



Política i requeriments de seguretat per a prestadors de serveis de confiança.

**Requeriments per a prestadors de
serveis de confiança que emetin
certificats qualificats a ANDORRA.**

Versió 1.0 · AGOST 2022

Índex

Índex.....	2
1. Referències	6
1.1. Referències normatives	6
1.2. Referències informatives	6
2. Definicions, abreviatures i anotacions	7
2.1. Definicions	7
2.2. Abreviatures.....	7
2.3. Anotacions	7
3. Conceptes generals.....	9
3.1. Conceptualització dels requisits generals de les polítiques de certificació	9
3.2. Política de certificació i Declaració de pràctiques de certificació.....	9
3.2.1. Visió general.....	9
3.2.2. Propòsit.....	9
3.2.3. Nivell d'especificitat.....	9
3.2.4. Aproximació	9
3.2.5. Política de certificació.....	9
3.3. Altres declaracions dels proveïdors de serveis de confiança	11
3.4. Serveis de certificació	11
4. Provisions generals sobre la Declaració de pràctiques de certificació i les polítiques de certificació	12
4.1. Requisits generals	12
4.2. Requisits de la Declaració de pràctiques de certificació.....	13
4.3. Denominació de les polítiques de certificació i identificació.....	13
4.4. Participants PKI	13
4.4.1. Autoritat de certificació	13
4.4.2. Subscriptor i subjecte	13
4.4.3. Altres.....	13
4.5. Ús dels certificats.....	13
4.5.1. AD-pcq-F	13
4.5.2. AD-pcq-J	13
4.5.3. AD-pcq-Fd	14

4.5.4.	AD-pcq-Jd	14
4.5.5.	AD-pcq-W	14
5.	Pràctiques dels proveïdors de serveis de confiança	15
5.1.	Publicació i responsabilitats dels dipòsits	15
5.2.	Identificació i autenticació	15
5.2.1.	Denominació	15
5.2.2.	Validació inicial de la identitat	15
5.2.3.	Identificació i autenticació per a sol·licituds de reentrada de claus	16
5.2.4.	Identificació i autenticació per a sol·licituds de revocació	16
5.3.	Requisits operatius del cicle de vida del certificat	17
5.3.1.	Sol·licitud del certificat	17
5.3.2.	Processament de la sol·licitud de certificat	17
5.3.3.	Expedició de certificats	17
5.3.4.	Acceptació de certificats	17
5.3.5.	Parell de claus i ús del certificat	17
5.3.6.	Renovació de certificats	18
5.3.7.	Renovació de certificats amb recanvi de claus	18
5.3.8.	Modificació de certificats	18
5.3.9.	Revocació i suspensió de certificats	18
5.3.10.	Serveis relatius a l'estat dels certificats	18
5.3.11.	Finalització de la subscripció	19
5.3.12.	Depòsit i recuperació de claus	19
5.4.	Controls operatius, de gestió i de serveis	19
5.4.1.	General	19
5.4.2.	Controls de seguretat física	19
5.4.3.	Controls procedimentals	19
5.4.4.	Controls de personal	19
5.4.5.	Processos de registre d'auditories	19
5.4.6.	Arxiu dels registres	19
5.4.7.	Canvis en les claus	20
5.4.8.	Compromís i recuperació de desastres	20
5.4.9.	Finalització de l'autoritat de certificació o de l'autoritat de registre	20
5.5.	Controls de seguretat tècnica	20

5.5.1.	Generació del parell de claus i instal·lació.....	20
5.5.2.	Protecció de la clau privada i controls d'enginyeria dels mòduls criptogràfics.....	21
5.5.3.	Altres aspectes de la gestió del parell de claus	21
5.5.4.	Dades d'activació	21
5.5.5.	Controls de seguretat dels ordinadors	21
5.5.6.	Controls de seguretat del cicle de vida.....	21
5.5.7.	Controls de seguretat del sistema	21
5.5.8.	Segellat del temps.....	21
5.6.	Perfils dels certificats, de les CRL i de l'OCSP.....	21
5.6.1.	Perfil del certificat.....	21
5.6.2.	Perfil de CRL	23
5.6.3.	Perfil d'OCSP	23
5.7.	Auditories de conformitat i altres avaluacions.....	23
5.8.	Altres qüestions empresarials i legals.....	24
5.8.1.	Honoraris	24
5.8.2.	Responsabilitat financera	24
5.8.3.	Confidencialitat de la informació empresarial.....	24
5.8.4.	Privacitat de les dades personals.....	24
5.8.5.	Drets de propietat intel·lectual.....	24
5.8.6.	Representacions i garanties.....	24
5.8.7.	Descàrrega de responsabilitats.....	24
5.8.8.	Limitació de responsabilitats	24
5.8.9.	Indemnitzacions.....	25
5.8.10.	Terme i finalització.....	25
5.8.11.	Notificacions individuals i comunicacions amb els participants.....	25
5.8.12.	Emendes.....	25
5.8.13.	Procediments per la resolució de conflictes.....	25
5.8.14.	Legislació aplicable	25
5.8.15.	Compliment amb la legislació aplicable.....	25
5.8.16.	Disposicions diverses	25
5.9.	Altres provisions	25
5.9.1.	Organitzatives	25
5.9.2.	Verificacions addicionals.....	25

5.9.3.	Discapacitats	25
5.9.4.	Termes i condicions	25
6.	Estructura per a la definició d'altres polítiques de certificació exposades en aquest document	27
6.1.	Gestió de la política de certificació	27
6.2.	Requisits addicionals.....	27
7.	ANNEX I. Història del document	28

1. Referències

1.1. Referències normatives

Els documents següents són necessaris per aplicar aquest document:

- Llei 35/2014, del 27 de novembre, de serveis de confiança electrònica.
- ETSI EN 319 401: “Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers supporting electronic signatures”.
- ETSI EN 319 411-1: “Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements”.

