DECLARACIÓ
DE PRÀCTIQUES
DE CERTIFICACIÓ
AC CAMERFIRMA S.A.

Camerfirma
Certificado Digital

Com Prestador de Serveis de Certificació Digital del

GOVERN D'ANDORRA

Govern d'Andorra

Versió 1.0

Idioma: **Català**

Data: Octubre 2013

Octubre 2013	V.1.0	Versió Inicial

Contingut

1. Introducció

1.1. Consideració Inicial

Per no haver-hi una definició taxativa dels conceptes de Declaració de Practiques de Certificació i Política de Certificació i a causa d'algunes confusions formades, Camerfirma entén que és necessari informar de la seua posició enfront d'estos conceptes.

Política de Certificació (CP) és el conjunt de regles que defineixen l'aplicabilitat d'un **certificat** en una comunitat i/o en alguna aplicació, amb requisits de seguretat i utilització comuna, és a dir, en general una Política de Certificació ha de definir l'aplicabilitat de tipus de certificat per a determinades aplicacions que exigeixen els mateixos requisits de seguretat i formes d'usos.

La Declaració de Practiques de Certificació (CPS) és definida com un conjunt de **pràctiques** adoptades per una Autoritat de Certificació per a l'emissió de certificats. En general conté informació detallada sobre el seu sistema de seguretat, suport, administració i emissió dels Certificats, a més sobre la relació de confiança entre el Signant/Subscriptor o Tercer que confia i l'Autoritat de Certificació. Poden ser documents absolutament comprensibles i robustos, que proporcionen una descripció exacta dels serveis oferts, procediments detallats de la gestió del cicle vital dels certificats, etc.

Estos conceptes de Polítiques de Certificació i Declaració de Practiques de Certificació són distints, però encara així és molt important la seua interrelació.

Una Declaració de Pràctiques de Certificació detallada no forma una base acceptable per a la Interoperabilitat d'Autoritats de Certificació. Les Polítiques de Certificació serveixen millor com a mitjà en el qual basar estàndards i criteris de seguretat comuna.

En definitiva una Política defineix **"quins"** requeriments de seguretat són necessaris per a l'emissió dels certificats. La Declaració de Practiques de Certificació ens diu "**com**" es compleixen els requeriments de seguretat imposats per la Política.

1.2. Vista General

El present document especifica la Declaració de Pràctiques de Certificació (d'ara en avant CPS) d'AC Camerfirma SA (d'ara en avant Camerfirma) per a l'emissió de certificats, i està basada en les especificacions dels estàndards:

- RCF 3647 – *Internet X. 509 Public Key Infrastructure Certificate Policy*, de l'IETF
- RFC 3739 3039 del IETF Internet X.509 Public Key Infrastructure: Qualified Certificates Profile
- RFC 5280, RFC 3280: Internet X.509 Public Key Infrastructure. Certificate and Certificate Revocation List (CRL)
- ETSI TS 101 456 V1.2.1 Policy requirements for certification authorities issuing qualified certificate
- ETSI TS 102 042 V1.1.1 Policy requirements for certification authorities issuing public key certificate

- ETSI TS 102 023 V1.2.1 Policy requirements for time - stamping authorities tècnicament equivalent al RFC 3628
- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates V1
- CA/Browser Forum EV SSL Certificate Guidelines V 1.3

i en els requisits establerts en les pròpies polítiques de certificació a les que aquesta CPS dona resposta. S'han tingut també en compte les recomanacions del document tècnic

Security CWA 14167-1 Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements.

Aquesta CPS es troba de conformitat amb les Polítiques de Certificació dels diferents certificats emesos per Camerfirma que vénen determinats en l'apartat 1.2.1 d'esta CPS. En cas de contradicció entre els dos documents prevaldrà el que disposen les Polítiques de Certificació concretes.

1.2.1. Jerarquies

En aquest apartat presentarem les jerarquies i Autoritats de Certificació (d'ara en avant AC o AC's) inclòs a l'abast d'aquesta CPS que gestiona Camerfirma. La utilització de jerarquies permet reduir els riscos associats a l'emissió de certificats i organitzar-los en diferents AC's.

Totes les autoritats de certificació (AC) descrites en aquest apartat poden emetre certificats de transponedor OCSP. Aquest certificat servirà per verificar les respostes del transponedor OCSP sobre l'estat dels certificats emesos per aquestes AC. Les respostes del servei OCSP de Camerfirma van signades electrònicament amb un certificat d'aquest tipus.

1.2.1.1. Jerarquia Chambersign Global ROOT (JCS) 1.3.6.1.4.1.17326.10.1.1

Aquesta Jerarquia està creada per a l'emissió de certificats baixos projectes concrets amb un/es determinada/es Entitat/s. Per aquest motiu, és una jerarquia oberta on els certificats i la gestió dels mateixos s'ajusten a les necessitats concretes del projecte. En aquest sentit, les Autoritats de Registre no solen trobar-se emmarcades en l'àmbit de les Cambres de Comerç ni els certificats emesos tenen perquè trobar-se emmarcats en un àmbit empresarial o de vinculació a entitat.

Les característiques principals d'aquesta jerarquia són:

- Àmbit Geogràfic no restringit
- Autoritats de Registre no restringides
- Àmbit no restringit a una relació d'empresa

En el marc d'aquesta Jerarquia penja l'Autoritat de Certificació Govern d'Andorra com una AC intermèdia així com el diferents tipus de certificats que s'emetin dins d'aquesta jerarquia:

Govern d'Andorra	2.16.20.2.1.3.1
Certificats de persona física (Nivell 1,2 i 3)	2.16.20.2.1.3.1.1.*
Certificats de representant (Nivell 1,2 i 3)	2.16.20.2.1.3.1.3.*
Certificats de professional (Nivell 1,2 i 3)	2.16.20.2.1.3.1.12.*
Certificats de persona física al servei d'una organització (Nivell 1,2 i 3)	2.16.20.2.1.3.1.4.*
Certificats de persona física al servei d'administració (Nivell 1,2 i 3)	2.16.20.2.1.3.1.5.*
Certificats de servidor segur (Nivell únic)	2.16.20.2.1.3.1.6.*
Certificats de seu electrònica (Nivell 1,2 i 3)	2.16.20.2.1.3.1.7.*
Certificats de persona jurídica (Nivell 1,2 i 3)	2.16.20.2.1.3.1.2.*
Certificats d'actuació de l'Administració (Nivell 1,2 i 3)	2.16.20.2.1.3.1.8.*
Certificats d'entitat de segellament de data i hora (Nivell únic)	2.16.20.2.1.3.1.9.*
Certificats de signatura de programari (Nivell únic)	2.16.20.2.1.3.1.10.*
Certificats de xifratge (Nivell únic)	2.16.20.2.1.3.1.11.*

On:

- Nivell 1 corresponen a un certificat que ofereix garantia d'identitat.
- Nivell 2 correspon a un certificat qualificat que ofereix garantia d'autenticitat documental.
- Nivell 3 que correspon a un certificat qualificat que ofereix garantia de reconeixement de signatura.

De manera general, la jerarquia pública de certificació d'Andorra inclou:

- L'emissió de certificats al sector públic d'Andorra i als ciutadans d'Andorra, entenent-se com a ciutadans d'Andorra les persones físiques o jurídiques de nacionalitat andorrana o amb residència legal a Andorra.
- L'admissió de certificats dels ciutadans andorrans i dels estrangers no residents a Andorra, en les seves relacions electròniques amb el sector públic d'Andorra.

Als efectes d'aquest document, per sector públic s'ha d'entendre:

- L'Administració Pública, tal i com es defineix a l'article 13 del Codi d'Administració:
- El Consell Executiu i els òrgans posats sota la seva direcció.
- Els Comuns i Quarts i els òrgans que en depenen.
- Els organismes autònoms o entitats parapúbliques.
- Les societats mercantils públiques, participades per l'Administració Pública.

En funció de l'ús dels certificats, s'estableix la següent classificació dels certificats:

- **Certificats de signatura electrònica**, que permeten el seu ús per a l'autenticació de documents per part d'una persona física, d'acord amb la definició continguda a l'article 7 de la Llei 6/2009, del 29 de desembre, de signatura electrònica. Els certificats poden ser ordinaris o qualificats, si compleixen l'article 13 de la Llei 6/2009, del 29 de desembre, de signatura electrònica.

  Amb caràcter general, els certificats ordinaris han de complir els requisits que es preveuen a l'especificació tècnica ETSI TS 102 042, per a la política *NCP* o *NCP+*, quan es requereixen superiors garanties de seguretat.

  Per la seva banda, els certificats qualificats han de complir els requisits que es preveuen a l'especificació tècnica ETSI TS 101 456, per a la política *QCP públic* o *QCP + SSCD*, quan s'emeten conjuntament amb un dispositiu segur de creació de signatura electrònica.

- **Certificats de segell electrònic**, que permeten el seu ús per a l'autenticació de documents per part d'una persona jurídica.

  Amb caràcter general, els certificats de segell electrònic han de complir els requisits que es preveuen a l'especificació tècnica ETSI TS 102 042, per a la política *NCP* o *NCP+*, quan es requereixen superiors garanties de seguretat.

- **Certificats d'identitat electrònica**, que permeten el seu ús per la identificació electrònica d'una persona física o jurídica.

  Amb caràcter general, els certificats d'identitat han de complir els requisits que es preveuen a l'especificació tècnica ETSI TS 102 042, per a la política *NCP* o *NCP+*, quan es requereixen superiors garanties de seguretat.

- **Certificats de xifratge**, que permeten el seu ús per a la garantia de la confidencialitat dels documents i les transmissions de dades.

Amb caràcter general, els certificats de xifratge han de complir els requisits que es preveuen a l'especificació tècnica ETSI TS 102 042, per a la política *NCP*.

En funció de l'adquirent dels certificats, aquesta política estableix la següent classificació:

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

Complementàriament, es defineix la següent tipologia de certificats:

- Certificats d'actuació de persona física.
    - Signatura electrònica.
    - Identitat electrònica.
    - Xifratge.
- Certificats d'actuació de representant.
    - Signatura electrònica.
    - Segell electrònic
    - Identitat electrònica.
    - Xifratge.
- Certificats de professional
    - Signatura electrònica.
    - Identitat electrònica.
    - Xifratge.
- Certificats d'actuació de persona física al servei de l'Administració.
    - Signatura electrònica.
    - Identitat electrònica.
    - Xifratge.
- Certificats d'actuació de persona física al servei d'una organització privada.
    - Signatura electrònica.
    - Identitat electrònica.
    - Xifratge.
- Certificats d'actuació de persona jurídica.
    - Segell electrònic.
    - Identitat electrònica.
    - Xifratge.

- Certificats d'actuació de l'Administració, òrgan o entitat de dret públic.
    - Segell electrònic.
    - Identitat electrònica.
    - Xifratge.
- Certificats de servidor segur.
- Certificats de seu electrònica.
- Certificats d'entitat de segellament de data i hora.
- Certificats de signatura de programari.

1.2.2. Autoritat de Polítiques

Esta CPS defineix la forma en què l'Autoritat de Certificació dóna resposta a tots els requeriments i nivells de seguretat imposats per les Polítiques de Certificació corresponents.

L'activitat de l'Autoritat de Certificació podrà ser sotmesa a la inspecció de l'Autoritat de les Polítiques (PA) o per personal delegat per la mateixa.

El Govern d'Andorra constitueix per tant en l'Autoritat de les Polítiques (PA) de les Jerarquies i Autoritats de Certificació descrites anteriorment sent responsable de l'administració de la CPS.

Pot contactar amb l'Autoritat de les Polítiques (PA) en:

Correu electrònic:	oficina.certificacio@govern.ad

En el que es refereix al contingut d'esta CPS, es considera que el lector coneix els conceptes bàsics de PKI, certificació i signatura digital, recomanant que, en cas de desconeixement dels dits conceptes, el lector s'informi a aquest respecte. En la Web de https://pki.govern.ad/politiques es pot trobar informació general sobre l'ús de la signatura digital i els certificats digitals.

1.3. Identificació

Nom:	CPS Camerfirma SA com Prestador de Serveis de Certificació Digital del GOVERN D'ANDORRA
Descripció:	Document de resposta als requeriments de les Polítiques amb identificatius:

	Política general de certificació del sector públic d'Andorra Codi de referència: E.0201 Versió: 1.0 Data de l'edició: 11/12/2012 Fitxer: Política de certificació digital v1r1
	Polítiques 2.16.20.2.1.3.1.1.* Polítiques 2.16.20.2.1.3.1.2. * Polítiques 2.16.20.2.1.3.1.3. * Polítiques 2.16.20.2.1.3.1.4. * Polítiques 2.16.20.2.1.3.1.5. * Polítiques 2.16.20.2.1.3.1.6. * Polítiques 2.16.20.2.1.3.1.7.* Polítiques 2.16.20.2.1.3.1.8. * Polítiques 2.16.20.2.1.3.1.9. * Polítiques 2.16.20.2.1.3.1.10. * Polítiques 2.16.20.2.1.3.1.11. * Polítiques 2.16.20.2.1.3.1.12. *
Versió:	1.0.0
Data primera Emissió: xxxxxxxx	
Localització:	xxxxxxxx

1.3.1. Combinacions de polítiques de certificats

Els certificats de signatura electrònica i segell electrònic poden oferir només aquestes funcionalitats o bé altres, com la identitat electrònica o el xifratge.

Per tant, es poden donar els següents escenaris:

- Expedició d'un únic certificat per a les funcionalitats de signatura/segellament, identitat i xifratge.
- En aquest cas, s'assignarà un únic OID al certificat.
- Expedició de dos certificats, un per a les funcionalitats de signatura/segellament i identitat, i un altre per al xifratge.
- Expedició de tres certificats, un per a cada funcionalitat.

En aquests dos casos, s'assignarà a cada certificat l'OID corresponent al nivell de seguretat aplicable. Per exemple, el certificat d'identitat típicament serà de nivell 1,

mentre que el certificat de signatura/segellament, de nivell 2 o 3. El certificat de xifratge sempre rep el mateix OID.

1.4. Comunitat i Àmbit d'Aplicació

1.4.1. Autoritat de Certificació (AC)

És l'entitat 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.

Als efectes de la present CPS totes les Autoritats de Certificació són gestionades per Camerfirma.

La informació relativa a l'AC pot trobar-se en l'Adreça Web de https://pki.govern.ad

1.4.2. Entitat d'Acreditació

L'entitat d'acreditació serà l'òrgan gestor corresponent que admet, acredita i supervisa les entitats de certificació.

A Espanya aquesta tasca recau en el Ministeri d'Indústria Turisme i Comerç, sent l'autoritat competents com a Estat membre de l'Espai Econòmic Europeu, d'acord amb la legislació dictada en compliment de la Directiva 1999/93/CE del Parlament Europeu i del Consell, de 13 de desembre, per la qual s'estableix un marc comunitari per a la signatura electrònica.

A Andorra, el Govern d'Andorra actuarà com prestador de serveis de certificació, en règim de lliure concurrència, en especial en el seu àmbit corporatiu, així com per a la garantia d'identitat administrativa de la ciutadania en cas d'establir-hi relacions fiables per via electrònica.

D'acord amb el que disposa l'article 5 del Codi d'Administració, la prestació del servei es realitzarà preferentment en qualsevol modalitat de gestió indirecta, mitjançant la creació d'una Entitat de Certificació de l'Administració Pública Andorrana.

1.4.3. Prestador de serveis de certificació (PSC)

En general entenem davall la present CPS, a un PSC com aquella entitat que presta els serveis concrets relatius al cicle de vida dels certificats i que pot gestionar una o més Autoritats de Certificació i serveis associats com l'emissió de segells de temps, provisió de dispositius de signatura o serveis de validació.

Un prestador de serveis de certificació és una persona física o jurídica que produeix certificats i presta altres serveis en relació amb la signatura electrònica, d'acord amb la Llei 6/2009, del 29 de desembre, de signatura electrònica. El prestador de serveis de

certificació genera els certificats digitals mitjançant l'operació d'entitats de certificació de la seva titularitat, que signen els certificats.

Poden ser prestadors de serveis de certificació totes les entitats que operin a Andorra, bé per trobar-se establertes al Principat d'Andorra o prestar el servei a través d'un establiment o oficina oberts al Principat d'Andorra, com disposa l'article 1.2 de la Llei 6/2009, del 29 de desembre, de signatura electrònica.

Així mateix, també poden ser prestadors de serveis de certificació les entitats que es trobin establertes a altres Estats quan es doni qualsevol dels supòsits previstos a l'article 17 de la Llei 6/2009, del 29 de desembre, de signatura electrònica.

En particular, es considera que els certificats electrònics qualificats emesos pels prestadors de serveis de certificació que es troben establerts a l'Espai Econòmic Europeu són, en general, admissibles si es donen les següents condicions:

- Que es trobin subjectes a supervisió o acreditació per les autoritats competents dels Estats membre de l'Espai Econòmic Europeu, d'acord amb la legislació dictada en compliment de la Directiva 1999/93/CE del Parlament Europeu i del Consell, de 13 de desembre, per la qual s'estableix un marc comunitari per a la signatura electrònica.
- Que es pugui verificar el seu estat favorable de supervisió o acreditació emprant una llista de serveis de confiança (TSL) emesa per l'autoritat competent, d'acord amb el que disposa la Decisió 2009/767/CE de la Comissió Europea, de 16 d'octubre, per la qual s'adopten mesures que faciliten l'ús de procediments per via electrònica a través de les "finestretes úniques" d'acord amb la Directiva 2006/123/CE del Parlament Europeu i del Consell relativa als serveis en el mercat interior, modificada per Decisió 2010/425/UE, de 28 de juliol.

La Unió Europea publica, als efectes anteriors, una compilació de totes les llistes de confiança emeses per les autoritats competents que es pot consultar a l'adreça

http://ec.europa.eu/information_society/policy/esignature/eu_legislation/trusted_lists/index_en.htm

En relació amb els certificats de la pròpia Administració Pública o ús tècnic, el prestador del servei de certificació serà determinat mitjançant un procediment públic sotmès a la legislació de contractes del sector públic.

