

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



Govern d'Andorra

Versió 3.0.

Idioma: Català

Índex

1	INTRODUCCIÓ	8
1.1	Visió general.....	8
1.2	Identificació i nom del document	8
1.3	Participants en la PKI	8
1.3.1	Autoritats de certificació	8
1.3.2	Autoritats de registre.....	9
1.3.3	Sol·licitant:	9
1.3.4	Signant	9
1.3.5	Subscriptor.....	9
1.3.6	Part que confia	9
1.3.7	Altres participants	10
1.4	Àmbit d'aplicació i usos	10
1.4.1	Usos apropiats dels certificats.....	10
1.4.2	Usos prohibits dels certificats.....	10
1.5	Autoritat de polítiques.....	10
1.5.1	Organització que administra el document	10
1.5.2	Dades de contacte de l'organització	10
1.5.3	Persona que determina la idoneïtat de la CPS per a la política	10
1.5.4	Procediments de gestió del document.....	10
1.6	Acrònims i definicions.....	10
1.6.1	Acrònims.....	10
1.6.2	Definicions	11
2	RESPONSABILITAT DE PUBLICACIÓ I DIPÒSITS	13
2.1	Repositoris	13
2.2	Publicació d'informació de certificació.....	13
2.3	Freqüència de publicació.....	13
2.4	Controls d'accés als repositoris	13
3	IDENTIFICACIÓ I AUTENTICACIÓ DELS TITULARS DELS CERTIFICATS	14
3.1	Noms	14
3.1.1	Tipus de noms.....	14
3.1.2	Significat dels noms	14
3.1.3	Anonimat o pseudònims de subscriptors	14
3.1.4	Regles utilitzades per interpretar diversos formats de noms	14
3.1.5	Unicitat dels noms	14
3.1.6	Procediment de resolució de disputes de noms	14
3.1.7	Reconeixement, autenticació i funció de marques registrades i altres signes distintius	14
3.2	Validació inicial de la identitat	15
3.2.1	Mètodes de prova de la possessió de la clau privada	15
3.2.2	Identificació de l'entitat o persona jurídica.....	15
3.2.3	Identificació de la identitat d'un individu.....	15
3.2.4	Informació de subscriptor no verificada.....	15
3.2.5	Comprovació de les facultats de representació	15
3.2.6	Autenticació de l'organització i de domini o IP	15
3.3	Identificació i autenticació de sol·licituds de renovació	15
3.3.1	Validació per a la renovació rutinària de certificats	15

3.3.2	Identificació i autenticació de la sol·licitud de renovació després d'una revocació	15
3.4	Identificació i autenticació de la sol·licitud de revocació.....	15
4	REQUISITS D'OPERACIÓ DEL CICLE DE VIDA DELS CERTIFICATS.....	16
4.1	Sol·licitud de certificats.....	16
4.1.1	Qui pot fer la sol·licitud d'un certificat	16
4.1.2	Registre de les sol·licituds	16
4.2	Processament de les sol·licituds de certificats.....	16
4.2.1	Execució de les funcions d'identificació i autenticació	16
4.2.2	Aprovació o refús de la sol·licitud	16
4.2.3	Termini per resoldre la sol·licitud.....	16
4.3	Emissió de certificats	16
4.3.1	Accions de la CA durant el procés d'emissió.....	16
4.3.2	Notificació de l'emissió al subscriptor.....	16
4.4	Acceptació de certificats	16
4.4.1	Conducta que constitueix acceptació del certificat	16
4.4.2	Publicació del certificat per la CA	17
4.4.3	Notificació d'emissió de certificat per la CA a altres entitats.....	17
4.5	Ús del parell de claus i els certificats.....	17
4.5.1	Ús del certificat i la clau privada del subscriptor.....	17
4.5.2	Ús de la clau pública i del certificat per la part que confia	18
4.6	Renovació del certificat.....	18
4.6.1	Circumstància per a la renovació del certificat	18
4.7	Renovació de claus	18
4.8	Modificació de certificats	18
4.8.1	Circumstància per modificar el certificat	18
4.8.2	Qui pot sol·licitar la modificació del certificat	18
4.8.3	Processament de sol·licituds de modificació de certificats	18
4.8.4	Notificació de l'emissió d'un nou certificat al subscriptor	18
4.8.5	Conducta que constitueix l'acceptació del certificat modificat	19
4.8.6	Publicació del certificat modificat per la CA.....	19
4.8.7	Notificació d'emissió de certificat per la CA a altres entitats.....	19
4.9	Suspensió de certificats.....	19
4.10	Revocació de certificats	19
4.10.1	Causes de revocació	19
4.10.2	Qui pot sol·licitar la revocació	20
4.10.3	Procediment de sol·licitud de revocació	20
4.10.4	Període de gràcia de la sol·licitud de revocació	20
4.10.5	Temps dins el qual CA ha de processar la sol·licitud de revocació.....	21
4.10.6	Requisits de comprovació de la revocació per les parts que confien en els certificats	21
4.10.7	Freqüència d'emissió de CRL.....	21
4.10.8	Màxima latència de CRL	21
4.10.9	Disponibilitat de comprovació en línia de la revocació.....	21
4.10.10	Requisits de la comprovació en línia de la revocació	21
4.10.11	Altres formes de divulgació d'informació de revocació disponibles.....	21
4.10.12	Requisits especials de revocació per compromís de les claus	22
4.10.13	Circumstàncies per a la suspensió.....	22
4.10.14	Qui pot sol·licitar la suspensió.....	22
4.10.15	Procediment de sol·licitud de suspensió	22
4.10.16	Límits del període de suspensió	22

4.11	Serveis de comprovació de l'estat dels certificats	22
4.11.1	Característiques operacionals	22
4.11.2	Disponibilitat del servei	22
4.11.3	Característiques opcionals.....	22
4.12	Finalització de la subscripció.....	22
4.13	Custòdia i recuperació de claus.....	22
4.13.1	Política i pràctiques de custòdia i recuperació de claus	22
4.13.2	Política i pràctiques d'encapsulació i recuperació de claus de sessió.....	22
5	CONTROLS DE LES INSTAL·LACIONS, DE GESTIÓ I OPERACIONALS	23
5.1	Controls de seguretat física	23
5.1.1	Ubicació i construcció.....	23
5.1.2	Accés físic.....	23
5.1.3	Alimentació elèctrica i aire condicionat	23
5.1.4	Exposició a l'aigua.....	23
5.1.5	Prevenició i protecció d'incendis.....	23
5.1.6	Sistema d'emmagatzematge	23
5.1.7	Eliminació de residus.....	24
5.1.8	Sistema de seguretat (backup) extern	24
5.2	Controls procedimentals.....	24
5.2.1	Rols de confiança.....	24
5.2.2	Nombre de persones requerides per tasca	25
5.2.3	Identificació i autenticació per a cada rol.....	25
5.2.4	Rols que requereixen separació de tasques.....	25
5.3	Controls del personal.....	25
5.3.1	Qualificacions, experiència i requisits d'autorització	25
5.3.2	Procediments de comprovació d'antecedents.....	25
5.3.3	Requisits de formació	26
5.3.4	Requisits i freqüència de l'actualització de la formació	26
5.3.5	Freqüència i seqüència de rotació de tasques	26
5.3.6	Sancions per accions no autoritzades	26
5.3.7	Requisits de contractació de personal	26
5.3.8	Documentació proporcionada al personal.....	26
5.4	Procediments de registre d'esdeveniments	26
5.4.1	Tipus d'esdeveniments registrats.....	26
5.4.2	Freqüència de tractament de registres d'auditoria	27
5.4.3	Períodes de retenció per als diaris (<i>logs</i>) d'auditoria.....	27
5.4.4	Protecció dels registres d'auditoria.....	27
5.4.5	Procediments de còpia de seguretat dels registres d'auditoria	28
5.4.6	Sistema de recollida d'informació d'auditoria	28
5.4.7	Notificació al subjecte causa de l'esdeveniment	28
5.4.8	Anàlisi de vulnerabilitats	28
5.5	Arxiu de registres.....	28
5.5.1	Tipus d'arxius registrats.....	28
5.5.2	Període de retenció per a l'arxivament	28
5.5.3	Protecció de l'arxiu	28
5.5.4	Procediments de còpia de seguretat de l'arxiu	28
5.5.5	Requisits per al segellament de temps dels registres	29
5.5.6	Sistema de recollida d'informació d'auditoria	29
5.5.7	Procediments per obtenir i verificar informació arxivada.....	29
5.6	Canvi de claus.....	29
5.7	Recuperació en cas de compromís de la clau o desastre	29