1.2. Referències informatives

Els documents següents no són necessaris per aplicar aquest document, però són d’ajuda per a l’usuari en relació amb cada àrea de coneixement concreta.

- Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, CA/Browser Forum.
- IETF RFC 3647: “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”.
- Guidelines for The Issuance and Management of Extended Validation Certificates v1.7.8, CA/Browser Forum.

2. Definicions, abreviatures i anotacions

2.1. Definicions

Per als objectius d'aquest document, s'apliquen els termes i les definicions proporcionades a l'ETSI EN 319 401, a l'ETSI EN 319 411-1 i a la Llei andorrana de signatura, entre d'altres:

- **Certificat qualificat andorrà:** un certificat qualificat que compleixi el que especifica la Llei 35/2014 del Principat d'Andorra.
- **Signatura electrònica qualificada/Dispositiu de creació de segells:** que compleixi el que especifica la Llei 35/2014 del Principat d'Andorra.

2.2. Abreviatures

Es tindran en compte les abreviatures següents:

- **AD-pcq-F:** Política andorrana de certificat qualificat expedit a una **persona física**.
- **AD-pcq-J:** Política andorrana de certificat qualificat expedit a una **persona jurídica**.
- **AD-pcq-Fd:** Política andorrana de certificat qualificat expedit a una **persona física** en què la clau privada i el certificat relacionat resideix en un **dispositiu qualificat** i segur de creació de signatura (DSCS).
- **AD-pcq-Jd:** Política andorrana de certificat qualificat expedit a una **persona jurídica** en què la clau privada i el certificat relacionat resideix en un **dispositiu qualificat** i segur de creació de signatura/segell qualificat (DSCS).
- **AD-pcq-W:** Política andorrana de certificat qualificat de **lloc web** expedit a una persona física o jurídica i que vincula el lloc web amb aquesta persona.
- **DSCS:** Dispositiu segur i qualificat de creació de signatures/segells electrònics qualificats.
- **PSC:** Prestador de serveis de confiança.

2.3. Anotacions

Els requisits identificats en aquest document inclouen:

- a. Requisits aplicables a qualsevol política de certificació. Aquests requisits estan indicats entre parèntesis sense cap marca addicional.
- b. Requisits aplicables sota certes circumstàncies. Aquests requisits estan indicats entre parèntesis marcats amb un "(CONDICIONAL)";

- c. Requisits aplicables als serveis indicats sota la política de certificació aplicable. Aquests tipus de requisits estan indicats entre parèntesis marcats amb l'indicador de política de certificació aplicable: "(AD-pcq-J)", "(AD-pcq-F)", "(AD-pcq-Jd)", "(AD-pcq-Fd)" i/o "(AD-pcq-W)".

3. Conceptes generals

3.1. Conceptualització dels requisits generals de les polítiques de certificació

S'ha d'aplicar la clàusula 4.1 de l'ETSI EN 319 411-1.

3.2. Política de certificació i Declaració de pràctiques de certificació

3.2.1. Visió general

S'han d'aplicar les explicacions identificades a la clàusula 4.2.1 de l'ETSI EN 319 411-1.

3.2.2. Propòsit

S'han d'aplicar les explicacions identificades a la clàusula 4.2.2 de l'ETSI EN 319 411-1.

3.2.3. Nivell d'especificitat

S'han d'aplicar les línies mestres identificades a la clàusula 4.2.3 de l'ETSI EN 319 411-1.

3.2.4. Aproximació

S'han d'aplicar les línies mestres identificades a la clàusula 4.2.4 de l'ETSI EN 319 411-1.

3.2.5. Política de certificació

Aquest document defineix cinc polítiques de certificació i assigna un identificador, anomenat *identificador de polítiques andorranes relatives als certificats qualificats*, a cada una d'aquestes polítiques de certificació. Aquests identificadors es defineixen a la clàusula 4.3.

Les polítiques de certificació es basen en les polítiques següents, especificades a l'ETSI EN 319 411-1:

- Política de certificació normalitzada (NCP);
- Política de certificació normalitzada millorada (NCP+); i
- Política de validació millorada de certificats (EVCP).

Les cinc polítiques andorranes relatives als certificats qualificats són:

- Una política per a certificats qualificats expedits a persones físiques (AD-pcq-F), que ofereix el nivell de qualitat definit en la llei andorrana per a certificats qualificats.**
 - Els requisits per a aquest certificat inclouen tots els de la política NCP, a més de les exigències addicionals adequades per incloure l'expedició i la gestió dels certificats qualificats andorrans, tal com s'especifica en els articles 5 i 6 de la Llei 35/2014.
 - Si la implementació d'aquesta política per part del prestador de serveis de confiança exigeix un dispositiu criptogràfic segur, els requisits per a la política (AD-pcq-F) influiran en tots els requisits exigits per una política NCP+, més les provisions

addicionals adients per admetre l'expedició i la gestió de certificats qualificats a Andorra, d'acord amb el que s'especifica en els articles 9, 10, 11 i 12 de la Llei 35/2014.

b. Una política per a certificats qualificats emesos a persones jurídiques (AD-pcq-J), que ofereix el nivell de qualitat definit a la llei andorrana per a certificats qualificats.

- Els requisits per a la política AD-pcq-J inclouen totes les exigències de les polítiques NCP més les provisions addicionals adients per incloure l'expedició i la gestió de certificats qualificats a Andorra, d'acord amb el que s'especifica en els articles 7 i 8 de la Llei 35/2014.
- Si la implementació d'aquesta política per part del prestador de serveis de confiança exigeix un dispositiu criptogràfic segur, els requisits relatius a la política AD-pcq-F influiran en tots els requisits exigits per una política NCP+, a més de les provisions addicionals adients per admetre l'expedició i la gestió de certificats qualificats a Andorra, d'acord amb el que s'especifica en els articles 9, 10, 11 i 12 de la Llei 35/2014.

c. Una política (AD-pcq-Fd) per a certificats qualificats andorrans emesos a persones físiques, que ofereixen el nivell de qualitat definit en l'article 3.37 de la Llei 35/2014, i que exigeixen l'ús d'un dispositiu qualificat i segur de creació de signatures (DSCS). Aquestes polítiques requereixen que la clau privada relacionada amb la clau pública certificada es trobi al DSCS.