Als efectes de la present CPS, Camerfirma és el PSC.

1.4.4. Autoritat de Registre (AR)

Persones físiques o jurídiques que actuen conforme aquesta CPS i, si és el cas, mitjançant un acord subscrit amb una AC concreta, les funcions de la qual són la gestió de les sol·licituds, identificació i registre dels sol·licitants del Certificat i aquelles que es

disposen en les Polítiques de Certificació concretes. Les AR són autoritats delegades de l'AC encara que esta, és l'última responsable del servei. L'AC pot en qualsevol moment exercir les labors d'AR.

Als efectes de la present CPS per a la Jerarquia Chambersign (JCS) podran actuar com AR:

- La pròpia Autoritat de Certificació.
- Qualsevol agent nacional o internacional que mantingui una relació contractual amb l'AC i superi els processos d'alta i les Auditories exigides en les Polítiques de Certificació.

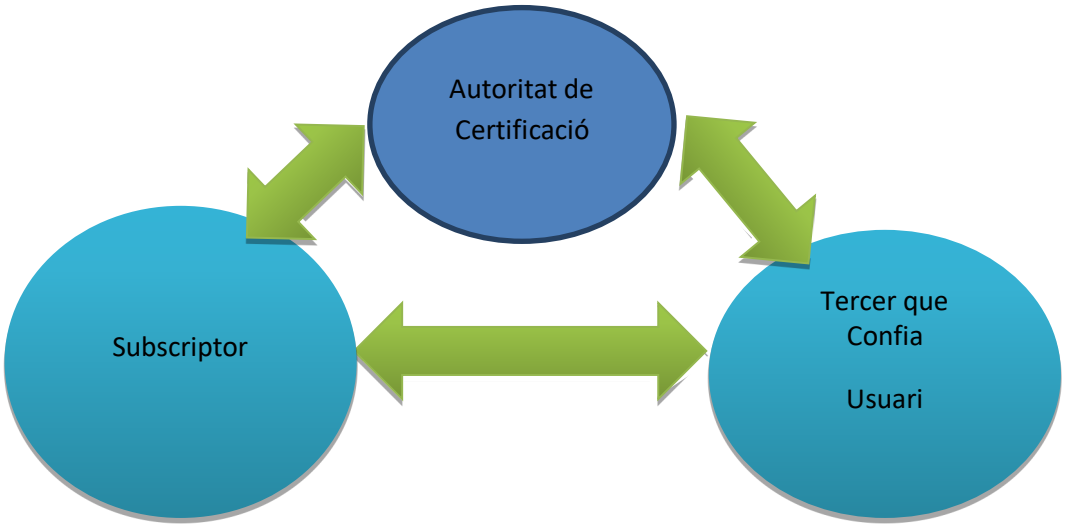
1.4.5. Signant/ Subscriptor

Entenem per Signant/Subscriptor, al Titular del certificat quan aquest sigui una persona física o jurídica. Quan s'emeti a nom d'un dispositiu maquinari o programari informàtic, es considerarà Signant/Subscriptor, la persona física o jurídica sol·licitant del certificat emès.

Abans d'emetre el certificat del signant / subscriptor es considerat com sol·licitant.

1.4.6. Tercer que confia

En aquesta CPS s'entén per Tercer que confia o usuari, la persona que rep una transacció electrònica realitzada amb un certificat emès per qualsevol de les AC de Camerfirma i que voluntàriament confia en el Certificat emès per esta.



1.4.7. Entitat

L'Entitat es constitueix com aquella empresa o organització amb què el Signant/Subscriptor manté una vinculació determinada que apareix definida en el camp ORGANITZACIÓ de cada certificat.

Així:

- En el cas del certificat de Persona física vinculada, l'Entitat es troba vinculada al Signant/Subscriptor per mitjà d'una relació mercantil, laboral, col·legial, etc.
- En el cas de certificats de Servidor Segur / Segell electrònic d'empresa/ Seu Electrònica, l'Entitat és la titular del domini d'Internet o del programari per al qual s'ha demanat el certificat.
- En el cas de certificats de signatura de programari. L'Entitat vinculada amb el desenvolupament realitzat sobre el que se produeix la signatura.

Com a norma general l'Entitat queda identificada dins del certificat en el camp organització i el seu identificador fiscal en el camp número de sèrie. Per a mes informació veure l'apartat 3.1.1.

1.4.8. Sol·licitant

S'entendrà per Sol·licitant la persona física que sol·licita el Certificat al PSC Camerfirma, podent ser directament o a través d'un representant autoritzat. El sol·licitant una vegada emès el certificat serà considerat com Signant/Subscriptor.

Poden ser sol·licitants:

- La persona que serà el futur subscriptor del certificat.
- Una persona autoritzada pel futur subscriptor del certificat.
- Una persona autoritzada per l'Entitat de Registre.
- Una persona autoritzada per l'Entitat de Certificació.

1.4.9. Responsable de certificats / Posseïdor de les claus

Per als certificats emesos a persones físiques, aquesta CPS considera responsable al titular del certificat (el Signant/Subscriptor).

Per als certificats emesos a persones jurídiques, aquesta CPS considera responsable a la persona física que realitza la sol·licitud (el sol·licitant) que deu estar identificat dintre del certificar, inclús si s'efectua la sol·licitud a través d'un tercer. Per als certificats que recullen un poder de representació, aquesta CPS considera responsable tant al Signant/Subscriptor com a la persona o Entitat representada.

Per als certificats de component, aquesta CPS considera responsable a la persona física que realitza la sol·licitud en el seu nom propi o a través d'un tercer.

1.4.10. Usuari Final

Els usuaris finals són les persones que obtenen i utilitzen certificats personals, d'entitat, de dispositius i d'objectes emesos per les Entitats de Certificació, i, en concret, podem distingir els següents usuaris finals:

- Els sol·licitants de certificats.
- Els subscriptors o titulars de certificats.
- Els posseïdors de claus.
- Els verificadors de firmes i certificats.

1.4.11. Àmbit d'Aplicació i Usos

Aquesta CPS dóna resposta a les Polítiques de Certificació descrites en l'apartat 1.2 de la present CPS.

Els certificats de Camerfirma podran fer-se servir en els termes establerts per les Polítiques de Certificació corresponents.

En termes generals, s'admeten els certificats per als següents usos:

- Autenticació basada en certificats X.509v3, d'acord amb la corresponent política d'autenticació electrònica.
- Signatura electrònica, avançada o reconeguda, basada en certificats X.509v3, d'acord amb la corresponent política de signatura electrònica.
- Xifratge asimètric o mixt, basat en certificats X.509v3, d'acord amb la corresponent política de xifratge.
- Protecció d'evidències electròniques, basada en certificats X.509v3, d'acord amb la corresponent política d'evidència electrònica.

1.4.12. Usos Prohibits i no Autoritzats

Els certificats només podran ser empleats amb els límits i per als usos per als que hagen sigut emesos en cada cas i que vénen descrits en les polítiques de certificació corresponents.

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

Els certificats no poden utilitzar-se per signar peticions d'emissió, renovació, suspensió o revocació de certificats, ni per signar certificats de clau pública de cap tipus, ni signar llistes de revocació de certificats o altres missatges d'informació d'estat de certificats o validació de signatures.

L'ús dels certificats digitals en operacions que contravenen les Polítiques de Certificació aplicable a cadascun dels Certificats, la CPS o els Contractes de l'AC amb les AR o amb

els seus Signants/Subscriptors tindran la consideració d'usos indeguts, als efectes legals oportuns, eximint-se per tant l'AC, en funció de la legislació vigent, de qualsevol responsabilitat per aquest ús indegut dels certificats que realitzí el Signant o qualsevol tercer.

Camerfirma no té accés a les dades sobre els quals es pot aplicar l'ús d'un certificat. Per tant, i com a conseqüència d'esta impossibilitat tècnica d'accedir al contingut del missatge, no és possible per part de Camerfirma emetre cap valoració sobre el dit contingut, assumint per tant el signatari qualsevol responsabilitat dimanant del contingut aparellat a l'ús d'un certificat. Així mateix, li serà imputable al signatari qualsevol responsabilitat que pogués derivar-se de la utilització del mateix fora dels límits i condicions d'ús arreplegues en les Polítiques de Certificació aplicable a cada un dels Certificats, la CPS i els contractes de l'AC amb els seus Signants, així com de qualsevol altre ús indegut del mateix derivat d'aquest apartat o que pugui ser interpretat com a tal en funció de la legislació vigent.

Camerfirma incorpora en el certificat informació sobre la limitació d'ús, bé en camps estanderditzats en els atributs "ús de la clau" "key usage" i "restriccions bàsiques" "Basic Constrains" marcats com a crítics en el certificat i per tant de compliment obligatori per part de les aplicacions que l'utilitzin, o bé per mitjà de textos incorporats el camp "user notice" d'ús "no crític" però de compliment obligatori per part del titular i de l'usuari del certificat.

1.5. Normativa legal aplicable

Camerfirma ve obligada al compliment de requeriments marcats en la **legislació espanyola i andorrana vigent com a** entitat mercantil prestadora de serveis de certificació digital (d'ara en avant, normativa o legislació vigent). Dita normativa queda definida en el document intern ***"Conformitat amb els requeriments legals"***.

1.6. Contacte

Aquesta CPS, està administrada i gestionada pel departament jurídic de Camerfirma podent ser contactat pels mitjans següents:

Correu electrònic:	juridico@camerfirma.com
	C/ Ribera del Loira, 122 8042 MADRID Telèfons: 902 361 207 +34 914 119 661 Direcció Internet de dades de contacte: https://www.camerfirma.com/address

2. Clàusules Generals

2.1. Obligacions

Camerfirma s'obliga d'acord el que disposen les Polítiques de Certificació implicades i en aquesta CPS, així com allò que s'ha disposat en normativa vigent sobre prestació de serveis de Certificació a:

- Respectar el que disposa esta CPS i en les Polítiques de Certificació.
- Protegir les seues claus privades de forma segura.
- Emetre certificats d'acord amb esta CPS, a les Polítiques de Certificació i als estàndards d'aplicació.
- Emetre certificats segons la informació que es troba en el seu poder i lliures d'errors d'entrada de dades.
- Emetre certificats el contingut del qual mínim estigui el definit per la normativa vigent per als certificats qualificats o reconeguts.
- Publicar els certificats emesos en un directori, respectant en tot cas allò que s'ha disposat en matèria de protecció de dades per la normativa vigent.
- Suspendre i revocar els certificats segons el que disposa esta Política i publicar les mencionades revocacions en la CRL.
- Informar els Signants/Subscriptors de la revocació o suspensió dels seus certificats, dins del termini i la forma escaient d'acord amb la legislació vigent.
- Publicar esta CPS i les Polítiques de Certificació corresponents en la seua pàgina Web.
- Informar sobre les modificacions d'esta CPS i de les Polítiques de Certificació als Signants/Subscriptors i a les AR's que estiguin vinculades a ella.
- No emmagatzemar ni copiar les dades de creació de signatura del Signant/Subscriptor excepte per als certificats de xifratge.
- Protegir, amb la degut atenció, les dades de creació de signatura mentre estiguin davall la seua custòdia, si és el cas.
- Establir els mecanismes de generació i custòdia de la informació rellevant en les activitats descrites, protegint-les davant de pèrdua o destrucció o falsificació.
- Conservar la informació sobre el certificat emès pel període mínim exigit per la normativa vigent.

2.1.1. AR

Les AR són les entitats delegades per Camerfirma per a realitzar aquesta tasca, per tant l'AR també s'obliga en els termes definits en les Pràctiques de Certificació per a l'emissió de certificats, principalment:

- Respectar el que disposa esta CPS i en la Política de Certificació corresponent.
- Protegir les seues claus privades.
- Comprovar la identitat dels Signants/Subscriptors i Sol·licitants dels certificats quan resulti necessari, acreditant definitivament la identitat del subscriptor, en cas de certificats individuals, o del posseïdor de claus, en cas de certificats d'organització, d'acord amb l'establert a les seccions corresponents d'aquest document.
- Verificar l'exactitud i autenticitat de la informació subministrada pel Sol·licitant.
- Proporcionar al subscriptor, en cas de certificats individuals, o al futur posseïdor de claus, en cas de certificats d'organització, accés al certificat.
- Lliurar, en el seu cas, el dispositiu criptogràfic corresponent.
- Arxivar, pel període disposat en la legislació vigent, els documents subministrats pel sol·licitant o subscriptor.
- Respectar el que disposen els contractes firmats amb Camerfirma i amb el Signant/Subscriptor
- Informar Camerfirma de les causes de revocació, sempre que tinguin coneixement.
- Assumir les dites obligacions inclús en els casos d'entitats delegades per estes (a PVP o AR Empresarial)
- En cas de certificats d'organització, es subministrarà:
    - Informació bàsica sobre la política i ús del certificat, incloent especialment informació sobre Camerfirma i la Declaració de Pràctiques de Certificació aplicable, així com de les seves obligacions, facultats i responsabilitats.
    - Informació sobre el certificat i el dispositiu criptogràfic.
    - Reconeixement del posseïdor de rebre el certificat i, en el seu cas, el dispositiu criptogràfic, i acceptació dels esmentats elements.
    - Obligacions del posseïdor de claus
    - Responsabilitat de posseïdor de claus
    - Mètode d'imputació exclusiva al posseïdor de la seva clau privada i de les seves dades d'activació del certificat i, en el seu cas, del dispositiu

criptogràfic, d'acord amb l'establert a les seccions corresponents d'aquest document.

- La data de l'acte de lliurament i acceptació.

Aquesta informació es subministra al subscriptor mitjançant l'acceptació de les clàusules d'us, de manera prèvia a la confirmació de la sol·licitud del certificat i mitjançant correu electrònic.

2.1.2. Sol·licitant del certificat

El Sol·licitant (bé directament o a través d'un tercer autoritzat) d'un certificat estarà obligat a complir amb allò que s'ha disposat per la normativa i a més a més a:

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

2.1.3. Signant/Subscriptor

El Signant/Subscriptor estarà obligat a complir amb allò que s'ha disposat per la normativa vigent i a més a més a:

- Utilitzar el certificat segons el que estableix la present CPS i en les Polítiques de Certificació aplicable.
- Respectar el que disposen els documents firmats amb Camerfirma i l'AR.
- Informar tan ràpidament com sigui possible de l'existència d'alguna causa de suspensió /revocació.
- Notificar qualsevol inexactitud o canvi en els dades aportades per a la creació del certificat durant el seu període de validesa.
- No utilitzar la clau privada ni el certificat des del moment que se sol·licita o és advertit per Camerfirma o l'AR de la suspensió o revocació del mateix, o una vegada 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 a les esmentades certificacions digitals.
- Autoritzar a Camerfirma a procedir al tractament de les dades personals contingudes als 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 de que tota la informació inclosa, per qualsevol mitjà, a l sol·licitud del certificat i en el mateix certificat sigui exacta, completa per a la

finalitat del certificat i estigui actualitzada en tot moment.

- Informar immediatament al 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 perdi la seva possessió, posar-ho en coneixement fefaent de l'entitat que l'hagi emès en el termini més breu possible i, en tot cas, dintre de les 24 hores següents a la producció de la mencionada circumstància, 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 realitzar 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 a la creació de 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.

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, en el seu cas qualificada, o el segell electrònic, en el seu cas qualificat.
- Crear les claus dins del dispositiu de creació de signatura o de segell, fent servir un dispositiu segur quan escaigui.
- Utilitzar longituds i algoritmes de clau reconeguts com a acceptables per a l signatura electrònica, en el seu cas qualificada, o el segell electrònic, en el seu cas qualificat.

2.1.4. Tercer que confia/Usuari

Serà obligació del Tercer que confia complir amb allò que s'ha disposat pel que disposa la normativa vigent i a més:

- Verificar la validesa dels certificats abans de realitzar qualsevol operació basada en els mateixos. Camerfirma disposa de diversos mecanismes per a realitzar la dita comprovació com l'accés a llistes de revocats o a serveis de consulta en línia com OCSP, tots estos mecanismes estan descrits en la pàgina Web https://pki.gover.ad

- Conèixer i acollir-se a les garanties, límits i responsabilitats aplicables en l'acceptació i ús dels certificats en què confia, i acceptar acollir-se a les mateixes.

2.1.5. Entitat

En el cas d'aquells certificats que impliquen vinculació a una Entitat, l'Entitat vindrà obligada a sol·licitar a l'AR la suspensió/revocació del certificat quan el Signant/Subscriptor cessi la dita vinculació respecte a l'organització.

2.1.6. Repositori

Camerfirma disposa d'un servei de consulta de certificats emesos i llistes de revocació. Estos serveis estan disponibles públicament en la seua pàgina Web https://pki.govern.ad

Aquesta informació és custodiada dins d'una base de dades relacional amb mesures d'integritat i accés que permeten la seua custòdia d'acord amb les exigències de les Polítiques de Certificació.

Camerfirma publica els certificats emesos, les llistes de revocació, polítiques i pràctiques de certificació de manera lliure i gratuïta.

2.2. Responsabilitat

La responsabilitat de Camerfirma

Camerfirma 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 establerts en la legislació vigent i en les Polítiques de Certificació.

En aquest sentit Camerfirma és l'única responsable (i) de l'emissió dels certificats, (ii) de la seva gestió durant tot el cicle de vida d'aquests i (iii) en particular , si cal , en cas de suspensió i revocació dels certificats . En concret, Camerfirma fonamentalment serà responsable de:

L'exactitud de tota la informació continguda en el certificat en la data de la seua emissió, per mitjà de la confirmació de les dades del sol·licitant i les pràctiques de AR. La garantia que, en el moment de l'entrega del certificat, es troba en poder del Signant/Subscriptor, la clau privada corresponent a la clau pública donada o identificada en el certificat quan el procés així ho requereix, per mitjà de la utilització de peticions estandarditzades en format PKCS#10.

