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

Govern d'Andorra

Versió 4.5

Idioma: Català

1. INTRODUCCIÓ

El 29 de juliol del 2021 l'Autoritat de Certificació de les Administracions Públiques andorranes (AC-APA) inicià una nova etapa canviant el proveïdor tècnic, que ofereix des de la seva infraestructura els serveis de confiança que el Govern d'Andorra posa a disposició de la ciutadania del Principat.

El nou proveïdor tècnic que allotjarà els serveis de confiança del Govern d'Andorra és l'empresa espanyola "Sistemas Informáticos Abiertos SA (SIA)".

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. Aquest document identifica les pràctiques i els procediments que empra l'Autoritat de Certificació de les Administracions Públiques andorranes (AC-APA) des d'ara, en l'emissió de certificats digitals.

Aquesta Declaració de Practiques de Certificació s'estructura en conformitat amb el document RFC-3647 "*Internet X.509 Public Key Infrastructure. Certificate Policy and Certificaction Practices Framework*", i també s'alinea amb la Llei 35/2014, de 27 de novembre, 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 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'Autoritat de Certificació de les Administracions Públiques andorranes (AC-APA).

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

L'AC-APA 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:

- 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.

TIPUS de certificats	**Emès en suport**	**OID propi AC-APA**	**ALTRES OIDs**
persona física individual			
Persona física (ciutadans o tenen NRT)	SOFT	**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 (ciutadans o tenen NRT)_Cartera Digital	SOFT	**2.16.20.2.1.3.1.1.2**	2.16.20.2.2.194112.1.0
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 /	NUVOL	**2.16.20.2.1.3.1.5.3**	2.16.20.2.2.194112.1.2

persona al servei d'una AAPP			
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**	2.16.20.2.194112.1.2
Segell electrònic de persona jurídica			
Segell d'empresa	SOFT	**2.16.20.2.1.3.1.2.2**	2.16.20.2.194112.1.1
Segell d'empresa	NUVOL	**2.16.20.2.1.3.1.2.3**	2.16.20.2.194112.1.3
Segell electrònic d'òrgan d'AAPP			
Segell d'òrgan	SOFT	**2.16.20.2.1.3.1.8.2**	2.16.20.2.194112.1.1
Segell d'òrgan	NUVOL	**2.16.20.2.1.3.1.8.3**	2.16.20.2.194112.1.3

1.3 Participants en la PKI

Les entitats i persones que intervenen son:

- Les Autoritats de Certificació;
- Les autoritats de registre;
- els signants/titulars;
- els subscriptors;
- les terceres parts que accepten els certificats emesos.

1.3.1 Autoritats de certificació

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

Una autoritat de certificació (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. En el cas de l'AC-APA l'entitat jurídica és el **Govern d'Andorra**.

L'AC-APA està gestionada per **l'Oficina de Serveis de Confiança Electrònica del Principat d'Andorra "OSCEPA**", com a oficina responsable per part del Govern d'Andorra.

L'AC-APA ofereix els seus serveis gràcies a l'allotjament que disposa en la infraestructura de l'empresa ***Sistemas Informáticos Abiertos* "SIA"**.

La informació relativa a l'AC-APA pot trobar- se en aquest document o a l'adreça web https://www.signaturaelectronica.ad/jerarquiapolitiques-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 l'AC-APA i superi

Els processos d'alta i les auditories que demostren 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

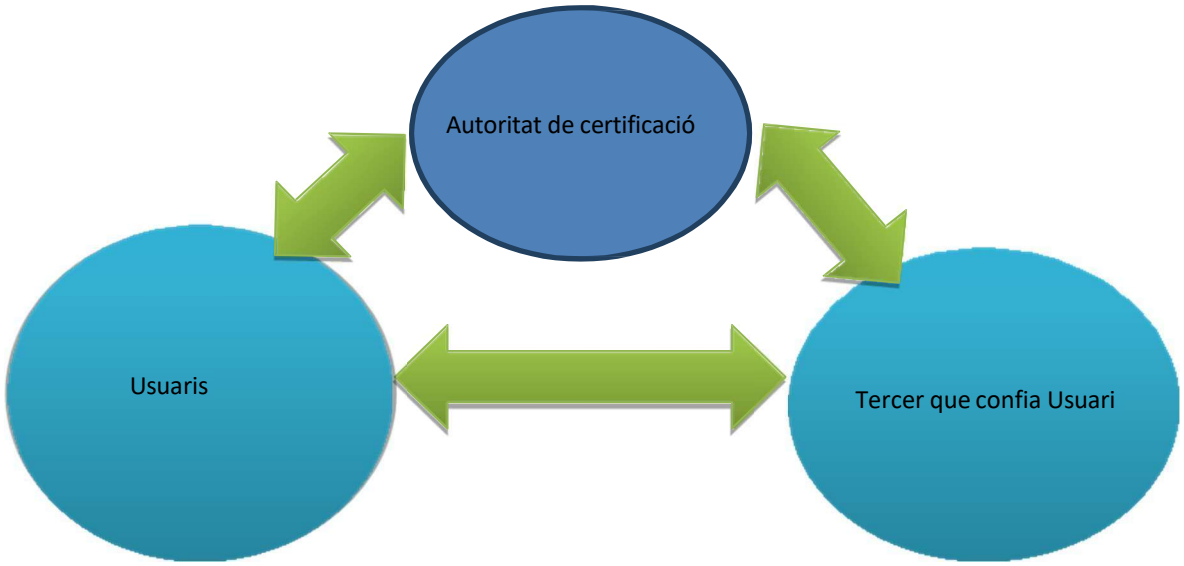
S'entén per signant la persona o titular del certificat que realitza o crea la signatura electrònica.

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'AC-APA 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 l'AC-APA, gestionada per l'Oscepa i que voluntàriament confia en el certificat emès.



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'AC-APA només pot ser utilitzat per als propòsits explícitament permesos i indicats en aquesta CPS i en la Política qualificada de Certificació a la que estiguin subjectes, 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.

A partir de l'any 2023 es comença a emetre el certificat de pseudònim on ja s'incorporen les polítiques ETSI. La resta de certificats encara s'emeten amb els perfils que inclouen les polítiques qualificades andorranes[1].

1.4.1.1 Certificat individual de persona física

Aquests certificats són emesos a tota persona física i identifiquen al subscriptor i signant com la mateixa persona per actuar a títol individual i que vulgui dur a terme tràmits electrònics segurs amb les administracions i els privats.

Aquest certificat disposa dels següents OID:

- En la jerarquia pròpia de l'AC-APA:
  - Emissió en software: 2.16.20.2.1.3.1.1.2
  - Emissió amb QSCD al Núvol: 2.16.20.2.1.3.1.1.3
- Altres OIDs que els qualifiquen:
  - Emissió en software:
    - 2.16.20.2.2.194112.1.0 (Polítiques qualificades andorranes)
  - Emissió amb QSCD al núvol
    - 2.16.20.2.2.194112.1.2 (Polítiques qualificades andorranes)

El certificat emès en software permet la "signatura electrònica avançada[2]" que és aquella que està vinculada al signatari de manera única, permet la identificació d'aquest signatari, ha estat creada utilitzant dades de creació de la signatura electrònica que el signatari pot utilitzar, amb un alt nivell de confiança electrònica, sota el seu control exclusiu, i que està vinculada amb les dades a què es refereix de manera que qualsevol modificació ulterior sigui detectable.