5.7.1	Procediments de gestió d'incidències i compromisos	29
5.7.2	Corrupció de recursos, aplicacions o dades	29
5.7.3	Compromís de clau privada de l'entitat	29
5.7.4	Continuïtat del negoci després d'un desastre	30
5.8	Cessament de la CA o RA.....	30
5.8.1	Autoritat de Certificació	30
5.8.2	Autoritat de Registre	30
6	CONTROLS DE SEGURETAT TÈCNICA	31
6.1	Generació i instal·lació del parell de claus.....	31
6.1.1	Generació del parell de claus	31
6.1.2	Lliurament de la clau privada al signant	31
6.1.3	Lliurament de la clau pública a l'emissor del certificat	31
6.1.4	Lliurament de la clau pública de la CA als usuaris	31
6.1.5	Mida de les claus	31
6.1.6	Paràmetres de generació de la clau pública i control de qualitat	31
6.1.7	Propòsits d'ús de claus (camp KeyUsage de X.509 v3).....	31
6.2	Protecció de la clau privada i estàndards per als mòduls criptogràfics	31
6.2.1	Controls i estàndards de mòduls criptogràfics	31
6.2.2	Control multipersonal (n d'entre m) de la clau privada	32
6.2.3	Dipòsit de clau privada	32
6.2.4	Còpia de seguretat de la clau privada	32
6.2.5	Arxiu de la clau privada	32
6.2.6	Transferència de la clau privada a o des del mòdul criptogràfic.....	32
6.2.7	Emmagatzematge de clau privada en el mòdul criptogràfic	32
6.2.8	Mètode d'activació de la clau privada.....	32
6.2.9	Mètode de desactivació de la clau privada	32
6.2.10	Mètode de destrucció de la clau privada	32
6.2.11	Qualificació del mòdul criptogràfic	32
6.3	Altres aspectes de la gestió del parell de claus	32
6.3.1	Arxiu de la clau pública	32
6.3.2	Període d'ús per a les claus públiques i privades	33
6.4	Dades d'activació.....	33
6.4.1	Generació i activació de les dades d'activació	33
6.4.2	Protecció de les dades d'activació.....	33
6.4.3	Altres aspectes de les dades d'activació	33
6.5	Controls de seguretat informàtica	33
6.5.1	Requisits tècnics de seguretat informàtica específics	33
6.5.2	Valoració de la seguretat informàtica	34
6.6	Controls de seguretat del cicle de vida.....	34
6.6.1	Controls de desenvolupament de sistema	34
6.6.2	Controls de gestió de la seguretat.....	34
6.6.3	Avaluació de la seguretat del cicle de vida.....	35
6.6.4	Controls del cicle de vida dels dispositius segurs de creació de Firma	35
6.7	Controls de seguretat de la xarxa	36
6.8	Fonts de temps.....	36
7	PERFILS DE CERTIFICAT, CRL I OCSP	37
7.1	Perfil de certificat	37
7.1.1	Número de versió	37
7.1.2	Extensions del certificat.....	37
7.1.3	Identificadors d'objecte (OID) dels algorismes.....	37

7.1.4	Format de noms	37
7.1.5	Restriccions dels noms	37
7.1.6	Identificador d'objecte (OID) de la política de certificació.....	37
7.1.7	Ús de l'extensió Policy Constraints.....	37
7.1.8	Sintaxi i semàntica dels qualificadors de política	37
7.1.9	Tractament semàntic per a l'extensió crítica Certificate Policy	37
7.2	Perfil de CRL	38
7.2.1	Número de versió	38
7.2.2	CRL i extensions	38
7.3	Perfil d'OCSP	38
7.3.1	Número de versió	38
7.3.2	Extensions OCSP	38
8	AUDITORIES DE CONFORMITAT	39
8.1	Freqüència o circumstàncies de les auditories Veure auditories No UE	39
8.1.1	Auditoria en les autoritats de registre.....	39
8.2	Identificació i qualificació de l'auditor	39
8.3	Relació entre l'auditor i la CA	39
8.4	Tòpics coberts per l'auditoria	39
8.5	Accions preses com a resultat de les deficiències	40
8.6	Comunicació de resultats	40
9	ASPECTES LEGALS I ALTRES ASSUMPTES	41
9.1	Tarifes	41
9.1.1	Tarifes d'emissió de certificats i renovació	41
9.1.2	Tarifes d'accés als certificats	41
9.1.3	Tarifes d'accés a la informació relativa a l'estat dels certificats o els certificats revocats	41
9.1.4	Tarifes per a l'accés al contingut d'aquestes pràctiques de certificació	41
9.1.5	Política de reintegraments	41
9.2	Responsabilitat financera.....	41
9.2.1	Cobertura de l'assegurança.....	41
9.3	Confidencialitat de la informació del negoci	41
9.3.1	Tipus d'informació que s'ha de mantenir confidencial	41
9.3.2	Tipus d'informació no confidencial	41
9.3.3	Responsabilitat de protegir la informació confidencial.....	41
9.4	Protecció de dades personals	42
9.4.1	Política de protecció de dades personals	42
9.4.2	Política de privacitat.	42
9.4.3	Informació no considerada privada.....	42
9.4.4	Responsabilitat de protegir la informació privada	42
9.4.5	Avís i consentiment per utilitzar informació privada	42
9.4.6	Divulgació de conformitat amb un procés judicial o administratiu	42
9.4.7	Altres circumstàncies de divulgació d'informació	42
9.5	Drets de propietat intel·lectual	42
9.6	Obligacions i responsabilitat civil	42
9.6.1	Obligació i responsabilitat de la CA	42
9.6.2	Obligació i responsabilitat de l'RA.....	43
9.6.3	Obligació i responsabilitat del subscriptor	45
9.6.4	Obligació i responsabilitat de terceres parts.....	46

9.6.5	Obligació i responsabilitat d'altres participants	46
9.7	Exoneració de responsabilitat	46
9.8	Limitació de responsabilitat	46
9.9	Indemnitzacions	47
9.10	Termini i finalització	47
9.10.1	Termini.....	47
9.10.2	Finalització	47
9.10.3	Efecte de la finalització i la supervivència	47
9.11	Notificacions individuals i comunicació amb els participants	47
9.12	Modificacions.....	47
9.12.1	Procediment de modificació.....	47
9.12.2	Mecanisme de notificació i terminis	47
9.12.3	Circumstàncies en què s'ha de canviar l'OID	47
9.13	Procediment de resolució de conflictes	47
9.14	Legislació aplicable.....	48
9.15	Conformitat amb la llei aplicable	48
9.16	Altres disposicions.....	48
9.16.1	Acord complet	48
9.16.2	Assignació	48
9.16.3	Separabilitat.....	48
9.16.4	Compliment (honoraris d'advocats i exempció de drets)	48
9.16.5	Força major.....	48
9.17	Altres provisions	48
9.17.1	Publicació i còpia de la política	48
9.17.2	Procediments d'aprovació de la CPS	48
10	ANNEX I. Història del document.....	49

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 Sistemas Informáticos Abiertos, S.A. (SIA). 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 SIA en la seva relació contractual amb l'OSCEPA.

Aquesta Declaració de Pràctiques de Certificació s'estructura en conformitat amb el document RFC-3647 "Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework", i també s'alinea amb la Llei 35/2014, de 27 de novembre, de serveis de confiança electrònica de serveis de confiança electrònica, l'article 10 de la Llei 9/2021, del 29 d'abril, de modificació de la Llei 35/2014, del 27 de novembre, de serveis de confiança electrònica de serveis de confiança electrònica, o que marca el Reglament eIDAS i de conformitat amb el dret nacional.

Per dotar d'un caràcter uniforme el document i facilitar la seva lectura i anàlisi, s'inclouen totes les seccions establertes en la RFC-3647. Quan no hi hagi res de previst en alguna secció apareixerà la menció "No Aplica".

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.

Certificat de persona física menor de 16 a 18 anys

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

Les entitats i persones que intervenen són:

- SIA com a entitat propietària de la infraestructura de custòdia i d'emissió dels certificats arrel i de les tipologies definides en el article 1.2 de la CA Entitat de Certificació de l'Administració Pública Andorrana,
- OSCEPA com a entitat responsable de la gestió de la Entitat (autoritat) de Certificació de l'Administració Pública Andorrana;
- Les autoritats de registre;
- els signants/titulars;
- els subscriptors;
- les terceres parts que accepten els certificats emesos.

1.3.1 Autoritats de certificació

SIA actua com a empresa emissora i custòdia dels certificats arrel de l'Autoritat arrel. Es propietària de la infraestructura emissora dels certificats i està vinculada amb l'autoritat de certificació arrel del Govern d'Andorra per un contracte de prestació de serveis.

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 (CA) utilitza autoritats de registre (RA) per dur a terme les tasques de comprovació i emmagatzematge de la documentació dels continguts incorporats en el certificat digital.

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

La informació relativa a la CA 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 (RA) pot ser una persona física o jurídica que actua d'acord amb aquesta CPS i, si escau, mitjançant un acord subscrit amb una CA 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 RA són autoritats delegades de la CA, encara que la CA és l'última responsable del servei en darrera instància.

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

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

1.3.3 Sol·licitant:

El sol·licitant es aquella persona que sol·licita la emissió d'un certificat en nom propi o en nom d'una organització.

1.3.4 Signant

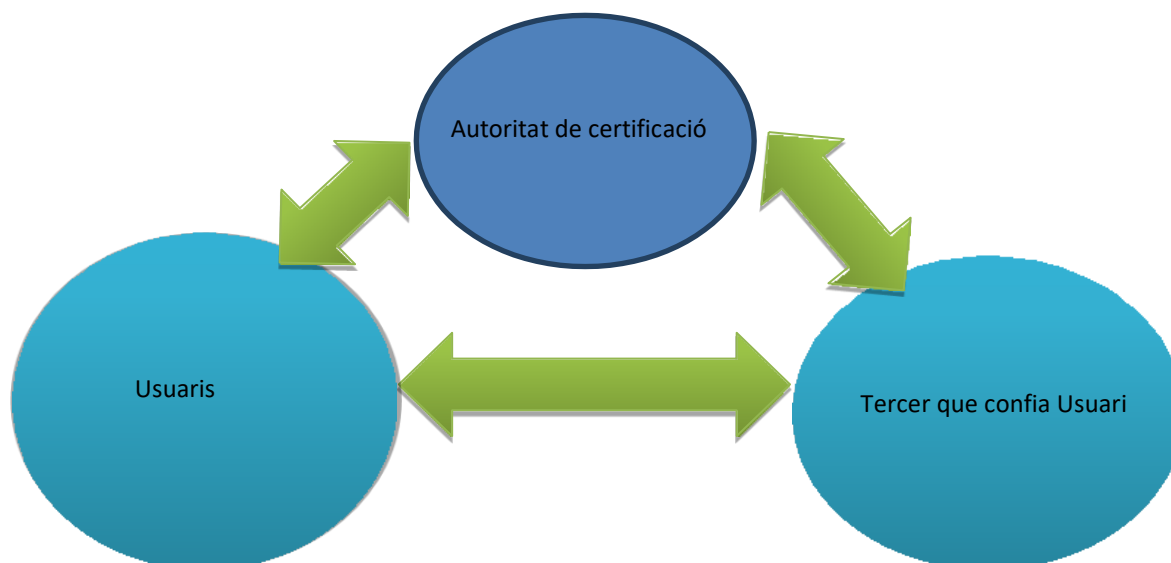
S'entén per signant la persona o titular del certificat que realitza o crea la signatura electrònica.

