònic.
- En conductes imputables a la part usuària, actuar de forma negligent, és a dir quan no comprovi o tingui en compte les restriccions que figuren en el certificat quant als seus possibles usos i el límit d'import de les transaccions; o quan no tingui en compte l'estat de vigència del certificat.
- Els danys ocasionats al subjecte o als tercers que confien en els certificats per la inexactitud de les dades que consten en el certificat electrònic, si li han estat acreditats mitjançant un document públic, inscrit en un registre públic si així resulta exigible.
- Un ús inadequat o fraudulent del certificat en el cas que el subjecte/titular n'hagi cedit o n'hagi autoritzat l'ús a favor d'una tercera persona en virtut d'un negoci jurídic com el mandat o apoderament, sent responsabilitat exclusiva del subjecte/titular el control de les claus associades al seu certificat.

L'Oscepa i les AR tampoc no seran responsables en cap cas quan es troben davant de qualsevol d'aquestes circumstàncies:

- Estat de guerra, desastres naturals o qualsevol altre cas de força major.
- Per l'ús dels certificats sempre que excedeixi el que disposen la normativa vigent i les polítiques de certificació.
- Per l'ús indegut o fraudulent dels certificats o CRL emesos per l'AC.
- Per l'ús de la informació continguda en el certificat o en la CRL.
- Pel perjudici causat en el període de verificació de les causes de revocació/suspensió.
- Pel contingut dels missatges o documents signats o xifrats digitalment.
- Per la no recuperació de documents xifrats amb la clau pública del subjecte.

## *9.8. Limitació de responsabilitat en cas de pèrdues per transaccions*

El límit màxim que l'Oscepa permet a les transaccions econòmiques efectuades és de 0 (zero) euros.

## *9.9. Indemnitzacions*

Vegeu l'apartat 9.2.

## *9.10. Termini i finalització*

### 9.10.1 Termini

Vegeu l'apartat 5.8.

### 9.10.2 Terminació

Vegeu l'apartat 5.8.

### 9.10.3 Efecte de la terminació i la supervivència

Vegeu l'apartat 5.8.

## *9.11. Notificacions individuals i comunicació amb els participants*

Qualsevol notificació referent a aquesta CPS es farà per correu electrònic o mitjançant correu certificat dirigit a qualsevol de les adreces esmentades a l'apartat "Dades de contacte" (1.5.2).

## *9.12. Modificacions*

### 9.12.1 Procediment de modificació

La CA es reserva el dret de modificar aquest document per raons tècniques o per reflectir qualsevol canvi en els procediments que s'hagin produït a causa de requisits legals o reglamentaris (eIDAS, CA / B Forum, organismes de supervisió nacional, etc.), o com a resultat de l'optimització del cicle de treball. Cada nova versió d'aquesta CPS substitueix totes les versions anteriors, que segueixen sent, però, aplicables als certificats emesos mentre aquestes versions estaven vigents i fins a la primera data de venciment d'aquests certificats. Es publicarà almenys una actualització anual. Aquestes actualitzacions quedaran reflectides en el quadre de versions.

Els canvis que poden fer-se a aquesta CPS no requereixen notificació excepte que afecti de forma directa els drets dels subjectes/signants dels certificats. En aquest cas podran presentar els seus comentaris a l'organització de l'administració de les polítiques dins dels quinze dies següents a la publicació.

### 9.12.2 Mecanisme de notificació i terminis

#### *9.12.2.1 Llista d'elements*

Qualsevol element d'aquesta CPS pot ser canviat sense preavís.

#### *9.12.2.2 Mecanisme de notificació*

Tots els canvis proposats d'aquesta política es publicaran immediatament al web de

l'Oscepa. https://www.signaturaelectronica.ad/jerarquia-politiques-i-practiques-de-

certificacio

En aquest mateix document hi ha un apartat de canvis i versions on es poden conèixer els canvis produïts des que es va crear i la data d'aquestes modificacions.