El certificat emès en QSCD permet la "signatura electrònica qualificada[3]" que és aquella que inclou a més a més d'allò indicat per a la signatura electrònica avançada, l'haver estat creada mitjançant un dispositiu de creació de signatures electròniques qualificat.

Els usos indicats en el seu perfil corresponen a la següent informació:

- El camp "key usage" té activades i per tant permet realitzar, les següents funcions:
  - Compromís amb el contingut, per a la realització de signatures electròniques

[1] https://www.signaturaelectronica.ad/images/stories/Docs/politiques-de-certificacio-v1-r0.pdf

[2] D'acord amb l'article 3, definició 36.

[3] D'acord amb l'article 3, definició 37, i l'article 5.3 de la Llei 35/2014.

        - Signatura digital, per a l'autenticació.
    - En el camp de "Qualified Certificate Statements" apareixen les següents declaracions:
        - Emissió com a certificat qualificat:
        - (OID= 2.16.20.2.2.1862.1.1)Usat amb un Dispositiu Segur de Creació de Signatura (només els emesos amb QSCD al núvol)
        - (OID= 2.16.20.2.2.1862.1.4)Que permet la creació de signatures electròniques
            - (OID= 2.16.20.2.2.1862.1.6.1)
    - En el camp de "Qualified Certificate Statements" apareixen les següents declaracions d'acord amb les normes ETSI:
        - Període de retenció EtsiQcsRetentionPeriod (0.4.0.1862.1.3)
        - Les adreces web de les PDS (QC PKI Disclosure Statements), opcionalment

1.4.1.2 Certificat individual de persona física menor, de 16 a 18 anys

Aquests certificats són emesos a tota persona física menor, de 16 a 18 anys i identifiquen al subscriptor i signant com la mateixa persona per actuar a títol individual .

Aquest certificat disposa dels següents OID:

- En la jerarquia pròpia de l'AC-APA:
    - Emissió amb QSCD al Núvol: 2.16.20.2.1.3.1.1.4
- Altres OIDs que els qualifiquen:
    - Emissió amb QSCD al núvol
        - 2.16.20.2.2.194112.1.2 (Polítiques qualificades andorranes)

El certificat emès en QSCD permet la "signatura electrònica qualificada[4]" que és aquella que inclou a més a més d'allò indicat per a la signatura electrònica avançada, l'haver estat creada mitjançant un dispositiu de creació de signatures electròniques qualificat.

Els usos indicats en el seu perfil corresponen a la següent informació:

- El camp "key usage" té activades i per tant permet realitzar, les següents funcions:
    - Compromís amb el contingut, per a la realització de signatures electròniques
    - Signatura digital, per a l'autenticació.
- En el camp de "Qualified Certificate Statements" apareixen les següents declaracions:
    - Emissió com a certificat qualificat:
        - (OID= 2.16.20.2.2.1862.1.1)
    - Usat amb un Dispositiu Segur de Creació de Signatura
        - (OID= 2.16.20.2.2.1862.1.4)
    - Que permet la creació de signatures electròniques
        - (OID= 2.16.20.2.2.1862.1.6.1)
- En el camp de "Qualified Certificate Statements" apareixen les següents declaracions d'acord amb

[4] D'acord amb l'article 3, definició 37, i l'article 5.3 de la Llei 35/2014.

les normes ETSI:

- Període de retenció EtsiQcsRetentionPeriod (0.4.0.1862.1.3)
- Les adreces web de les PDS (QC PKI Disclosure Statements), opcionalment

1.4.1.3 Certificat individual de persona física amb professió regulada

Certificat emès a tota persona física amb professió regulada que incorpora les dades de la seva professió.

Aquest certificat disposa dels següents OID:

- En la jerarquia pròpia de l'AC-APA:
  - Emissió amb QSCD al Núvol: 2.16.20.2.1.3.1.12.3
- Altres OIDs que els qualifiquen:
  - Emissió amb QSCD al núvol
    - 2.16.20.2.2.194112.1.2 (Polítiques qualificades andorranes)

El certificat emès en QSCD permet la "signatura electrònica qualificada[5]" que és aquella que inclou a més a més d'allò indicat per a la signatura electrònica avançada, l'haver estat creada mitjançant un dispositiu de creació de signatures electròniques qualificat.

Els usos indicats en el seu perfil corresponen a la següent informació:

- El camp "key usage" té activades i per tant permet realitzar, les següents funcions:
  - Compromís amb el contingut, per a la realització de signatures electròniques
  - Signatura digital, per a l'autenticació.
- En el camp de "Qualified Certificate Statements" apareixen les següents declaracions:
  - Emissió com a certificat qualificat:
    - (OID= 2.16.20.2.2.1862.1.1)
  - Usat amb un Dispositiu Segur de Creació de Signatura
    - (OID= 2.16.20.2.2.1862.1.4)
  - Que permet la creació de signatures electròniques
    - (OID= 2.16.20.2.2.1862.1.6.1)
- En el camp de "Qualified Certificate Statements" apareixen les següents declaracions d'acord amb les normes ETSI:
  - Període de retenció EtsiQcsRetentionPeriod (0.4.0.1862.1.3)
  - Les adreces web de les PDS (QC PKI Disclosure Statements), opcionalment

1.4.1.4 Certificat corporatiu 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.

Existeix un tipus de perfil d'aquest certificat emès amb pseudònim.

[5] D'acord amb l'article 3, definició 37, i l'article 5.3 de la Llei 35/2014.

Aquest certificat disposa dels següents OID:

- En la jerarquia pròpia de l'AC-APA:
  - Emissió amb QSCD al Núvol: 2.16.20.2.1.3.1.5.3
  - Emissió amb QSCD al Núvol amb pseudònim: 2.16.20.2.1.3.1.16.3
- Altres OIDs que els qualifiquen:
  - Emissió amb QSCD al núvol
    - Perfil PF: 2.16.20.2.2.194112.1.2 (Polítiques qualificades andorranes)
    - Perfil PF amb pseudònim: 0.4.0.194112.1.2 (ETSI)

El certificat emès en QSCD permet la "signatura electrònica qualificada[6]" que és aquella que inclou a més a més d'allò indicat per a la signatura electrònica avançada, l'haver estat creada mitjançant un dispositiu de creació de signatures electròniques qualificat.

Els usos indicats en el seu perfil corresponen a la següent informació:

- El camp "key usage" té activades i per tant permet realitzar, les següents funcions:
  - Compromís amb el contingut, per a la realització de signatures electròniques
  - Signatura digital, per a l'autenticació.
- En el camp de "Qualified Certificate Statements" apareixen les següents declaracions:
  - Emissió com a certificat qualificat:
    - Perfils PF (OID= 2.16.20.2.2.1862.1.1)
    - Perfils PF amb pseudònim:
      - (EtsiQcsCompliance= 0.4.0.1862.1.1)
      - (EtsiQcsQcCClegislation = 0.4.0.1862.1.7): AD
  - Usat amb un Dispositiu Segur de Creació de Signatura
    - Perfils PF (OID= 2.16.20.2.2.1862.1.4)
    - Perfils PF amb pseudònim (EtsiQcsQcSSCD= 0.4.0.1862.1.4)
  - Que permet la creació de signatures electròniques
    - Perfils PF (OID= 2.16.20.2.2.1862.1.6.1)
    - Perfils PF amb pseudònim (EtsiQctEsign (0.4.0.1862.1.6.1)
- En el camp de "Qualified Certificate Statements" apareixen les següents declaracions d'acord amb les normes ETSI:
  - Període de retenció EtsiQcsRetentionPeriod (0.4.0.1862.1.3)
  - Les adreces web de les PDS (QC PKI Disclosure Statements), opcionalment

1.4.1.5 Certificat corporatiu 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.

[6] D'acord amb l'article 3, definició 37, i l'article 5.3 de la Llei 35/2014.