- Els requisits per a la política AD-pcq-Fd inclouen totes les exigències de les polítiques AD-pcq-F (incloent tots els requisits de la política NCP+, més les provisions addicionals adients per admetre l'expedició i la gestió de certificats qualificats a Andorra, d'acord amb el que s'especifica en els articles 9, 10, 11 i 12 de la Llei 35/2014, incloent el que s'especifica a la provisió dels DSCS).

d. Una política (AD-pcq-Jd) per a certificats qualificats andorrans emesos a persones jurídiques, que ofereixen el nivell de qualitat definit en l'article 3.29 de la Llei 35/2014 per a aquest tipus de certificat, i que exigeixen l'ús d'un dispositiu qualificat i segur de creació de segells (DSCS). Aquestes polítiques requereixen que la clau privada relacionada amb la clau pública certificada es trobi al DSCS.

- Els requisits per a la política AD-pcq-Jd inclouen totes les exigències de les polítiques AD-pcq-J (incloent tots els requisits de les polítiques NCP+), més les provisions addicionals adients per admetre l'expedició i la gestió de certificats qualificats a Andorra, d'acord amb el que s'especifica en els articles 9, 10, 11 i 12 de la Llei 35/2014, incloent les que s'especifiquen a la provisió dels DSCS.

e. Una política per a certificat qualificat de lloc web (AD-pcq-W), que ofereix el nivell de qualitat definit en l'article 3.3 de la Llei 35/2014 per a aquest tipus de certificats (s'exigeixi o no l'ús d'un dispositiu criptogràfic segur), emprat per suportar l'autenticació del lloc web.

- Quan el certificat s'expedeixi a una persona jurídica, els requisits per a la política AD-pcq-W inclouran tots els requisits de la política EVCP, a més de les provisions

addicionals adients per admetre l'expedició i la gestió de certificats qualificats a Andorra, d'acord amb el que s'especifica en l'article 19 de la Llei 35/2014.

- Quan el certificat s'expedeixi a una persona física, els requisits per a la política AD-pcq-W inclouran tots els requisits de la política NCP, a més de les provisions addicionals adients per suportar l'expedició i la gestió de certificats qualificats a Andorra, d'acord amb el que s'especifica en l'article 19 de la Llei 35/2014.

3.3. Altres declaracions dels proveïdors de serveis de confiança

Hauran d'aplicar-se les directrius de la clàusula 4.3 de l'ETSI EN 319 411-1.

3.4. Serveis de certificació

Per al servei d'expedició de certificats qualificats cal aplicar-hi les directrius de la clàusula 4.4 de l'ETSI EN 319 411-1.

4. Provisions generals sobre la Declaració de pràctiques de certificació i les polítiques de certificació

4.1. Requisits generals

En línies generals, aquest document té una estructura alineada amb l'IETF RFC 3647 per ajudar els prestadors de serveis de confiança a aplicar aquestes exigències a les seves pròpies polítiques i pràctiques.

Hauran d'aplicar-s'hi els requisits generals especificats a la clàusula 5.1 de ETSI EN 319 411-1.

- a) (AD-pcq-F) i (AD-pcq-J) (CONDICIONAL):
 - i. Si als termes i a les condicions del prestador de serveis de confiança no se'ls exigeix un dispositiu criptogràfic segur, s'hauran d'aplicar tots els requisits definits per NCP a l'ETSI EN 319 411-1. Si un requisit per NCP és definit de manera diferent per les persones físiques que per les persones jurídiques, aquesta exigència s'haurà d'aplicar, consegüentment, a AD-pcq-F i a AD-pcq-J.
 - ii. Si als termes i a les condicions del prestador de serveis de confiança se'ls exigeix un dispositiu criptogràfic segur, s'hauran d'aplicar tots els requisits definits per NCP+ a l'ETSI EN 319 411-1. Si un requisit per NCP és definit de manera diferent per les persones físiques que per les persones jurídiques, aquesta exigència s'haurà d'aplicar, consegüentment, a AD-pcq-F i a AD-pcq-J.
- b) (AD-pcq-W) (CONDICIONAL):
 - i. Si el certificat s'expedeix a una persona jurídica, s'hi hauran d'aplicar tots els requisits definits a l'ETSI EN 319 411-1 per EVCP.
 - ii. Si el certificat s'expedeix a una persona física, s'hi hauran d'aplicar tots els requisits definits a l'ETSI EN 319 411-1 per NCP.
- c) (AD-pcq-Fd): s'hi hauran d'aplicar tots els requisits definits per AD-pcq-F, incloent totes les exigències definides a l'ETSI EN 319 411-1. Si un requisit per NCP+ és definit de manera diferent per les persones físiques que per les persones jurídiques, a l'AD-pcq-Fd s'hi haurà d'aplicar el requeriment per a la persona física.
- d) (AD-pcq-Jd): s'hi hauran d'aplicar tots els requisits definits per AD-pcq-J, incloent totes les exigències definides a l'ETSI EN 319 411-1 per les polítiques NCP+. Si un requisit per NCP+ és definit de manera diferent per les persones físiques que per les persones jurídiques, a AD-pcq-Jd s'hi haurà d'aplicar el requeriment per a la persona jurídica.

4.2. Requisits de la Declaració de pràctiques de certificació

S'hi han d'aplicar els requisits descrits en la clàusula 5.2 de l'ETSI EN 319 411-1.