1.3.5 Subscriptor

En cas d'un vincle entre el signant i una entitat mitjançant una relació laboral o contractual, el subscriptor es la entitat que subscriu un contracte amb l'OSCEPA per la emissió de certificats als seus usuaris o tercers amb un vincle amb l'empresa. Tanmateix podrà sol·licitar la revocació del certificat quan cessi el vincle del signant amb el subscriptor.

1.3.6 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 la CA gestionada per l'Oscepa i que voluntàriament confia en el certificat emès per aquesta última.



1.3.7 Altres participants

No és aplicable.

1.4 Àmbit d'aplicació i usos

1.4.1 Usos apropiats dels certificats

Un certificat emès per l'OSCEPA només pot ser utilitzat per als propòsits explícitament permesos i indicats en aquesta CPS i en la corresponent Política de Certificació (PC), per la qual cosa hi ha certes limitacions en l'ús dels certificats de SIA.

Els certificats s'han de fer servir únicament de conformitat amb la legislació que els sigui aplicable, especialment tenint en compte les restriccions d'importació i exportació en matèria criptogràfica existents a cada moment.

1.4.2 Usos prohibits dels certificats

Els certificats s'han d'utilitzar per a la seva funció pròpia i finalitat establerta, sense que es puguin emprar en altres funcions i amb altres finalitats de les descrites per a cadascun d'ells a l'apartat 1.4.1 Usos apropiats/permesos dels certificats.

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 de l'Oscepa.

1.5.2 Dades de contacte de l'organització

Adreça:	Telèfon:	Carrer de la Grau, Edifici Prat del Rull, Andorra la Vella
A/e:		+376 875 700
		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 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

CA	Autoritat de certificació
RA	Autoritat de registre
CPS	<i>Certification Practice Statement</i> . Declaració de pràctiques de certificació

CRL	<i>Certificate Revocation List</i> . Llista de certificats revocats		
CSR	<i>Certificate Signing Request</i> . Petició de signatura de certificat	<i>DES</i>	<i>Data Encryption Standard</i> . Estàndard de xifratge de dades
DN	<i>Distinguished Name</i> . Nom distintiu dins del certificat digital		
DSA	<i>Digital Signature Algorithm</i> . 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	International Organization for Standardization. Organisme Internacional d'Estandardització		
ITU	<i>International Telecommunications Union</i> . Unió Internacional de Telecomunicacions		
LDAP	Lightweight Directory Access Protocol. Protocol d'accés a directoris		
OCSP	<i>Online Certificate Status Protocol</i> . Protocol d'accés a l'estat dels certificats		
OID	<i>Object Identifier</i> . Identificador d'objecte		
PA	<i>Policy Authority</i> . Autoritat de polítiques		
PC	Política de certificació		
PIN	<i>Personal Identification Number</i> . Número d'identificació personal	PKI	<i>Public Key Infrastructure</i> . Infraestructura de clau pública
RSA	Rivest-Shamir-Adleman. Tipus d'algorisme de xifratge		
SHA	<i>Secure Hash Algorithm</i> . Algorisme segur de Hash		
SSL	<i>Secure Sockets Layer</i> . 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	<i>Transmission Control Protocol / Internet Protocol</i> . 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: Es 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 CA, 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 la CA.

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 de xifratge de dades. També anomenada *dades de creació de signatura*. La clau privada de la CA 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 la CA.

Dades d'activació: Dades privades, com PIN o contrasenyes emprades per activar la clau privada.

DSADC: 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 algorismes coneguts, per garantir d'aquesta manera:

- a) Que les dades no han estat modificades (integritat)
- b) Que la persona que signa les dades és qui diu ser (identificació)
- 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 la CA 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'CA, 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 certificació

El contingut d'aquesta CPS, juntament amb les PC per a cada tipus de certificat, estarà disponible en forma de lliure accés a les adreces indicades a l'apartat: 2.1 Repositoris.

Les noves versions del document es publicaran a l'adreça web indicada substituint la versió anterior. Es mantindran publicades les versions anteriors de tota la documentació.

2.3 Freqüència de publicació

La DPC i les PC es publicaran en el moment de la seva aprovació i es tornaran a publicar en el moment que s'aprovi qualsevol modificació sobre aquesta. Les modificacions es faran públiques al lloc web indicat a l'apartat 2.1 Repositoris. La CA afegirà els certificats revocats a la CRL pertinent dins del període de temps estipulat a l'apartat 4.9.7 Freqüència d'emissió de CRLs.

2.4 Controls d'accés als repositoris

La CA de l'OSCEPA té implantats controls per mantenir la integritat del seu repositori intern, de manera que:

- Es pugui comprovar l'autenticitat dels certificats.
- Les persones no autoritzades no puguin alterar les dades.
- Els certificats només seran accessibles en els supòsits o les persones que el signant indiqui.
- es detecti qualsevol canvi tècnic que afecti els requisits de seguretat.

3 IDENTIFICACIÓ I AUTENTICACIÓ DELS TITULARS DELS CERTIFICATS

3.1 Noms

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

Les regles utilitzades per l'OSCEPA per interpretar els noms distintius dels titulars de certificats que emet és ISO/IEC 9595 (x.500) Distinguished Name (DN) i ISO/IEC 9594-8 (X.509).

Els certificats expedits per l'OSCEPA compleix les recomanacions de la RFC 5280 ("Internet X.509 Public Key Infrastructure. Certificate and CRL Profile") respecte a la utilització de la codificació dels atributs dels camps Issuer (Emissor) i Subject (Subjecte). Concretament, per mitjà de la codificació en format UTF8String.

La RA disposa de l'associació entre aquests noms o pseudònims i les entitats a què estan assignats..

3.1.5 Unicitat dels noms

Dins de la mateixa CA 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 Procediment de resolució de disputes de noms

Qualsevol conflicte concernent a la propietat de noms es resoldrà segons allò estipulat a l'apartat, 9.13 Reclamacions i jurisdicció, d'aquesta CPS.

l'OSCEPA es reserva el dret de rebutjar una sol·licitud de certificat degut a un conflicte sobre noms.

3.1.7 Reconeixement, autenticació i funció de marques registrades i altres signes distintius

L'Oscepa no assumeix compromisos respecte a l'ús de marques comercials als certificats ni determina si el signant

té dret sobre la marca. Així mateix, es reserva el dret de rebutjar una sol·licitud de certificat a causa d'un conflicte de marques registrades.

3.2 Validació inicial de la identitat

3.2.1 Mètodes de prova de la possessió de la clau privada

Com que el procediment de generació del parell de claus depèn del tipus de certificat emès, la prova de possessió de la clau privada es descriurà a cada política de certificació específica.

La clau privada tant de la CA Arrel com de les CA Subordinades es genera de forma segura en un mòdul hardware criptogràfic (HSM) i en cap moment no en sortirà.

3.2.2 Identificació de l'entitat o persona jurídica

L'autenticació de la identitat per als certificats de client s'especifica a la Política de Certificació corresponent.

3.2.3 Identificació de la identitat d'un individu

L'autenticació de la identitat per als certificats de client s'especifica a la Política de Certificació corresponent.

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 Comprovació de les facultats de representació

Cada Política de Certificació establirà el procediment de comprovació de les facultats que es reclamin per a cada cas.

3.2.6 Autenticació de l'organització i de domini o IP

No Aplica.

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

Aquest apartat depèn del tipus de certificat i està recollit a la seva corresponent Política de Certificació. Així mateix, la PC estableix els passos que cal seguir en la seva tramitació.

4.1.2 Registre de les sol·licituds

L'OSCEPA o un intermediari de l'OSCEPA que actuï com a RA per gestionar la sol·licitud del certificat, és el responsable de fer-ne el procediment d'alta. Aquesta informació serà donada d'alta a la base de dades de l'autoritat de registre per tal de fer consultes posteriors, sobre l'estat de la sol·licitud del sol·licitant o dels certificats sol·licitats per a un subscriptor particular.

4.2 Processament de les sol·licituds de certificats

En el moment en què l'OSCEPA o un intermediari de l'OSCEPA que actuï com a RA rep una sol·licitud de certificat, se'n procedeix al registre mitjançant l'aplicació de registre corresponent associada a l'Autoritat de Certificació.

Durant el procés de sol·licitud hi ha una comprovació que l'usuari realment pertany al sistema, aquesta comprovació és duta a terme mitjançant consulta al repositori de l'OSCEPA, on cal trobar necessàriament la informació del sol·licitant.

4.2.1 Execució de les funcions d'identificació i autenticació

És responsabilitat de l'RA realitzar de manera fefaent la identificació i l'autenticació del sol·licitant. Aquest procés s'ha de fer prèviament a l'emissió del certificat.

Aquesta secció és dependent del tipus de certificat en particular i està recollit a la seva corresponent Política de Certificació.

4.2.2 Aprovació o refús de la sol·licitud

En el moment de la personació o procediment equivalent, l'RA verifica la informació proporcionada pel sol·licitant, incloent-hi la validació de la identitat del signant o subscriptor. Si aquesta informació és correcta, es procedeix a la signatura de l'instrument jurídic vinculant entre el signant i l'OSCEPA.

Cal consultar les especificitats de cada tipus de certificat a la Política específica per a cada certificat.

Aleshores es podrà procedir a l'emissió del certificat..

4.2.3 Termini per resoldre la sol·licitud

No Aplica.

4.3 Emissió de certificats

4.3.1 Accions de la CA durant el procés d'emissió

Aquesta informació s'especifica a la Política de Certificació corresponent.