La garantia que la clau pública i privada funcionen conjunta i complementàriament, utilitzant dispositius i mecanismes criptogràfics certificats.

La correspondència entre el certificat sol·licitat i el certificat entregat.

Qualsevol responsabilitat que s'estableixi per la legislació vigent.

En compliment de la legislació vigent Camerfirma disposa d'una assegurança de responsabilitat civil que cobreix els requeriments marcats per les polítiques de certificació afectades per estes pràctiques de certificació.

La responsabilitat de les AR:

Les AR subscriuen un contracte de prestació de servei amb Camerfirma mitjançant el qual Camerfirma delega les funcions de registre en les AR, consistent fonamentalment en:

1. Obligacions prèvies a l'expedició d'un certificat.

   - Informar adequadament als sol·licitants de la signatura de les seves obligacions i responsabilitats.

   - L'adequada identificació dels sol·licitants, que han de ser persones capacitades o autoritzades per sol·licitar un certificat digital.

   - La correcta comprovació de 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 d'Autoritat de Registre per gestionar les sol·licituds i els certificats emesos.

2. Obligacions un cop expedit el certificat.
   - Subscriure els contractes de Prestació de Serveis de Certificació Digital amb els sol·licitants.

   - El manteniment dels certificats durant la seva vigència (extinció, suspensió, Revocació).

   - Arxivar les còpies de la documentació presentada i els contracte degudament signats pels sol·licitants de conformitat amb Polítiques de certificació publicades per Camerfirma i la legislació vigent.

Així doncs, les AR es responsabilitzen de les conseqüències en cas d'incompliment o compliment incorrecte de les seves tasques de registre , i a través del qual es comprometen a respectar més les normes reguladores internes de l'entitat certificadora Camerfirma (Polítiques i CPS) les quals hauran de ser perfectament controlades per part de les AR i que hauran servir de manual de referència.

En cas de reclamació per un Signant , una entitat , o un usuari, L'AC haurà d'aportar la prova de l'actuació diligent i si es constata que l'origen de la reclamació rau en un error en la validació o comprovació de les dades, l'AC podrà en virtut dels acords signats amb les AR , fer suportar a l'AR responsable l'assumpció de les conseqüències . Perquè , encara que legalment sigui l'AC la persona jurídica responsable davant al Signant, una entitat , o Tercer que Confia, i que per això disposa d'una assegurança de responsabilitat civil ,

segons l'acord vigent i les Polítiques vinculants, l'AR té com a obligació contractual "identificar i autenticar correctament al Sol·licitant i, si és el cas, a l'entitat que correspongui", i en virtut d'això haurà de respondre davant Camerfirma dels seus incompliments.

Per suposat , no és intenció de Camerfirma descarregar tot el pes de l'assumpció de responsabilitat a les AR quant als possibles danys l'origen vindria d'un incompliment de les tasques delegades a les AR . Per aquesta raó, igual que el previst per a l'AC , l'AR es veu sotmesa a un règim de control que serà exercit per Camerfirma, no solament a través dels controls d'arxius i procediments de conservació dels arxius assumits per l'AR mitjançant la realització d'auditories per avaluar entre d'altres, els recursos emprats i el coneixement i control dels procediments operatius per oferir els serveis d'AR.

2.2.1. Exoneració de responsabilitat

Segons la legislació vigent, la responsabilitat de CAMERFIRMA i de l'AR no estén a aquells supòsits en què la utilització indeguda del certificat té la seva origen en conductes imputables al Signant, i al Tercer que confia per:

- No haver proporcionat informació adequada, inicialment o posteriorment com conseqüència de modificacions de les circumstàncies reflectides en el certificat electrònic, quan el seu inexactitud no hagi pogut ser detectada pel prestador de serveis de certificació;

- Haver incorregut en negligència respecte a la conservació de les dades de creació de signatura i a la seua confidencialitat.
- No haver sol·licitat la suspensió o revocació de les dades del certificat electrònic en cas de dubte sobre el manteniment de la confidencialitat;
- Haver utilitzat la signatura després d'haver expirat el període de validesa del certificat electrònic;
- Superar els límits que figurin al certificat electrònic.
- En conductes imputables al Tercer que confia si aquest actua de forma negligent, és dir quan no comprovi o tingui en compte les restriccions que figuren en el certificat quant als seus possibles usos i límit d'import de les transaccions, o quan no tingui en compte l'estat de vigència del certificat.

- Dels danys ocasionats nats al signant o tercers que confia per la inexactitud de les dades que constin en el certificat electrònic, si aquests li han estat acreditades mitjançant document públic, inscrit en un registre públic si així resulta exigible.

Camerfirma i les RA's tampoc seran responsables en cap cas quan es troben davant de qualsevol d'estes circumstàncies:

- Estat de Guerra, desastres naturals o qualsevol altre cas de Força Major.

- Per l'ús dels certificats sempre que excedeixi del que disposa la normativa vigent i en les Polítiques de Certificació

- Per l'ús indegut o fraudulent dels certificats o CRL's emesos per l'AC
- Per l'ús de la informació continguda en el Certificat o en la CRL.
- Pel perjuí causat en el període de verificació de les causes de revocació /suspensió.
- Pel contingut dels missatges o documents firmats o xifrats digitalment.
- Per la no recuperació de documents xifrats amb la clau pública del Signant.

2.2.2. Límit de responsabilitat en cas de pèrdues per transaccions

El límit monetari del valor de les transaccions s'expressa en el propi certificat per mitjà de la inclusió d'una extensió "**qcStatements**", (OID 1.3.6.1.5.5.7.1.3), tal com es defineix en la **RFC 3039**. L'expressió del valor monetari s'ajustarà al que disposa la secció 5.2.2 de la norma **TS 101 862** de l'ETSI (European Telecommunications Estàndards Institute, *www.etsi.org*).

Si l'extensió del certificat anteriorment exposada no ho contradiu, el límit màxim que Camerfirma permet en les transaccions econòmiques realitzades és de 0 (zero) euros.

2.3. Responsabilitat financera

Camerfirma, en la seva activitat com PSC, disposa d'una assegurança de responsabilitat civil que contempla les seves responsabilitats, per indemnitzar per danys i perjudicis que es puguin ocasionar als usuaris dels seus serveis: el Signant / Subscriptor i el Tercer que confia i a tercers, per un import conjunt de **3.700.000 euros**.

2.4. Interpretació i execució

2.4.1. Legislació

L'execució, interpretació, modificació o validesa de la present CPS es regirà pel que disposa la legislació andorrana vigent i en particular per la Llei 6/2009, de 29 de Desembre, de firma electrònica.

2.4.2. Independència

La invalidesa d'una de les clàusules contingudes en aquesta CPS no afectarà a la resta del document. En aquest cas es tindrà la mencionada clàusula per no posada.

2.4.3. Notificació

Qualsevol notificació referent a la present CPS es realitzarà per correu electrònic o per mitjà de correu certificat dirigit a qualsevol de les direccions referides en l'apartat dades de contacte.

2.4.4. Procediment de resolució de disputes.

Tota controvèrsia o conflicte que es derivi del present document, es resoldrà definitivament, per mitjà de l'arbitratge de dret d'un àrbitre, en el marc de La Cort Espanyola d'Arbitratge, de conformitat amb el seu Reglament i Estatut, a la que 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.

2.5. Tarifes

2.5.1. Tarifes d'emissió de certificats i renovació.

Els preus dels serveis de certificació o qualsevol altres serveis relacionats estan disponibles per als usuaris en la pàgina Web https://pki.govern.ad

Cada tipus de certificat te publicat el seu preu concret.

2.5.2. Tarifes d'accés als certificats

L'accés als certificats emesos és gratuït, no obstant això, AC Camerfirma implementa controls per a evitar els casos de descàrrega massiva de certificats. Qualsevol altra circumstància que segons el juí de Camerfirma degui de ser considerada a aquest respecte es publicarà en la pàgina Web https://pki.govern.ad

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

Camerfirma proveeix un accés a la informació relativa a l'estat dels certificats o dels certificats revocats gratuït a través de llistes de certificats revocats o per mitjà d'accés via Web https://pki.govern.ad

Camerfirma ofereix actualment el servei OCSP de manera gratuïta, però es reserva el dret a facturar per aquests serveis. En cas de ser facturats les tarifes d'estos serveis estaran publicades en l'adreça https://pki.govern.ad

2.5.4. Tarifes per l'accés al contingut d'aquestes Polítiques de Certificació.

L'accés al contingut de la present CPS és gratuït, en l'Adreça Web https://pki.govern.ad.

2.5.5. Política de reintegraments.

AC Camerfirma no disposa d'una política de reintegraments específica i s'acull a la normativa general vigent.

2.6. Publicació i repositoris

2.6.1. Publicació d'informació de l'AC

De manera general Camerfirma publica les següents informacions al seu repositori:

- Un directori actualitzat de certificats en el que s'indicaran els certificats expedits i si estan vigents, o si la seva vigència ha estat suspesa, o extingida.
- Les llistes de certificats revocats i altres informacions d'estat de revocació dels certificats.
- La política general de certificació i, quan sigui convenient, les polítiques específiques.
- Els perfils dels certificats i de les llistes de revocació dels certificats.
- La Declaració de Pràctiques de Certificació.
- Els instruments jurídics vinculants amb subscriptors i verificadors.

Tot canvi en les especificacions o condicions del servei serà comunicat als usuaris per l'Entitat de Certificació, a través del dipòsit.

No es podrà retirar la versió anterior del document objecte del canvi, però s'indicarà que ha estat substituït per la versió nova.

2.6.1.1. Polítiques i Pràctiques de Certificació

La present CPS i Polítiques actuals estan disponibles públicament en el lloc d'Internet: https://pki.govern.ad/politiques.

2.6.1.2. Termes i condicions

Camerfirma posa a disposició dels usuaris els termes i condicions del servei en les seues polítiques y pràctiques de certificació. El Signant/Subscriptor rep la informació del termes i condicions en el procés d'emissió del certificat, bé mitjançant la forma del contracte físic o bé mitjançant el procés d'acceptació de condicions abans de procedir a la sol·licitud.

2.6.1.3. Difusió dels certificats

Es podrà accedir als certificats emesos, sempre que *el Signant/Subscriptor doni del seu consentiment*, en el lloc d'Internet https://pki.govern.ad. Les claus arrel de las jerarques Camerfirma es poden descarregar des de la direcció: http://www.camerfirma.com/area-de-usuario/descarga-de-claves-publicas

El procés de consulta de certificats es realitza des d'una pàgina Web en mode segur, introduint el correu electrònic del subscriptor. La resposta del sistema, si troba un subscriptor amb eixe correu electrònic, és una pàgina amb tots els certificats associats ja estiguin actius, caducats, o revocats. D'esta manera la consulta no és lliure ni es poden descarregar certificats de forma massiva.

El servei de dipòsit de certificats està disponible durant les 24 hores dels 7 dies de la setmana i, en cas de fallada del sistema fora de control de Camerfirma, aquesta realitzarà els seus millors esforços perquè el servei es trobi disponible de nou en el termini establert a la secció corresponent i la CPS aplicable.

2.6.2. Freqüència de publicació

AC Camerfirma **publica els certificats** immediatament després d'haver sigut emesos i sempre després de l'aprovació del Signant/Subscriptor.

AC Camerfirma emet i publica **llistes de revocats** de forma periòdica d'acord la taula següent, e immediatament després de produir-se una revocació.

CA	S'emeten cada...	Durada
CHAMBERSIGN ROOT - 2008	365 dies	365 dies
GOBIERNO DE ANDORRA_AD_SUBCA	24 hores	48 hores

Camerfirma publica de forma immediata en https://pki.govern.ad/ qualsevol modificació **en les Polítiques i la CPS**, mantenint un històric de versions.

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

Els canvis en la CPS es regiran per l'establert a la secció corresponent de la CPS.

La informació d'estat de revocació de certificats es publicarà d'acord amb l'establert a la secció 3 d'aquesta CPS.

Al cap de 15 (quinze) dies des de la publicació de la nova versió, es podrà retirar la referència al canvi de la pàgina principal i serà inserida en el dipòsit. Les versions antigues de la documentació seran conservades, per un període de 15 (quinze) anys per l'Entitat de Certificació, podent ser consultades, per causa raonada pels interessats.

2.6.3. Controls d'accés

Camerfirma publica els certificats i CRL's a la seua pàgina Web. Per a l'accés al directori de certificats es necessitarà el correu electrònic del titular i passar un control antibot eliminant així la possibilitat de busques i descàrregues massives.

L'accés a la informació de revocació així com als certificats emesos per Camerfirma és lliure i gratuït.

Camerfirma utilitza sistemes fiables per al repositori, de tal manera que:

- Es pugui comprovar l'autenticitat dels certificats. El mateix certificat mitjançant la firma per la autoritat de certificació garanteix la seva autenticitat.
- Les persones no autoritzades no puguin alterar les dades. La firma electrònica de l'Autoritat de Certificació, protegeix de la manipulació de les dades incloses al certificat.
- Els certificats només siguin accessibles en els supòsits o a la persones que el signant hagi indicat. El sol·licitant autoritza o no a la publicació del seu certificat al procés de sol·licitud.
- Es pugui detectar qualsevol canvi tècnic que afecti els requisits de seguretat. La base de dades que serveix de repositori posseeix mecanismes de protecció en integritat y accessos no autoritzats.

2.7. Auditories

Camerfirma és una empresa compromesa amb la seguretat i la qualitat dels seus serveis.

Els objectius de Camerfirma respecte a la seguretat i la qualitat han sigut fonamentalment l'obtenció de la certificació **ISO/IEC 27001:2005, ISO/IEC 20000-1:2007** i la realització d'Auditories internes biennals al Sistema de Certificació Camerfirma, i fonamentalment auditories de les Autoritats de registre, per a garantir el compliment dels procediments interns.

Camerfirma està subjecta a unes auditories periòdiques amb el segell **WEBTRUST for CA i WEBTRUST EV** que assegura que els documents de polítiques i CPS tenen un format i abast adequat al mateix temps que estan completament.

Camerfirma ha passat l'any 2007 un procés d'inspecció ordinària del Ministeri d'Indústria. El Ministeri d'Indústria és l'ens regulador encarregat de supervisar les activitats dutes a terme pels prestadors de serveis de certificació espanyols.

Les autoritats de Registres subjectes a un procés d'auditoria interna. Aquestes auditories es realitzen periòdicament amb una freqüència no superior a 2 anys. La freqüència de les auditories (1 o 2 anys) a les autoritats de registre són calculades pel nombre de certificats emesos i nombre d'operadors de registre.

2.7.1. Freqüència de les auditories

Como s'ha indicat en el apartat 2.6, Camerfirma du a terme una auditoria de conformitat anualment, a més a més de les auditories internes que du a terme sota el seu propi criteri o en qualsevol moment, a causa d'una sospita d'incompliment d'alguna mesura de seguretat o per un compromís de claus.

2.7.2. Identificació i qualificació de l'auditor

Les auditories són realitzades per les companyies independents externes següents d'ampli reconeixement en seguretat informàtica, en seguretat de Sistemes d'Informació i en auditories de conformitat d'Autoritats de Certificació i els elements relacionats, d'acord amb les especificacions tècniques ETSI TS 101 456 i TS 102 042:

- Per a l'auditoria WEBTRUST Ernst&Young:
  http://www.ey.com/global/content.nsf/spain/home
- Per a les auditories ISO/IEC 27001/ISO 20000 AENOR:
  http://www.aenor.es/aenor/inicio/home/home.asp
- Per a les Auditories Internes:
  http://dnbcons.com/

2.7.3. Relació entre l'auditor i l'AC

Les empreses d'auditoria són de reconegut prestigi amb departaments especialitzats en la realització d'auditories informàtiques, per la qual cosa no hi ha cap conflicte d'interessos que pugui desvirtuar la seua actuació en relació amb l'AC.

2.7.4. Tòpics coberts per l'auditoria

L'auditoria verifica:

a) Que Camerfirma té un sistema que garanteix la qualitat del servei prestat.
b) Que Camerfirma compleix amb els requeriments de les Polítiques de Certificació que governeu l'emissió dels distints certificats digitals.
c) Que la CPS, s'ajusta al que estableixen les Polítiques, amb allò que s'ha acordat per l'Autoritat aprovadora de la Política i amb el que estableix la normativa vigent.

d) Que Camerfirma gestiona de forma adequada els seus sistemes d'informació

En particular, els elements objecte d'auditoria seran els següents:

- Processos de Camerfirma, ARs i elements relacionats.
- Sistemes d'informació.
- Protecció del centre de procés de dades.
- Documents.

2.7.5. Auditoria en les autoritats de registre

Totes les AR són auditades. Aquestes auditories es realitzen almenys cada dos anys i comproven el compliment dels requeriments exigits per les Polítiques de Certificació per al desenvolupament de les tasques de registre exposades en el contracte de servei signat.

Dins de la auditoria interna realitzada es realitzaran mostrejos sobre certificats emesos, verificant el seu correcte processament.

Documentació de referència:

IN-2010-04-12-Procedimento de Evaluación de la Seguridad en AR

IN-2010-04-15-Ficha de la visita de evaluación.doc
IN-2010-04-16-Lista de Chequeo
IN-2006-03-08-Procediment Labores AR.
IN-2010-04-17-Informe de Evaluación

2.7.6. Accions a emprendre com a resultat d'una falta de conformitat

Una vegada rebut l'informe de l'auditoria de compliment portada a terme, Camerfirma discutirà, amb l'entitat que ha executat l'auditoria, les deficiències trobades i desenvoluparà i executarà un pla correctiu que solucioni les esmentades deficiències.