Aquest certificat disposa dels següents OID:

- En la jerarquia pròpia de l'AC-APA:
  - Emissió en software: 2.16.20.2.1.3.1.8.2
  - Emissió amb QSCD al Núvol: 2.16.20.2.1.3.1.8.3
- Altres OIDs que els qualifiquen:
  - Emissió en software:
    - 2.16.20.2.2.194112.1.1 (Polítiques qualificades andorranes)
  - Emissió amb QSCD al núvol
    - 2.16.20.2.2.194112.1.3 (Polítiques qualificades andorranes)

El certificat emès en software permet el "segell electrònic avançat[7]" que és aquell que està vinculat al creador del segell de manera única, permet la identificació del creador corporatiu del segell, ha estat creat utilitzant dades de creació del segell electrònic que el creador pot utilitzar, amb un alt nivell de confiança electrònica, sota el seu control exclusiu, i que està vinculat amb les dades a què es refereix de manera que qualsevol modificació ulterior sigui detectable.

El certificat emès en QSCD permet el "segell electrònic qualificat[8]" que és aquell que inclou a més a més d'allò indicat per al segell electrònic avançat, l'haver estat creat mitjançant un dispositiu de creació de segells electrònics qualificat.

Els usos indicats en el seu perfil corresponen a la següent informació:

- El camp "key usage" té activades i per tant permet realitzar, les següents funcions:
  - Compromís amb el contingut, per a la realització de segellat electrònic
  - Signatura digital, per a l'autenticació.
- En el camp de "Qualified Certificate Statements" apareixen les següents declaracions:
  - Emissió com a certificat qualificat:
    - (OID= 2.16.20.2.2.1862.1.1)
  - Usat amb un Dispositiu Segur de Creació de Signatura (només els emesos amb QSCD al núvol)
    - (OID= 2.16.20.2.2.1862.1.4)
  - Que permet la creació de signatures electròniques
    - Perfils (OID= 2.16.20.2.2.1862.1.6.2)
- En el camp de "Qualified Certificate Statements" apareixen les següents declaracions d'acord amb les normes ETSI:
  - Període de retenció EtsiQcsRetentionPeriod (0.4.0.1862.1.3)
  - Les adreces web de les PDS (QC PKI Disclosure Statements), opcionalment

[7] D'acord amb l'article 3, definició 28.
[8] D'acord amb l'article 3, definició 29, i l'article 6 de la Llei 35/2014.

1.4.1.6 Certificat corporatiu 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.

Aquest certificat disposa dels següents OID:

- En la jerarquia pròpia de l'AC-APA:
  - Emissió amb QSCD al Núvol: 2.16.20.2.1.3.1.4.3
- Altres OIDs que els qualifiquen:
  - Emissió amb QSCD al núvol
    - 2.16.20.2.2.194112.1.2 (Polítiques qualificades andorranes)

El certificat emès en QSCD permet la "signatura electrònica qualificada[9]" que és aquella que inclou a més a més d'allò indicat per a la signatura electrònica avançada, l'haver estat creada mitjançant un dispositiu de creació de signatures electròniques qualificat.

Els usos indicats en el seu perfil corresponen a la següent informació:

- El camp "key usage" té activades i per tant permet realitzar, les següents funcions:
  - Compromís amb el contingut, per a la realització de signatures electròniques
  - Signatura digital, per a l'autenticació.
- En el camp de "Qualified Certificate Statements" apareixen les següents declaracions:
  - Emissió com a certificat qualificat:
    - (OID= 2.16.20.2.2.1862.1.1)
  - Usat amb un Dispositiu Segur de Creació de Signatura (només els emesos amb QSCD al núvol)
    - Perfils antics (OID= 2.16.20.2.2.1862.1.4)
  - Que permet la creació de signatures electròniques
    - Perfils antics (OID= 2.16.20.2.2.1862.1.6.1)
- En el camp de "Qualified Certificate Statements" apareixen les següents declaracions d'acord amb les normes ETSI:
  - Període de retenció EtsiQcsRetentionPeriod (0.4.0.1862.1.3)
  - Les adreces web de les PDS (QC PKI Disclosure Statements), opcionalment

1.4.1.7 Certificat corporatiu de Segell d'empresa

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.

Aquest certificat disposa dels següents OID:

- En la jerarquia pròpia de l'AC-APA:
  - Emissió en software: 2.16.20.2.1.3.1.2.2

[9] D'acord amb l'article 3, definició 37, i l'article 5.3 de la Llei 35/2014.

- Emissió amb QSCD al Núvol: 2.16.20.2.1.3.1.2.3

- Altres OIDs que els qualifiquen:
  - Emissió en software:
    - 2.16.20.2.2.194112.1.1 (Polítiques qualificades andorranes)
  - Emissió amb QSCD al núvol
    - 2.16.20.2.2.194112.1.3 (Polítiques qualificades andorranes)

El certificat emès en software permet el "segell electrònic avançat[10]" que és aquell que està vinculat al creador del segell de manera única, permet la identificació del creador corporatiu del segell, ha estat creat utilitzant dades de creació del segell electrònic que el creador pot utilitzar, amb un alt nivell de confiança electrònica, sota el seu control exclusiu, i que està vinculat amb les dades a què es refereix de manera que qualsevol modificació ulterior sigui detectable.

El certificat emès en QSCD permet el "segell electrònic qualificat[11]" que és aquell que inclou a més a més d'allò indicat per al segell electrònic avançat, l'haver estat creat mitjançant un dispositiu de creació de segells electrònics qualificat.

Els usos indicats en el seu perfil corresponen a la següent informació:

- El camp "key usage" té activades i per tant permet realitzar, les següents funcions:
  - Compromís amb el contingut, per a la realització de segellat electrònic
  - Signatura digital, per a l'autenticació.
- En el camp de "Qualified Certificate Statements" apareixen les següents declaracions:
  - Emissió com a certificat qualificat:
    - (OID= 2.16.20.2.2.1862.1.1)
  - Usat amb un Dispositiu Segur de Creació de Signatura (només els emesos amb QSCD al núvol)
    - (OID= 2.16.20.2.2.1862.1.4)
  - Que permet la creació de signatures electròniques
    - (OID= 2.16.20.2.2.1862.1.6.2)
- En el camp de "Qualified Certificate Statements" apareixen les següents declaracions d'acord amb les normes ETSI:
  - Període de retenció EtsiQcsRetentionPeriod (0.4.0.1862.1.3)
  - Les adreces web de les PDS (QC PKI Disclosure Statements), opcionalment

1.4.1.8 Certificat de representant de persona jurídica privada, pública o entitat sense personalitat jurídica.

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

Aquest certificat disposa dels següents OID:

- En la jerarquia pròpia de l'AC-APA:

[10] D'acord amb l'article 3, definició 28.
[11] D'acord amb l'article 3, definició 29, i l'article 6 de la Llei 35/2014.