#### *9.12.2.3 Període de comentaris*

Els signants/subscriptors i tercers que confien ,afectats poden presentar els seus comentaris a l'organització de l'administració de les polítiques dins dels quinze dies següents a la recepció de la notificació..

#### *9.12.2.4 Mecanisme de tractament dels comentaris*

Qualsevol acció presa com a resultat d'uns comentaris queda a la discreció de la PA.

### 9.12.3 Circumstàncies en què s'ha de canviar l'OID

No estipulat.

## *9.13. Procediment de resolució de conflictes*

Tota controvèrsia o conflicte que es derivi d'aquest document es resoldrà definitivament, mitjançant l'arbitratge de dret d'un àrbitre, en el marc de
Llei 13/2018, del 31 de maig, del Tribunal d'Arbitratge del Principat d'Andorra, de conformitat amb el seu Reglament i Estatut, a la qual s'encomana l'administració de l'arbitratge i la designació de l'àrbitre o tribunal arbitral. Les parts fan constar el seu compromís de complir el laude que es dicti.

## *9.14. Legislació aplicable*

L'execució, interpretació, modificació o validesa d'aquesta CPS es regiran pel que disposa la legislació andorrana vigent en cada moment.

## *9.15. Conformitat amb la llei aplicable*

Vegeu el punt 9.14.

## *9.16. Altres disposicions*

### 9.16.1 Acord complet

Els titulars i tercers que confien en els certificats assumeixen íntegrament el contingut d'aquesta Declaració de pràctiques i polítiques de certificació.

### 9.16.2 Assignació

Les parts d'aquesta CPS no poden cedir cap dels seus drets o obligacions sota aquesta CPS o acords aplicables sense el consentiment per escrit de l'Oscepa.

### 9.16.3 Separabilitat

Si les disposicions individuals d'aquesta CPS resulten ineficaces o incompletes, això es farà sense perjudici de l'efectivitat de totes les altres disposicions.

La disposició ineficaç serà reemplaçada per una disposició efectiva que es considera que reflecteix més de prop el sentit i el propòsit de la disposició ineficaç. En el cas de disposicions incompletes, s'ha d'acordar una modificació que es consideri que correspon al que raonablement s'hauria acordat d'acord amb el sentit i els propòsits d'aquesta CPS, si l'assumpte s'hagués considerat per endavant.

### 9.16.4 Compliment (honoraris d'advocats i exempció de drets)

L'Oscepa pot sol·licitar una indemnització i honoraris d'advocats d'una part per danys, pèrdues i despeses relacionats amb la conducta d'aquesta part. El fet que l'Oscepa no faci complir una disposició d'aquesta CPS no elimina el dret de l'Oscepa de fer complir les mateixes disposicions més endavant o el dret de fer complir qualsevol altra disposició d'aquesta CPS. Per ser efectiva, qualsevol renúncia ha d'estar per escrit i signada per l'Oscepa.

### 9.16.5 Força major

Les clàusules de força major, si n'hi ha, estan incloses en l'"Acord del subscriptor".

## *9.17. Altres provisions*

### 9.17.1 Publicació i còpia de la política

Una còpia d'aquesta CPS estarà disponible en format electrònic a l'adreça d'Internet:

https://www.signaturaelectronica.ad/jerarquia-politiques-i-practiques-de-certificacio

### 9.17.2 Procediments d'aprovació de la CPS

La publicació de les revisions d'aquesta CPS ha d'estar aprovada per l'autoritat de polítiques de l'Oscepa.

L'Oscepa publica al seu lloc web cada nova versió. La CPS es publica en format PDF signat electrònicament per l'Oscepa.

# ANNEX I. Història del document

| Octubre del 2013 | V1.0 | Versió inicial |
|---|---|---|
| **Novembre del 2017** | V1.0 | **Revisió** |
| **Octubre del 2019** | V2.0 | **Canvi d'ordre, denominació i desenvolupament en diversos punts per alinear-se amb l'RFC3647** |
| **Febrer 2020** | V2.1 | **Canvi de sintaxis** |
| **Març-Abril 2020** | V2.2 | **Revisió CPS** |