

TEXT DIVULGATIU – PDS
AUTORITAT DE CERTIFICACIÓ DE LES
ADMINISTRACIONS PÚBLIQUES
ANDORRANES (AC-APA)



Govern d'Andorra



INFORMACIÓ GENERAL

Control de versions				
Versió	Parts que canvien	Descripció del canvi	Autor del canvi	Data del canvi
1.0	Original	Creació del document	OSCEPA	15-09-2022
1.1		Revisió anual S'incorpora certificat amb pseudònim	OSCEPA	18-09-2023



Índex

1. Informació de contacte	5
1.1. Organització responsable	5
1.2. Organització que administra el document	5
1.3. Persona de contacte	5
1.4. Contacte per a processos de revocació	5
2. Tipus i finalitat del certificat	6
2.1. Certificats individuals	6
2.1.1. Certificats individuals de persona física (núvol)	6
2.1.2. Certificats individuals de persona física (programari).....	6
2.1.3. Certificats individuals de persona física menor, de 16 a 18 anys	6
2.1.4. Certificats individuals de persona física amb professió regulada	6
2.2. Certificats corporatius en l'àmbit de l'Administració Pública	6
2.2.1. Certificats corporatius de persona física al servei d'una Administració Pública	6
2.2.2. Certificats corporatius de segell d'òrgan, Administració Pública o entitat de dret públic.....	7
2.2.3. Certificats corporatius de persona física amb pseudònim al servei d'una Administració Pública	7
2.2.4. Certificats corporatius de segell d'òrgan, Administració Pública o entitat de dret públic (núvol)	7
2.2.5. Certificats corporatius de segell d'òrgan, Administració Pública o entitat de dret públic (programari).....	7
2.3. Certificats corporatius en l'àmbit de les organitzacions privades	7
2.3.1. Certificats corporatius de persona física al servei d'una organització privada	8
2.3.2. Certificats corporatius de segell d'empresa (núvol).....	8
2.4. Certificats corporatius de segell d'empresa (programari)	8
2.5. Certificats de representant de persona jurídica privada, pública o entitat sense personalitat jurídica.....	8
2.6. Tipus de certificats.....	9



2.7.	Autoritat de Certificació emissora	9
2.8.	Validació dels certificats	10
3.	Límits d'ús dels certificat	10
3.1.	Usos apropiats dels certificats	10
3.2.	Usos prohibits dels certificats.....	10
4.	Obligacions dels signataris i titulars dels certificats	10
4.1.	Generació de claus	10
4.2.	Sol·licitud de certificats	11
4.3.	Veracitat de la informació	11
4.4.	Obligacions de custòdia	11
5.	Obligacions dels signatari i dels creadors de segells	11
6.	Obligacions de les tercers parts	12
7.	Obligacions de l'EC-APA.....	13
7.1.	En relació amb la prestació del servei de certificació digital	13
7.2.	En relació amb les comprovacions del registre	13
8.	Garanties limitades.....	13
8.1.	Garantia de L'AC-APApels serveis de certificació digital	13
8.2.	Exoneració de responsabilitats.....	14
8.3.	Limitacions de responsabilitats	15
9.	Acords aplicables i DPC	15
9.1.	Acords aplicables	15
9.2.	Declaració de pràctiques de certificació	15
10.	Política de protecció de dades personals.....	16
11.	Política de privacitat	16
12.	Política de reintegraments	16
13.	Llei aplicable, jurisdicció competent i règim de reclamacions i disputes.	16
14.	Freqüència o circumstàncies de les auditories.....	16
15.	Auditoria en les autoritats de registre.....	16
16.	Tòpics coberts per la auditoria.....	17
17.	Divisibilitat de les clàusules, supervivència, acord íntegre i notificació.	17



1. Informació de contacte

1.1. Organització responsable

La redacció i el control d'aquesta PDS correspon a l'AC-APA, gestionada per la direcció de l'Oscepa:

ENTITAT DE CERTIFICACIÓ DE LES ADMINISTRACIONS PÚBLIQUES ANDORRANES
(OFICINA DE SERVEIS DE CONFIANÇA ELECTRÒNICA DEL PRINCIPAT D'ANDORRA - OSCEPA)