Si l'Entitat de Certificació auditada és incapaç de desenvolupar i/o executar l'esmentat pla o si les deficiències trobades suposen una amenaça immediata per a la seguretat o integritat del sistema s'haurà de comunicar immediatament al Comitè Secretaria General del Govern d'Andorra, que podrà executar les següents accions:

- Cessar les operacions transitòriament.
- Revocar la clau de l'Entitat de Certificació, i regenerar la infraestructura.
- Acabar el servei de l'Entitat de Certificació.
- Altres accions complementàries que resultin necessàries.

2.7.7. Tractament dels informes d'auditoria

Camerfirma lliurarà els informes de resultats d'auditoria al Comitè d'homologació de les Polítiques de Certificació del Govern d'Andorra d'acord a les Política definida, en un termini màxim de 15 dies després de l'execució de l'auditoria.

2.8. Confidencialitat

2.8.1. Tipus d'informació a mantenir confidencial

Camerfirma considerarà confidencial tota la informació que no estigui catalogada expressament com publica. No es difon informació declarada com a confidencial sense el consentiment expressi per escrit de l'entitat o organització que l'hagi atorgat el caràcter de confidencialitat, llevat que existeixi una imposició legal.

Camerfirma disposa d'una adequada política de tractament de la informació i dels models d'acord que hauran de signar totes les persones que tingui accés a informació confidencial.

Documentació de referència:

IN-2005-02-04-Política de Seguridad
IN-2006-02-03-Normativa Seguridad

Camerfirma compleix en tot cas amb la normativa vigent en matèria de protecció de dades.

Documentació de referència:

IN-2006-05-11-Conformidad de Requerimientos legales

2.8.2. Tipus d'informació considerada no confidencial

Camerfirma considera com a informació no confidencial:

a) La continguda en la present CPS i en les Polítiques de Certificació

b) La informació continguda en els certificats sempre que el Signant/Subscriptor haja atorgat el seu consentiment.

c) Qualsevol informació la publicitat del qual sigui imposada per la normativa vigent.

2.8.3. Divulgació d'informació de revocació / suspensió de certificats

Camerfirma difon la informació relativa a la suspensió o revocació d'un certificat per mitjà de la publicació periòdica de les corresponents CRLs.

Es disposa d'un servei de consulta de CRL i Certificats en el lloc d'Internet http://crl.govern.ad/GovernAndorra.crl

2.8.4. Enviament a l'Autoritat Competent

Camerfirma proporcionarà la informació sol·licitada per l'autoritat competent en els casos i forma establerts a la legislació vigent.

2.8.5. Drets de propietat intel·lectual

La propietat intel·lectual d'aquesta CPS pertany a Camerfirma.

3. Identificació i Autenticació

3.1. Registre inicial

3.1.1. Tipus de noms

El Signants/Subscriptor es descriu en els certificats per mitjà d'un nom distintiu (DN o "Distinguished Name", Subject) al camp Subjetc conforme a l'estàndard X.501. Les descripcions del camp DN estan reflectides en cadascun de les fitxes de perfil dels certificats. Així mateix inclou un component "Common Name" (CN=)

L'estructura sintàctica i el contingut dels camps de cada certificat emès per Camerfirma així com el seu significat semàntic es troba descrit en cadascun de les fitxes de perfil dels certificats.

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 realitzarà per mitjà de la seva denominació o raó social, i el seu NRT.

3.1.2. Pseudònims i anònims

En general no es poden utilitzar pseudònims per identificar una organització. Els certificats personals poden utilitzar pseudònims en lloc del nom real del posseïdor de la clau corresponent al certificat, sempre que en cas necessari es pugui determinar aquesta identitat. El pseudònim constarà com tal de manera inequívoca.

L'admissió o no de pseudònims és tractada en cadascuna de les Polítiques de certificació. En cas de ser necessaris Camerfirma utilitzarà el Pseudònim en l'atribut CN del nom del Signant/Subscriptor guardant confidencialment la identitat real del Signant/Subscriptor.

El càlcul del pseudònim en aquells certificats on es permeti, es realitza de manera que s'identifica unívocament al titular real del **certificat annexant al número de sèrie del certificat més un acrònim de l'organització.**

L'ús d'anònims està totalment prohibit.

3.1.3. Regles utilitzades per a interpretar diversos formats de noms

Camerfirma atén en tot cas a allò que s'ha marcat per l'estàndard X.500 de referència en la ISO/IEC 9594.

3.1.4. Unicitat dels noms

No es pot tornar a assignar un nom de subscriptor que ja haja sigut ocupat, a un subscriptor diferent, això s'aconsegueix incorporant el identificador fiscal únic a la cadena del nom que distingeix al titular del certificat.

3.1.4.1. Emissió de diversos certificats per a un mateix titular

Un subscriptor pot demanar més d'un certificat sempre que la combinació dels següents valors existents a la sol·licitud fora 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 coincideixi NIA, NTR, Tipus, amb un certificat vàlid, sempre que hi hagi algun element diferenciador entre ambdós, en els camps TITLE i / o DEPARTAMENT.

3.1.5. Procediment de resolució de disputes de noms

Camerfirma no té responsabilitat en el cas de resolució de disputes de noms. En tot cas l'assignació de noms es realitzarà basant-se en la seua orde d'entrada.

Camerfirma no arbitrarà aquest tipus de disputes que hauran de ser resoltes directament per les parts.

Camerfirma en tot cas s'até al que disposa l'apartat 2.4.4 d'esta CPS.

3.1.6. Reconeixement, autenticació i funció de les marques registrades

Camerfirma no assumeix compromisos en l'emissió de certificats respecte a l'ús d'una marca comercial. Camerfirma no permet deliberadament l'ús d'un nom el dret d'ús del qual no sigui propietat del Signant/Subscriptor. No obstant això, Camerfirma no està obligada a buscar evidències de la possessió de marques registrades abans de l'emissió dels certificats.

3.1.7. Mètodes de prova de la possessió de la clau privada.

Camerfirma empra diversos circuits per a l'emissió de certificats on la clau privada es gestiona de diferent forma. La clau privada pot ser generada tant per l'usuari com per Camerfirma.

El model de generació de claus utilitzat ve indicat en el propi certificat, tant en el seu identificador de Política com en l'atribut Descripció del camp DN del certificat.

Estos codis vénen descrits en les Polítiques corresponents.

a) Generació de claus per part de Camerfirma.

   S'entreguen al subscriptor en mà o per mitjà de correu per mitjà de fitxers protegits utilitzant l'Estàndard **PKCS#12**. La seguretat del procés queda garantida ja que la clau d'accés al fitxer, que possibilita la instal·lació d'aquest en les aplicacions, és entregada per un mitjà diferent a l'utilitzat en l'entrega del PKCS#12 (correu, telèfon, entrega personal, SMS…)

   Les claus poden ser entregades per Camerfirma al Signant/Subscriptor, directament o a través d'una autoritat de registre en una targeta criptogràfica (DSCF).

b) Generació de les claus pel subscriptor.

   El subscriptor disposa d'un mecanisme de generació de claus ja sigui programari o maquinari, La prova de possessió de la clau privada en estos casos és la petició rebuda per Camerfirma en format **PKCS#10**.

   Quan el subscriptor cregui les seues pròpies claus en un dispositiu criptogràfic i demana a Camerfirma emetre un certificat digital amb una política de generació de claus en dispositiu maquinari, el subscriptor ha d'acompanyar a la petició una declaració incorporant:
   - El procés seguit per a la creació de les claus
   - Les persones implicades
   - L'entorn en què s'ha realitzat
   - L'equip HSM utilitzat (model i marca)
   - Polítiques de seguretat emprades: (mida de claus, paràmetres de creació de la clau, exportable / no exportable i qualsevol dada rellevant addicional)
   - La sol·licitud PKCS # 10 generada.
   - Incidències presentades i la seva resolució

   Aquest informe pot ser redactat i signat bé per un tercer (empresa que realitzi la instal·lació pel client) o por el client en una declaració responsable.

   El informe ha de ser visat abans de l'emissió del certificat pel responsable del departament tècnic de Camerfirma.

   AC Camerfirma es reserva el dret a valorar l'aval de l'auditor extern com a favorit o bé rebutjar-ho.

3.1.8. Autenticació de la identitat d'un individu, l'entitat i la seua vinculació.

La comprovació de la identitat està associada al tipus de certificat emès.

Camerfirma autenticarà, amb caràcter previ a l'emissió i lliurament d'un certificat d'operador, per a qualsevol dels components d'una Autoritat de Registre, la identitat de l'AR i de l'operador, establerts a la secció corresponent per a certificats reconeguts.

Per a realitzar una correcta identificació de la identitat del Sol·licitant, de l'entitat i de la seua vinculació, Camerfirma a través de l'AR, exigeix:

En els Certificats reconeguts:

- Identificació del Sol·licitant:
  S'exigeix la presència física del Signant/Subscriptor quan aquest és també Sol·licitant, o d'un representant del Sol·licitant quan aquest és una entitat jurídica, així com la presentació d'un document oficial que acrediti de forma fefaent la seva identitat (Document oficial d'identitat, targeta de residència, passaport o qualsevol altre document admès en dret) d'acord amb el que disposa l'article 16 de la Llei 6/2009, del 29 de desembre, de signatura electrònica, sempre que contingui, almenys, la següent informació:
  a) Nom i cognoms de la persona.
  b) Lloc i data de naixement.
  c) Número d'identitat reconegut legalment.
  d) Altres atributs de la persona que hagin de constar al certificat.

  La presència física no és obligatòria en els casos previstos a la legislació vigent.

- Identificació de l'entitat:
  Amb caràcter previ a l'emissió i lliurament d'un certificat d'organització cal autenticar les dades relatives a la constitució i la personalitat jurídica de la entitat. S'exigeix la identificació de l'entitat, per al que l'AR requerirà la documentació pertinent en funció del tipus d'entitat. Esta informació varia depenent del tipus d'entitat i està inclosa en els Manuals operatius de l'AR i en la Web de Camerfirma. En general seran dades relatives a la constitució i la personalitat jurídica de l'entitat, i a l'extensió i la vigència de les facultats o poders de representació del sol·licitant, mitjançant els documents públics que els acreditin de forma fefaent i la consulta al pertinent registre públic, quan es tracti de dades que han de figurar-hi. Es comprovarà:

  a) Nom legal complet de l'organització.
  b) Estat legal de l'organització.
  c) Número de registre tributari.
  d) Dades d'identificació registral

- Identificació de la vinculació:

  Per a**ls Certificats de** Representació **s'exigeix** la documentació sobre la capacitat de **representació** del Signant/Subscriptor respecte de l'altra persona, per mitjà de l'entrega de les escriptures notarials que demostren els seus

poders o facultats de representació. Es presentarà un certificat expedit pel registre públic corresponent amb menys de **10 dies** d'antiguitat. L'AR pot disposar també de mitjans telemàtics per a la consulta en línia de l'estat i nivell de representació del sol·licitant.

Per als **Certificats de vinculació** l'AR ha d'obtenir una acreditació documental de la vinculació de la persona física amb l'organització, mitjançant qualsevol mitjà admès en dret. Amb caràcter previ a la emissió y entrega d'un certificat de organització es necessari autenticar les dades relatives a la constitució i la personalitat jurídica de l'entitat. En concret, quan escaigui s'ha de fer servir certificat de pertinència a l'organització signat i segellat per l'organització lliurat per la CASS. En general, serà necessària la presentació d'una autorització firmada per un representant legal o apoderat general de l'entitat.

En els **Certificats de persona jurídica**, en els quals el Signant/Subscriptor i el Sol·licitant són distints, s'haurà de demostrar documentalment que el Sol·licitant té poders suficients per a realitzar la dita sol·licitud de certificat per compte del Signant/Subscriptor, per mitjà de la presentació d'un certificat del registre públic corresponent no superior a 10 dies o per mitjà de consulta en línia realitzada per la pròpia RA a les dades del registre públic corresponent.

En els Certificats **d'Empleat públic/Seu i Segell** no s'exigeix la documentació acreditativa de l'existència de l'administració pública, organisme o entitat de dret públic, atès que la dita identitat forma part de l'àmbit corporatiu del Govern d'Andorra. S'exigeix la documentació d'identitat de la persona que actua com a responsable, en nom de la dita Administració Pública, organisme o entitat de dret públic. El Sol·licitant/responsable s'identificarà davant de l'AR amb el seu NIA i un document acreditatiu de la seua pertinença com a empleat a l'Administració Publica, organisme o entitat de dret públic on consti a més el NRT d'aquesta.

En cas de certificats corporatius públics, la informació d'identificació de posseïdors de claus de certificats es validarà comparant la informació de la sol·licitud amb els registres interns de l'Administració corresponent, que ha d'assegurar-se de la correcció de la informació a certificar.

La informació d'identificació de subscriptors de certificats personals, així com de posseïdors de claus de certificats d'organització, s'ha de realitzar contrastant la informació de la sol·licitud amb la documentació aportada, electrònicament o en suport físic.

<u>En els Certificats Tècnics o de component</u>:

En els Certificats **de servidor segur OV (Organization Validation)** es comprova:

1. **L'existència de l'entitat** per mitjà de l'accés als registres públics. L'entitat està descrita en el camp Organització del certificat i correspondrà al propietari del domini.

2. **L'existència del domini** o la direcció IP i el dret a l'ús d'aquest pel subscriptor que es comprova per mitjà de l'accés a les bases de dades de dominis Internet WHOIS. L'ús de noms de dominis o direccions IP privades s'accepta però està en desús (i prohibit més enllà d'Octubre de 2016 pel que Camerfirma deixarà d'emetre certificats d'aquest tipus l'1 de Novembre de 2015. En tot cas es revocaran els certificats emesos d'aquestes característiques que tinguin una data d'expiració més enllà d'Octubre 2015), fet el qual es notifica al client abans de l'emissió del certificat.

   La informació del domini s'agafarà del servei WHOIS del registrador del domini per al qual s'apliquen les regles marcades per la seva corresponent ccTLD.

3. **El control del domini per part de l'entitat subscriptora**, comprovant que les dades obtinguts en la consulta al servei WHOIS coincideixen clarament amb les dades de l'entitat presentats en la sol·licitud.

   Pot produir que el domini estigui assignat a la base de dades del registrador a un tercer encarregat de seva gestió. En aquest cas perquè apareguin les dades del titular últim del domini en el certificat, es necessitarà:

   a. Una autorització d'aquest per a l'emissió del certificat.
   b. Una comunicació de l'organització o persona que controla el registre del domini indicant aquesta circumstància.

El certificat s'entrega per mitjà de correu electrònic, al menys als responsables administratius i tècnics que apareixen en les bases de dades de dominis.

En els Certificats **de segell electrònic d'empresa** se suporta documentalment per mitjà de la consulta de l'existència de l'empresa/entitat es realitza mitjançant el accés al registres públics, tal com es fa en l'emissió dels Certificats de servidor segur OV anteriorment vist. El correu electrònic del sol·licitant ha de procedir d'un compte de correu el domini al qual estigui associat a l'empresa o organisme que ha realitzat la sol·licitud.

El certificat s'entregarà en la dita adreça de correu. El codi d'activació en el cas d'entregar-se un fitxer en format PKCS12 de forma telefònica. El telèfon serà localitzat accedint als serveis de consulta telefònica o per mitjà de crida a serveis de localització de telèfons. Esta informació quedarà reflectida en l'expedient d'emissió del certificat.

En el camp titular dels certificats (CN) de segell d'empresa pot aparèixer: el nom de l'empresa, el nom del programari per al qual s'ha generat el certificat o una referència interna. Camerfirma no realitzarà cap comprovació sobre estes dades.

Es sol·licitarà per completar el tràmit una autorització de l'entitat subscriptora, podent ser aquesta autorització emesa per un departament jurídic o de recursos humans.

En els Certificats **de signatura de programari,** s'utilitza el mateix mecanisme de comprovació que per a l'emissió del Certificat de segell electrònic.

En els Certificats **de xifratge** s'emetran de forma telemàtica utilitzant un certificat reconegut vàlid.

És possible davall esta CPS establir emissions de certificats de xifrat en processos de lots. En estos casos, la comprovació de la identitat pot ser realitzada en processos no presencia'ls entregant una RA o a Camerfirma, un document amb la identitat del sol·licitant i la seua vinculació amb una entitat. Aquest procés no presencial es realitzarà només quan el certificat permeti l'ús exclusiu de xifrat.

3.2. Renovació de la clau

Abans de renovar un certificat, Camerfirma haurà de comprovar que la informació utilitzada per verificar la identitat i la resta de dades del subscriptor i del posseïdor de la clau continuen sent vàlides.

L'autenticació del posseïdor és realitza sobre la base del seu certificat vàlid, que podrà renovar el seu certificat a l'ARA a partir d'un mes abans de la data de caducitat del certificat.

Si qualsevol informació del subscriptor o del posseïdor de la clau ha canviat, es registrarà adequadament la nova informació, d'acord amb l'establert a la secció corresponent.

Si qualsevol informació del subscriptor o posseïdor de la clau ha canviat, es registrarà adequadament la nova informació, d'acord amb l'establert a la secció corresponent.

Camerfirma realitza renovacions de certificats emetent sempre noves claus, per tant el procés és paregut al què es segueix quan es realitza una nova petició.

En el cas dels certificats qualificats o reconeguts per a signatura electrònica no es necessita presència física ja que la Llei 6/2009, del 29 de desembre, de signatura electrònica permet fins a un període de **3 anys** des de l'últim registre presencial, una vegada superat aquest termini el subscriptor haurà de realitzar un procés d'emissió presencial igual al realitzat la primera vegada. Si en el moment de l'emissió del certificat no han transcorregut més de 3 anys, Camerfirma entén que no és necessària la presència física del titular, independentment de la durada de la caducitat del certificat emès.

Els certificats tècnics, és a dir servidor segur, segell empresarial i signatura de programari, no es permet renovació, havent de realitzar-s'hi una emissió nova.
Camerfirma realitzarà quatre avisos (30 dies, 15 dies, 7 dies, 1 dia) via email al subscriptor notificant que el seu certificat va a caducar suggerint la realització del procés de renovació. Si el certificat actiu a renovar caduca abans de realitzar la renovació s'haurà

de realitzar un procés d'emissió nou.