4.3.2 Notificació de l'emissió al subscriptor

Aquesta informació s'especifica a la Política de Certificació corresponent.

4.4 Acceptació de certificats

4.4.1 Conducta que constitueix acceptació del certificat

L'acceptació del certificat és l'acció mitjançant la qual el titular dona inici a les obligacions respecte al prestador de serveis de confiança SIA. El certificat s'acceptarà en el moment que l'instrument jurídic vinculant entre el sol·licitant i el SIA hagi estat signat i el certificat estigui en possessió del signant.

Com a evidència de l'acceptació haurà de quedar un full d'acceptació signat pel signant. És podrà començar a utilitzar el certificat a partir de la data en què es va signar el full d'acceptació.

En l'àmbit del certificat de signatura centralitzada, en el cas de generació del certificat de signatura electrònica el mateix acte d'emissió comporta l'acceptació implícita del certificat de signatura i l'acceptació i signatura del document de conformitat amb l'emissió del certificat qualificat de signatura centralitzada .

Des del moment de l'acceptació, aquesta DPC amb relació al signant desplega tots els seus efectes.

4.4.2 Publicació del certificat per la CA

Els certificats es publicaran als repositoris a aquest efecte.

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

No Aplica.

4.5 Ús del parell de claus i els certificats

4.5.1 Ús del certificat i la clau privada del subscriptor

Les responsabilitats i limitacions d'ús del parell de claus i del certificat s'establiran al PC corresponent. El titular només podrà utilitzar el parell de claus i el certificat després d'acceptar les condicions d'ús, establertes a la DPC i PC, el document d'acceptació mitjans i d'acord amb allò establert a les extensions "Key Usage" i "Extended KeyUsage" del certificat.

L'aplicació d'aquests límits dependrà en gran part de la implementació correcta per aplicacions informàtiques de tercers, i la regulació quedarà fora de l'abast d'aquest document.

Després de l'extinció de la vigència o la revocació del certificat, el titular haurà de deixar d'utilitzar la clau privada associada i els corresponents certificats.

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	critical, digitalSignature	clientAuth, emailProtection	critical, CA: false
Persona física menor de 16 a 18 anys en DSCF	critical, digitalSignature	clientAuth, emailProtection	critical, CA: false
PERSONA FÍSICA AMB professió regulada en DSCF	critical, nonRepudiation	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 privada en DSCF	critical, nonRepudiation	clientAuth, emailProtection	critical, CA: false
PERSONA FÍSICA al servei de l'ADMINISTRACIÓ a DSCF	critical, nonRepudiation	clientAuth, emailProtection	critical, CA: false
PERSONA FÍSICA al servei de l'ADMINISTRACIÓ a DSCF –XIFRAT	critical, keyEncipherment, dataEncipherment	clientAuth, emailProtection	critical, CA: false

SEGELL D'EMPRESA (persona jurídica) en DSCF - Segell electrònic	critical, nonRepudiation	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 en DSCF	critical, digitalSignature	clientAuth, emailProtection	critical, CA: false
SEGELL d'Òrgan, administració pública o entitat de dret públic a programari	critical, digitalSignature, keyEncipherment, dataEncipherment, nonRepudiation	clientAuth, emailProtection	critical, CA: false
REPRESENTANT DE PERSONA JURÍDICA en DSCF	critical, digitalSignature	clientAuth, emailProtection	critical, CA: false

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

Els tercers que confien en els certificats podran utilitzar els certificats per allò que estableix aquesta DPC i la PC corresponent, i amb allò establert als camps "Key Usage" i "Extended Key Usage" del certificat.

És responsabilitat dels tercers verificar l'estat del certificat mitjançant els serveis oferts per SIA concretament per a això i especificats al present document.

4.6 Renovació del certificat

4.6.1 Circumstància per a la renovació del certificat

En l'àmbit de la CA de l'Oscepa no es realitzarà la renovació de certificats sense canvi de claus.

4.7 Renovació de claus

Les condicions particulars de renovació s'especifiquen a la corresponent Política de Certificació.

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 formen 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 Suspensió de certificats.

No és aplicable.

4.10 Revocació de certificats

La revocació d'un certificat suposa la pèrdua de validesa i és irreversible.

Les revocacions i suspensions tenen efecte des del moment en què la indicació de la dita revocació o suspensió s'inclogui al servei de consulta sobre la vigència dels certificats de l'OSCEPA.

Tots els serveis de consulta de l'estat de revocació de certificats han de disposar de la informació de manera consistent en el moment de produir-se la revocació o la suspensió d'un certificat. Atesa la naturalesa de cada servei, CRLs i OCSP, hi ha la possibilitat d'una petita desincronització que en cap cas no superarà els cinc (5) minuts. Això cal tenir en compte per tercers que necessitin dur a terme validacions de l'estat de revocació de certificats emesos per aquest PSC amb les màximes garanties sobre la sincronització de la informació de revocació.

4.10.1 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 la CA 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.

4.10.2 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'RA o la CA.
- També es preveu la possibilitat que tercers o parts interessades puguin comunicar frauds, mals usos, conductes inadequades o dades errònies. En aquest cas, l'RA o la CA podrà revocar el certificat després de comprovar la veracitat d'aquestes causes de revocació.

4.10.3 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'RA, en horari d'atenció al públic, mostrant un document d'identificació 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·licita la revocació del certificat.
- A través de la plataforma del portal de gestió de certificats centralitzat Siacert.

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

4.10.4 Període de gràcia de la sol·licitud de revocació

El període de revocació des que l'Oscepa o un RA té coneixement autènticat 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.

4.10.5 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 4.10.3.

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.

4.10.6 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 la CA que ha emès el certificat. La CRL conté un camp (NextUpdate) amb la data de la seva pròxima actualització.

4.10.7 Frequència d'emissió de CRL

Els CRL per als certificats de final de l'entitat es generaran cada 24 hores o més, si n'hi ha, en el moment en què es revoqui un certificat amb una validesa de 24 hores.

El CRL dels certificats CA (ARL) s'emet cada 12 mesos o quan es produeix una revocació.

Si s'emet l'últim CRL per a la validació de certificats d'entitat final, el camp nextUpdate s'establirà en "99991231235959Z", tal com estableix la norma ETSI EN 319 411-1.

4.10.8 Màxima latència de CRL

L'OSCEPA publicarà amb caràcter immediat la CRL que s'hagi generat en qualsevol dels casos indicats a l'apartat 4.9.7, per mitjà d'un procés automatitzat.

4.10.9 Disponibilitat de comprovació en línia de la revocació

La informació relativa a l'estat dels certificats estarà disponible en línia les 24 hores del dia, els 7 dies de la setmana.

En cas de fallada del sistema, o qualsevol altre factor que no estigui sota el control de la CA, aquesta realitzarà els esforços més grans per assegurar que aquest servei d'informació no estigui indisponible durant més temps que el període màxim de 24 hores.

Aquest termini no és d'aplicació sota els supòsits on l'OSCEPA no sigui responsable incloent fonts d'alimentació elèctrica, comunicacions, components de maquinari i programari del qual l'OSCEPA no sigui titular o altres anàlogues.

4.10.10 Requisits de la comprovació en línia de la revocació

L'OSCEPA té previst un servei de validació de certificats mitjançant el protocol OCSP. Aquest servei serà d'accés lliure i ha de considerar:

- Comprovar l'adreça continguda a l'extensió AIA (Authority Information Access) del certificat.
- Comprovar que la resposta OCSP està signada. El certificat de signatura de respostes OCSP emesos per CA OSCEPA són conformes a la norma: RFC 6960 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP".
- La informació proporcionada a través del servei OCSP s'actualitza almenys cada quatre dies i la validesa de la resposta és de 10 dies.

4.10.11 Altres formes de divulgació d'informació de revocació disponibles

Per a l'ús del servei de CRLs, que és d'accés lliure, cal considerar que:

- S'haurà de comprovar en tot cas l'última CRL emesa, que es podrà descarregar a l'adreça URL continguda als propis certificats d'entitat final a l'extensió "CRL Distribution Point" o en aquesta mateixa DPC com a les corresponents PC.
- L'usuari haurà de comprovar addicionalment les CRL pendents de la cadena de certificació de la

jerarquia.

- L'usuari ha d'assegurar-se que la llista de revocació estigui signada per l'autoritat que ha emès el certificat que vol validar.
- Els certificats revocats que expirin no seran retirats de la CRL, mantenint aquests durant quinze (15) anys per als certificats qualificats i almenys 7 anys per a la resta.

4.10.12 Requisits especials de revocació per compromís de les claus

No estipulat.

4.10.13 Circumstàncies per a la suspensió

No aplica

4.10.14 Qui pot sol·licitar la suspensió

No aplica

4.10.15 Procediment de sol·licitud de suspensió

No aplica

4.10.16 Límits del període de suspensió

No aplica

4.11 Serveis de comprovació de l'estat dels certificats

4.11.1 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.signaturaelectronica.ad>

4.11.2 Disponibilitat del servei

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

4.11.3 Característiques opcionals

No estipulat.

4.12 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.

4.13 Custòdia i recuperació de claus

4.13.1 Política i pràctiques de custòdia i recuperació de claus

La clau privada de la CA arrel com les de les CA Subordinades de SIA han estat generades sobre mòduls de seguretat criptogràfics, complint amb nivells de seguretat necessaris.

Les condicions particulars de custòdia de les claus privades emeses als usuaris s'especifiquen a la corresponent Política de Certificació. En cas contrari, el TSP en cap moment custodiarà ni copiarà la clau privada emesa als usuaris. Per tant, el TSP en cap moment podrà recuperar la clau dels usuaris. En cas de pèrdua d'aquesta, s'haurà de revocar el certificat i emetre'n un de nou.

4.13.2 Política i pràctiques d'encapsulació i recuperació de claus de sessió

No Aplica.