CARRER DE LA GRAU, EDIFICI PRAT DEL RULL, ANDORRA LA VELLA

TELÈFON: +376 875 700

1.2. Organització que administra el document

ENTITAT DE CERTIFICACIÓ DE LES ADMINISTRACIONS PÚBLIQUES ANDORRANES
(OFICINA DE SERVEIS DE CONFIANÇA ELECTRÒNICA DEL PRINCIPAT D'ANDORRA - OSCEPA)

CARRER DE LA GRAU, EDIFICI PRAT DEL RULL, ANDORRA LA VELLA

TELÈFON: +376 875 700

1.3. Persona de contacte

Responsable de l'Oficina de Serveis de Confiança Electrònica del Principat d'Andorra (OSCEPA)

C/PRAT DE LA CREU, 62, AD500 ANDORRA LA VELLA

TELÈFON: +376 875 700

1.4. Contacte per a processos de revocació

Pels processos de revocació, dirigeixin-se a:

ENTITAT DE CERTIFICACIÓ DE LES ADMINISTRACIONS PÚBLIQUES ANDORRANES
(OFICINA DE SERVEIS DE CONFIANÇA ELECTRÒNICA DEL PRINCIPAT D'ANDORRA – OSCEPA)

CARRER DE LA GRAU, EDIFICI PRAT DEL RULL, ANDORRA LA VELLA

TELÈFON: +376 875 700

MÒBIL: +376 601 098



2. Tipus i finalitat del certificat

2.1. Certificats individuals

2.1.1. Certificats individuals de persona física (núvol)

Aquests certificats són emesos a tota persona física, andorrana o resident al Principat d'Andorra, per actuar a títol individual, que vulgui dur a terme tràmits electrònics segurs amb les administracions i els privats.

Seguint el document *política i requeriments de seguretat per a prestadors de serveis de confiança*, aquest certificat disposa de la política "AD-pcq-Fd". Així els certificats emesos sota aquests requisits inclouen la signatura electrònica qualificada tal com es defineix en els articles 3.37 i 5.3 de la Llei 35/2014, del 27 de novembre, de serveis de confiança electrònica.

2.1.2. Certificats individuals de persona física (programari)

Aquests certificats són emesos a tota persona física, andorrana o resident al Principat d'Andorra, per actuar a títol individual, que vulgui dur a terme tràmits electrònics segurs amb les administracions i els privats.

Seguint el document *política i requeriments de seguretat per a prestadors de serveis de confiança*, aquest certificat disposa de la política "AD-pcq-F". Així els certificats emesos sota aquests requisits inclouen la signatura electrònica avançada tal com es defineix en els articles 3.36 i 6 de la Llei 35/2014, del 27 de novembre, de serveis de confiança electrònica.

2.1.3. Certificats individuals de persona física menor, de 16 a 18 anys

Aquests certificats són emesos a tota persona física menor, de 16 a 18 anys, andorrana o resident al Principat d'Andorra, per actuar a títol individual, per consultar l'aplicació Andorra Salut.

Seguint el document *política i requeriments de seguretat per a prestadors de serveis de confiança*, aquest certificat disposa de la política "AD-pcq-Fd". Així els certificats emesos sota aquests requisits inclouen la signatura electrònica qualificada tal com es defineix en els articles 3.37 i 5.3 de la Llei 35/2014, del 27 de novembre, de serveis de confiança electrònica.

2.1.4. Certificats individuals de persona física amb professió regulada

Aquets certificats són emesos a tota persona física amb professió regulada que incorpora les dades de la seva professió.

Seguint el document *política i requeriments de seguretat per a prestadors de serveis de confiança*, aquest certificat disposa de la política "AD-pcq-Fd". Així els certificats emesos sota aquests requisits inclouen la signatura electrònica qualificada tal com es defineix en els articles 3.37 i 5.3 de la Llei 35/2014, del 27 de novembre, de serveis de confiança electrònica.

2.2. Certificats corporatius en l'àmbit de l'Administració Pública

2.2.1. Certificats corporatius de persona física al servei d'una Administració Pública

Certificat emès a la persona física com a treballadora pública vinculada laboralment amb l'Administració per actuar dins de l'àmbit de l'organització.