El procés de renovació s'inicia en la pàgina Web https://pki.govern.ad. Aquest procés requereix disposar del certificat actiu a renovar.

- Una vegada identificat en el sistema de renovació, el sistema presenta el subscriptor les dades del certificat antic i demana la confirmació de dites dades. El sistema permet al subscriptor modificar només el email assignat al certificat. Si hi ha altres dades incorporades al certificat que han canviat, el certificat ha de revocar-s'hi i procedir a realitzar una emissió nova.

- La petició s'incorpora al programari de AR on l'operador una vegada revisats les dades i el pagament, procedeix a demanar l'emissió del certificat a l'AC.

- **L'AC emet un nou certificat prenent com a inici de validesa la finalització del certificat a renovar.**

3.3. Reemissió després d'una revocació

Al quedar el certificat invalidat no es podrà realitzar la renovació automatitzada. El sol·licitant haurà d'iniciar un procés d'emissió nova.

Excepció

Quan la revocació es produeix com a conseqüència d'un procés de substitució del certificat per error en la seua emissió es considera que la renovació després de la revocació pot realitzar-s'hi. Sempre que reflecteixi la situació actual, es reutilitzarà la documentació suport entregada per a l'emissió del certificat substituït i s'elimina la presència personal física si aquesta fora requerida per la natura del certificat.. Camerfirma actualitzarà el nombre d'anys des de l'última presència personal física a l'estat que tindria el certificat a substituir, de la mateixa manera que si aquest procés haguera sigut conseqüència d'una renovació ordinària.

3.4. Renovació de certificats sense renovació de claus

AC Camerfirma no permet la renovació de claus sense renovació de claus.

3.5. Renovació de certificat amb renovació de claus

Aquest es el procediment habitual de renovació de certificats de la AC Camerfirma, pel que tots el procediments descrits en aquesta secció es refereixen a aquest mètode de renovació.

3.6. Modificació de certificats

Qualsevol necessitat de modificació de certificats implicarà una sol·licitud en aquest sentit al prestador de serveis de certificació corresponent, d'acord amb la política o

declaració de serveis de certificació aplicable. Es considerarà una renovació i així computa a l'hora del càlcul dels anys de renovació sense presencia física.

Es podrà procedir a la modificació de certificats quan els atributs del subscriptor o, quan sigui necessari, del posseïdor de claus que no formin part del control d'unicitat previst per aquesta política hagin variat.

El procediment per a la modificació serà el mateix que el procediment de renovació de certificats sense renovació de claus.

Si la sol·licitud de modificació es fa dintre del període ordinari previst per a la renovació del certificat es procedirà a realitzar l'esmentada renovació, enlloc de la modificació.

3.7. Sol·licitud de revocació

La forma de realitzar les sol·licituds de revocació s'estableixen en l'apartat següent.

4. Requeriments Operacionals

4.1. Sol·licitud de certificats

Les sol·licituds dels certificats es realitzen per mitjà de l'accés als formularis de sol·licitud en l'adreça

https://pki.govern.ad

En la pàgina Web https://pki.govern.ad es troben els formularis necessaris per a realitzar la petició per a cada tipus de certificat distribuït per Camerfirma en diferents formats i els dispositius de generació de signatura, si aquests foren necessaris.

Es permeten també circuits de sol·licitud per mitjà de lots. En aquet cas, s'enviarà pel sol·licitant a l'AR un fitxer estructurat segons un disseny prefixat per Camerfirma amb les dades dels sol·licitants. L'AR procedirà a la càrrega de les dites peticions en el programari de gestió.

Quan el sol·licitant genera les claus, la sol·licitud de certificats es realitzar entregant una petició d'emissió de certificat estandarditzada tipus PKCS#11 o CSR juntament amb les dades addicionals a la petició.

Per a cada tipus de certificat el subscriptor ha d'acceptar els termes i condicions d'ús entre el propi subscriptor, l'autoritat de registre i l'autoritat de certificació. Aquest procés es realitza, per a l'obtenció d'alguns certificats, per mitjà de la signatura manuscrita d'un contracte i en altres certificats per mitjà d'una acceptació de termes visualitzats en una pàgina Web abans de procedir a la creació i descàrrega del certificat.

Amb l'objecte d'incorporar la integració d'aplicacions de tercers amb la plataforma de gestió de certificats de Camerfirma (STATUS), s'ha desenvolupat una capa de Web Services (WS) que ofereixen els serveis d'emissió, renovació i revocació de certificats. Les trucades a aquests WS estan signades per un operador de registre autoritzat, de manera que les operacions es realitzen directament a la plataforma.

L'AR ha d'assegurar-se que les sol·licituds de certificats són completes, precises i estan degudament autoritzades.

Abans de l'emissió i lliurament del certificat, l'AR informarà el subscriptor, en cas de certificats individuals o al posseïdor de claus, en cas de certificats d'organització, dels termes i condicions aplicables al certificat.

En certificats d'organització, aquest requisit es podrà complir lliurant l'instrument jurídic que vincula a Camerfirma amb el subscriptor o lliurant un full de lliurament al posseïdor de claus que inclogui aquesta informació. L'esmentada informació es comunicarà en suport perdurable, en paper o electrònicament i en llenguatge fàcilment comprensible.

A la sol·licitud es podrà acompanyar documentació justificativa de la identitat del subscriptor i altres circumstàncies, en cas de certificats individuals, o del posseïdor de claus, en cas de certificats d'organització o d'entitat, d'acord amb l'establert a la secció corresponent d'aquesta política de certificats. També es podrà acompanyar una adreça

física, o altres dades, que permetin contactar amb el subscriptor, en cas de certificats individuals, o al posseïdor de claus, en cas de certificats d'organització o d'entitat.

En cas de pèrdua, robatori o incidència que de qualsevol altra forma impliqui la incapacitat per fer servir el certificat, es podrà sol·licitar més d'un certificat per a cada persona, com a mesura de contingència si no es pot garantir la reposició en menys de 24 hores d'un certificat.

4.2. Processament de la sol·licitud de certificació

Una vegada hagi tingut lloc una petició de certificat, l'AR ha de verificar la informació proporcionada, conforme a la secció corresponent d'aquesta política.

Si la informació no és correcta, l'AR ha de denegar la petició. En cas que les dades es verifiquin correctament l'Entitat de Registre aprovarà l'emissió del certificat.

En cas d'un certificat qualificat, la documentació justificativa de l'aprovació de la sol·licitud s'ha de conservar degudament registrada i amb garanties de seguretat i integritat durant el termini de 15 anys des de l'expiració del certificat, fins i tot en cas de pèrdua anticipada de vigència per revocació.

El termini de conservació de la documentació acreditativa de la sol·licitud de certificats no qualificats no podrà ser inferior a 5 anys des de l'expiració del certificat.

4.3. Petició de certificació encreuada

Camerfirma no té actualment cap procés de certificació encreuada actiu.

4.4. Emissió de certificats

L'emissió dels certificats s'inicia a l'aplicació gestor de certificats (STATUS) utilitzats per un operador de AR autoritzat després de realitzar les comprovacions acordes amb el certificat a emetre. El operador de AR revisarà les sol·licituds pendents, la documentació del sol·licitant y comprovarà el pago dels serveis si fora pertinent. Una vegada aquestes operacions el operador de AR validarà amb la seva firma electrònica la emissió del certificat.

A partir d'ací encontrem el següents casos:

Certificats en Programari: L'usuari rep en el compte de correu associada al certificat un enllaç per a procedir a la generació i descàrrega del certificat. Per a la seua instal·lació necessitarà del codi de producte que li ha sigut entregat amb el contracte i un codi d'instal·lació que s'haurà entregat en un correu electrònic independent conjuntament amb un codi de revocació

Certificats en HW (Dispositiu Segur de Creació de Firma):
L'usuari rep a les dependències de l'AR el dispositiu de firma amb els certificats y les claus generades.
L'operador de l'Autoritat de Registre elegirà el tipus de targeta criptogràfica per

a realitzar la generació de les claus per això l'estació de treball del operador de l'autoritat de registre estarà configurada adequadament amb el CSP (Criptographyc Service Provider) corresponent. Actualment AC Camerfirma admet diversos tipus de targetes y tokens USB tots ells certificats CWA 14169 SSCD Type 3.
El subscriptor, per altra banda rebrà en el compte de correu associat el codi d'accés al dispositiu criptogràfic i el codi de desbloqueig , així com una clau de revocació.

El subscriptor, per altra banda rebrà en el compte de correu associat el codi d'accés al dispositiu criptogràfic i el codi de desbloqueig , així com una clau de revocació.

Peticions en Lots: Els certificats es poden sol·licitar per mitjà de lots de peticions. Aquests lots s'entreguen a l'AR en un fitxer estructurat que posteriorment introdueixen en la plataforma de gestió. L'operador de AR posteriorment a la recopilació de la documentació i la comprovació de la identitat procedirà a realitzar la validació dels certificats bé un a un o en blocs.

En els certificats tècnics (Segell d'empresa, Servidor Segur i Signatura de Programari) no es requereix presència física per a la seua emissió. Únicament l'enviament de la documentació corresponent a l'oficina d'AR. Una vegada comprovada la documentació i realitzat el pagament si correspon, AC Camerfirma emet un certificat, bé sigui per mitjà de l'emissió d'un fitxer PKCS12, o per mitjà d'un PKCS7 si el client haguera entregat un PKCS10.

Més informació a la web https://pki.govern.ad

En general indicar que Camerfirma durant aquest procés:

- Inclou al certificat les informacions establertes a l'article 14 de la Llei 6/2009, del 29 de desembre, de signatura electrònica.
- Garanteix que es pugui precisar la data i l'hora en què es va expedir el certificat, mitjançant la utilització de diferents mètodes de sincronització de temps basats en 3 fonts diferents.
- Utilitza sistemes i productes fiables que estan protegits contra tota alteració i que garanteixin la seguretat tècnica i, en el seu cas, criptogràfica dels processos de certificació a què serveixen de suport. Mitjançant el sistemes de gestió integrats d'aplicacions.
- S'assegurarà que el certificat és emès per sistemes que utilitzin protecció contra falsificació i, en cas que l'Autoritat de Registre o de Certificació generi claus privades, que garanteixin el secret de les claus durant el procés de generació de les esmentades claus. Mitjançant el procediment descrit a aquest document.
- En cas que l'AR o la AC aporti el dispositiu segur de creació de signatura, s'utilitzarà un procediment de gestió que asseguri que l'esmentat dispositiu és lliurat de forma segura al subscriptor, en cas de certificats individuals, o al posseïdor de claus, en cas de certificats d'organització. Com es descriu en aquest document.

4.5. Acceptació de certificats

Una vegada entregat o descarregat el certificat, el usuari disposa d'un període de 7 dies per a comprovar el seu correcte funcionament.

Si el certificat no ha segut emès correctament per causes tècniques, el certificat es revocarà i s'emetrà un nou.

4.6. Notificació de l'emissió als interessats

Camerfirma notificarà al sol·licitant l'aprovació o denegació de la sol·licitud.

També es notificarà al subscriptor, en cas de certificats individuals, o al futur posseïdor de claus, en cas de certificats d'organització, que s'ha creat el certificat, es troba disponible i la forma d'obtenir-lo, quan els anteriors no siguin els sol·licitants del seu certificat.

4.7. Publicació del certificat

Els certificats emesos seran publicats al Dipòsit indicat a la secció corresponent d'aquesta Declaració de Pràctiques de Certificació, on estaran a disposició del públic per ser consultats.

4.8. Notificació de l'emissió a tercers

Els certificats emesos a les entitats de sector públic podran ser objecte de publicació a registres de personal i altres dipòsits tècnics, a efectes de facilitar el seu ús corporatiu.

4.9. Suspensió i revocació de certificats.

4.9.1. Aclariments previs

S'entendrà per revocació aquell canvi en l'estat d'un certificat motivat per la pèrdua de validesa d'aquest en funció d'alguna circumstància diferent de la de la seua caducitat.

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

En general, les causes de suspensió de certificats seran les causes legalment establertes a la normativa vigent en matèria de signatura electrònica que resulti aplicable a Camerfirma. Addicionalment, l'Entitat de Certificació de l'Administració Pública Andorrana considerarà causa de suspensió del certificat la sospita de l'ús fraudulent del certificat en qualsevol sistema informàtic del sector públic.

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

Els motius de suspensió d'un certificat venen definits en la política de certificació concreta.

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

- Caducitat del certificat

- Certificat revocat per causa de suspensió que un cop revisat no troben causes per la revocació definitiva.

4.9.2. Causes de revocació i documents justificatius

Les causes de revocació d'un certificat vénen definides en la seua política de certificació concreta.

Com a norma general es procedirà a la revocació d'un certificat:

Circumstàncies que afecten la informació continguda en el certificat

- Modificació d'algunes de les dades continguts en el certificat.
- Descobriment que algun dels dades aportades en la sol·licitud de certificat és incorrecte, així com l'alteració o modificació de les circumstàncies verificades per a l'expedició del certificat.
- Descobriment que algunes de les dades continguts en el certificat és incorrecte.

Circumstàncies que afecten la seguretat de la clau o del certificat

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

Circumstàncies que afecten la seguretat del dispositiu criptogràfic

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

Circumstàncies que afecten el subscriptor o responsable del certificat.

- Acabament de la relació entre Entitat de Certificació i subscriptor o responsable del certificat.
- Modificació o extinció de la relació jurídica subjacent o causa que va provocar l'emissió del certificat al subscriptor o responsable del certificat.
- Infracció pel sol·licitant del certificat dels requisits preestablís per a la sol·licitud d'aquest.
- Infracció pel subscriptor o responsable del certificat, de les seues obligacions, responsabilitat i garanties, establides en l'instrument jurídic corresponent o en aquesta Declaració de Pràctiques de Certificació.
- La incapacitat sobrevinguda o la mort del subscriptor o responsable del certificat.
- L'extinció de la persona jurídica subscriptora del certificat, així com la finalitat de l'autorització del subscriptor al responsable del certificat o la finalització de la relació entre subscriptor i responsable del certificat.
- Sol·licitud del subscriptor de revocació del certificat, d'acord amb el que estableix aquesta CPS.

Altres circumstàncies

- La suspensió del certificat digital per un període superior a l'establert a aquesta CPS.
- La finalització del servei de l'Entitat de Certificació, d'acord amb el que estableix la secció en aquesta CPS.

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

L'instrument jurídic que vincula a l'Entitat de Certificació amb el subscriptor establirà que el subscriptor haurà de sol·licitar la revocació del certificat en cas de tenir coneixement d'alguna de les circumstàncies indicades anteriorment.

Els subscriptors disposen dels codis de revocació que poden usar en els serveis de revocació via Web o per mitjà de trucada telefònica als serveis de suport.

4.9.3. Qui pot sol·licitar la revocació

La revocació d'un certificat podrà ser sol·licitada per

- El Signant/Subscriptor

- El Sol·licitant responsable
- L'Entitat (a través d'un representant de la mateixa)
- L'AR o l'AC

Addicionalment, quan una entitat del sector públic detecti la concurrència d'alguna circumstància que podria donar lloc a la revocació d'un certificat, ho comunicarà a l'AC, però continuarà emprant el certificat mentre aquest no sigui revocat, ja que és responsabilitat exclusiva del prestador decidir la finalització anticipada del període de vida del certificat.

La norma anterior no s'aplicarà en cas d'ús fraudulent del certificat en els sistemes de l'entitat del sector públic, que donarà lloc al bloqueig immediat de l'ús del certificat i a la posterior sol·licitud de revocació davant del prestador de serveis de certificació corresponent.

Addicionalment les que marquen les polítiques de certificació concretes.

4.9.4. Procediment de sol·licitud de revocació.

L'entitat que necessiti revocar un certificat ha de sol·licitar-ho a l'Entitat de Certificació o, en el seu cas, a l'ARA que va aprovar la sol·licitud de certificació, aportant la següent informació:

- Data de sol·licitud de la revocació.
- Identitat del subscriptor.
- Raó detallada per a la petició de revocació.
- Identificació de la persona que demana la revocació.
- Informació de contacte de la persona que demana la revocació.

Totes les sol·licituds hauran de realitzar-se:

- A través del Servei de Revocació ONLINE, accedint al servei de revocació localitzat en la pàgina de la Web de i introduint el PIN de Revocació.

  https://pki.govern.ad

- A través de la presència personal física en l'AR en horari d'atenció al públic mostrant el Document oficial de identificació del Signant/Subscriptor o Sol·licitant.
- Enviant a Camerfirma un document signat per un representant amb suficient de l'entitat sol·licitant la revocació del certificat.

- Per als certificats de **servidor segur, segell d'empresa o certificat de signatura de programari** pot sol·licitar-s'hi a través del correu des del qual se sol·licità l'emissió del certificat enviant la sol·licitud a gestión_soporte@camerfirma.com. L'operador de Camerfirma confirmarà telefònicament la sol·licitud de revocació per a donar-li curs.

Camerfirma manté en la seua pàgina Web tota la informació relativa als processos de revocació dels certificats.

https://pki.govern.ad

Tant **el servei de gestió de les revocacions com el servei de consulta són** considerats **serveis crítics i així consten en el Pla de contingències o el pla de continuïtat de negoci de Camerfirma.** Estos serveis estaran disponibles les 24 hores del dia, els 7 dies de la setmana. En cas de fallada del sistema, o qualsevol altre factor que no estigui sota el control de Camerfirma. Camerfirma realitzarà els majors esforços per a assegurar que estos serveis no es troben inaccessibles durant un període màxim de **24 hores.**

4.9.5. Període de revocació

El període de revocació des de que Camerfirma o una AR té coneixement autentificat de la revocació d'un certificat es produeix de manera immediata, incorporant-se en la propera CRL a emetre.