- Emissió amb QSCD al Núvol: 2.16.20.2.1.3.1.14.2

- Altres OIDs que els qualifiquen:
  - Emissió amb QSCD al núvol
    - 2.16.20.2.2.194112.1.2 (Polítiques qualificades andorranes)

El certificat emès en QSCD permet la "signatura electrònica qualificada[13]" que és aquella que inclou a més a més d'allò indicat per a la signatura electrònica avançada, l'haver estat creada mitjançant un dispositiu de creació de signatures electròniques qualificat.

Els usos indicats en el seu perfil corresponen a la següent informació:

- El camp "key usage" té activades i per tant permet realitzar, les següents funcions:
  - Compromís amb el contingut, per a la realització de signatures electròniques
  - Signatura digital, per a l'autenticació.
- En el camp de "Qualified Certificate Statements" apareixen les següents declaracions:
  - Emissió com a certificat qualificat:
    - (OID= 2.16.20.2.2.1862.1.1)
  - Usat amb un Dispositiu Segur de Creació de Signatura (només els emesos amb QSCD al núvol)
    - (OID= 2.16.20.2.2.1862.1.4)
  - Que permet la creació de signatures electròniques
    - (OID= 2.16.20.2.2.1862.1.6.1)
- En el camp de "Qualified Certificate Statements" apareixen les següents declaracions d'acord amb les normes ETSI:
  - Període de retenció EtsiQcsRetentionPeriod (0.4.0.1862.1.3)
  - Les adreces web de les PDS (QC PKI Disclosure Statements), opcionalment

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.

1.4.3 Emissió de certificats de proves

L'AC-APA emet certificats de proves per la seva revisió en processos d'inspecció, revisió o en els d'avaluació en auditories. Aquests certificats disposaran de la següent informació:
Certificats de persona física

[12] D'acord amb l'article 3, definició 36.
[13] D'acord amb l'article 3, definició 37, i l'article 5.3 de la Llei 35/2014.

Certificats de persona física

- Given Name: Nom
- Surname: Cognom1 Cognom2
- SerialNumber: IDCAD-000000X

Certificats de segell electrònic

- Organization: Empresa exemple SL
- SerialNumber:
- Locality: Andorra la Vella
- OU: Operacions de prova

1.5 Autoritat de polítiques

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

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 l'AC-APA.

1.5.1 Organització que administra el document

La redacció i el control d'aquesta CPS correspon a l'AC-APA, gestionat per la responsable de l'Oscepa.

1.5.2 Dades de contacte de l'organització

Autoritat de Certificació de les Administracions Públiques andorranes *(Oficina de Serveis de Confiança Electrònica - OSCEPA)*	
Adreça postal	Carrer de la Grau, Edifici Prat del Rull, Andorra la Vella
Telèfon	+376 875 700
Adreça-e	oficina.certificacio@govern.ad

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

L'AC-APA disposa d'un telèfon mòbil **+376601098** dins de l'horari laboral.

L'AC-APA disposa d'un servei de permanència fora de l'horari laboral **+376610093**.

. La prestació dels serveis de confiança en règim de disponibilitat 24x7 constitueix una funció crítica que impacta

directament en la seguretat, la continuïtat i la confiança del servei. En aquest sentit, la seva gestió ha de ser assumida per l'OSCEPA o per personal directament dependent, sota el seu control efectiu.

D'acord amb el Reglament (UE) 910/2014 (eIDAS), el prestador és responsable de garantir la seguretat i la correcta prestació dels serveis. Aquesta responsabilitat no és delegable en termes materials, especialment en aquelles funcions que afecten la disponibilitat i la resposta davant incidents.

Els serveis 24x7 inclouen la gestió d'incidències, revocacions, validacions i altres operacions essencials que poden tenir impacte immediat sobre la validesa dels certificats i la confiança del sistema. Aquestes funcions han de ser executades sota control directe de l'organització, garantint:

- integritat del procés
- confidencialitat de la informació
- traçabilitat de les actuacions

La gestió d'operacions crítiques implica accés a informació sensible. La dependència directa del personal assegura un major control sobre:

- obligacions de confidencialitat
- compliment normatiu
- responsabilitat individual

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

La responsable de l'AC-APA gestiona per tant l'autoritat de les polítiques (PA) de les jerarquies i autoritats de certificació descrites anteriorment i és responsable de l'administració de la CPS.

1.5.3 Procediments de gestió del document

La publicació de les revisions d'aquesta CPS ha d'estar aprovada per l'AC-APA i gestionat per la responsable de l'Oscepa.

L'Administració pública andorrana publica a la seva pàgina web cada nova versió. La CPS està publicada en format

PDF signat o segellat electrònicament amb un certificat digital.

1.6 Acrònims i definicions

1.6.1 Acrònims

AC	Autoritat de certificació
RA	Autoritat de registre
CPS	Certification Practice Statement. Declaració de pràctiques de certificació
CRL	Certificate Revocation List. Llista de certificats revocats
CSR	Certificate Signing Request. Petició de signatura de certificat
DES	Data Encryption Standard. Estàndard de xifratge de dades
DN	Distinguished Name. Nom distintiu dins del certificat digital
DSA	Digital Signature Algorithm. Estàndard d'algoritme de signatura
DSCF	Dispositiu segur de creació de signatura
DSADCF	Dispositiu segur de magatzem de dades de creació de signatura
FIPS	Federal Information Processing Standard Publication
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization. Organisme Internacional d'Estandardització
ITU	International Telecommunications Union. Unió Internacional de Telecomunicacions

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

1.6.2 Definicions

AC	Autoritat de certificació
RA	Autoritat de registre
CPS	Certification Practice Statement. Declaració de pràctiques de certificació
CRL	Certificate Revocation List. Llista de certificats revocats
CSR	Certificate Signing Request. Petició de signatura de certificat
DES	Data Encryption Standard. Estàndard de xifratge de dades
DN	Distinguished Name. Nom distintiu dins del certificat digital
DSA	Digital Signature Algorithm. Estàndard d'algoritme de signatura
DSCF	Dispositiu segur de creació de signatura
DSADCF	Dispositiu segur de magatzem de dades de creació de signatura
FIPS	Federal Information Processing Standard Publication
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization. Organisme Internacional d'Estandardització
ITU	International Telecommunications Union. Unió Internacional de Telecomunicacions

LDAP	Lightweight Directory Access Protocol. Protocol d'accés a directoris
OCSP	Online Certificate Status Protocol. Protocol d'accés a l'estat dels certificats
OID	Object Identifier. Identificador d'objecte
PA	Policy Authority. Autoritat de polítiques
PC	Política de certificació
PIN	Personal Identification Number. Número d'identificació personal
PKI	Public Key Infrastructure. Infraestructura de clau pública
RSA	Rivest-Shamir-Adleman. Tipus d'algorisme de xifratge
SHA	Secure Hash Algorithm. Algorisme segur de Hash
SSL	Secure Sockets Layer. Protocol dissenyat per Netscape i convertit en estàndard de la xarxa. Permet la transmissió d'informació xifrada entre un navegador d'Internet i un servidor.

TCP / IP	Transmission Control. Protocol / Internet Protocol. Sistema de protocols, definits en el marc de la IEFT. El protocol TCP s'usa per dividir en origen la informació en paquets, per després recompondre-la en destinació. El protocol IP s'encarrega d'adreçar adequadament la informació cap al seu destinatari.