Seguint el document *política i requeriments de seguretat per a prestadors de serveis de confiança*, aquest certificat disposa de la política "AD-pcq-Fd". Així els certificats emesos sota aquests requisits inclouen la



signatura electrònica qualificada tal com es defineix en els articles 3.37 i 5.3 de la Llei 35/2014, del 27 de novembre, de serveis de confiança electrònica.

2.2.2. Certificats corporatius de segell d'òrgan, Administració Pública o entitat de dret públic

Certificat emès a l'administració pública o entitat de dret públic per utilitzar-lo com a mecanisme d'identificació en sistemes per a l'actuació administrativa automatitzada a més de poder segellar electrònicament per dotar aquest fet de presumpció legal de garantia de l'origen i la integritat de les dades a les que està vinculat.

Seguint el document *política i requeriments de seguretat per a prestadors de serveis de confiança*, aquest certificat disposa de la política "AD-pcq-Jd". Així els certificats emesos sota aquests requisits inclouen el segell electrònic qualificat tal com es defineix en els articles 3.29 i 7.3 de la Llei 35/2014, del 27 de novembre, de serveis de confiança electrònica.

2.2.3. Certificats corporatius de persona física amb pseudònim al servei d'una Administració Pública

Certificat amb pseudònim emès a la persona física com a treballadora pública vinculada laboralment amb l'Administració per actuar dins de l'àmbit de l'organització

Aquest certificat s'emet d'acord amb les polítiques ETSI. Així els certificats emesos sota aquests requisits inclouen la signatura electrònica qualificada tal com es defineix en els articles 3.37 i 5.3 de la Llei 35/2014, del 27 de novembre, de serveis de confiança electrònica.

2.2.4. Certificats corporatius de segell d'òrgan, Administració Pública o entitat de dret públic (núvol)

Certificat emès a l'administració pública o entitat de dret públic per utilitzar-lo com a mecanisme d'identificació en sistemes per a l'actuació administrativa automatitzada a més de poder segellar electrònicament per dotar aquest fet de presumpció legal de garantia de l'origen i la integritat de les dades a les que està vinculat.

Seguint el document *política i requeriments de seguretat per a prestadors de serveis de confiança*, aquest certificat disposa de la política "AD-pcq-J". Així els certificats emesos sota aquests requisits inclouen el segell electrònic avançat tal com es defineix en els articles 3.28 i 8 de la Llei 35/2014, del 27 de novembre, de serveis de confiança electrònica.

2.2.5. Certificats corporatius de segell d'òrgan, Administració Pública o entitat de dret públic (programari)

Certificat emès a l'administració pública o entitat de dret públic per utilitzar-lo com a mecanisme d'identificació en sistemes per a l'actuació administrativa automatitzada a més de poder segellar electrònicament per dotar aquest fet de presumpció legal de garantia de l'origen i la integritat de les dades a les que està vinculat.

Seguint el document *política i requeriments de seguretat per a prestadors de serveis de confiança*, aquest certificat disposa de la política "AD-pcq-J". Així els certificats emesos sota aquests requisits inclouen el segell electrònic avançat tal com es defineix en els articles 3.28 i 8 de la Llei 35/2014, del 27 de novembre, de serveis de confiança electrònica.

2.3. Certificats corporatius en l'àmbit de les organitzacions privades



2.3.1. Certificats corporatius de persona física al servei d'una organització privada

Certificats per a persones físiques que els vinculen a una organització privada per actuar dins de l'àmbit corporatiu de l'organització i garanteix la identitat de la persona física titular del certificat, així com la seva vinculació a una determinada entitat en virtut del càrrec que hi ocupa.

Seguint el document *política i requeriments de seguretat per a prestadors de serveis de confiança*, aquest certificat disposa de la política "AD-pcq-Fd". Així els certificats emesos sota aquests requisits inclouen la signatura electrònica qualificada tal com es defineix en els articles 3.37 i 5.3 de la Llei 35/2014, del 27 de novembre, de serveis de confiança electrònica.

2.3.2. Certificats corporatius de segell d'empresa (núvol)

Certificat emès a empreses per segellar electrònicament i així dotar aquest fet de presumpció legal de garantia de l'origen i la integritat de les dades a les que està vinculat.

Pot ser emprat per una aplicació informàtica de forma desatesa i també per persones autoritzades.