4.9.6. Suspensió

No estipulat

4.9.7. Procediment per a la sol·licitud de suspensió

No estipulat

4.9.8. Límits del període de suspensió

No estipulat

4.9.9. Freqüència d'emissió de CRL's

Veure 2.5.2.

4.9.10. Requisits de comprovació de CRL's

Els Tercers que confien han de comprovar l'estat dels certificats en els quals confiarà, havent de comprovar en tot cas l'última CRL emesa, que podrà descarregar-se en la següent des de la seua pàgina Web:

https://pki.govern.ad

Camerfirma emet CRLs firmades per l'AC que ha emès el certificat. Els accessos a la CRL venen també referits en l'extensió del certificat "Punts de Distribució de CRL".

4.9.11. Disponibilitat de comprovació online de la revocació

AC proporciona un servei online de comprovació de revocacions via HTTP en:

https://pki.govern.ad

També per mitjà de consultes OCSP en

https://pki.govern.ad

Les direccions d'accés a estos serveis vénen referides en el certificat digital. Per a les CRL i ARL en l'extensió punts de distribució de CRL "CRL distribution Point" i la direcció d'OCSP en l'extensió Accés a la Informació de l'Autoritat "Authority Information Access".

En els certificats pot aparèixer més d'una direcció d'accés a les CRL per a garantir la seua disponibilitat.
El servei d'OCSP s'alimenta de les CRL emeses per les diferents autoritats de certificació a què dóna servei. Les dades tècniques d'accés així com els certificats de validació de les respostes OCSP es troben publicades en la Web https://pki.govern.ad

Estos serveis estaran disponibles les **24 hores del dia els 7 dies de la setmana, 365 dies al any**.

Camerfirma realitzarà tots els esforços necessaris perquè el servei mai es trobi inaccessible de forma contínua més de **24 hores**, sent aquest un servei crític en les activitats de Camerfirma i per tant tractat de forma adequada en el Pla de contingències **i de continuïtat de negoci**.

En cas necessari, Camerfirma subministrarà informació als verificadors sobre el funcionament del servei d'informació d'estat de certificats.

4.9.12. Requisits de la comprovació online de la revocació

Per a realitzar la comprovació d'una revocació el Tercer que confia haurà de conèixer el correu electrònic associat al certificat que es desitja consultar si es realitza per mitjà d'accés Web.

Els requisits per a accedir al servei **OCSP** i els certificats necessaris per a la seua validació estaran actualitzats en la pàgina https://pki.govern.ad

4.9.13. Altres formes de divulgació d'informació de revocació disponibles

Els mecanismes que Camerfirma posa a disposició dels usuaris del sistema, estaran publicats a la seva pagina Web https://pki.govern.ad

4.9.14. Requisits de comprovació per a altres formes de divulgació d'informació de revocació

No estipulat

4.9.15. Requisits especials de revocació per compromís de les claus

El compromís de la clau privada de l'AC, provoca la revocació immediata de tots el certificats emesos sota la dita AC. AC Camerfirma notificarà mitjançant email aquest fet a tots els titulars dels certificats afectats.

4.10. Procediments de Control de Seguretat

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

4.10.1. Tipus d'esdeveniments registrats

Camerfirma registra i guarda els LOG's de tots els esdeveniments relatius al sistema de seguretat de l'AC.

Es registren els esdeveniments següents:

- Encesa i apagat del sistema.
- Intents de creació, esborrament, establiment de contrasenyes o canvi de privilegis.
- Intents d'inici i fi de sessió.
- Intents d'accessos no autoritzats al sistema de l'AC a través de la xarxa.
- Intents d'accessos no autoritzats al sistema d'arxius.
- Accés físic als LOGs.
- Canvis en la configuració i manteniment del sistema.
- Registres de les aplicacions de l'AC.
- Encesa i apagat de l'aplicació de l'AC.
- Canvis en els detalls de l'AC i/o les seues claus.
- Canvis en la creació de polítiques de certificats.
- Generació de claus pròpies.
- Creació i revocació de certificats.

- Registres de la destrucció dels mitjans que contenen les claus, dades d'activació.
- Esdeveniments relacionats amb el cicle de vida del mòdul criptogràfic, com a recepció, ús i desinstal•lació d'aquest

Camerfirma també conserva, ja sigui manualment o electrònicament, la següent informació:

- La cerimònia de generació de claus i les bases de dades de gestió de claus.
- Registres d'accés físic.
- Manteniments i canvis de configuració del sistema.
- Canvis en el personal.
- Informes de compromisos i discrepàncies.
- Registres de la destrucció de material que contingui informació de claus, dades d'activació o informació personal del subscriptor, en cas de certificats individuals, o del posseïdor de claus, en cas de certificats d'organització.
- Possessió de dades d'activació, per a operacions amb la clau privada de l'Entitat de Certificació.
- Informes complets dels intents d'intrusió física en les infraestructures que donen suport a l'emissió i gestió de certificats.

4.10.2. Freqüència de processat de Logs

Camerfirma revisa els seus LOGs quan es produeixi una alerta del sistema motivada per l'existència d'algun incident.

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

Camerfirma manté un sistema que permet garantir:

- Espai suficient per a l'emmagatzematge de logs
- Que els fitxers de logs no es reescriuen.
- Que la informació que es guarda inclou com a mínim: tipus d'esdeveniment, data i hora, usuari que executa l'esdeveniment i resultat de l'operació.
- Els fitxers de logs es guardaren en fitxers estructurats susceptibles d'incorporar en una BBDD per a la seua posterior exploració.

4.10.3. Períodes de retenció per als LOGs d'auditoria

Camerfirma emmagatzema la informació dels LOGs almenys durant **5 anys**.

4.10.4. Protecció dels LOGs d'auditoria

Els logs dels sistemes són protegits de la seua manipulació per mitjà de la signatura dels fitxers que els contenen.

Són emmagatzemats en dispositius ignífugs.

Es protegeix la seua disponibilitat per mitjà del magatzem en instal·lacions externes al centre on s'ubica l'AC.

L'accés als fitxers de Logs està reservat només a les persones autoritzades (Auditor).

Els dispositius són manejats en tot moment per personal autoritzat.

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

4.10.5. Procediments de backup dels Logs d'auditoria

Camerfirma disposa d'un procediment adequat de backup de manera que, en cas de pèrdua o destrucció d'arxius rellevants, estiguin disponibles en un període curt de temps les corresponents còpies de backup dels logs.

Camerfirma té implementat un procediment de back up segur dels logs d'auditoria, realitzant setmanalment una còpia de tots els logs en un medi extern.

Addicionalment es manté còpia en centre de custòdia extern.

Documentació de referència: **IN-2005-04-10**-procedimiento de gestió de logs

4.10.6. Sistema d'arreplega d'informació d'auditoria

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

4.10.7. Notificació al subjecte causa de l'esdeveniment

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

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

4.10.8. Anàlisi de vulnerabilitats

L'anàlisi de vulnerabilitats queda cobert pels processos d'auditoria de Camerfirma.

Les anàlisi de vulnerabilitat han de ser executades, repassades i revisades per mitjà d'un examen d'aquests esdeveniments monitoritzats

Aquestes anàlisis han de ser executades diàriament, mensualment i anualment.

Anualment es revisen els processos de gestió de riscos i vulnerabilitats dins del marc de revisió de la certificació ISO/IEC 27001 que estan reflectits en el document d'Anàlisi de riscos amb codi **CONF-2005-05-01**. En aquest document s'especifiquen els controls implantats per a garantir els objectius de seguretat requerits.

Les dades d'auditoria dels sistemes són emmagatzemats a fi de ser utilitzats en la investigació de qualsevol incidència i localitzar vulnerabilitats.

4.11. Arxiu de registres

4.11.1. Tipus d'arxius registrats

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

- ✓ Totes les dades d'auditoria de sistema.
- ✓ Totes les dades relatives als certificats, incloent-hi els contractes amb els Signants i les dades relatives a la seua identificació i la seua ubicació.
- ✓ Sol·licituds d'emissió i revocació de certificats.
- ✓ Tipus de document presentat a la sol·licitud del certificat.
- ✓ Identitat de l'Entitat de Registre que accepta la sol·licitud de certificat.
- ✓ Número d'identificació únic proporcionat pel document anterior.
- ✓ Tots els certificats emesos o publicats.
- ✓ CRL's emeses o registres de l'estat dels certificats generats.
- ✓ L'historial de claus generades.
- ✓ Les comunicacions entre els elements de la PKI.
- ✓ Polítiques i Pràctiques de Certificació

Camerfirma és responsable del correcte arxiu de tot aquest material.

4.11.2. Període de retenció per a l'arxiu

Els certificats, els contractes amb els Signants/Subscriptors i qualsevol informació relativa a la identificació i autenticació del Signant/Subscriptor seran conservats durant almenys **15 anys**.

Les versions antigues de la documentació també seran conservades, per un període de 15 (quinze) anys per l'Entitat de Certificació, podent ser consultades, per causa raonada pels interessats.

4.11.3. Protecció de l'arxiu

Camerfirma assegura la correcta protecció dels arxius per mitjà de l'assignació de personal qualificat per al seu tractament i l'emmagatzematge en caixes de seguretat ignífugues i instal·lacions externes.

Document relacionat: **IN-2005-04-06-Procedimiento de Backups de ficheros críticos**

4.11.4. Procediments de backup de l'arxiu

Camerfirma disposa d'un centre d'emmagatzematge extern per a 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.

Document relacionat: **IN-2005-04-06-Procedimiento de Backups de ficheros críticos**

Camerfirma com a mínim realitza còpies de suport incrementals diàries de tots els seus documents electrònics i realitzar còpies de suport completes setmanalment per a casos de recuperació de dades

4.11.5. Requeriments per al segellat de temps dels registres

Els registres estan datats amb una font fiable via NTP des del ROA, GPS i sistemes de sincronització via Ràdio.

Camerfirma disposa d'un document de seguretat informàtica on descriu la configuració de temps dels equips utilitzats en l'emissió de certificats

Document relacionat: **IN-2006-04-01-Sincronizacion de tiempos**

4.11.6. Sistema d'arreplega d'informació d'auditoria

Camerfirma disposa d'un sistema centralitzat d'arreplega d'informació de l'activitat dels equips implicats en el servei de gestió de certificats.

Documentació de referència: **IN-2005-04-10-procedimiento de gestión de logs**

4.11.7. Procediments per a obtenir i verificar informació arxivada

Camerfirma disposa d'un document de seguretat informàtica on es descriu el procés per a verificar que la informació arxivada és correcta i accessible.

Document relacionat: **IN-2005-04-06-Procedimiento de Backups de ficheros críticos**

4.12. Canvi de clau

Abans de que l'ús de la clau privada de l'AC caduqui es realitzarà un canvi de claus. La vella AC i la seua clau privada només s'usaran per a la signatura de CRLs mentre existeixen certificats actius emesos per l'AC vella. Es generarà una nova AC amb una clau privada nova i un nou DN.

El canvi de claus del subscriptor és realitzat per mitjà de la realització d'un nou procés d'emissió (vegeu apartat 3.2. d'esta CPS).

Document de referència: **IN-2005-04-04-Procedimiento de cambio de claves.**

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

Camerfirma ha desenrotllat un Pla de contingències per a recuperar els sistemes crítics, si fóra necessari un centre de dades alternatiu.

El pla de continuïtat i contingències esta redactat al document CONF-2003-00-01 Continuidad y Disponibilidad.

El cas de compromís de la clau arrel ha de prendre's com un cas separat en el procés de contingència i continuïtat de negoci. Esta incidència afecta, en cas de substitució de les claus, als reconeixements per diferents programaris i serveis privats i públics. Una recuperació de l'efectivitat de les claus en termes de negoci dependrà principalment de la duració d'estos processos. El document de contingència i continuïtat de negoci tractarà els termes purament operatius perquè les noves claus estiguin disponibles, no així el seu reconeixement per tercers.

Qualsevol fallada en la consecució de les metes marcades per aquest Pla de Contingències, serà tractat com raonablement inevitable llevat que la dit fallada es degui a un incompliment de les obligacions de Camerfirma per a implementar els dits processos.

4.13.1. La clau d'una entitat es compromet

El Pla de contingències de Camerfirma tracta el compromís de la clau privada de l'AC com una situació de desastre

En cas de compromís d'una clau arrel:

- Informarà tots els Signants/Subscriptors, Tercer que confia i altres AC's amb els quals tingui acords o un altre tipus de relació del compromís.
- Indicarà que els certificats i informació relativa a l'estat de la revocació firmats usant esta clau no són vàlids.

4.13.2. Instal·lació de seguretat després d'un desastre natural o un altre tipus de desastre

Camerfirma restablirà els serveis crítics (Revocació i publicació de revocats) d'acord amb el pla de contingències i continuïtat de negoci existent restaurant l'operació normal dels serveis anteriors en les 24 hores següents al desastre.

Camerfirma disposa d'un centre alternatiu en cas de ser necessari per a la posada en funcionament dels sistemes de certificació descrit en el pla de continuïtat de negoci.

4.14. Cessament de l'AC

Abans del cessament de la seua activitat Camerfirma realitzarà les actuacions següents:

- Proveirà dels fons necessaris (per mitjà de assegurança de responsabilitat civil) per a continuar la finalització de les activitats de revocació.
- Informarà tots Signants/Subscriptors, Tercer que confien i altres AC's amb els quals tingui acords o un altre tipus de relació del cessament amb una anticipació mínima de **6 mesos**.
- Revocarà tota autorització a entitats subcontractades per a actuar en nom de l'AC en el procediment d'emissió de certificats.
- Transferirà les seues obligacions relatives al manteniment de la informació del registre i dels logs durant el període de temps indicat als subscriptors i usuaris.
- Les claus privades de l'AC seran destruïdes o inhabilitades per al seu ús.
- Camerfirma mantindrà els certificats actius i el sistema de verificació i revocació fins a l'extinció de tots els certificats emesos.

5. Controls de Seguretat Física, Procedimental i de Personal

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

5.1. Controls de Seguretat física

Camerfirma té establerts controls de seguretat física i ambiental per a protegir els recursos de les instal·lacions on es troben els sistemes, els propis sistemes i els equipaments empleats per a les operacions.

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

- Accés físic no autoritzat
- Desastres naturals
- Incendis
- Fallada dels sistemes de suport (energia electrònica, telecomunicacions, etc.)
- Afonament o demolició de l'estructura
- Inundacions
- Robatori
- Recuperació de desastres
- Eixida no autoritzada d'equipaments, informacions, suports i aplicacions relatius a components empleats per als serveis del Prestador de Serveis de Certificació

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

Document de referència: **IN-2005-01-01-Control de acceso físico**

5.1.1. Ubicació i construcció

Les instal·lacions de Camerfirma estan construïdes amb materials que garanteixen la protecció enfront d'atacs per força bruta i ubicada en una zona de baix risc de desastres i permet un ràpid accés.

En concret, la sala on es realitzen les operacions criptogràfiques és una caixa de faraday amb protecció a radiacions externes, doble sòl, detecció i extinció d'incendis, sistemes anti-humitat, doble sistema de refrigeració i sistema doble de subministrament elèctric.

5.1.2. Accés físic

L'accés físic a les dependències de Camerfirma on es duen a terme processos de certificació està limitat i protegit per mitjà d'una combinació de mesures físiques i procedimentals.

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

Les instal·lacions compten amb detectors de presència en 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 realitza amb lectors de targeta d'identificació i gestionat per un sistema informàtic que manté un log d'entrades i eixides automàtic.

L'accés als elements més crítics del sistema es realitza a través de tres zones prèvies de pas amb accés limitat incrementalment.

L'accés als sistemes de certificació està protegit amb 4 nivells d'accés. Edifici, Oficines, CPD i Sala criptogràfica.

5.1.3. Alimentació elèctrica i aire condicionat

Les instal·lacions de Camerfirma disposen d'equips estabilitzadors de corrent i un sistema d'alimentació elèctrica d'equips duplicat amb un grup electrogen.

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

5.1.4. Exposició a l'aigua

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

5.1.5. Protecció i prevenció d'incendis

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

Els dispositius criptogràfics, i suports que emmagatzemin claus de les Entitats de Certificació, compten amb un sistema específic i addicional a la resta de la instal•lació, per a la protecció davant del foc.

5.1.6. Sistema d'emmagatzematge

Cada Mitjà d'Emmagatzematge desmuntable (cintes, cartutxos, disquets, etc.) roman només a l'abast de personal autoritzat.

La informació amb classificació Confidencial, independentment del dispositiu d'emmagatzematge es guarda en armaris ignífugs o baix clau permanentment en requerint-s'hi autorització expressa per a la seua retirada.

5.1.7. Eliminació de residus

Quan haja deixat de ser útil, la informació sensible és destruïda en la forma més adequada al suport que la contingui.

- Impresos i paper: per mitjà de trituradores o en papereres disposades a aquest efecte per a posteriorment ser destruïts, baix control.

- Mitjans d'emmagatzematge: abans de ser rebutjats o reutilitzats han de ser processats per al seu esborrament físicament destruïts o fer il·legible la informació continguda.

Document de referència: **IN-2005-01-03-Seguridad medioambiental**

5.1.8. Còpia de Seguretat fora de les instal·lacions

Camerfirma utilitza un magatzem extern segur per a la custòdia de documents, dispositius magnètics i electrònics que són independents del centre operacional.

Es requereix almenys dos persones autoritzades expressament per a l'accés, depòsit o retirada de dispositius.

Document relacionat: **IN-2005-04-06-Procedimiento de Backups de ficheros críticos**

5.2. Controls procedimentals

5.2.1. Rols de confiança

Els rols de confiança o fiables són els que es descriuen en les respectives Polítiques de Certificació de manera que es garanteix una segregació de funcions que dissemina el control i limita el frau intern, no permetent que una sola persona controli de principi a fi totes les funcions de certificació, i amb una concessió de mínim privilegi, quan sigui possible.