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

5.1 Controls de seguretat física

Els aspectes referents als controls de seguretat física es troben recollits detalladament en la documentació que SIA ha desenvolupat a aquest efecte. En aquest apartat s'han de recollir les mesures adoptades més rellevants.

5.1.1 Ubicació i construcció

Els edificis on es troba ubicada la infraestructura de la CA de SIA disposen de mesures de seguretat de control d'accés, de manera que només se'n permet l'entrada a les persones degudament autoritzades, els quals compleixen els requisits físics següents:

- Ubicat en emplaçament específics per evitar danys per possibles incendis.
- Absència de finestres a l'exterior de l'edifici. Càmeres de vigilància a les àrees d'accés restringit.
- Controls d'accessos basats en la targeta i la contrasenya.
- Sistemes de protecció i de prevenció d'incendis.
- Protecció del cablatge contra danys i intercepció de la transmissió de dades..

5.1.2 Accés físic

L'accés físic a les dependències de SIA on es duen a terme processos de certificació és 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 mateix, incloent-hi filmació per circuit tancat de televisió i el seu arxiu.

Les instal·lacions tenen detectors de presència a tots els punts vulnerables així com sistemes d'alarma per a detecció d'intrusisme amb avís per canals alternatius.

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

5.1.3 Alimentació elèctrica i aire condicionat

Els equips informàtics de la CA de SIA estan convenientment protegits davant de fluctuacions o talls de subministrament elèctric, que puguin danyar-los o interrompre el servei.

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

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

Es realitzen controls periòdics dels generadors i fonts d'energia per validar el correcte funcionament..

5.1.4 Exposició a l'aigua

Les instal·lacions del SIA on es troben els equips estan protegides per evitar-ne les exposicions a l'aigua, mitjançant detectors d'humitat i altres mecanismes de seguretat.

Es fan controls periòdics d'aquests elements.

5.1.5 Prevenció i protecció d'incendis

Les instal·lacions on es troben els equips de la CA de SIA compten amb les mesures adequades de protecció contra el foc, com ara detectors de fum sensors iònics, alarmes, extintors i gas HFC-227 en cas d'incendi.

Es fan controls periòdics de tots aquests elements.

5.1.6 Sistema d'emmagatzematge

SIA ha establert els procediments necessaris per disposar de còpies de seguretat de tota la informació de la seva infraestructura productiva. Les còpies de seguretat s'emmagatzemen de manera segura.

SIA ha disposat plans de còpia de seguretat, per a tota la informació sensible i aquella considerada com a necessària per a la persistència de la seva activitat..

5.1.7 Eliminació de residus

S'ha adoptat una política de gestió de residus que garanteix la destrucció de qualsevol material que pogués contenir informació així com una política de gestió dels suports removibles.

5.1.8 Sistema de seguretat (backup) extern

SIA disposa de còpies de seguretat en ubicacions diferents que reuneixen les mesures precises de seguretat i amb una separació física adequada..

5.2 Controls procedimentals

Per raons de seguretat, la informació relativa als controls de procediment es considera matèria confidencial i només se n'inclou una part. Així mateix, SIA garanteix que els seus sistemes s'operen i s'administren de forma segura, i per a aquest propòsit estableix i implanta procediments per a les funcions que afectin la provisió dels seus serveis.

5.2.1 Rols de confiança

Els rols de confiança garanteixen una segregació de funcions que dissemi 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'CA:

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'CA són incompatibles amb les tasques de certificació i sistemes.

Operador d'CA:

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

Les tasques de l'operador d'CA són incompatibles amb les d'administrador d'CA 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

La CA SIA garanteix almenys tres persones, per realitzar les tasques que requereixin un control multi-persona detallades a continuació:

- Generació de la clau de les ACs.
- Recuperació i backup de la clau privada de les ACs
- Emissió de certificats de les ACs.
- Activació de la clau privada de les ACs.
- Qualsevol altra activitat realitzada sobre els recursos de maquinari i programari que donen suport a la CA arrel.

5.2.3 Identificació i autenticació per a cada rol

Les persones assignades per a cada rol són identificades per assegurar que només duu a terme les operacions per a les quals està assignada.

L'accés a recursos es fa en funció dels rols, garantint l'accés als mateixos mitjançant dispositius segurs.

5.2.4 Rols que requereixen separació de tasques

La norma CWA 14167-1 estableix les següents incompatibilitats entre rols:

- Incompatibilitat entre oficial de seguretat i operador de l'HSM.
- Incompatibilitat entre els rols administratius (administrador de sistema i operador de l'RA).
- Incompatibilitat entre els administradors i els operadors de l'HSM.
- Incompatibilitat entre el rol auditor de sistema i qualsevol altre rol.

5.3 Controls del personal

5.3.1 Qualificacions, experiència i requisits d'autorització

El personal que presta els seus serveis en l'àmbit de l'Autoritat de Certificació de SIA posseeix el coneixement, l'experiència i la formació suficients, per a la comesa correcta de les funcions assignades. Per això, SIA duu a terme els processos de selecció de personal que estima necessaris per tal que el perfil professional de l'empleat s'adeqüi el més possible a les característiques pròpies de les tasques a desenvolupar.

El personal de l'OSCEPA 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'RA són fiables i pertanyen a un organisme delegat per dur a terme les tasques de registre.

L'administrador d'RA 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 delictiu 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

Els processos de selecció de personal són els ja definits per SIA. Aquestes pràctiques asseguruen els requisits d'experiència, qualificació i historial necessaris per a cada lloc, siguin d'un rol de confiança o no.

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

SIA i l'Oscepa proveeixen el personal relacionat amb l'explotació de la CA de tota la informació i la documentació necessària sobre els procediments operatius relatius a aquesta.

SIA i l'Oscepa supervisen la realització de la formació i el grau de confiança per part del personal i duu a terme els tests necessaris per poder avaluar el nivell adequat de coneixements assimilats.

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 Aplica.

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

5.4.1 Tipus d'esdeveniments registrats

SIA registrarà tots els esdeveniments relacionats amb l'operació i la gestió del sistema, així com els relacionats amb la seguretat del mateix, entre d'altres:

- Arrencada i aturada d'aplicacions.
- Intents amb èxit o fracassats d'inici i fi de sessió.
- Intents reeixits o fracassats de crear, modificar o esborrar usuaris del sistema autoritzats.
- Els relacionats amb la gestió del cicle de vida dels certificats i CRLs.

- Informes complets dels intents d'intrusió física a les infraestructures que donen suport a l'emissió i la gestió de certificats.
- Backup, arxiu i restauració. Canvis en la configuració del sistema.
- Actualitzacions de programari i maquinari.
- Manteniment del sistema.
- Canvis de personal.
- Canvis a les claus de l'Autoritat de Certificació.
- Canvis a les polítiques d'emissió de certificats i a la present DPC.
- Registres de la destrucció de material que contingui informació de claus, dades d'activació o informació personal del subscriptor.
- Informes de compromisos i discrepàncies.
- Registres d'accés físic.
- Esdeveniments relacionats amb el cicle de vida del mòdul criptogràfic, com ara recepció, ús i desinstal·lació d'aquesta cerimònia de generació de claus i les bases de dades de gestió de claus.

Les operacions es divideixen en esdeveniments, per la qual cosa es desa informació sobre un o més esdeveniments per a cada operació rellevant. Els esdeveniments registrats tenen, com a mínim, la informació següent:

Categoria: Indica la importància de l'esdeveniment.

- Informatiu: els esdeveniments d'aquesta categoria contenen informació sobre operacions realitzades amb èxit.
- Marca: cada cop que comença i acaba una sessió d'administració, es registra un esdeveniment d'aquesta categoria.
- Advertiment: indica que s'ha detectat un fet inusual durant una operació, però que no va provocar que l'operació fallés.
- Error: indica la fallada d'una operació a causa d'un error predictable.
- Error Fatal: indica que ha passat una circumstància excepcional durant una operació.

Data: Data i hora en què va passar l'esdeveniment.

Autor: nom distintiu de l'autoritat que genera l'esdeveniment.

Rol: Tipus d'Autoritat generada per l'esdeveniment.

Tipus d'esdeveniment: Identifica el tipus de l'esdeveniment, distingint, entre d'altres, els esdeveniments criptogràfics d'interfície d'usuari, llibreria.

Mòdul: Identifica el mòdul que va generar l'esdeveniment. Els possibles mòduls són:

- CA
- RA
- Repositori d'informació.
- Llibreries de control d'emmagatzematge d'informació.

Descripció: representació textual de l'esdeveniment. Per a alguns esdeveniments, la descripció va seguida d'una llista de paràmetres els valors dels quals variaran depenent de les dades sobre les quals es va executar l'operació. Alguns exemples dels paràmetres que s'inclouen per a la descripció de l'esdeveniment "Certificat generat" són: el número de sèrie, el nom distintiu del titular del certificat emès i la plantilla de certificació que s'ha aplicat.

5.4.2 Freqüència de tractament de registres d'auditoria

Els registres s'analitzaran de manera manual quan sigui necessari, per exemple en cas que es produeixi una alerta del sistema motivada per l'existència d'algun incident, i no hi haurà una freqüència definida per a aquest procés.

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

SiA manté en línia la informació relativa als certificats qualificats generada pels registres d'auditoria fins que és arxivada. Un cop arxivats, els registres d'auditoria es conservaran, almenys, durant quinze (15) anys i la relativa a la resta de certificats, durant almenys 7 anys.

5.4.4 Protecció dels registres d'auditoria

SiA protegeix els fitxers de registres d'auditoria contra lectures, modificacions, esborrats o qualsevol altre tipus de manipulació no autoritzada utilitzant controls d'accés lògic i físic.

Els registres de programari de la CA estan protegits per tècniques criptogràfiques, de manera que ningú, excepte l'aplicació de visualització d'esdeveniments, amb un control d'accés adequat, hi pot accedir.