4.3. Denominació de les polítiques de certificació i identificació

- a) **AD-pcq-F:** 2.16.20.2.2.194112.1.0
- b) **AD-pcq-J:** 2.16.20.2.2.194112.1.1
- c) **AD-pcq-Fd:** 2.16.20.2.2.194112.1.2
- d) **AD-pcq-Jd:** 2.16.20.2.2.194112.1.3
- e) **AD-pcq-W:** 2.16.20.2.2.194112.1.4

4.4. Participants PKI

4.4.1. Autoritat de certificació

S'hi apliquen els conceptes descrits a la clàusula 5.4.1 de l'ETSI EN 319 411-1.

NOTA: L'article 32.1 de la Llei 35/2014, del 27 de novembre, de serveis de confiança electrònica, aborda la responsabilitat dels prestadors de serveis de confiança i estableix que: "són responsables dels danys i perjudicis causats a qualsevol personal, inclòs el lucre cessant, per raó de l'incompliment de les obligacions que estableix aquesta Llei, llevat que puguin provar que han actuat amb la diligència deguda."

4.4.2. Subscriptor i subjecte

S'hi aplica la clàusula 5.4.2 de l'ETSI EN 319 411-1.

4.4.3. Altres

S'hi apliquen les directrius identificades a la clàusula 5.4.3 de l'ETSI EN 319 411-1.

4.5. Ús dels certificats

4.5.1. AD-pcq-F

Els certificats emesos sota aquests requisits inclouen la signatura electrònica avançada basada en un certificat qualificat definit en els articles 3.36 i 6 de la Llei 35/2014, del 27 de novembre, de serveis de confiança electrònica.

4.5.2. AD-pcq-J

Els certificats emesos sota aquests requisits inclouen el segell electrònic avançat basat en un certificat qualificat definit en els articles 3.28 i 8 de la Llei 35/2014, del 27 de novembre, de serveis de confiança electrònica, al Principat d'Andorra.

4.5.3. AD-pcq-Fd

Els certificats emesos sota aquests requisits inclouen la signatura electrònica qualificada tal com es defineix en els articles 3.37 i 5.3 de la Llei 35/2014, del 27 de novembre, de serveis de confiança electrònica.

4.5.4. AD-pcq-Jd

Els certificats emesos sota aquests requisits inclouen el segell electrònic qualificat tal com es defineix en els articles 3.29 i 7.3 de la Llei 35/2014, del 27 de novembre, de serveis de confiança electrònica.

4.5.5. AD-pcq-W

Els certificats emesos sota aquests requisits inclouen l'autenticació de llocs web basada en un certificat qualificat definit en els articles 3.3 i 19 de la Llei 35/2014, del 27 de novembre, de serveis de confiança electrònica.

Els certificats emesos sota aquests requisits inclouen l'exigència de certificats EV, el propòsit dels quals es descriu en la clàusula 5.5 de l'ETSI EN 319 411-1. Addicionalment, els certificats qualificats andorrans emesos sota aquesta política podrien ser emprats per proporcionar els mitjans amb els quals un visitant a un lloc web concret tingui la certesa i la seguretat que darrere d'aquest lloc web hi ha una entitat autèntica i legítima.

5. Pràctiques dels proveïdors de serveis de confiança

5.1. Publicació i responsabilitats dels dipòsits

S'han d'aplicar els requisits descrits en la clàusula 6.1 de l'ETSI EN 319 411-1.

5.2. Identificació i autenticació

5.2.1. Denominació

S'han d'aplicar els requisits descrits en la clàusula 6.2.1 de l'ETSI EN 319 411-1.

Consulteu també la clàusula 5.6.1 d'aquest document.

5.2.2. Validació inicial de la identitat

S'hi han d'aplicar els requisits identificats en la clàusula 6.2.2. de l'ETSI EN 319 411-1.

Adicionalment, s'hi apliquen els requisits específics següents:

Registre

1. (AD-pcq-F) i (AD-pcq-Fd): L'article 26.2 de la Llei 35/2014, del 27 de novembre, de serveis de confiança electrònica, estableix que: "el prestador de serveis de confiança electrònica qualificat ha de verificar de forma fefaent la identitat i, si escau, qualsevol altre atribut específic de la persona física a la qual expedeix el certificat electrònic qualificat, per mitjà de l'exhibició dels documents públics o privats que els acreditin de forma suficient. Aquesta informació ha de ser verificada pel prestador de serveis qualificat o per un tercer autoritzat que actuï sota la responsabilitat del prestador de serveis qualificats:
 - i. A través de la presència física d'aquesta persona, o
 - ii. A distància, utilitzant altres certificats electrònics qualificats emesos per un prestador de serveis qualificat."

D'altra banda, l'article 26.3 de la Llei 35/2014, del 27 de novembre, de serveis de confiança electrònica, estableix que en el cas de: "certificats electrònics emesos a persones físiques però que tenen una vinculació amb una organització, entitat, institució, societat o un altra persona jurídica, els prestadors de serveis de confiança han de comprovar, a més a més de la identitat del sol·licitant i de la persona identificada al certificat electrònic, les dades relatives a la constitució i la personalitat jurídica de l'entitat, o a l'extensió i la vigència de les facultats o els poders de representació del sol·licitant, mitjançant els documents públics que els acreditin de forma fefaent o la consulta al registre públic pertinent, quan es tracti de dades que han de figurar-hi."