És adequat per la facturació electrònica, el segellat de comprovants de recepció electrònics, segellat de butlletins d'informació o comunicacions d'empresa, segellat de diaris d'activitat (logs) i còpies de seguretat.

Seguint el document *política i requeriments de seguretat per a prestadors de serveis de confiança*, aquest certificat disposa de la política "AD-pcq-Jd". Així els certificats emesos sota aquests requisits inclouen el segell electrònic qualificat tal com es defineix en els articles 3.29 i 7.3 de la Llei 35/2014, del 27 de novembre, de serveis de confiança electrònica.

2.4. Certificats corporatius de segell d'empresa (programari)

Certificat emès a empreses per segellar electrònicament i així dotar aquest fet de presumpció legal de garantia de l'origen i la integritat de les dades a les que està vinculat.

Pot ser emprat per una aplicació informàtica de forma desatesa i també per persones autoritzades.

És adequat per la facturació electrònica, el segellat de comprovants de recepció electrònics, segellat de butlletins d'informació o comunicacions d'empresa, segellat de diaris d'activitat (logs) i còpies de seguretat.

Seguint el document *política i requeriments de seguretat per a prestadors de serveis de confiança*, aquest certificat disposa de la política "AD-pcq-J". Així els certificats emesos sota aquests requisits inclouen el segell electrònic avançat tal com es defineix en els articles 3.28 i 8 de la Llei 35/2014, del 27 de novembre, de serveis de confiança electrònica.

2.5. Certificats de representant de persona jurídica privada, pública o entitat sense personalitat jurídica

S'expedeixen a les persones físiques que representen persones jurídiques, i incorporen les dades de la representació i de la persona jurídica representada, com, per exemple, societats S.A. o S.L., associacions o unions d'associacions, centres docents d'ensenyament privat, clubs, comunitats de béns, fundacions, unions temporals d'empreses o col·legis professionals, entre d'altres.

Seguint el document *política i requeriments de seguretat per a prestadors de serveis de confiança*, aquest certificat disposa de la política "AD-pcq-Fd". Així els certificats emesos sota aquests requisits inclouen la signatura electrònica qualificada tal com es defineix en els articles 3.37 i 5.3 de la Llei 35/2014, del 27 de novembre, de serveis de confiança electrònica.

2.6. Tipus de certificats

TIPUS de certificats	Emès en suport	OID propi AC-APA	ALTRES OIDs
persona física individual			
Persona física (ciutadans o tenen NRT)	PROGRAMARI	2.16.20.2.1.3.1.1.2	2.16.20.2.2.194112.1.0
Persona física (ciutadans o tenen NRT)	NUVOL	2.16.20.2.1.3.1.1.3	2.16.20.2.2.194112.1.2
Persona física menor (16 a 18)	NUVOL	2.16.20.2.1.3.1.1.4	2.16.20.2.2.194112.1.2
PF de professió regulada	NUVOL	2.16.20.2.1.3.1.12.3	2.16.20.2.2.194112.1.2
persona física vinculada / al servei d'una empresa			
Persona física vinculada	NUVOL	2.16.20.2.1.3.1.4.3	2.16.20.2.2.194112.1.2
persona física empleat públic / al servei d'una Administració			
Empleat públic / persona al servei d'una AAPP	NUVOL	2.16.20.2.1.3.1.5.3	2.16.20.2.2.194112.1.2
Empleat públic / persona al servei d'una AAPP amb pseudònim	NUVOL	2.16.20.2.1.3.1.16.3	0.4.0.194112.1.2
persona física representant			
Persona física representant d'una persona jurídica (privada o pública o ESPJ)	NUVOL	2.16.20.2.1.3.1.14.2	2.16.20.2.2.194112.1.2
Segell electrònic de persona jurídica			
Segell d'empresa	PROGRAMARI	2.16.20.2.1.3.1.2.2	2.16.20.2.2.194112.1.1
Segell d'empresa	NUVOL	2.16.20.2.1.3.1.2.3	2.16.20.2.2.194112.1.3
Segell electrònic d'òrgan d'AAPP			
Segell d'òrgan	PROGRAMARI	2.16.20.2.1.3.1.8.2	2.16.20.2.2.194112.1.1
Segell d'òrgan	NUVOL	2.16.20.2.1.3.1.8.3	2.16.20.2.2.194112.1.3

2.7. Autoritat de Certificació emissora

Aquests certificats són emesos per l'AUTORITAT DE CERTIFICACIÓ DE LES ADMINISTRACIONS PÚBLIQUES ANDORRANES (AC-APA), identificada per les dades indicades anteriorment.