2. RESPONSABILITAT DE PUBLICACIÓ I DIPÒSITS

2.1 Repositoris

L'AC-APA fa públic el seu certificat de 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'AC-APA sol·licita prèviament l'autorització del titular abans de publicar el certificat.

2.2 Publicació d'informació de certificació

El contingut d'aquesta CPS, 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. L'AC-APA 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

L'AC-APA 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.

4. IDENTIFICACIÓ I AUTENTICACIÓ DELS TITULARS DELS CERTIFICATS

4.1 Noms

4.1.1 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

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.

4.1.2 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.

4.1.3 Anonimat o pseudònims de subscriptors

S'emeten certificats de pseudònim.

4.1.4 Regles utilitzades per interpretar diversos formats de noms

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

Els certificats expedits per l'AC-APA 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 (Emisor) 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.

4.1.5 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.

4.1.5.1 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.

4.1.6 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'AC-APA es reserva el dret de rebutjar una sol·licitud de certificat degut a un conflicte sobre noms.

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

L'AC-APA 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.

4.2 Validació inicial de la identitat

Per a les *persones físiques individuals*, la seva identitat es valida mitjançant la identificació per un operador autoritzat per l'AC-APA. Bé presencialment o per identificació remota. Aquest cas d'identificació remota solament és possible per demanar un certificat individual de persona física de ciutadà no obstant això es podrà valorar a curt termini l'acceptació d'altres tipologies de certificats.

En el cas d'identificació remota l'article 26.2.e de la Llei 35/2014, del 27 de novembre, modificada per la Llei 9/2021, del 20 d'abril, s'especifica que "Els sistemes de videoconferència també estaranadmesos si es compleixen els requisits previstos en aquest article i els que es puguin desenvolupar reglamentàriament, pel que fa els nivells de garantia necessaris" per tal de "verificar de forma fefaent la identitat i, si escau, qualsevol altre atribut específica de la persona física o jurídicaa la qual expedeix el certificat electrònic qualificat" com així s'indica en l'article 26.2 de l'esmentada llei.

Per a les persones físiques corporatives, la seva identitat es valida mitjançant la identificació per un operador autoritzat per l'AC-APA o bé mitjançant els registres corporatius de l'entitat, empresa o organització de dret públic o privat.

4.2.1 Mètodes de prova de la possessió de la clau privada

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.

La possessió de la clau privada es demostra d'acord amb el procediment fiable d'entrega i acceptació del certificat pel titular del certificat.

4.2.2 Identificació de la identitat d'un individu

En els certificats de persona física individuals, la identitat d'aquesta persona es valida mitjançant la presentació del seu document oficial d'identificació (NIA, passaport, o un altre reconegut en dret) de manera presencial davant l'operador autoritzat per l'AC-APA.

També podem utilitzar l'eina d'identificació remota des de la Seu Electrònica.

En els certificats corporatius de persona física, la identitat d'aquesta es valida presencialment comparant la informació de la sol·licitud davant els registres de l'entitat, empresa o organització de dret públic o privat a la que està relacionada, assegurant la correcció de la informació a incloure en el certificat.

4.2.2.1 Necessitat de presencia personal

En els certificats de persona física individuals, aquesta cal que es personi amb el seu document oficial d'identitats davant un operador autoritzat de l'AC-APA.

L'AC-APA verificarà tota la documentació aportada guardant-la per tal d'acreditar la seva validesa.

L'AC-APA admès la sol·licitud d'un certificat de persona física per un tercer sempre que aquest porti poders notarials generals o específics per a tal finalitat. Als poders notarials específics ha de constar aquesta casuística. Quan es tracti de poders d'un altre país que no sigui Espanya, França o Portugal han d'estar a postil·lats.

La presencia física no serà necessària si es demana un certificat de ciutadà per identificació remota.

4.2.2.2 Vinculació de la persona física

La justificació documental de la relació que vincula a una persona física identificada en un certificat amb l'entitat, empresa o organització de dret públic o privat ve donada per la seva constància en els registres interns, administratius o públics (contracte de treball si és empleat, contracte mercantil, l'acta del seu càrrec, la sol·licitud com a membre de l'entitat, etc.) de cada una de les persones jurídiques públiques o privades amb les que disposa d'aquesta relació de pertinença.

4.2.3 Informació de subscriptor no verificada

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

4.2.4 Validació de l'autoritat

L'AC-APA podrà consultar els registres públics corresponents per a comprovar l'existència de la corporació sol·licitant, les seves dades actuals així com el nomenament i vigència de la persona física autoritzada.

Aquestes validacions podran fer-se per mitjans electrònics. En cas d'aportació d'aquesta documentació en paper cal escanejar-lo.

4.2.5 Criteris d'interoperació

L'AC-APA es reserva el dret de proporcionar serveis d'interoperació amb altres Autoritats de Certificació. Aquests serveis cal que s'estableixin per contracte.

4.3 Identificació i autenticació de sol·licituds de renovació

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 cincs anys des de l'última verificació física o procés equivalent.

4.4 Identificació i autenticació de la sol·licitud de revocació

L'AC-APA 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.

Tant l'AC-APA com una de les Autoritats de Registre existents poden autenticar les peticions i informes relatius a la revocació d'un certificat comprovant sempre que provenen d'una persona autoritzada.

Per comprovar-ho els mètodes acceptables seran els següents:

- L'enviament d'una sol·licitud de revocació per part de la corporació en certificats corporatius, signada electrònicament amb el certificat a revocar.
- L'enviament d'una sol·licitud de revocació per part de la persona física identificada en el certificats (individual o corporatiu), signada electrònicament amb el certificat a revocar.
- L'ús d'informació que només coneix el titular del certificat i que li permet revocar de forma automàtica el certificat.

L'enviament d'una sol·licitud de revocació signada manuscritament o digitalment es suficient per revocar o donar de baixa un certificat.

[14] D'acord amb l'article 26.4 de la Llei 35/2014, de 27 de novembre, de certificació i confiança electrònica.

5. REQUISITS D'OPERACIÓ DEL CICLE DE VIDA DELS CERTIFICATS

L'AC-APA 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.

5.1 Sol·licitud de certificats

1. El titular proporciona les seves dades personals i s'escau documentació que no es pugi consultar a les BBDD de govern.
2. Es verifica la identitat de la persona
3. Es generen les claus (públiques i privades)

5.2 Emissió

1. L'autoritat de certificació valida la informació
2. Es crea el certificat signat per la CA
3. S'associa la clau pública de l'usuari amb la seva identitat
4. S'estableix període de validesa .

5.3 Distribució

1. Entrega segura del certificat al titular
2. Instal·lació en dispositius o sistemes

5.4 Ús

1. Autenticació i signatura
2. La clau privada si el certificat està a núvol està dins d'un entorn segur.
3. La clau privada si el certificat està en software està emmagatzemada a un dispositiu
4. La clau pública es pot compartir lliurement donant que serveix per verificar signatures

5.5 Verificació

1. Comprovació de la validesa del certificat mitjançant consultes a les llistes de revocació (CLR) i serveis en línia

5.6 Renovació

1. Sol·licitud d'un nou certificat abans del venciment actual o al seu venciment

5.7 Revocació

1. Invalidació del certificat abans de la seva caducitat per motius com:
    a. Compromís de la clau privada
    b. Canvi dades del titular
    c. Cessament d'activitat
    d. Sol·licitud del propi titular
    e. Ús indegut del certificat

5.8 Caducitat

1. Expiració automàtica al termini de la data de validesa
2. Necessitat d'emetre un nou certificat.

5.9 Auditoria

1. Conservació de registres per auditories
2. Magatzematge segur de dades històriques relacionats amb el certificat.

3. CONTROLS DE LES INSTAL·LACIONS, DE GESTIÓ I OPERACIONALS

a. Controls de seguretat física

En aquest apartat s'han recollit les mesures adoptades més rellevants.