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

- Deures associats a la funció.

- Nivell d'accés.
- Monitorització de la funció.
- Formació i conscienciació.
- Habilitats requerides.

Els rols són:

Auditor Intern:
Responsable del compliment 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. Estes funcions estaran subordinades a la direcció d'operacions, reportant tant a esta com a la direcció tècnica.

Administrador de Sistemes:
Responsable del funcionament correcte del maquinari i programari suport de la plataforma de certificació

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

Operador d'AC:
Responsable necessari conjuntament amb l'Administrador d'AC de la custòdia de material d'activació de les claus criptogràfiques, també responsable de les operacions de backup i manteniment de l'AC.

Administrador d'AR:
Persona responsable d'aprovar les peticions de certificació realitzades pel subscriptor.

Responsable de Seguretat:
Encarregat de coordinar, controlar i fer complir les mesures de seguretat definides per les polítiques de seguretat de Camerfirma. S'ha d'encarregar de qualsevol aspecte relacionat amb la seguretat de la informació: lògica, física, xarxes, organitzativa, etc.

5.2.2. Nombre de persones requerides per tasca

Camerfirma garanteix almenys dos persones per a realitzar les tasques que es detallen en les Polítiques de Certificació corresponents. Principalment en la manipulació del dispositiu de custòdia de les claus d'AC Root i AC intermèdies.

5.2.3. Identificació i autentificació per a cada rol

Les persones assignades per a cada rol són identificades per l'auditor intern que s'assegurarà que cada persona realitza les operacions per a les que està assignat.

Cada persona només controla els actius necessaris per al seu rol, assegurant així que cap persona accedeix a recursos no assignats.

L'accés a recursos es realitza depenent de l'actiu per mitjà de targetes criptogràfiques i codis d'activació.

5.2.4. Arrencada i parada del sistema de gestió PKI .

El sistema de PKI es compon dels següents mòduls :

Mòdul de Gestió d'AR, per la qual cosa s'activaran o desactivaran els serveis del gestor de pàgines específic.

Ell apagat es realitza desactivant els serveis del gestor de pàgines.

Mòdul de gestió de sol·licituds, per la qual cosa s'activés o desactivés els serveis del gestor de pàgines específic.

Mòdul de gestió de claus, ubicat a l'equip HSM. S'activa o desactiva mitjançant encès físic.

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

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

Mòdul TSA. Servidor de segells de temps. Arrencada i parada del servei.

El procés d'apagada de mòduls seguiria la seqüència :

- Mòdul de sol · licitud
- Mòdul d'AR
- Mòdul OCSP
- Mòdul TSA
- Mòdul BBDD
- Mòdul gestió de claus.

Es realitzarà l'encesa en procés invers.

Documents interns de referència: **IN-2005-05-01-Procediment per a l'apagat manual d'equips**

5.3. Controls de seguretat de personal

5.3.1. Requeriments d'antecedents, qualificació, experiència, i acreditació

Tot el personal que realitza tasques qualificades com de confiança, porta almenys un any treballant en el centre de producció i té contractes laborals fixos.

Tot el personal esta qualificat i ha sigut instruït convenientment per a realitzar les operacions que li han sigut assignades.

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

Camerfirma s'assegura de que el personal de registre o Administradors de RA és fiable i pertany a una Cambra de Comerç o de l'organisme delegat per a realitzar les tasques de registre.

L'Administrador de RA haurà realitzat un curs de preparació per a la realització de les tasques de validació de les peticions.

En general, Camerfirma retirarà de les seues funcions de confiança a un empleat quan es tingui coneixement de l'existència de la comissió d'algun fet delictiu que pogues afectar l'exercici de les seues funcions.

Documentació de referència:

IN-2005-02-07 Funciones y responsabilidad del personal.

IN-2005-02-17-Gestión Recursos humanos

IN-2008-00-06 Formato de Perfil Profesional

IN-2008-00-09-Registros de Formación

IN-2006-02-03-Organizacion para la Seguridad

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

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

5.3.2. Procediments de comprovació d'antecedents

Camerfirma dins dels seus procediments de RRHH realitza les investigacions pertinents abans de la contractació de qualsevol persona.

A la sol•licitud per al lloc de treball s'informa sobre la necessitat de sotmetre's a una investigació prèvia i s'adverteix que la negativa a sotmetre's a la investigació implicarà el rebuig de la sol•licitud. Així mateix 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.

La investigació es repetirà amb una periodicitat suficient

Camerfirma mai assigna tasques fiables a personal amb menys d'una antiguitat **d'un any**.

5.3.3. Requeriments de formació

El personal encarregat de tasques de confiança ha sigut format en els termes que estableixen les Polítiques de Certificació. Hi ha un pla de formació que forma part dels controls ISO/IEC 27001.

La formació inclou els següents continguts:

- Principis i mecanismes de seguretat de la jerarquia pública de certificació.
- Versions de maquinària i aplicacions en ús.
- Tasques que ha de realitzar la persona.
- Gestió i tramitació d'incidents i compromisos de seguretat.
- Procediments de continuïtat de negoci i emergència.
- Procediment de gestió i de seguretat en relació amb el tractament de les dades de caràcter personal.

5.3.4. Requeriments i freqüència de l'actualització de la formació

Camerfirma realitza els cursos d'actualització necessaris per a assegurar-se de la correcta realització de les tasques de certificació, especialment quan es realitzen modificacions substancials en les mateixes.

5.3.5. Freqüència i seqüència de rotació de tasques

No estipulat

5.3.6. Sancions per accions no autoritzades

Camerfirma disposa d'un règim sancionador intern, descrit en la seua política de RRHH, per a la seua aplicació quan un empleat realitzí accions no autoritzades podent arribar al seu cessament.

5.3.7. Requeriments de contractació de personal

Els empleats contractats per a realitzar tasques fiables firmen anteriorment les clàusules de confidencialitat i la requeriments operacionals empleats per Camerfirma. Qualsevol

acció que comprometi la seguretat dels processos acceptats podrien una vegada avaluats 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 previsions realitzades en aquesta secció, o en altres parts de la CPS, seran aplicats i complerts pel tercer que realitzi les funcions d'operació dels serveis de certificació, l'entitat de certificació serà responsable en tot cas de l'efectiva execució.

Aquests aspectes queden concretats a l'instrument jurídic utilitzat per acordar la prestació dels serveis de certificació pel tercer diferent de Camerfirma.

5.3.8. Documentació proporcionada al personal

Camerfirma posa a disposició de tot el personal la documentació on es detallen les funcions encomanades, en particular la normativa de seguretat i la CPS.

Addicionalment se subministrarà la documentació que precisi el personal en cada moment, a fi de que pugi desenrotllar de forma competent les seues funcions.

6. Controls de Seguretat Tècnica

6.1. Generació i instal·lació del parell de claus

6.1.1. Generació del parell de claus

Per a la generació de les clau de les AC's s'utilitzà un dispositiu que compleix els requeriments que es detallen en el **FIPS 140-1, en el seu nivell 3.** Les dades de l'equip són: nShield PCI 500 F3 de nCipher. Es disposen de HSM Eracom amb la mateixa certificació per a l'emissió de respostes OCSP i segells de temps.

Les claus corresponents a l'AC que emet certificats de servidor segur i segell d'empresa varen ser creades en un entorn segur per mitjà de mecanismes programari i baix control dual.

Es varen generar en respectives cerimònies de què hi ha documentació detallada.

AC ROOT-Chambersign Global Root 2008	**4.096**	**30 Anys**
GOBIERNO DE ANDORRA_AD_SUBCA	**4.096**	30 Anys
Certificats de persona física	2.048	3 anys
Certificats de representant	2.048	3 anys
Certificats de professional	2.048	3 anys
Certificats de persona física al servei d'una organització	2.048	3 anys

Certificats de persona física al servei d'administració	2.048	3 anys
Certificats de servidor segur	2.048	3 anys
Certificats de seu electrònica	2.048	3 anys
Certificats d'actuació de persona jurídica	2.048	3 anys
Certificats d'actuació de l'Administració	2.048	3 anys
Certificats d'entitat de segellament de data i hora	2.048	1,2,3,4,5,6 anys
Certificats de signatura de programari	2.048	3 anys
Certificats de xifratge	2.048	3 anys

Més informació en https://pki.govern.ad/politiques

Documentació de referència:
CONF-00-2012-01/06/07/08 ACTAS **de ceremonias de creación de claves.**

CONF-00-2012-02/04 **SCRIPTS de Generación de claves.**

CONF-00-2012-05 **Informe Auditores E&Y**

CONF-00-2012-03 **Reparto de claves entre operadores**

6.1.1.1. Generació del parell de claus del subscriptor

Les claus del Signant/Subscriptor poden ser creades per ell mateix per mitjà de dispositius maquinari o programari autoritzats per Camerfirma o poden ser creades per Camerfirma en format programari **PKCS#12.**

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

Les claus Tenen una longitud mínima de **2048 bits**.

En el cas que el subscriptor generi les claus en un dispositiu criptogràfic propi. Camerfirma exigirà un informe tècnic d'auditoria que valorarà abans d'emetre un certificat marcat amb claus generades en dispositiu maquinari. Si el subscriptor no aportarà el document o no fóra satisfactori Camerfirma només estaria en condicions d'emetre un certificat catalogat com a claus generades en dispositiu programari.

6.1.2. Entrega de la clau publica a l'emissor del certificat

L'enviament de la clau pública a Camerfirma per a la generació del certificat quan el circuit així ho requereixi, es realitza per mitjà d'un format estàndard preferiblement en format **PKCS#10** o **X509 autosignat**.

6.1.3. Entrega de la clau pública de l'AC als usuaris

El certificat de l'AC i el seu fingerprint (empremta digital) estaran a disposició dels usuaris en la pàgina Web https://pki.govern.ad

6.1.4. Longitud i període de validesa de les claus de l'emissor

Consultar apartat 6.1.1

6.1.5. Longitud i període de validesa de les claus del subscriptor

Les claus privades del Signant/Subscriptor estan basades en l'algoritme **RSA** amb una longitud mínima de **2048** bits.

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

6.1.6. Paràmetres de generació de la clau pública.

La clau pública de l'AC Arrel i de l'AC Subordinada i dels certificats dels subscriptors està codificada d'acord amb RFC 3280 i PKCS#1. L'algoritme de generació de claus és el RSA.

6.1.7. Comprovació de la qualitat dels paràmetres

- Longitud del Mòdul = 2048
- Algoritme de generació de claus: rsagen1
- Mètode de farcit: emsa-pkcs1-v1_5
- Funcions criptogràfiques de Resum: SHA-1.

6.1.8. Maquinari/programari de generació de claus

Les claus dels Signants/Subscriptors poden ser generades per ells mateixos en un dispositiu autoritzat per Camerfirma. Veure 6.1.1.1

Les claus de les AC´s han sigut generades en un mòdul criptogràfic nShield PCI 500 F3 de nCipher. Aquest dispositiu compleix les especificacions FIPS 140-2 level 2 i level 3.

6.1.9. Fins de l'ús de la clau

En el següent gràfic es descriu els usos de la clau per als distints certificats emesos. La

solució adoptada per a la diferenciació d'usos és la següent:

Certificats per a autenticació bit DS (pot conviure amb altres usos)

Certificats per a signatura electrònica bit DS + NR (pot conviure amb altres usos)

Certificats exclusius de signatura reconeguda bit NR (NO pot conviure amb altres usos). Actualment Camerfirma no emet certificats exclusius de signatura electrònica reconeguda però aquest model marca les pautes que s'ha de seguir en el moment de la seua incorporació.

AC	DS	NR	KE	DE	KA	KCS	CRL	EO	DO
AC ROOT - Chambersign Global						x	x		
Entitat de Certificació de l'Administració Pública Andorrana - SubCA	x					x	x		
Certificat d'actuació de PERSONA FÍSICA INDIVIDUAL (en DSCF) Perfil de SIGNATURA		x							
Certificat d'actuació de PERSONA FÍSICA INDIVIDUAL (en DSCF) Perfil d'IDENTITAT	x								
Certificat d'actuació de PERSONA FÍSICA INDIVIDUAL (en programari)	x	x	x						
Certificat d'actuació de PERSONA FÍSICA PROFESSIONAL (en DSCF) Perfil de SIGNATURA		x							
Certificat d'actuació de PERSONA FÍSICA PROFESSIONAL (en DSCF) Perfil d'IDENTITAT	x								
Certificat d'actuació de PERSONA FÍSICA PROFESSIONAL (en programari)	x	x	x						
Certificat d'actuació de PERSONA FÍSICA PROFESSIONAL		x							

AC	DS	NR	KE	DE	KA	KCS	CRL	EO	DO
COL•LEGIAT (en DSCF) Perfil de SIGNATURA									
Certificat d'actuació de PERSONA FÍSICA PROFESSIONAL COL•LEGIAT (en DSCF) Perfil d'IDENTITAT	x								
Certificat d'actuació de PERSONA FÍSICA PROFESSIONAL COL•LEGIAT (en programari) Perfil de XIFRAT			x	x					
Certificat d'actuació de PERSONA FÍSICA PROFESSIONAL COL•LEGIAT (programari)	x	x	x						
Certificat d'actuació de PERSONA FÍSICA al servei d'una ORGANITZACIÓ (en DSCF) Perfil de SIGNATURA		x							
Certificat d'actuació de PERSONA FÍSICA al servei d'una ORGANITZACIÓ (en DSCF) Perfil d'IDENTITAT	x								
Certificat d'actuació de PERSONA FÍSICA al servei d'una ORGANITZACIÓ (programari)	x	x	x						
Certificat d'actuació de PERSONA FÍSICA al servei de l'ADMINISTRACIÓ (en DSCF) Perfil de SIGNATURA		x							
Certificat d'actuació de PERSONA FÍSICA al servei de l'ADMINISTRACIÓ (en DSCF) Perfil d'IDENTITAT	x								
Certificat d'actuació de PERSONA FÍSICA al servei de l'ADMINISTRACIÓ (programari) Perfil de XIFRAT			x	x					

AC	DS	NR	KE	DE	KA	KCS	CRL	EO	DO
Certificat d'actuació de PERSONA FÍSICA al servei de l'ADMINISTRACIÓ (en programari)	x	x	x						
Certificat de SEU ELECTRÒNICA per les ADMINISTRACIONS Andorranes, amb Extend Validation. Perfil en Dispositiu Segur (HSM)		x							
Certificat de SEU ELECTRÒNICA per les ADMINISTRACIONS Andorranes, amb Extend Validation. Perfil en programari			x	x					
Certificat d'actuació d'Administració, Òrgan o Entitat de Dret Públic. Perfil en Dispositiu Segur (HSM)	x		x						
Certificat d'actuació d'Administració, Òrgan o Entitat de Dret Públic. Perfil en programari	x	x	x	x					
Certificat d'actuació de SEGELL D'EMPRESA (Persona Jurídica) en HSM. Perfil de segell electrònic		x							
Certificat d'actuació de SEGELL D'EMPRESA (Persona Jurídica) en HSM. Perfil d'identitat	x								
Certificat d'actuació de SEGELL D'EMPRESA (Persona Jurídica) en programari	x	x	x	x					
Certificat d'actuació de REPRESENTANT PERSONA FÍSICA (en DSCF) Perfil de SIGNATURA		x							
Certificat d'actuació de REPRESENTANT PERSONA FÍSICA (en DSCF) Perfil d'IDENTITAT	x								

AC	DS	NR	KE	DE	KA	KCS	CRL	EO	DO
Certificat d'actuació de REPRESENTANT PERSONA FÍSICA (en programari)	x	x	x	x					
Certificat d'actuació de REPRESENTANT PERSONA JURÍDICA (en HSM) Perfil de SIGNATURA		x							
Certificat d'actuació de REPRESENTANT PERSONA JURÍDICA (en HSM) Perfil d'IDENTITAT	x								
Certificat d'actuació de REPRESENTANT PERSONA JURÍDICA (en programari)	x	x	x	x					
Certificat de SERVIDOR SEGUR, amb Extend Validation. Perfil en Dispositiu Segur (HSM)	x		x						
Certificat de SERVIDOR SEGUR, amb Extend Validation. Perfil en programari	x		x						
Certificat de SIGNATURA DE PROGRAMARI	x	x							
Certificat d'entitat de Segellament de data i hora (Marcatge de Temps)	x	x							

DS Signatura Digital

NR No Repudi, "ContentCommitment"

KE Xifrat de Clau

DE Xifrat de Dades

CA Acord de clau

KCS Signatura de certificats

CRLS Signatura de CRL

EO Només Xifrat

DO Només desxifrat

(*) A pesar de que és possible tècnicament Camerfirma no es responsabilitza del seu ús per a estos fins

6.2. Protecció de la clau privada

Clau privada de l'AC

La clau privada de signatura de l'AC és mantinguda i usada en un dispositiu criptogràfic segur que compleix els requeriments **FIPS 140-1 nivell 3**.

Per a la gestió de les claus de les Autoritats de Certificació s'utilitza un equip criptogràfic nShield PCI 500 F3 de nCipher **homologat dispositiu FIPS 140-1 nivell 2 i nivell 3.**

Per a les claus de les autoritats d'OCSP i TSA s'utilitza un equip **Eracom certificat FIPS 140-1 nivell 3 o custodia de claus en dispositiu smartcard amb certificació CWA14169.**

Quan al clau privada de l'AC està fora del dispositiu esta es manté xifrada i partida en diferents dispositius.

Hi ha un back-up de la clau privada de signatura de l'AC, que és emmagatzemada i recuperada només pel personal autoritzat segons els rols de confiança, usant, almenys un control dual en un medi físic segur.

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

Clau privada del subscriptor

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

Quan s'emmagatzemi en format programari Camerfirma oferirà les instruccions de configuració adequada per a un ús segur en les aplicacions reconegudes.

Respecte als dispositius criptogràfics amb certificats per a signatura electrònica avançada, aptes com a dispositius segurs de creació de signatura, compleixin el nivell de seguretat CC EAL4+ i suporten els estàndards PKCS#11 i CSP.