2. (AD-pcq-J) i (AD-pcq-Jd): L'article 26.2 de la Llei 35/2014, del 27 de novembre, de serveis de confiança electrònica, estableix que: "el prestador de serveis de confiança electrònica

qualificat ha de verificar de forma fefaent la identitat i, si escau, qualsevol altre atribut específic de la persona jurídica a la qual expedeix el certificat electrònic qualificat, per mitjà de l'exhibició dels documents públics o privats que els acreditin de forma suficient. Aquesta informació ha de ser verificada pel prestador de serveis qualificat o per un tercer autoritzat que actuï sota la responsabilitat del prestador de serveis qualificats:

- i. A través de la presència física d'un representant autoritzat de la persona jurídica, o
 - ii. A distància, utilitzant altres certificats electrònics qualificats emesos per un prestador de serveis qualificat.”
3. (AD-pcq-W) (CONDICIONAL):
- i. Si el subscriptor és una persona física, la seva identitat i el vincle amb el nom del domini a certificar i, si és aplicable, qualsevol atribut específic de la persona serà verificat de la mateixa manera que en el punt anterior 1).
 - ii. Si el subscriptor és una persona jurídica, la seva identitat i el vincle amb el nom del domini a certificar i, si és aplicable, qualsevol atribut específic de la persona serà verificat de la mateixa manera que en el punt anterior 2).

Finalment, l'article 26.4 de la Llei 35/2014, del 27 de novembre, de serveis de confiança electrònica, estableix que no caldrà aplicar els requeriments de verificació de la identitat descrits anteriorment quan: “es tracti d'un sol·licitant la identitat i les circumstàncies del qual siguin conegudes pel prestador de serveis de confiança electrònica, a causa d'una relació preexistent en la qual hagi emprat els mitjans d'identificació que hi són establerts, si no han passat tres anys des de la identificació i si es té constància que totes les dades són vigents.”

5.2.3. Identificació i autenticació per a sol·licituds de reentrada de claus

S'han d'aplicar els requisits descrits en la clàusula 6.2.3 de l'ETSI EN 319 411-1.

5.2.4. Identificació i autenticació per a sol·licituds de revocació

S'han d'aplicar els requisits descrits en la clàusula 6.2.4 de l'ETSI EN 319 411-1.

5.3. Requisits operatius del cicle de vida del certificat

5.3.1. Sol·licitud del certificat

NOTA: Consulteu la clàusula 6.2.2 relativa a la verificació de la identitat.

S'han d'aplicar els requisits descrits en la clàusula 6.3.1 de l'ETSI EN 319 411-1.

5.3.2. Processament de la sol·licitud de certificat

S'han d'aplicar els requisits descrits en la clàusula 6.3.2 de l'ETSI EN 319 411-1.

5.3.3. Expedició de certificats

S'han d'aplicar els requisits descrits en la clàusula 6.3.3 de l'ETSI EN 319 411-1.

5.3.4. Acceptació de certificats

S'han d'aplicar els requisits descrits en la clàusula 6.3.4 de l'ETSI EN 319 411-1.

5.3.5. Parell de claus i ús del certificat

S'han d'aplicar les obligacions generals descrites en la clàusula 6.3.5 de l'ETSI EN 319 411-1.

Adicionalment:

- a. (AD-pcq-Fd) i (AD-pcq-Jd) (CONDICIONAL): Si el prestador de serveis de confiança gestiona el dispositiu segur de creació de signatura pel subjecte:
 - i. La clau privada no s'ha d'emprar per signar, amb l'excepció de les signatures efectuades dins del DSCS.
 - ii. (AD-pcq-Fd): la clau privada del subjecte s'ha d'emprar sota el control únic del subjecte.
 - iii. (AD-pcq-Jd): la clau privada del subjecte s'ha d'emprar sota el control del subjecte.
 - iv. (AD-pcq-Fd): el parell de claus del subjecte s'ha d'emprar únicament per a signatures electròniques.
 - v. (AD-pcq-Jd): el parell de claus del subjecte s'ha d'emprar únicament per a segells electrònics.
- b. Les obligacions del subscriptor (vegeu la clàusula 5.3.4) o les obligacions del prestador de serveis de confiança que gestiona la clau en representació del subjecte, han de requerir que:
 - i. (AD-pcq-F) i (AD-pcq-Fd): La clau privada del subjecte es mantingui (o sigui emprada) sota el control únic del subjecte.
 - ii. (AD-pcq-J) i (AD-pcq-Jd): La clau privada del subjecte s'empri sota el control del subjecte.
 - iii. (AD-pcq-Fd) i (AD-pcq-Jd): Les signatures digitals únicament es creïn en un dispositiu DSCS.
- c. Les obligacions del subscriptor (vegeu la clàusula 5.3.4) o les obligacions del prestador de serveis de confiança derivades de la gestió de la clau en representació del subjecte haurien de recomanar que:

- i. (AD-pcq-F) i (AD-pcq-Fd): el parell de claus del subjecte únicament s'emprin per a signatures electròniques.
 - ii. (AD-pcq-J) i (AD-pcq-Jd): el parell de claus del subjecte únicament s'emprin per a segells electrònics.
- d. Notificació a les parts que confien:
- i. La notificació a les parts que confien ha d'informar que, com a part de les condicions per a que un certificat sigui fiable com un certificat qualificat a Andorra, s'ha d'identificar amb una ancla de confiança per a la verificació del certificat amb un identificador en una entrada apropiada a la (TL) llista de confiança de prestadors qualificats a l'Estat d'Andorra.

5.3.6. Renovació de certificats

S'han d'aplicar els requisits descrits en la clàusula 6.3.6 de l'ETSI EN 319 411-1.

5.3.7. Renovació de certificats amb recanvi de claus

NOTA: Consulteu la clàusula 5.2.3.

5.3.8. Modificació de certificats

S'han d'aplicar els requisits descrits en la clàusula 6.3.8 de l'ETSI EN 319 411-1.

5.3.9. Revocació i suspensió de certificats

S'han d'aplicar els requisits descrits en la clàusula 6.3.9 de l'ETSI EN 319 411-1.

5.3.10. Serveis relatius a l'estat dels certificats

S'han d'aplicar els requisits descrits en la clàusula 6.3.10 de l'ETSI EN 319 411-1.