5.1.1 Ubicació i construcció

Els edificis on es troba ubicada la infraestructura de la CA 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 on es duen a terme processos de certificació és limitat i protegit mitjançantuna 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 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 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 compten amb les mesures adequades de protecció contrael 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

S'han 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.

S'han 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

L'AC-APA, en el corresponent proveïdor tècnic, disposa de còpies de seguretat en ubicacions diferents que reuneixen les mesures precises de seguretat i amb una separació física adequada.

b. 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, es garanteix que els 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 dissemina el control i limita el frau intern, i no permet que una sola persona controli de principi a fi totes les funcions de certificació, amb una concessió de mínim privilegi, quan sigui possible.

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

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

Els rols són els següents:

- **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 responsable

- **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 de la 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 de la CA són incompatibles amb les tasques de certificació i sistemes.

- **Operador de la CA:**

Responsable necessari, conjuntament amb l'administrador de la 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 de la CA són incompatibles amb les d'administrador de la CA i no pot dur a terme tasques d'auditor ni auditor intern.

- **Operador de la RA:**

Persona responsable d'aprovar les peticions de certificació efectuades pel signant.

Les operacions d'operador de la RA són incompatibles amb les d'administrador de la 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'AC-APA. 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

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.

c. Controls del personal

5.3.1 Qualificacions, experiència i requisits d'autorització

El personal que presta els seus serveis en l'àmbit de l'AC-APA posseeix el coneixement, l'experiència i la formació suficients, per a la comesa correcta de les funcions assignades. Per això, 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'AC-APAestà 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'AC-APA 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'AC-APA 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'AC-APA no assignarà a un lloc fiable o de gestió una persona que no sigui idònia per al lloc, especialment per haver estat condemnada per un delicte o una falta que afecti la seva idoneïtat per al lloc. Per aquest motiu, prèviament es duu a terme una investigació, fins on permeti la legislació aplicable, relativa als aspectes següents:

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

5.3.2 Procediments de comprovació d'antecedents

L'AC-APA, 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'AC-APA, 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

L'AC-APA proveeix el personal relacionat amb l'explotació de la CA de tota la informació i la documentació necessària sobre els procediments operatius relatius a aquesta.

L'AC-APA supervisen la realització de la formació i el grau de confiança per part del personal

5.3.4 Requisits i freqüència de l'actualització de la formació

L'AC-APA 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'AC-APA, 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 confidencialitati 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'AC-APA 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' AC-APA. 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.

d. Procediments de registre d'esdeveniments

5.4.1 Tipus d'esdeveniments registrats

ÉS 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 predictible.
- 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 genero 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

L'AC-APA, per mitjà del proveïdor subcontractat, 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

L'AC-APA, per mitjà del proveïdor subcontractat, 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

L'AC-APA, per mitjà del proveïdor subcontractat, fa còpies de seguretat periòdiques dels registres d'auditoria generats per la CA.

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

L'AC-APA, per mitjà del proveïdor subcontractat, 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.

e. Arxiu de registres

L'AC-APA, per mitjà del proveïdor subcontractat, conserva tota la informació rellevant sobre les operacions realitzades amb els certificats durant els períodes de temps estipulats, tot mantenint un registre d'esdeveniments.

Les sol·licituds dels subscriptors es conserven en un arxiu digital (AS400)

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 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

És 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 especifica en aquest document, 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 l'AC-APA, per mitjà del proveïdor subcontractat. 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 l'AC-APA, per mitjà del proveïdor subcontractat, per a les còpies de seguretat de la resta de sistemes d'informació. Aquesta còpia de seguretat s'executa automàticament al Centre de Backups.

L'AC-APA, per mitjà del proveïdor subcontractat, 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'AC-APA, per mitjà del proveïdor subcontractat 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 l'AC-APA, per mitjà del proveïdor subcontractat garanteixen el registre del temps en què es realitzen. L'instant de tempsdels 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 espanyola".

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 l'AC-APA, per mitjà del proveïdor subcontractat.

5.5.7 Procediments per obtenir i verificar informació arxivada

Els esdeveniments registrats per l'AC-APA, per mitjà del proveïdor subcontractat 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'AC-APA, per mitjà del proveïdor subcontractat disposa d'un document de seguretat informàtica en què es descriu el procés per verificar que la informació arxivada és correcta i accessible.

f. Canvi de claus

Els procediments per proporcionar, en cas de canvi de claus, una nova clau pública de 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 l'AC-APA (vegeu apartat 2.1 Repositoris).

g. Recuperació en cas de compromís de la clau o desastre

5.7.1 Procediments de gestió d'incidències i compromisos

L'AC-APA, per mitjà del proveïdor subcontractat 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, l'AC-APA, per mitjà del proveïdor subcontractat informarà 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, l'AC-APA, per mitjà del proveïdor subcontractat 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

L'AC-APA, per mitjà del proveïdor subcontractat 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, L'AC-APA 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 a les cossos i autoritat judicial per si hi pogués haver activitats constitutives de delicte.

5.7.4 Continuïtat del negoci després d'un desastre

L'AC-APA, per mitjà del proveïdor subcontractat restablirà els serveis crítics (revocació i publicació de certificats revocats) d'acord amb aquesta DPC dins de les24 hores posteriors a un desastre o emergència imprevista prenent com a base el pla de contingència i continuïtatde negoci existent.

L'AC-APA, per mitjà del proveïdor subcontractat disposa d'un centre alternatiu, si cal, per a la posada en funcionament dels sistemes de certificació.

h. Cessament de la CA o RA

5.8.1 Autoritat de Certificació

Abans del cessament de la seva activitat, l'AC-APA 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 acordso 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 elperíode 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'AC-APA, mentre hi hagi l'obligació de mantenir arxivada la informació, i si no és així, aquesta serà destruïda de manera segura.

4. CONTROLS DE SEGURETAT TÈCNICA

a. 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'AC-APA son generades i emmagatzemades en un mòdul de maquinari criptogràfic segur (HSM), que compleix els requisits de seguretat necessaris.

Quan les claus són centralitzades el titular les protegeix amb el seu PIN o contrasenya, a més d'un segon factor d'autenticació per a la realització de la signatura electrònica qualificada.

6.1.2 Lliurament de la clau privada al signant

La clau la genera el titular amb un procediment d'emissió previst per l'AC-APA, un cop s'ha personat físicament davant una RA o amb un procediment equivalent i validat d'acord amb la llei vigent.

La clau privada es genera en un dispositiu qualificat de creació de signatra sota el control exclusiu del signatari, i per tant, no existeix cap entrega de la clau privada al titular.

Quan l'emissió no es centralitzada, la generació i emmagatzematge de la clau s'ha realitzat en programari. La clau privada es troba en possessió del titular amb la recomanació de protegir-la adequadament per evitar usos no desitjats d'aquesta.

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

La clau pública que cal certificar es generada juntament amb la clau privada sobre un dispositiu qualificat de creació de signatura o pot ser generada en programari essent entregada a l'AC-APA per mitjà de l'enviament d'una sol·licitud de certificació en format PKCS#10.