5.4.5 Procediments de còpia de seguretat dels registres d'auditoria

SIA fa còpies de seguretat periòdiques dels registres d'auditoria generats per la CA.

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.

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 .

5.4.7 Notificació al subjecte causa de l'esdeveniment

No es preveu notificar automàticament l'acció dels fitxers de registre d'auditoria al causant de l'esdeveniment.

5.4.8 Anàlisi de vulnerabilitats

SIA d'acord amb el procediment intern en la seva política de seguretat, realitza revisions de discrepàncies a la informació dels logs i activitats sospitoses periòdicament.

5.5 Arxiu de registres

SIA conserva tota la informació rellevant sobre les operacions realitzades amb els certificats durant els períodes de temps estipulats, tot mantenint un registre d'esdeveniments.

5.5.1 Tipus d'arxius registrats

Els tipus d'esdeveniments que es registren al fitxer són:

- Certificats i llistes de revocació.
- Dades relacionades amb el procés de sol·licitud i registre de certificats.
- Les Pràctiques i Polítiques de Certificació i el seu històric.
- Logs d'auditoria de la secció 5.4.1. Tipus d'esdeveniment.
- Esdeveniments d'error en els processos realitzats.

5.5.2 Període de retenció per a l'arxivament

SIA conservarà tota la informació i documentació relativa als certificats qualificats durant un mínim de quinze (15) anys i la relativa a la resta de certificats, durant almenys 7 anys

Per als registres d'auditoria es preveu el que especifica l'apartat 5.4.3, sempre atenent qualsevol particularitat específica a la Política de Certificació del Certificat corresponent a les dades involucrades.

5.5.3 Protecció de l'arxiu

Els fitxers de registre estan protegits mitjançant xifratge, de manera que ningú, excepte les pròpies aplicacions de visualització, amb el seu control d'accessos, pugui accedir-hi.

La destrucció d'un fitxer de registre només es pot fer amb l'autorització de l'administrador del sistema, el coordinador de seguretat i l'administrador d'auditories de SIA. Aquesta destrucció es pot iniciar per la recomanació escrita de qualsevol d'aquestes tres autoritats o de l'administrador del servei auditat, i sempre que hagi transcorregut el període mínim de retenció de quinze (15) anys. Aquesta destrucció requerirà l'autorització expressa i per escrit.

5.5.4 Procediments de còpia de seguretat de l'arxiu

Les còpies de seguretat dels fitxers de registre es realitzaran segons les mesures estàndard establertes per SIA per a les còpies de seguretat de la resta de sistemes d'informació. Aquesta còpia de seguretat s'executa automàticament al Centre de Respatller.

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 sistemes d'informació emprats per SIA garanteixen el registre del temps en què es realitzen. L'instant de temps dels sistemes prové d'una font segura que constata la data i l'hora. Tots els servidors que conformen la Infraestructura de Certificació Electrònica estan sincronitzats en data i hora. Les fonts de temps utilitzades, basades en el protocol NTP (Network Time Protocol), se sincronitzen utilitzant com a referència la del Reial Institut i Observatori de l'Armada.

La sincronització dels servidors es duu a terme, almenys, una vegada cada 24 hores.

5.5.6 Sistema de recollida d'informació d'auditoria

El sistema de recollida d'informació és intern a l'Autoritat i correspon a SIA.

5.5.7 Procediments per obtenir i verificar informació arxivada

Els esdeveniments registrats per SIA estan protegits mitjançant tècniques criptogràfiques, de manera que ningú tret de les pròpies aplicacions de visualització i gestió d'esdeveniments hi pugui accedir. Només el personal autoritzat té accés als fitxers físics de suports i fitxers informàtics, per dur a terme verificacions d'integritat o altres.

Aquesta verificació l'ha de dur a terme l'administrador d'auditoria que ha de tenir accés a les eines de verificació i control d'integritat del registre d'esdeveniments de la PKI.

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

Els procediments per proporcionar, en cas de canvi de claus, una nova clau pública d'CA als titulars i tercers acceptants dels certificats són els mateixos que per proporcionar la clau pública en vigor. En conseqüència, la nova clau es publicarà al repositori de SIA (vegeu apartat 2.1 Repositoris).

5.7 Recuperació en cas de compromís de la clau o desastre

5.7.1 Procediments de gestió d'incidències i compromisos

SIA té establert un Pla de Contingències que defineix les accions a realitzar, recursos a utilitzar i personal a emprar en el cas de produir-se un esdeveniment intencionat o accidental que inutilitzi o degradació dels recursos i els serveis de confiança prestats.

El Pla de Contingències contempla, entre altres aspectes, els següents:

- La redundància dels components més crítics.
- La resposta en marxa d'un centre de respatller alternatiu.
- La revisió completa i periòdic dels serveis de còpia de seguretat.

En cas que es veiés afectada la seguretat de les dades de creació de signatura d'alguna Autoritat de Certificació, SIA informará tots els titulars de certificats, organisme supervisor i tercers acceptants coneguts que tots els certificats i llistes de revocació signats amb aquestes dades ja no són vàlids. Tan aviat com sigui possible es procedirà al restabliment del servei.

5.7.2 Corrupció de recursos, aplicacions o dades

Quan tingui lloc un esdeveniment d'anomalies de recursos de maquinari, programari i/o dades, SIA procedirà a aturar els serveis de la CA fins que es pugui verificar la seguretat de l'entorn, si és necessari substituint els components afectats per altres la integritat dels quals sigui degudament verificada. Alhora, es realitzarà una auditoria per identificar la causa de l'alteració i assegurar-ne la no reproducció.

En el cas de veure's afectats els certificats emesos, es notificarà del fet als usuaris dels mateixos i es procedirà a una nova certificació.

5.7.3 Compromís de clau privada de l'entitat

SIA considera el compromís o la sospita de compromís de la clau privada de la CA com un desastre. En cas de veure's compromesa la seguretat de la clau privada de la CA, SIA procedirà a realitzar les accions següents:

- Revocar el certificat de la CA actual, de manera que els certificats emesos per aquesta CA deixin de tenir

validesa.

- Informar tots els titulars i subscriptors de certificats que tots els certificats emesos per aquesta CA ja no són vàlids. Així mateix, notificarà a l'organisme supervisor aquest fet.
- Revocar el certificat de la CA subordinada i de tots els certificats vigents i expedits per aquesta CA. Si el certificat revocat és la CA arrel, eliminareu el certificat del dipòsit i avisareu d'aquest fet a la pàgina web del prestador de serveis de confiança.
- Publicar l'ARL corresponent.
- Generar una nova CA amb una clau de signatura i certificats nous.
- Restablir, tan aviat com sigui possible, el servei.
- Donar coneixement als cossos i forces de seguretat de l'estat i/o la Fiscalia General de l'Estat i/o Autoritat Judicial per si hi pogués haver activitats constitutives de delictes.

5.7.4 Continuïtat del negoci després d'un desastre

SIA restablirà els serveis crítics (revocació i publicació de certificats revocats) d'acord amb aquesta DPC dins de les 24 hores posteriors a un desastre o emergència imprevista prenent com a base el pla de contingència i continuïtat de negoci existent.

SIA disposa d'un centre alternatiu, si cal, per a la posada en funcionament dels sistemes de certificació.

5.8 Cessament de la CA o RA

5.8.1 Autoritat de Certificació

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 CA 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 la CA 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 la CA 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

5.8.2 Autoritat de Registre

Quan l'RA cessi en l'exercici de les funcions, transferirà els registres que mantingui a l'OSCEPA, mentre hi hagi l'obligació de mantenir arxivada la informació, i si no és així, aquesta serà destruïda de manera segura i acreditant-ho de manera fefaent.

6 CONTROLS DE SEGURETAT TÈCNICA

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

6.1.1 Generació del parell de claus

El parell de claus de la CA arrel com de la CA subordinada de l'OSCEPA son generades i emmagatzemades en un mòdul de maquinari criptogràfic segur (HSM) per SIA, que compleix els requisits de seguretat necessaris.

Les claus i els certificats d'entitats s'emeten segons el que disposa la Política de Certificació corresponent al tipus de certificat..

6.1.2 Lliurament de la clau privada al signant

L'enviament de la clau privada al titular es farà d'acord amb allò que disposa la Política de Certificació de cada tipus de certificat.

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

L'enviament de la clau privada al titular es farà d'acord amb allò que disposa la Política de Certificació de cada tipus de certificat.

6.1.4 Lliurament de la clau pública de la CA als usuaris

Tant el certificat de la CA arrel com el de la CA subordinada, es publiquen als repositoris indicats a l'apartat 2.1 Repositoris d'aquesta mateixa DPC.

6.1.5 Mida de les claus

Les claus de la CA arrel de l'OSCEPA són de 4096 bits.

Les claus de la CA subordinada de l'OSCEPA són 4096 bits.

La longitud de les claus dels titulars de certificats s'especifica a la corresponent Política de Certificació..

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

La clau pública de la CA arrel i de la CA subordinada es codifica d'acord amb RFC 5280 i PKCS#1. L'algorisme de generació de claus és RSA.

Els paràmetres de generació de claus per a cada tipus de certificat emès, s'especifica a la corresponent política de Certificació.

Els procediments i mitjans de comprovació de la qualitat dels paràmetres per cada tipus de certificat emès, s'especifica a la corresponent Política de Certificació.

6.1.7 Propòsits d'ús de claus (camp KeyUsage de X.509 v3)

Els usos admesos de la clau estan definits d'acord amb el que disposa la Política de Certificació de cada tipus de certificat.

Tots els certificats emesos per l'OSCEPA contenen l'extensió "Key Usage" definida per l'estàndard X.509 v3, que es qualifica com a crítica. Així mateix, es poden establir limitacions addicionals mitjançant l'extensió "Extended Key Usage".