Adicionalment, s'hi apliquen els requisits següents:

NOTA 1: L'article 26.7 de la Llei 35/2014, del 27 de novembre, de serveis de confiança electrònica, estableix que: "els prestadors de serveis de confiança electrònica qualificats que expedeixin certificats electrònics qualificats, han de proporcionar a qualsevol part usuària informació sobre l'estat de validesa o revocació dels certificats electrònics qualificats expedits per ells. Aquesta informació haurà d'estar disponible en qualsevol moment almenys per cada certificat electrònic en una forma automatitzada que sigui gratuïta i eficient."

Estat del procés de revocació

- a. La informació relativa a l'estat del procés de revocació ha d'estar disponible més enllà del període de validesa del certificat.
- NOTA 2: L'obligació d'incloure llistes de revocació OCSP prevista a l'ETSI EN 319 411-1 no és aplicable un cop hagi expirat el certificat.

- b. El prestador de serveis de confiança ha de documentar de manera precisa a la seva DPC i en els seus termes i condicions com dona compliment al requisit a), incloent la finalització del servei del prestador (vegeu la clàusula 5.4.9).

NOTA 3: Hi ha una planificació per dur a terme més activitats d'estandardització per tractar l'estat del procés de revocació més enllà del període de validesa del certificat.

5.3.11. Finalització de la subscripció

Sense requisits.

5.3.12. Depòsit i recuperació de claus

S'han d'aplicar els requisits descrits en la clàusula 6.3.12 de l'ETSI EN 319 411-1.

5.4. Controls operatius, de gestió i de serveis

5.4.1. General

S'han d'aplicar els requisits descrits en la clàusula 6.4.1 de l'ETSI EN 319 411-1.

5.4.2. Controls de seguretat física

S'han d'aplicar els requisits descrits en la clàusula 6.4.2 de l'ETSI EN 319 411-1.

5.4.3. Controls procedimentals

S'han d'aplicar els requisits descrits en la clàusula 6.4.3 de l'ETSI EN 319 411-1.

5.4.4. Controls de personal

S'han d'aplicar els requisits descrits en la clàusula 6.4.4 de l'ETSI EN 319 411-1.

5.4.5. Processos de registre d'auditories

S'han d'aplicar els requisits descrits en la clàusula 6.4.5 de l'ETSI EN 319 411-1.

Adicionalment, per al registre de la informació relativa als certificats qualificats del Principat d'Andorra s'apliquen els requisits següents:

General

- a. S'ha de mantenir la informació necessària per complir amb els requisits legals més enllà de la finalització dels serveis del prestador (vegeu la clàusula 5.4.9).

NOTA: L'apartat e) de l'article 26.1 de la Llei 35/2014, del 27 de novembre, de serveis de confiança electrònica, estableix que els prestadors de serveis de confiança qualificats "han de registrar, durant un període mínim de quinze anys comptadors des de l'acabament de la vigència del servei prestat, tota la informació pertinent referent a les dades que hagin generat i rebut, en particular les que serveixin de prova en els procediments legals. Aquesta activitat de registre es pot fer per mitjans electrònics."

5.4.6. Arxiu dels registres

S'han d'aplicar els requisits descrits en la clàusula 6.4.6 de l'ETSI EN 319 411-1.

5.4.7. Canvis en les claus

Sense requisits.

5.4.8. Compromís i recuperació de desastres

S'han d'aplicar els requisits descrits en la clàusula 6.4.8 de l'ETSI EN 319 411-1.

5.4.9. Finalització de l'autoritat de certificació o de l'autoritat de registre

S'han d'aplicar els requisits descrits en la clàusula 6.4.9 de l'ETSI EN 319 411-1.

5.5. Controls de seguretat tècnica

5.5.1. Generació del parell de claus i instal·lació

S'han d'aplicar els requisits descrits en la clàusula 6.5.1 de l'ETSI EN 319 411-1.

Adicionalment:

Subministrament de dispositius al subjecte

- a) (AD-pcq-Fd) i (AD-pcq-Jd): Malgrat que el dispositiu hagi estat preparat (o no) pel prestador, ha de verificar que estigui certificat com un DSCS.

NOTA: L'article 11.1 de la Llei 35/2014, del 27 de novembre, de serveis de confiança electrònica, estableix que: "els dispositius de creació de signatures electròniques qualificades i de segells electrònics qualificats han de ser certificats pels organismes públics o privats designats pel Govern, sempre que hagin estat sotmesos a un procés d'avaluació de la seguretat dut a terme de conformitat amb les normes per a l'avaluació de la seguretat dels productes de tecnologia de la informació."

- b) (AD-pcq-Fd) i (AD-pcq-Jd) (CONDICIONAL):
- i. Si el dispositiu és gestionat per un tercer prestador en representació del subjecte, que no és el mateix prestador que emet el certificat, el prestador que expedeixi el certificat ha de verificar que aquest tercer prestador estigui complint amb els requisits adequats en termes de qualificació.
 - ii. El procés de sol·licitud de certificats ha d'assegurar que la clau pública a certificar prové d'un parell de claus generades pel DSCS.
 - iii. Si el parell de claus del subjecte és creat per un prestador i importat a un DSCS emprat per a la creació de signatures/segells, aquest prestador ha d'acomplir amb les assumpcions de l'entorn i amb els objectius de seguretat del dispositiu certificat (DSCS emprat per a la creació de claus i un DSCS utilitzat per a la creació de signatures/segells).
 - iv. Si la clau privada del subjecte es mou entre dispositius, s'han de determinar les vulnerabilitats potencials i adequar els mecanismes implementats amb l'objectiu de mitigar qualsevol vulnerabilitat.

- c) (AD-pcq-Fd) i (AD-pcq-Jd): El prestador de serveis de confiança ha d'adoptar les mesures apropiades en cas de modificació de l'estat de certificació del DSCS fins al final del període de validesa del certificat.
- d) (AD-pcq-Fd) i (AD-pcq-Jd): El prestador de serveis de confiança ha de documentar a la seva DPC les mesures adoptades en cas de modificació de l'estat del DSCS produïda amb anterioritat al final del període de validesa del certificat.