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 d'aquesta mateixa DPC.

6.1.5 Mida de les claus

Les claus de la CA arrel de l'AC-APA són de 4096 bits.

Les claus de la CA subordinada de l'AC-APA són 4096 bits.

La longitud de les claus dels titulars de certificats d'entitat final són com a mínim de 2048 bits.

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.

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

Tots els certificats emesos per l'AC-APA 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'AC-APA.

En els certificats de persona física centralitzats:

- Quan el certificat permeti la creació de signatura electrònica qualificada s'inclourà la Key Usage "nonrepudiation".
- Quan el certificat permeti l'ús per a autenticar-se s'inclourà la key Usage "digitalSignature".

En els certificats de segell electrònic:

- Per a la creació de segellat electrònic s'inclourà la Key Usage "nonrepudiation".
- Per a l'autenticació s'inclourà la key usage "digitalSignature".

En els certificats en programari de segell electrònic, a més:

- S'inclourà la Key Usage "Key Encipherment".

b. 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 l'AC-APA, per mitjà del proveïdor subcontractat, compleixen els requisits deseguretat 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.

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 de la 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'HSMi mai no surt del mateix.

6.2.4 Còpia de seguretat de la clau privada

L'AC-APA, per mitjà del proveïdor subcontractat, 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

En el cas del dispositiu qualificat de creació de signatures i de claus generades en programari, l'AC-APA manté les copies de seguretat amb les claus privades protegides, essent aquestes únicament accessibles pel titular.

En el cas de les claus generades en programari, és el titular o usuari autoritzat l'encarregat del seu arxiu i aquest serà el responsable de mantenir-les sota el seu control exclusiu.

6.2.6 Transferència de la clau privada al 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 de 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, l'AC-APA, per mitjà del proveïdor subcontractat, destruirà la clau privada de la CA i la seva còpia de seguretat per garantir que no es mantéinformació 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 resistents a manipulacions intrusives a nivell maquinari (tamper protection).

c. Altres aspectes de la gestió del parell de claus

6.3.1 Arxiu de la clau pública

L'AC-APA, per mitjà del proveïdor subcontractat,, 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 les autoritats de certificacióduran el període exigit 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'AC-APA generada pel proveïdor tècnic tenen una validesa de quinze (15) anys i els de la CA subordinada de l'AC-APA generada pel proveïdor tècnic 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.

d. Dades d'activació

6.4.1 Generació i activació de les dades d'activació

Per activar les claus privades de la CA, per part del proveïdor tècnic, 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, consisteix en la creació de la contrasenya que custodiarà les claus i la generació d'aquestes, ja sigui en programari o en el dispositiu qualificat de creació de signatura.

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 és el propi signatari qui generarà el parell de claus al dispositiu qualificat de creació de signatura. Per tant, aquest signatari és el responsable de la protecció de les dades d'activació de la seva clau privada. Es necessari disposar d'aquesta protecció i un mecanisme de segon factor d'autenticació, en certificats centralitzats, per a l'accès a la clau privada.

Per als certificats d'entitat final en programari, la instal·lació i inicialització de la clau privada associada al certificat, requereix la utilització dels sistemes de seguretat el propi titular del certificat, havent d'introduir al menys una contrasenya només coneguda per ell, i no emmagatzemada als sistemes.

Aquestes contrasenyes són confidencials, personals i intransferibles i és el paràmetre que protegeix les claus privades permetent la utilització dels certificats en els serveis oferts per mitjà d'una xarxa de comunicacions, pel que es recomana que:

- Es memoritzi les contrasenyes i no s'apuntin en cap lloc físic ni electrònic.
- No s'enviï ni comuniqui a ningú per cap mitjà.
- Si s'adona que la contrasenya és coneguda per algú altre caldrà canviar-la o notificar a l'AC-APA aquest fet, ja que

es motiu de revocació del certificat associat a aquesta clau.

- No incloure informació personal o codis fàcilment predicibles per terceres persones (com la data de naixement, el número de telèfon, repeticions de números consecutius, parts del nom del titular o del document d'identitat...).

6.4.3 Altres aspectes de les dades d'activació

No estipulats.

e. 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'AC-APA empra sistemes fiables per oferir els seus serveis de certificació. L'AC-APA 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'AC-APA, 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, l'AC-APA, per mitjà del proveïdor subcontractat, segueix l'esquema previst a la UNE-ISO27002 (anteriorment anomenada ISO 17799), Codi de Bones Pràctiques per a la Seguretat de la Informació

6.5.2 Valoració de la seguretat informàtica

L'AC-APA, per mitjà del proveïdor subcontractat, 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.

f. 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 l'AC-APA o del proveïdor tècnic.

6.6.2 Controls de gestió de la seguretat

El proveïdor tècnic 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'AC-APA 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.

L'AC-APA tédocumentat tot el procediment relatiu a les funcions i responsabilitats del personal implicat en el control i la manipulació d'elements continguts en el procés decertificació.

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

L'AC-APA 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

L'AC-APA, per mitjà del proveïdor tècnic realitzarà les revisions oportunes per verificar l'estat de validesa de la certificació dels dispositius segurs decreació de signatura.

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

g. Controls de seguretat de la xarxa

L'AC-APA 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 detallafocs.

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 debloqueig 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.

h. Fonts de temps

L'hora del sistema està sincronitzada amb el Reial Observatori de l'Armada espanyola, 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.

5. PERFILS DE CERTIFICAT, CRL I OCSP

a. Perfil de certificat

Els certificats emesos pels sistemes de l'AC-APA, seran conformes amb el que disposen les normes següents i especificacions tècniques:

i. ETSI EN 319 412-5: Profiles for Trust Service Providers issuing certificats; Part 5: Extension for QualifiedCertificate profile.
ii. RFC 5280 "Internet X.509 Public Key Infrastructure. Certificate and CRL Profile".
iii. RFC 3739 "Internet x509 Public Key Infrastructure. Qualified Certificates Profile".
iv. Perfils de Certificats derivats de la Llei 6/2020, de 11 de novembre, reguladora de determinats aspectesdels serveis electrònics de confiança, la Llei 40/2015 d'1 d'Octubre, de Règim Jurídic del Sector Publico (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).
v. ETSI EN 319 412-2 (Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificateprofile for certificats issued to natural persons).
vi. ETSI EN 319 412-3 (Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3:Certificate profile for certificates issued to legal persons).
vii. ETSI EN 319 412-4: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificateprofile for web site certificats.
viii. ETSI TS 119495: Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; QualifiedCertificate Profiles and TSP Policy Requirements un the payment services Directive (EU) 2015/2366.

7.1.1 Número de versió

L'AC-APA emet certificats X.509, versió 3

7.1.2 Extensions del certificat

Els certificats d'usuari emesos per L'AC-APA 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'AC-APA.

7.1.3 Identificadors d'objecte (OID) dels algoritmes

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 l'AC-APA 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'AC-APA potutilitzar restriccions de nom (utilitzant l'extensió del certificat *nameconstraints*) en els certificats de CA subordinada emesos a terceres parts de manera que només es pugui emetre per la CA subordinada al conjunt de certificats permès en aquestaextensió.

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

Tots els certificats tenen un identificador de política de la AC-APA, corresponent al Govern d'Andorra = 2.16.20.2.x
En l'apartat **1.2** s'identifiquen tots els certificats d'aquesta jerarquia.