Cal tenir en compte que l'eficàcia de les limitacions basades en les extensions dels certificats depèn de vegades de l'operativitat d'aplicacions informàtiques que no han estat creades ni controlades per l'OSCEPA.

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

6.2.1 Controls i estàndards de mòduls criptogràfics

Els mòduls utilitzats per a la creació de claus de la CA arrel i la CA subordinada per SIA compleixen els requisits de seguretat necessaris i en garanteixen la protecció.

La posada en marxa de cadascuna de les CA, tenint en compte que s'utilitzen mòduls criptogràfics de seguretat (HSM), comporta les tasques següents:

- Inicialització de l'HSM.
- Creació dels mitjans d'accés per als rols d'administració i operador.

- Generació de les claus de la CA.

Les mesures exercides per a la custòdia de les claus dels signants venen detallades a la seva corresponent Política de Certificació.

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

L'accés a la clau privada, tant de la CA Arrel com d'CA Subordinada, requereix de la presència d'un mínim de tres persones amb els rols específics per poder accedir-hi, sent aquests rols tant de controls físics com controls lògics.

6.2.3 Dipòsit de clau privada

Les claus privades tant de la CA arrel com de la CA subordinada, es troben emmagatzemades i protegides a l'HS M i mai no surt del mateix.

6.2.4 Còpia de seguretat de la clau privada

SIA fa còpies de seguretat de la clau privada de la CA durant el procés de generació de les mateixes.

Aquestes còpies es fan a efectes de continuïtat de negoci per a la recuperació davant de desastres. Les còpies de seguretat tenen el mateix nivell de seguretat que la clau original, atès que forma part del mateix mòdul de seguretat criptogràfic.

Les còpies de la clau es guarden en una localització diferent d'aquella on està ubicada la CA.

6.2.5 Arxiu de la clau privada

Les condicions particulars de custòdia de les claus privades emeses als usuaris s'especifiquen a la corresponent Política de Certificació. En cas contrari, les claus privades dels certificats qualificats dels signants mai no seran arxivades per l'AC.

6.2.6 Transferència de la clau privada a o des del mòdul criptogràfic

La transferència de la clau privada només es pot fer entre mòduls criptogràfics (HSM) i requereix la intervenció de tres persones amb rols diferents.

6.2.7 Emmagatzematge de clau privada en el mòdul criptogràfic

Les claus privades es generen al mòdul criptogràfic en el moment d'activació de cadascuna de les CA que fan ús dels mòduls.

6.2.8 Mètode d'activació de la clau privada

Tal com s'estipula a l'apartat 6.2.2 Control multipersonal de la clau privada, la clau privada tant de la CA arrel com de la CA subordinada, s'activa mitjançant la inicialització del programari d'CA per mitjà de la personació mínima de tres persones amb rols específics. Aquest és l'únic mètode d'activació d'aquesta clau privada..

6.2.9 Mètode de desactivació de la clau privada

Un administrador pot desactivar la clau de les Autoritats de Certificació mitjançant la detenció del programari de la CA. Per a la seva reactivació cal la intervenció mínima dels rols descrits en apartats anteriors.

6.2.10 Mètode de destrucció de la clau privada

Quan sigui necessari, SIA destruirà la clau privada de la CA i la seva còpia de seguretat per garantir que no es manté informació residual que es pugui utilitzar per reconstruir la clau privada.

En termes generals, la destrucció sempre ha de ser precedida per una revocació del certificat associat a la clau, si aquest encara és vigent.

6.2.11 Qualificació del mòdul criptogràfic

Els dispositius criptogràfics utilitzats per les autoritats de certificació compleixen els requisits de seguretat necessaris per garantir la protecció de les claus de les autoritats de certificació.

Aquests dispositius són resistent a manipulacions intrusives a nivell maquinari (tamper protection).

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

6.3.1 Arxiu de la clau pública

SIA, en compliment del que estableix l'article 26 de la Llei 35/2014, del 27 de novembre, de serveis de confiança electrònica, conservarà totes les claus públiques de l'OSCEPA durant el període exigít per la legislació vigent i d'acord amb allò establert en aquest document.

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

El certificat i el parell de claus de la CA arrel de l'OSCEPA generada per SIA tenen una validesa de quinze (15) anys i els de la CA subordinada de l'OSCEPA generada per SIA de quinze (15) anys.

La caducitat produirà automàticament la invalidació dels certificats, originant el cessament permanent de la seva operativitat conforme als usos que li són propis i, en conseqüència, de la prestació dels serveis de confiança. Si no es produeix un cessament de l'activitat del TSP, prèvia a la caducitat del certificat de la CA, es generarà una nova CA (nou parell de claus) en les mateixes condicions de seguretat que la que està apunt d'expirar, i es notificarà a totes les parts l'existència de la nova CA. El certificat de la nova CA es publicarà i distribuirà tal com s'especifica per a l'actual a aquesta DPC.

Tot aquest procés de generació de la nova CA es farà amb suficient antelació i previsió per tal de minimitzar l'impacte en tercers.

El període de validesa de la resta de certificats estarà establert per la Política de Certificació aplicable a cadascun.

6.4 Dades d'activació

6.4.1 Generació i activació de les dades d'activació

Per activar les claus privades de la CA, per part de SIA, cal la intervenció mínima de l'administrador de sistemes, els operadors de la CA i els administradors de l'HSM. Aquest és l'únic mètode d'activació d'aquesta clau privada.

En el cas de les claus dels certificats d'entitat final, la generació de dades d'activació s'indica a la política de certificació corresponent.

6.4.2 Protecció de les dades d'activació

Només el personal autoritzat té coneixement de les dades d'activació de les claus privades de la CA arrel i CA subordinada.

Per als certificats d'entitat final es detallarà a la seva corresponent política de certificació.

6.4.3 Altres aspectes de les dades d'activació

No estipulats.

6.5 Controls de seguretat informàtica

Les dades concernents a aquest apartat es consideren informació confidencial i només es proporcionen a qui acrediti la necessitat de conèixer-les, com en el cas d'auditories tant externes com internes i inspeccions. 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.

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

Les dades concernents a aquest apartat es consideren informació confidencial i només es proporcionaran a qui acrediti la necessitat de conèixer-les.

No obstant això, pel que fa a la gestió de la seguretat de la informació, SIA segueix l'esquema previst a la UNE-ISO 27002 (anteriorment anomenada ISO 17799), Codi de Bones Pràctiques per a la Seguretat de la Informació

6.5.2 Valoració de la seguretat informàtica

SIA avalua de forma contínua el seu nivell de seguretat amb vista a identificar possibles debilitats i establir les corresponents accions correctores mitjançant auditories externes i internes, així com la realització contínua de controls de seguretat.

Els productes utilitzats per a la prestació de serveis de certificació disposen de certificació Common Criteria i/o FIPS 140-2.

6.6 Controls de seguretat del cicle de vida

Les dades concernents a aquest apartat es consideren informació confidencial i només es proporcionen a qui acrediti la necessitat de conèixer-les, com en el cas d'auditories tant externes com internes i inspeccions..

6.6.1 Controls de desenvolupament de sistema

Els requisits de seguretat són exigibles, des del seu inici, tant en l'adquisició de sistemes informàtics com en el desenvolupament dels mateixos ja que podrien tenir algun impacte sobre la seguretat de SIA.

6.6.2 Controls de gestió de la seguretat

SIA compta amb una organització de seguretat encarregada de la seva gestió sobre la base de la norma UNE-ISO/IEC 27001:2007 sotmesa a auditories periòdiques per part de AENOR.

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:

CA 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'altres 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 la CA.

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'CA.

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 la CA emmagatzemada en el maquinari criptogràfic s'eliminarà un cop s'ha retirat el dispositiu.

La configuració de sistema de la CA, 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

SIA té definits controls de seguretat al llarg de tot el cicle de vida dels sistemes amb possibles impactes a la seguretat de la mateixa.

6.6.4 Controls del cicle de vida dels dispositius segurs de creació de Firma

SIA realitzarà les revisions oportunes per verificar l'estat de validesa de la certificació dels dispositius segurs de creació de signatura.

La font de consulta és la següent: https://esignature.ec.europa.eu/efda/notification-tool/#/screen/browse/list/QSCD_SSCD

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'hora del sistema està sincronitzada amb el Reial Observatori de l'Armada, seguint el protocol NTP a través d'Internet. La descripció del protocol NTP es pot trobar a RFC5905. Network Time Protocol Version 4: Protocol and Algorithms Specification.

La sincronització es farà, almenys, cada 24 hores..

7 PERFILS DE CERTIFICAT, CRL I OCSP

7.1 Perfil de certificat

Els certificats emesos pels sistemes de SIA, seran conformes amb el que disposen les normes següents i especificacions tècniques:

- ETSI EN 319 412-5: Profiles for Trust Service Providers issuing certificats; Part 5: Extension for Qualified Certificate profile.
- RFC 5280 "Internet X.509 Public Key Infrastructure. Certificate and CRL Profile".
- RFC 3739 "Internet x509 Public Key Infrastructure. Qualified Certificates Profile".
- Perfils de Certificats derivats de la Llei 6/2020, de 11 de novembre, reguladora de determinats aspectes dels serveis electrònics de confiança, la Llei 40/2015 d'1 d'Octubre, de Règim Jurídic del Sector Público (LRJ) i al Reglament (UE) 910/2014, relatiu a la identificació electrònica i els serveis de confiança per a les transaccions electròniques al mercat interior (eIDAS).
- ETSI EN 319 412-2 (Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificats issued to natural persons).
- ETSI EN 319 412-2 3 (Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons).
- ETSI EN 319 412-4: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificats.
- ETSI TS 119495: Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements un the payment services Directive (EU) 2015/2366.