5.5.2. Protecció de la clau privada i controls d'enginyeria dels mòduls criptogràfics

S'han d'aplicar els requisits descrits en la clàusula 6.5.2 de l'ETSI EN 319 411-1.

5.5.3. Altres aspectes de la gestió del parell de claus

S'han d'aplicar els requisits descrits en la clàusula 6.5.3 de ETSI EN 319 411-1.

5.5.4. Dades d'activació

S'han d'aplicar els requisits descrits en la clàusula 6.5.4 de l'ETSI EN 319 411-1.

5.5.5. Controls de seguretat dels ordinadors

S'han d'aplicar els requisits descrits en la clàusula 6.5.5 de l'ETSI EN 319 411-1.

5.5.6. Controls de seguretat del cicle de vida

S'han d'aplicar els requisits descrits en la clàusula 6.5.6 de l'ETSI EN 319 411-1.

5.5.7. Controls de seguretat del sistema

S'han d'aplicar els requisits descrits en la clàusula 6.5.7 de l'ETSI EN 319 411-1.

5.5.8. Segellat del temps

S'han d'aplicar els requisits descrits en la clàusula 6.5.8 de l'ETSI EN 319 411-1.

5.6. Perfils dels certificats, de les CRL i de l'OCSP

5.6.1. Perfil del certificat

S'han d'aplicar els requisits especificats en la clàusula 6.6.1 de l'ETSI EN 319 411-1.

Adicionalment, s'apliquen els requisits següents:

Creació de certificats

- a. El certificat ha d'incloure tots els qcStatements adequats, de la manera següent:

Indicació de certificat emès com a qualificat (id-AD-cq)	2.16.20.2.2.1862.1.1
Indicació de limitació econòmica (QcLimitValue)	0.4.0.1862.1.2
Indicació del període de retenció (QcRetentionPeriod)	0.4.0.1862.1.3
Indicació d'ús exclusiu amb DSCS (id-AD-dscs)	2.16.20.2.2.1862.1.4
Indicació d'ubicació PDS (QcPDS)	0.4.0.1862.1.5
Indicació del tipus de certificat (id-AD-t):	2.16.20.2.2.1862.1.6

1. Emissió de signatura-e (id-AD-tsign)	2.16.20.2.2.1862.1.6.1
2. Emissió d'un segell-e (id-AD-tseg)	2.16.20.2.2.1862.1.6.2
3. Emissió d'una autenticació web (id-AD-tweb)	2.16.20.2.2.1862.1.6.3

- b. (AD-pcq-Fd) i (AD-pcq-Jd): El certificat ha d'incloure la *qcStatement* per DSCS:

Indicació d'ús exclusiu amb DSCS (id-AD-dscs)	2.16.20.2.2.1862.1.4
---	----------------------

- c. La *qcStatement* per DSCS (id-AD-dscs) no s'ha d'incloure en els certificats que no siguin emesos d'acord amb els requisits de (AD-pcq-Fd) o (AD-pcq-Jd).
- d. (AD-pcq-F): El certificat ha d'incloure, com a mínim, una de les identifications de les polítiques següents:
- i. La política d'identificació definida a l'apartat a) de la clàusula 4.3, i/o
 - ii. Un OID assignat pel prestador (o qualsevol tercer pertinent que hi estigui interessat) amb la política de certificació aplicada per l'emissió de certificats.
- e. (AD-pcq-J): El certificat ha d'incloure, com a mínim, una de les identifications de les polítiques següents:
- i. La política d'identificació definida a l'apartat b) de la clàusula 4.3, i/o
 - ii. Un OID assignat pel prestador (o qualsevol tercer pertinent que hi estigui interessat) amb la política de certificació aplicada per l'emissió de certificats.
- f. (AD-pcq-Fd): El certificat ha d'incloure, com a mínim, una de les identifications de les polítiques següents:
- i. La política d'identificació definida a l'apartat c) de la clàusula 4.3, i/o
 - ii. Un OID assignat pel prestador (o qualsevol tercer pertinent que hi estigui interessat) amb la política de certificació aplicada per l'emissió de certificats.
- g. (AD-pcq-Jd): El certificat haurà d'incloure, com a mínim, una de les identifications de les polítiques següents:
- i. La política d'identificació definida a l'apartat d) de la clàusula 4.3, i/o
 - ii. Un OID assignat pel prestador (o qualsevol tercer pertinent que hi estigui interessat) amb la política de certificació aplicada per l'emissió de certificats.
- h. (AD-pcq-W): El certificat haurà d'incloure, com a mínim, una de les identifications de les polítiques següents:
- i. La política d'identificació definida a l'apartat e) de la clàusula 4.3, i/o
 - ii. Un OID assignat pel prestador (o qualsevol tercer pertinent que hi estigui interessat) amb la política de certificació aplicada per l'emissió de certificats.
- i. (AD-pcq-W) (CONDICIONAL): Addicionalment a l'identificador de política requerit al punt h), si el certificat s'expedeix a una persona jurídica, s'hi podria incloure l'identificador especificat a l'EVC.

- j. (AD-pcq-W) (CONDICIONAL): Addicionalment a l'identificador requerit al punt h), si el certificat s'expedeix a una persona física, s'hi podria incloure l'identificador de la política NCP, tal com es descriu a l'ETSI EN 319 411-1.
- k. (CONDICIONAL) Si el certificat conté únicament un OID assignat per un prestador, la política de certificació s'ha d'elaborar d'acord amb el que s'estableix a la clàusula 6. En concret, s'ha d'identificar clarament quina de les polítiques incloses en aquest document adopta com a base.

NOTA: Les raons per emetre una política de certificació s'exposen a la clàusula 3.