En l'apartat **1.4.1** es descriuen tots els certificats emesos en aquesta jerarquia i els seus corresponents OIDs.

7.1.7 Ús de l'extensió Policy Constraints

L'AC-APA pot utilitzar restriccions de política (utilitzant l'extensió del certificat *Policy Constraints*) en els certificats de CA subordinada emesos a terceres 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'AC-APA associa explícitament amb el certificat. L'extensió pot contenir un qualificador de la política. Vegeu el 7.1.6.

b. Perfil de CRL

7.2.1 Número de versió

L'AC-APA utilitza CRLs X,509 Versió 2.

7.2.2 CRL i extensions

Las CRLs emeses per l'AC-APA seran conformes amb la norma RFC 5280: Internet X.509 Public Key Infrastructure – Certificate and CRL Profile, April 2002.

c. Perfil d'OCSP

Els certificats emesos per l'AC-APA 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 d'OCSP Responder utilitzaran l'estàndard X.509 Versió 3 (X.509 v3)

7.3.2 Extensions OCSP

Les principals extensions per OCSP són 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

6. AUDITORIES DE CONFORMITAT

a. Freqüència o circumstàncies de les auditories Veure auditories No UE

L'AC-APA 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.

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

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 mostrejos sobre certificats emesos, verificant- ne el processament correcte.

b. Identificació i qualificació de l'auditor

Les auditories poden ser de caràcter tant intern com 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.

c. Relació entre l'auditor i la CA

Al marge de la funció d'auditoria, l'auditor extern i la part auditada (l'AC-APA i el proveïdor tècnic) 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:

i. La manca de vinculació laboral, mercantil a favor d'apoderaments amb l'organització auditada.
ii. Cap interès directe o indirecte amb l'entitat auditada.
iii. 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.

iv. Manca de familiaritat o confiança, per la influència i proximitat excessiva amb els administradors odirectius de l'entitat auditada.
v. La no execució prèvia de serveis relatius a la definició i implantació de mesures de seguretat al'organització auditada per part de l'equip auditor.
vi. Els honoraris oferts no suposen un percentatge significatiu de la facturació de la companyia.

d. Tòpics coberts per l'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.

e. 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.

f. Comunicació de resultats

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

7. ASPECTES LEGALS I ALTRES ASSUMPTES

a. 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'AC-APA implanta controls per evitar els casos de descàrrega massiva de certificats. Qualsevol altra circumstància que segons el parer de l'AC-APA hagi de ser considerada a aquest efecte es publica al lloc web: https://www.signaturaelectronica.ad

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

L'AC-APA 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: https://www.signaturaelectronica.ad/jerarquia-politiques-i-practiques-de-certificacio.

9.1.5 Política de reintegraments

L'AC-APA no té una política de reintegraments específica, i s'acull a la normativa general vigent del Govern d'Andorra

b. Responsabilitat financera

9.2.1 Cobertura de l'assegurança

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.

c. Confidencialitat de la informació del negoci

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

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

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.

9.3.3.2 Enviament a l'autoritat competent

L'AC-APA 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.

d. Protecció de dades personals

9.4.1 Política de protecció de dades personals

L'AC-APA compleix 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.

9.4.2 Política de privacitat.

L'AC-APA disposa d'una política de privacitat que pot ser consultada a: https://www.signaturaelectronica.ad/oscepa-privacitat

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 vigent (la Llei 29/2021, del 28 d'octubre).

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'AC-APA 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.

e. Drets de propietat intel·lectual

L'AC-APA és titular dels drets de propietat intel·lectual sobre aquesta CPS.

f. Obligacions i responsabilitat civil

9.6.1 Obligació i responsabilitat de la CA

9.6.1.1 CA

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

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

escau.
- Establir els mecanismes de generació i custòdia de la informació rellevant en les activitats descrites, protegint-les de pèrdua o destrucció o falsificació.
- Conservar la informació sobre el certificat emès pel període mínim exigit per la normativa vigent.

L'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 suspendre'ls i revocar-los. En concret, l'AC-APA 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 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.

En compliment de la legislació vigent l'AC-APA 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'AC-APA i amb el subjecte/signant.
- Informar l'AC-APA 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'AC-APA i la Declaració de pràctiques de certificació aplicable, així com de les seves obligacions, facultats iresponsabilitats.
- 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.

9.6.3 La responsabilitat de les RA

Les RA subscriuen un contracte de prestacióde servei amb l'AC-APA 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 aquesta DPC 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'AC-APA (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 constataque 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'AC-APA dels seus incompliments.

Per descomptat, no és intenció de l'AC-APA 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'AC-APA, 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.

9.6.4 Obligació i responsabilitat del subscriptor

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

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

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

9.6.4.2 Sol·licitant del certificat

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.

9.6.4.3 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.

9.6.5 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'AC-APA 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'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 comprovantque l'autoritat de certificació que ha emès el certificat es troba publicada a la llista de confiança del supervisor nacional corresponent.

9.6.6 Obligació i responsabilitat d'altres participants

No estipulat.

g. Exoneració de responsabilitat

Segons la legislació vigent, la responsabilitat de l'AC-APA 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:

i. 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.
ii. Haver incorregut en negligència pel que fa a la conservació de les dades de creació de signatura i a la seva confidencialitat.
iii. No haver sol·licitat la suspensió o revocació de les dades del certificat electrònic en cas de dubte sobre el manteniment de la confidencialitat.
iv. Haver utilitzat la signatura després d'haver expirat el període de validesa del certificat electrònic.
v. Superar els límits que figuren en el certificat electrònic.
vi. 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.
vii. 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.
viii. 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-APA i les RA tampoc no seran responsables en cap cas quan es troben davant de qualsevol d'aquestes circumstàncies:

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

h. Limitació de responsabilitat

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

i. Indemnitzacions

Vegeu l'apartat 9.2.Termini i finalització

j. 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.

k. 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).

l. 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 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: 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.

m. 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.

n. Legislació aplicable

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

o. Conformitat amb la llei aplicable

Vegeu el punt 9.14.

p. 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'AC-APA.

9.16.3 Separabilitat

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

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

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

L'AC-APA 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'AC-APA no faci complir una disposició d'aquesta CPS no elimina el dret de l'AC-APA 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'AC-APA.

9.16.5 Força major

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

q. 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'AC-APA.

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

8. 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 segons les diferents normatives aplicables**
Agost 2021	V2.3.3	**Certificats a menors de 16 anys i entre 16 i 18 anys**
Febrer 2022	V3.0	**Adaptació a auditories ETSI**
Setembre 2022	**V4**	**Revisió DPC amb nova Jerarquia pròpia**
Setembre 2023	**V4.1**	**Revisió anual** **Incorporació de la identificació per videoconferència (ap 3.2).** **Actualització apartat 3.3**
Agosto 2024	**V4.2**	**Revisió anual** **Incorporació poders notarials** **Arxiu digital** **Certificat de pseudònim**
Setembre 2025	**V4.3**	**Revisió anual** **Nou certificat de persona física en software per a cartera digital** **Modificació sol·licitud de segell**
Octubre 2025	**V4.4**	**Sol·licitud del certificat electrònic per a persones amb discapacitat.**
Febrer 2026	**V4.5**	**Revisió anyal** **Sol·licitud biomètrica.** **Sol·licitud vídeo identificació.**

Signat digitalment per:
MARTA OSUNA SANCHEZ
(SIGNATURA)