7.1.1 Número de versió

L'Oscepa emet certificats X.509, versió 3

7.1.2 Extensions del certificat

Els certificats d'usuari emesos per SIA pel compte de l'OSCEPA vinculen la identitat d'una persona a una clau pública determinada. Per garantir l'autenticitat i el no repudi, tota aquesta informació estarà signada electrònicament per l'OSCEPA, entitat encarregada de l'emissió.

7.1.3 Identificadors d'objecte (OID) dels algorismes

Identificador de l'algoritme criptogràfic amb Objecte (OID): SHA-256 with RSA Encryption (1.2.840.113549.1.1.11).

7.1.4 Format de noms

Els certificats emesos per SIA pel compte de l'OSCEPA contenen el "distinguished name X.500" de l'emissor i del titular del certificat als camps "issuer" i "subject" respectivament..

7.1.5 Restriccions dels noms

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

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

L'OID de la present política és 2.16.20.2.1.13.1.1.

Tots els certificats adjudicatària tenen un identificador de política que comença des de la base 1.3.6.5.5.7.48. i Govern d'Andorra (OSCEPA) = 2.16.20.2.

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'CA subordinada emesos a tercers parts de manera que només es pugui emetre per la CA 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

7.2.1 Número de versió

L'Oscepa utilitza CRLs X.509 versió 2.

7.2.2 CRL i extensions

Las CRLs emeses per SIA pel compte de l'OSCEPA seran conformes amb la norma RFC 5280: Internet X.509 Public Key Infrastructure – Certificate and CRL Profile, April 2002.

7.3 Perfil d'OCSP

Els certificats emesos per CA SIA són conformes a la norma RFC 6960 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP".

La informació proporcionada a través del servei OCSP s'actualitza com a mínim cada quatre dies.

7.3.1 Número de versió

Els certificats de OCSP Responder utilitzaran l'estàndard X.509 Versió 3 (X.509 v3)

7.3.2 Extensions OCSP

Les principals extensions per OCSP son les que es veuen a la taula següent:

Camp	Obligatori	Crític
1. Issuer Alternative Name	No	No
2. Authority/Subject keyIdentifier	No	No
3. CRL Distribution Point	No	No
4. Key usage	Si	Si
5. Enhanced Key usage	Si	No
7. NoCheck	No	No

8 AUDITORIES DE CONFORMITAT

8.1 *Freqüència o circumstàncies de les auditories Veure auditories No UE*

Es faran auditories internes periòdiques, generalment amb caràcter anual. Així mateix, l'OSCEPA portarà a terme una auditoria externa cada any i realitzada per una entitat reconeguda i acreditada a fi de confirmar que els serveis d'expedició de certificats compleixen amb els requisits establerts legalment. Aquesta auditoria tindrà en compte l'auditoria realitzada a SIA el mateix any.

Amb caràcter extraordinari es podran dur a terme auditories específiques davant de possibles incidents de seguretat i/o per qualsevol altres motius aprovats pel Responsable de Seguretat.

Finalment, el prestador qualificat de serveis de confiança serà auditat, almenys cada 24 mesos per un organisme d'avaluació de la conformitat segons s'estableix a eIDAS, exactament amb l'Informe d'avaluació de la conformitat en el marc del reglament (UE) no 910/2014, relatiu a la identificació electrònica i els serveis de confiança en les transaccions electròniques al mercat interior (reglament eIDAS).

8.1.1 Auditoria en les autoritats de registre

Totes les RA 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 aquesta CPS per al desenvolupament de les tasques de registre exposades en el contracte de servei signat.

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

8.2 *Identificació i qualificació de l'auditor*

Les auditories poden ser de caràcter tant intern com a extern. En aquest segon cas, les realitzen empreses de reconegut prestigi en l'àmbit de les auditories. L'auditor tindrà qualificació i experiència acreditades per fer aquest tipus de tasques.

8.3 *Relació entre l'auditor i la CA*

Al marge de la funció d'auditoria, l'auditor extern i la part auditada (OSCEPA+SIA) no han de tenir cap relació que pugui derivar en un conflicte d'interessos. En el cas dels auditors interns, aquests no poden tenir relació funcional amb l'àrea objecte de l'auditoria. Els auditors són independents de l'activitat auditada i lliures de biaix i conflicte d'interessos. Els auditors mantindran una actitud objectiva a l'ordre del procés d'auditoria per assegurar-se que les troballes i conclusions de l'auditoria estaran basades només en l'evidència de l'auditoria.

L'equip auditor és plenament independent, havent-se verificat amb anterioritat a aquests efectes:

- La manca de vinculació laboral, mercantil a favor d'apoderaments amb l'organització auditada.
- Cap interès directe o indirecte amb l'entitat auditada.
- La inexistència de vincles de matrimoni, consanguinitat o afinitat fins al primer grau o consanguinitat col·lateral fins a segon grau, amb els empresaris, administradors o els responsables de l'àrea de sistemes d'informació i/o seguretat de la informació.
- Manca de familiaritat o confiança, per la influència i proximitat excessiva amb els administradors o directius de l'entitat auditada.
- La no execució prèvia de serveis relatius a la definició i implantació de mesures de seguretat a l'organització auditada per part de l'equip auditor.
- Els honoraris oferts no suposen un percentatge significatiu de la facturació de la companyia.

8.4 *Tòpics coberts per l'auditoria*

L'auditoria determinarà l'adequació dels serveis de l'OSCEPA+SIA amb aquesta DPC. També determinarà els riscos de l'incompliment de l'adequació amb l'operativa definida per aquests documents.

En general, els criteris establerts a la secció 3.3 ("Introduction to conformity assessment of Certification Authorities") i 3.5 ("Guidance on the conformity assessment process") de la CWA 14172-2. I en particular per a TSPs qualificats en concordança amb el Reglament eIDAS i segons les normes tècniques ETSI TS 319 401, ETSI TS 319 411-1 i ETSI TS 319 411-2 i ETSI TS 119 495 addicionalment per als certificats PSD2.

8.5 *Accions preses com a resultat de les deficiències*

La identificació de deficiències detectades com a resultat de l'auditoria donarà lloc a adoptar mesures correctives. El responsable de l'aprovació de les polítiques, en col·laboració amb l'auditor, serà l'encarregat de prendre'n la determinació amb la màxima diligència possible.

8.6 *Comunicació de resultats*

L'equip auditor comunicarà els resultats de l'auditoria al responsable de l'aprovació de polítiques de la CA de l'OSCEPA, al gestor de seguretat del sistema, així com als administradors de la CA i els administradors on es detectin les incidències..

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 certificats revocats de manera gratuïta, per mitjà d'un servei en línia OCSP i de la publicació de les corresponents CRLs.

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/ierarquia-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.

9.3 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 no confidencial

L'Oscepa considera com a informació no confidencial:

- Els certificats.
- Els usos i límits econòmics ressenyats al certificat.
- El període de validesa del certificat, així com la data d'emissió del certificat i la data de caducitat.
- El número de sèrie del certificat.
- Els diferents estats o situacions del certificat i la data de l'inici de cadascun, en concret:
 - pendent de generació i/o entrega, vàlid, revocat o caducat i el motiu que va provocar el canvi d'estat.
- Les llistes de revocació de certificats, així com la resta d'informacions d'estat de revocació.

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 http://crl2.govern.ad/GovernAndorra_SUB01.crl

L'Oscepa disposa d'un servei de consulta en línia d'estat dels certificats basat en l'estàndard OCSP, a l'adreça <http://va.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 Protecció de dades personals

9.4.1 Política de protecció de dades personals

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 Política de privacitat.

L'OSCEPA disposa d'una política de privacitat que pot ser consultada a:

<https://www.signaturaelectronica.ad/oscepa-privacitat.html>

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 CA

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 exigint 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'RA.
- 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'RA

Les RA són les entitats delegades per la CA per dur a terme les tasques de registre i aprovació de les sol·licituds de certificats; per tant, l'RA 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 RA

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

- Obligacions prèvies a l'expedició d'un certificat:
 - Informar adequadament els sol·licitants de la signatura de les seves obligacions i responsabilitats.
 - Identificar adequadament els sol·licitants, que han de ser persones capacitades o autoritzades per sol·licitar un certificat digital.
 - 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.
 - Accedir a l'aplicació de l'autoritat de registre per gestionar les sol·licituds i els certificats emesos.
- Obligacions un cop expedit el certificat:
 - 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.
 - El manteniment dels certificats durant la seva vigència (extinció, suspensió, revocació).
 - 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 RA 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 RA i que hauran de servir-los de manual de referència.

En cas de reclamació per un subjecte, una entitat o un usuari, la CA 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, la CA podrà, en virtut dels acords signats amb les RA, fer suportar a l'RA responsable l'assumpció de les conseqüències. Perquè, encara que legalment sigui la CA 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'RA 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 RA pel que fa als possibles danys l'origen dels quals vindria d'un incompliment de les tasques delegades a les RA. Per aquesta raó, igual que el que està previst per a la CA, l'RA 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'RA 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'RA.

Les mateixes responsabilitats les hauran d'assumir les RA 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'RA.
- 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'RA 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 algorisme 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 algorismes 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'RA 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'RA 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'RA 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 RA 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 la CA.
- 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

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. Termini i finalització

9.10 Termini i finalització

Vegeu l'apartat 5.8.

9.10.1 Termini

Vegeu l'apartat 5.8.

9.10.2 Finalització

Vegeu apartat 5.8

9.10.3 Efecte de la finalització 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, 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 la 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'assumepte 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.

10 ANNEX I. Història del document

Període	Versió	Modificació
Octubre del 2013	V1.0	Versió inicial
Novembre 2017	V1.0	Revisió
Octubre 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
Juliol 2021	V2.3.2	Identificació de la identitat d'un individu: nova redacció per a incorporar tots els mètodes d'identificació previst pel Reglament eIDAS i les normes nacionals
Agost 2021	V2.3.3	Certificats a menors de 16 anys i entre 16 i 18 anys
Febrer 2022	V3.0	Adaptació a auditories eIDAS