L'AC-APA subcontracta els serveis de producció de certificats a SIA, que sempre actua seguint les indicacions de l'AC-APA.

2.8. Validació dels certificats

Les llistes de certificats revocats (CRL) es poden consultar al lloc d'Internet http://crl2.govern.ad/GovernAndorra_SUB01.crl

L'AC-APA 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.

3. Límits d'ús dels certificat

3.1. Usos apropiats dels certificats

Un certificat emès per l'AC-APA només pot ser utilitzat per als propòsits explícitament permesos i indicats en la DPC per la qual cosa hi ha certes limitacions en l'ús dels certificats.

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.

3.2. 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.

Els certificats han d'emprar-se únicament d'acord amb la llei aplicable.

No es poden usar per a signar peticions d'emissió, renovació o revocació de certificats, ni per a signar certificats de clau pública, ni signar llistes de revocació.

L'ús d'aquests certificats en operacions que contravenen aquesta PDS o els contractes amb els signataris i titulars, tenen la consideració d'ús indegut als efectes legals oportuns, eximint-se per tant a l'AC-APA, en funció de la legislació vigent, de qualsevol responsabilitat per aquest ús indegut dels certificats.

L'AC-APA no té accés a les dades sobre les que es pot aplicar l'ús d'un certificat. Per tant, al no poder tècnicament accedir al contingut del missatge, no és possible per part de l'AC-APAemetre valoració sobre el seu contingut.

4. Obligacions dels signataris i titulars dels certificats

4.1. Generació de claus

En els certificats al núvol, s'autoritza al signatari o titular dels certificats a generar les seves pròpies claus privada i pública, i sol·licita l'emissió del certificat a l'AC-APA.

En els certificats de segell, el titular autoritza a l'AC-APA a generar les claus, per al seu ús pels creadors de segells i sol·licita en el seu nom l'emissió del certificat.



4.2. Sol·licitud de certificats

El titular o signatari del certificat s'obliga a realitzar les sol·licitud d'acord amb el procediment i els components tècnics subministrats, quan així sigui, per l'AC-APA, de conformitat amb el que estableix la DPC i els procediments de l'AC-APA.

4.3. Veracitat de la informació

El titular o signatari es responsabilitza que tota la informació inclosa en la sol·licitud del certificat sigui exacta, completa per a la finalitat del certificat i estigui actualitzada.

El titular o signatari ha d'informar immediatament a l'AC-APA de qualsevol inexactitud detectada al certificat un cop s'hagi emès, així com dels canvis en la informació aportada per a l'emissió.

4.4. Obligacions de custòdia

El responsable de l'Autoritat de Registre s'obliga a custodiar tota la informació que generi la seva activitat.

5. Obligacions dels signatari i dels creadors de segells

El signatari o creador de segells estarà obligat a complir el que disposa la normativa vigent i a més a:

- Utilitzar el certificat segons el que estableixen tant la DPC com les polítiques de certificació aplicables.
- Respectar el que disposen els documents signats amb l'AC-APA 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'AC-APA 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 esmentats certificats digitals.
- Autoritzar l'AC-APA 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 qualsevol 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 signatari o creador de segells genera les seves pròpies claus, s'obliga a:

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

El sol·licitant 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.

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.

6. Obligacions de les tercers parts

Serà obligació de la tercera part 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'AC-APAdisposa 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'AC-APA. 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 tercers 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'AC-APAc comprovant que l'autoritat de certificació que ha emès el certificat es troba publicada a la llista de confiança del supervisor nacional corresponent.

Serà obligació de la tercera part 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'AC-APAdisposa 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'AC-APA. 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'AC-APA comprovant que l'autoritat de certificació que ha emès el certificat es troba publicada a la llista de confiança del supervisor nacional corresponent.

L'AC-APA disposa d'un servei de consulta de CRL i certificats en el lloc d'Internet: http://crl2.govern.ad/GovernAndorra_SUB01.crl

L'AC-APA 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.