5.6.2. Perfil de CRL

S'han d'aplicar els requisits especificats en la clàusula 6.6.2 de l'ETSI EN 319 411-1.

5.6.3. Perfil d'OCSP

S'han d'aplicar els requisits especificats en la clàusula 6.6.3 de l'ETSI EN 319 411-1.

5.7. Auditories de conformitat i altres avaluacions

S'han d'aplicar els requisits especificats en la clàusula 6.7 de l'ETSI EN 319 411-1.

5.8. Altres qüestions empresarials i legals

5.8.1. Honoraris

Els requeriments d'aquesta política no tenen perquè implicar qualsevol limitació en el cobrament pels serveis del prestador.

5.8.2. Responsabilitat financera

S'han d'aplicar els requisits especificats a la clàusula 6.8.2 de l'ETSI EN 319 411-1

5.8.3. Confidencialitat de la informació empresarial

Sense requeriments per part de la política.

5.8.4. Privacitat de les dades personals

S'han d'aplicar requisits especificats a la clàusula 6.8.4 de l'ETSI EN 319 411-1 i els requeriments expressats en l'article 28 de la Llei 35/2014, del 27 de novembre, de serveis de confiança electrònica, relatius a la protecció de les dades personals.

5.8.5. Drets de propietat intel·lectual

Sense requeriments per part de la política.

5.8.6. Representacions i garanties

S'han d'aplicar les obligacions generals establertes a la clàusula 6.8.6 de l'ETSI EN 319 411-1. Addicionalment:

- a. (AD-pcq-F) i (AD-pcq-J) (CONDICIONAL):
 - i. Si els termes i les condicions del prestador NO EXIGEIXEN un dispositiu criptogràfic segur, s'han d'aplicar totes les obligacions especificades a l'ETSI EN 319 411-1 per la política normalitzada de certificació (NCP).
 - ii. Si els termes i condicions del prestador EXIGEIXEN un dispositiu criptogràfic segur, s'han d'aplicar totes les obligacions especificades a l'ETSI EN 319 411-1 per la política normalitzada i estesa de certificació (NCP+).
- b. (AD-pcq-Fd) i (AD-pcq-Jd): s'han d'aplicar totes les obligacions especificades a l'ETSI EN 319 411-1 per la política normalitzada i estesa de certificació (NCP+).
- c. (AD-pcq-W): s'han d'aplicar totes les obligacions especificades a l'ETSI EN 319 411-1 per EVCP.

5.8.7. Descàrrega de responsabilitats

Consulteu la clàusula [5.8.6](#).

Consulteu també la clàusula A.2 d'ETSI EN 411-1 per a informació addicional.

5.8.8. Limitació de responsabilitats

S'han d'aplicar els requisits especificats a la clàusula 6.8.8 de l'ETSI EN 319 411-1.

5.8.9. Indemnitzacions

Sense requeriments per part de la política.

5.8.10. Terme i finalització

Sense requeriments per part de la política.

5.8.11. Notificacions individuals i comunicacions amb els participants

Sense requeriments per part de la política.

5.8.12. Emendes

Sense requeriments per part de la política.

5.8.13. Procediments per la resolució de conflictes

S'han d'aplicar els requisits especificats a la clàusula 6.8.13 de l'ETSI EN 319 411-1.

5.8.14. Legislació aplicable

Llei 35/2014, del 27 de novembre, de serveis de confiança electrònica.

5.8.15. Compliment amb la legislació aplicable

S'han d'aplicar els requisits especificats a la clàusula 6.8.15 de l'ETSI EN 319 411-1.

5.8.16. Disposicions diverses

Sense requeriments per part de la política.

5.9. Altres provisions

5.9.1. Organitzatives

S'han d'aplicar els requisits especificats a la clàusula 6.9.1 de l'ETSI EN 319 411-1.

5.9.2. Verificacions addicionals

S'han d'aplicar els requisits especificats a la clàusula 6.9.2 de l'ETSI EN 319 411-1.

5.9.3. Discapacitats

S'han d'aplicar els requisits especificats a la clàusula 6.9.3 de l'ETSI EN 319 411-1.

5.9.4. Termes i condicions

S'han d'aplicar els requisits especificats a la clàusula 6.9.4 de l'ETSI EN 319 411-1.

Adicionalment, s'hi apliquen els requisits específics següents:

- a. La política de certificació ha d'incloure una declaració clara en què s'indiqui que la política esmentada és per a certificats qualificats del Principat d'Andorra i si requereix l'ús d'un DSCS.
- b. S'hi ha d'incloure un text divulgatiu del servei (PDS).
- c. El text divulgatiu (PDS) del servei s'ha d'estructurar segons el que s'estableix a l'annex A de l'ETSI EN 319 411-1.

NOTA 1: Aquest text divulgatiu (PDS) del servei pot ajudar el prestador a respondre a requeriments i aspectes reguladors, particularment els que es relacionen amb la implementació en el consumidor.

6. Estructura per a la definició d'altres polítiques de certificació exposades en aquest document

6.1. Gestió de la política de certificació

S'han d'aplicar els requisits especificats a la clàusula 7.1 de l'ETSI EN 319 411-1.

A més, s'hi han d'aplicar els requisits específics següents:

- a) La política de certificació ha d'incorporar, o limitar, tots els requisits addicionals identificats a les clàusules 4 i 5 d'aquest document, com una qüestió apropiada per a l'ús, i hi ha d'incloure els requisits de la política de certificació adequada, de la manera com es defineix en aquest document.

NOTA: la clàusula 3.4. proporciona les bases per redactar una política de certificació.

6.2. Requisits addicionals

S'han d'aplicar els requisits identificats a la clàusula 7.2. de l'ETSI EN 319 411-1.

7. ANNEX I. Història del document

Període	Versió	Modificació
Agosto del 2022	V1.0	Versió inicial