7. Obligacions de l'AC-APA

7.1. En relació amb la prestació del servei de certificació digital

- Emetre, entregar, administrar, revocar i renovar certificats d'acord amb les instruccions del titular del certificat, d'acord amb els motius descrits a la DPC.
- Executar els serveis amb els mitjans tècnics i materials adequats, i amb personal que disposi de les corresponents condicions de qualificació i experiència indicades a la DPC.
- Complir els nivells de qualitat del servei indicats a la DPC.
- Notificar al titular del certificat (signatari o creador de segells) amb anterioritat suficient a la data d'expiració del certificat, de la possibilitat de renovar-los o de revocar-los.
- Comunicar a les terceres parts l'estat dels certificats.

7.2. En relació amb les comprovacions del registre

L'AC-APA s'obliga a l'emissió de certificats en base a les dades subministrades pel subscriptor, per tant podrà realitzar les comprovacions que consideri oportunes.

Si l'AC-APA detecta errors en les dades que s'han d'incloure als certificats o que els justifiquen, podrà realitzar els canvis que consideri necessaris abans d'emetre el certificat o suspendre el procés d'emissió i gestionar la incidència.

L'AC-APA es reserva el dret a no emetre el certificat, quan consideri que la justificació documental resulti insuficient per a la correcta identificació del titular del certificat.

8. Garanties limitades

8.1. Garantia de l'AC-APA pels serveis de certificació digital

L'AC-APA s'obliga segons el que disposa la DPC, així com el que disposa la normativa vigent sobre prestació de serveis de certificació, a:

- Respectar el que disposa l'abast de la seva DPC.
- Protegir les seves claus privades de forma segura.



- Emetre certificats d'acord amb la seva DPC, 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.
- Suspènre i revocar els certificats segons el que disposa la DPC 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 la DPC al seu lloc web.
- Informar sobre les modificacions de la DPC als 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 exigít per la normativa vigent.

L'AC-APA 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'AC-APA 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 suspènre'ls i revocar-los. En concret, l'AC-APAFonamentalment 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 de la 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.

L'AC-APA, 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.

8.2. Exoneració de responsabilitats

Segons la legislació vigent, la responsabilitat de l'AC-APAI 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'AC-APAI 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.

8.3. Limitacions de responsabilitats

El límit màxim que l'AC-APAPERMET a les transaccions econòmiques efectuades és de 0 (zero) euros.

9. Acords aplicables i DPC

9.1. Acords aplicables

Els acords aplicables a aquests certificats són els següents:

- Els convenis o contractes de serveis de certificació.
- Aquesta PDS.
- La DPC, que regula l'emissió i utilització dels certificats.

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

9.2. Declaració de pràctiques de certificació



Els serveis de certificació de L'AC-APase regulen tècnicament i operativa per la DPC de L'AC-APAi de la subcontractada SIA, com a prestador tècnic, per les seves actualitzacions posteriors, així com per documentació complementària.

Una còpia de la DPC estarà disponible en format electrònic a l'adreça d'Internet:

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

10. Política de protecció de dades personals

L'AC-APacompleix en tot cas la normativa vigent en cada moment en matèria de protecció de dades, en particular ha adaptat els seus procediments a la Llei 29/2021, del 28 d'octubre, qualificada de protecció de dades personals.

Es 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

11. Política de privacitat

L'AC-APAdisposa d'una política de privacitat que pot ser consultada a:

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

12. Política de reintegraments

L'AC-APAno té una política de reintegraments específica, i s'acull a la normativa general vigent del Govern d'Andorra.

13. Llei aplicable, jurisdicció competent i règim de reclamacions i disputes.

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

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

14. Frequència o circumstàncies de les auditories

L'AC-APAportarà 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.

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

15. 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 DPC 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.



16. Tòpics coberts per la auditoria

L'auditoria determinarà l'adequació dels serveis de l'AC-APA 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 la Llei 35/2014, del 27 de novembre, de serveis de confiança electrònica i segons les normes tècniques ETSI TS 319 401 i ETSI TS 319 411-1.

17. Divisibilitat de les clàusules, supervivència, acord íntegre i notificació.

Les clàusules de la present PDS són independents entre sí, pel que, si qualsevol clàusula es considerés invàlida o inaplicable, la resta de les clàusules continuaran essent aplicables, excepte en acord exprés al contrari, de les parts.