Camerfirma utilitza com a suport criptogràfic aquells permesos en el seu programari de registre i que asseguraran la generació de signatura electrònica reconeguda.

La informació respecte al tipus de creació i custòdia de claus esta incorporada en el propi certificat digital permetent a la Tercer que confia actuar en conseqüència.

6.3. Estàndards per als mòduls criptogràfics

Veure 6.2

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

Es requereix un control multi-persona per a l'activació de la clau privada de l'AC. En el cas d'esta CPS, en concret hi ha una política de **2 de 4** persones per a l'activació de les claus.

Documentació de referència: **CONF-00-2012-03-Reparto de claves entre operadores**

6.3.2. Custòdia de la clau privada

Camerfirma no emmagatzema ni còpia claus privades dels subscriptors quan estes són generades pel PSC i estan subjectes a la llei 6/2009, del 29 de desembre, de signatura electrònica. Per a certificats en suport maquinari és l'usuari qui genera i custòdia la clau privada en la targeta criptogràfica entregada pel PSC.

Camerfirma únicament emmagatzemarà una còpia de la clau privada del subscriptor quan esta s'utilitzi "exclusivament" per a xifrat de dades o aquells certificats associats a les claus que no estiguin subjectes a la llei 6/2009, del 29 de desembre, de signatura electrònica.

6.3.3. Còpia de seguretat de la clau privada

Camerfirma realitza una còpia de back up de les claus privades de les AC's que fan possible la seua recuperació en cas de desastre, de pèrdua o deteriorament de les mateixes. Tant la generació de la còpia com la recuperació d'esta necessiten almenys de la participació de dos persones.

Estos fitxers de recuperació s'emmagatzemen en armaris ignífugs i en el centre de custòdia extern.

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

Les claus del subscriptor en maquinari no es poden copiar ja que no poden eixir del dispositiu criptogràfic.

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

Documentació de referència: **CONF-00-2012-01-Acta de backup de las claves de las claves de root**

6.3.4. Arxiu de la clau privada

Les claus privades de les ACS són arxivades per un període de **10 anys** després de l'emissió de l'últim certificat. S'emmagatzemaren en arxius ignífugs segurs i en el centre de custòdia extern. Almenys serà necessària la col·laboració de dos persones per a recuperar la clau privada de les AC en el dispositiu criptogràfic inicial.

El subscriptor podrà emmagatzemar les claus entregades en programari durant el període de duració del certificat, posteriorment haurà de destruir-les assegurant-se abans de que no té cap informació xifrada amb la clau publica.

Només en cas de certificats de xifrat el subscriptor podrà emmagatzemar la clau privada el temps que cregui oportú. En aquest cas Camerfirma també guardarà còpia de la clau privada associada al certificat de xifrat.

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

6.3.5. Introducció de la clau privada en el mòdul criptogràfic.

Les claus de les Autoritats de certificació es creïn a l'interior dels dispositius criptogràfics. Veure cerimònies de creació de les claus de l'Autoritat de Certificació de Camerfirma.

CONF-00-2012-01/06/07/08 ACTAS **de ceremonias de creación de claves.**

Les claus en programari dels subscriptors es creïn en els sistemes de Camerfirma i són entregades al subscriptor final en un dispositiu programari PKCS#12. Veure procediment de creació de claus pel subscriptor.

Les claus en maquinari dels subscriptors es creïn dintre del dispositiu criptogràfic entregat per l'AC. Veure procediment de creació de claus pel subscriptor.

La introducció de la clau en mòdul criptogràfic es realitzarà almenys amb la participació de dos persones.

Les claus associades als subscriptors no poden ser transferides.

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

6.3.6. Mètode d'activació de la clau privada.

L'accés a la clau privada del subscriptor es realitza per mitjà d'un PIN que coneixerà només el subscriptor i que evitarà tindre-ho per escrit.

Les claus de l'AC s'activen per un procés de m de n. Vegeu apartat 6.3.1

L'activació de les claus privades de la AC intermèdia són gestionades pel programari de gestió.

Documentació de referència: **CONF-2008-04-09-Acceso_PKCS#11_CAS_online**

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

6.3.7. Mètode de desactivació de la clau privada

La clau privada del subscriptor quedarà desactivada una vegada es retiri el dispositiu criptogràfic de creació de signatura del dispositiu de lectura.

Quan la clau estigi en suport programari, podrà ser desactivada per mitjà de l'esborrament de les dites claus de l'aplicació corresponent en què estiguin instal·lades.

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

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

6.3.8. Mètode de destrucció de la clau privada

Anteriorment a la destrucció de les claus s'emetrà una revocació del certificat de les claus públiques associades a les mateixes.

Es destruiran físicament o reinicialitzaran a baix nivell els dispositius que tinguin emmagatzemada qualsevol part de les claus privades de les AC's de les Jerarquies. Per a l'eliminació se seguiran els passos descrits en el manual de l'administrador de l'equip criptogràfic.

Finalment es destruiran de forma segura les còpies de seguretat.

Les claus del subscriptor en programari es podran destruir per mitjà de l'esborrament d'estes seguint les instruccions de l'aplicació que les alberga.

Les claus del subscriptor en maquinari podran ser destruïdes per mitjà d'un programari especial en els punts de Registre o en l'AC.

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

Document de referència: **IN-2006-05-01-Destrucción Claves de Usuario**

6.4. Altres aspectes de la gestió del parell de claus

6.4.1. Arxiu de la clau pública

L'AC, en compliment d'allò que s'ha establert per l'article 20 d) de la llei 6/2009, del 29 de desembre, de signatura electrònica, mantindrà els seus arxius per un període mínim **de quinze (15) anys** sempre que la tecnologia de cada moment ho permeti. Dins de la documentació a custodiar es troben els certificats de clau pública emesos als seus subscriptors i els certificats de clau pública propis.

6.4.2. Període d'ús per a les claus públiques i privades

Un certificat de clau pública o la clau privada corresponent no hauria de ser usat després del període de validesa del mateix.

Una clau privada podrà ser utilitzada fora del període marcat pel certificat digital corresponent, únicament per a la recuperació de dades xifrats.

6.5. Cicle de vida del dispositiu segur de creació de signatura.

Els certificats de l'AC s'emmagatzemen en un dispositiu segurs de creació de signatura **(Maquinari)** o en dispositiu segur de magatzem de dades de creació de signatura **(programari)** quedant esta situació reflectida en el contingut del propi certificat.

El dispositiu programari s'entrega en format PKCS#12 per a importar-ho en les aplicacions. El fitxer queda en custòdia del subscriptor per a la seua possible recuperació, havent de guardar les dades d'instal·lació en un lloc separat del fitxer de claus.

Un altre cas de dispositiu programari és l'utilitzat en els certificats de servidor segur on les claus es generen amb els recursos de l'aplicació del servidor de pàgines.
El dispositiu **maquinari** és una targeta criptogràfica o token USB que compleix els requeriments d'acreditació determinats en la legislació vigent o almenys **ITSEC E4+.** Estos dispositius estaran exposats en la pàgina Web https://pki.govern.ad http://www.bit4id.com/es/descargas_camerfirma_bit4id.htm

Respecte als dispositius maquinari

a) Els dispositius maquinari són preparats i estampades per un proveïdor extern.
b) La gestió de distribució del suport la realitza el proveïdor extern que ho distribueix a les autoritats de registre per al seu entrega al subscriptor.
c) El subscriptor o l'AR utilitza el dispositiu per a generar el parell de claus i enviar la clau pública a l'AC.
d) L'AC envia un certificat de clau pública al subscriptor o la RA que és introduït en el dispositiu.
e) El dispositiu és reutilitzable i pot mantenir de forma segura diversos parells de claus.

6.6. Controls de seguretat informàtica

Camerfirma empra sistemes fiables per a oferir els seus serveis de certificació. Camerfirma ha realitzat controls i auditories informàtiques a fi d'establir una gestió dels seus actius informàtics adequats amb el nivell de seguretat requerit en la gestió de sistemes de certificació electrònica.

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

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

1. Configuració de seguretat del 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 Log.
6. Pla de backup i recuperació.
7. Configuració contra virus
8. Requeriments de tràfic de xarxa

6.6.1. Requeriments tècnics de seguretat informàtica específics

Cada servidor de Camerfirma inclou les funcionalitats següents:

- ✓ control d'accés als serveis d'AC i gestió de privilegis
- ✓ imposició de separació de tasques per a la gestió de privilegis
- ✓ identificació i autenticació de rols associats a identitats
- ✓ arxiu de l'historial del subscriptor i l'AC i dades d'auditoria
- ✓ auditoria d'esdeveniments relatius a la seguretat
- ✓ auto-diagnòstic de seguretat relacionat amb els serveis de l'AC
- ✓ Mecanismes de recuperació de claus i del sistema d'AC

Les funcionalitats exposades són realitzades per mitjà d'una combinació de sistema operatiu, programari de PKI, protecció física i procediments.

6.6.2. Valoració de la seguretat informàtica

La seguretat dels equips ve reflectida per una anàlisi de riscos inicials de tal forma que les mesures de seguretat implantades són resposta a la probabilitat i impacte produït quan un grup d'amenaces definides puguin aprofitar bretxes de seguretat.

6.7. Controls de seguretat del cicle de vida

6.7.1. Controls de desenvolupament del sistema

Camerfirma posseeix un procediment de control de canvis en les versions de sistemes operatius i aplicacions que impliquen una millora en les seues funcions de seguretat o que corregeixin qualsevol vulnerabilitat detectada.

Documentació de referència:

IN-2006-05-02-Clausulas exigibles a desarrolladores externos

IN-2006-03-04-Control de cambios a Sistemas y Software

6.7.2. Controls de gestió de la seguretat

6.7.2.1. Gestió de seguretat

Camerfirma exerceix les activitats precises per a la formació i conscienciació dels empleats en matèria de seguretat. Els materials empleats per a la formació i els documents descriptius dels processos són actualitzats després de la seua aprovació per un grup per a la gestió de la seguretat.

Par a realitzar aquesta funció disposa d'un pla de formació anual.

Camerfirma exigeix per mitjà de contracte, les mesures de seguretat equivalents a qualsevol proveïdor extern implicat en les labors de certificació.

6.7.2.2. Classificació i gestió d'informació i béns

Camerfirma manté un inventari d'actius i documentació i un procediment per a la gestió d'aquest material per a garantir el seu ús.

Documentació de referència: **IN-2005-02-15-Clasificación e Inventario de Activos**

La política de seguretat de Camerfirma detalla els procediments de gestió de la informació on es classifica segons el seu nivell de confidencialitat.

Els documents estan catalogats en tres nivells: PÚBLIC, ÚS INTERN i CONFIDENCIAL.

Documentació de referència: **IN-2005-02-04-Política de Seguridad**

6.7.2.3. Operacions de gestió

Camerfirma disposa d'un adequat procediment de gestió i resposta d'incidències, per mitjà de la implementació d'un sistema d'alertes i la generació de reports periòdics.

En el document de seguretat de Camerfirma es desenrotlla en detall el procés de gestió d'incidències.

Documentació de referència: **IN-2010-10-08 Gestión de incidencias**

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

Documentació de referència: **IN-2005-02-07 Funciones y responsabilidad del personal**

Tractament dels suports i seguretat

Tots els suports són tractats de forma 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 tornaran a ser requerits.

Documentació de referència:
CONF-2006-01-04-Procedimiento de Registro de Entradas y Salidas de Soportes
IN-2005-02-15-Clasificación e Inventario de Activos

Planning del sistema

El departament de Sistemes de la Camerfirma 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.

Documentació relacionada:

IN-2010-10-10 Gestión de Configuración
IN-2010-10-05 Gestión de la capacidad
IN-2010-10-03 Gestión de la Disponibilidad
IN-2010-10-01 Gestión del Nivel de Servicio
IN-2010-10-00 Manual de Gestión de Servicios de TI
IN-2010-10-13 Planificación de Nuevos Servicios

Reports d'incidències i resposta

Camerfirma disposa d'un procediment per al seguiment d'incidències i la seua resolució on es registren les respostes i una avaluació econòmica que suposa la resolució de la incidència.

Documentació de referència: **IN-2010-10-08 Gestión de incidencias**

Procediments operacionals i responsabilitats

Camerfirma defineix activitats, assignades a persones amb un rol de confiança, diferents de les persones encarregades de realitzar les operacions quotidianes que no tenen caràcter de confidencialitat.

Documentació de referència: **IN-2005-02-07 Funciones y responsabilidad del personal**

6.7.2.4. Gestió del sistema d'accés

Camerfirma realitza tots els esforços que raonablement estan al seu abast per a confirmar que el sistema d'accés està limitat a les persones autoritzades.

Documentació de referència: **IN-2011-04-10-CONTROL_DE_ACCESOS_A_RED**

En particular:

AC General

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

b) Les dades sensibles són protegits per mitjà de tècniques criptogràfiques o controls d'accés amb identificació forta.

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

d) Camerfirma disposa de procediments per a assegurar que les operacions es realitzen respectant la política de rols.

e) Cada persona té associat un rol per a realitzar les operacions de certificació.

f) El personal de Camerfirma és responsable dels seus actes per mitjà del compromís de confidencialitat firmat amb l'empresa.

Generació del certificat

L'autenticació per al procés d'emissió es realitza per mitjà d'un sistema m de n operadors per a l'activació de la clau privada de l'AC.

Gestió de la revocació

La revocació es realitzarà per mitjà d'autenticació forta amb targeta a les aplicacions d'un administrador autoritzat. Els sistemes de logs generaran les proves que garanteixen el no repudi de l'acció realitzada per l'administrador d'AC.

Estat de la revocació

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

6.7.2.5. Gestió del cicle de vida del maquinari criptogràfic

Camerfirma s'assegura que el maquinari criptogràfic usat per a la signatura de certificats no es manipula durant el seu transport per mitjà de la inspecció del material entregat.

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

Camerfirma registra tota la informació pertinent del dispositiu per a afegir al catàleg d'actius.

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

Camerfirma realitza test de proves periòdiques per a assegurar el funcionament correcte del dispositiu.

El dispositiu maquinari criptogràfic només és manipulat per personal fiable.

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

La configuració del sistema de l'AC així com les seues modificacions i actualitzacions són documentades i controlades.

Camerfirma posseeix un contracte de manteniment del dispositiu. Els canvis o actualitzacions són autoritzats pel responsable de seguretat i queden reflectits en les actes de treball corresponents. Estes configuracions es realitzaran almenys per dos persones fiables.

6.7.3. Avaluació de la seguretat del cicle de vida

No estipulat

6.8. Controls de seguretat de la xarxa

Camerfirma protegeix l'accés físic als dispositius de gestió de xarxa i disposa d'una arquitectura que ordena el tràfic generat basant-se en les seues característiques de seguretat creant seccions de xarxa clarament definides. Esta divisió es realitza per mitjà de l'ús de tallafocs.

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

Documentació de referència: **IN-2011-04-10-CONTROL_DE_ACCESOS_A_RED**

6.9. Fonts de Temps

Camerfirma té un procediment de sincronització de temps coordinat amb el ROA (Reial Institut i Observatori de l'Armada) en San Fernando via NTP. També obté una font segura via GPS i sincronització via Ràdio.

Document relacionat: **IN-2006-04-01-Sincronizacion de tiempos**

6.10. Controls d'enginyeria dels mòduls criptogràfics

Totes les operacions criptogràfiques de l'AC són realitzades en mòduls validats almenys per **FIPS 140-1 nivell 3**.

7. Perfils de Certificat i CRL

7.1. Perfil de Certificat

Tots els certificats emesos davall esta política estan de conformitat amb l'estàndard X.509 versió 3 i al RFC 3739 y ETSI 101 867 "QualifiedCertificate Profile".

7.1.1. Número de versió

Camerfirma emet certificats X.509 Versió 3

7.1.2. Extensions del certificat

Els documents de les extensions dels certificats es troben detallats en documents independents que poden ser accedits des de la pàgina Web de Camerfirma.

Aquest mètode de publicació permet mantenir versions de les polítiques i CPS més estables i deslligar-los dels molt freqüents ajustos en els perfils dels certificats.

7.1.3. Identificadors d'objecte (OID) dels algoritmes

L'identificador d'objecte de l'algoritme de signatura és:

- 1.2.840.113549.1.1.5 sha1WithRSAEncryption
- 1.2.840.113549.1.1.11 - sha256WithRSAEncryption

L'identificador d'objecte de l'algoritme de la clau pública és:

- 1.2.840.113549.1.1.1 rsaEncryption

7.1.4. Format de Noms

Els certificats hauran de contenir les informacions que resultin necessàries per al seu ús, segons determini la corresponent política d'autenticació, signatura electrònica, xifrat o evidència electrònica.

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

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

Aquesta norma no s'aplica als certificats amb pseudònim, que han d'identificar aquesta condició.

7.1.5. Restriccions dels noms

Els noms continguts en els certificats estan restringits a "Distinguished Names" X.500, que són únics i no ambigus.

Addicionalment es poden establir restriccions de noms en relació amb els certificats a la corresponent política d'autenticació, signatura electrònica, xifratge o evidència electrònica, sempre que les mateixes resultin objectives, proporcionades, transparents i no discriminatòries.

7.1.6. Identificador d'objecte (OID) de la Política de Certificació

Tots els certificats tenen un identificador de política que s'ajusta al model següent:

2.16.20.2.1.3.1.X.Y

X = Tipus de certificat

Y = Nivell de Seguretat del certificat.

Per a les autoritats de Certificació Intermèdies s'ha definit també un OID de política amb el prefix 2.16.20.2.1.3.1.

El OID en les entitats de certificació limita el conjunt de polítiques que es troben al llarg de la cadena de certificació. En el nostre cas en tota la cadena ha d'aparèixer el OID 2.16.20.2.1.3.1

7.2. Perfil de CRL

El perfil de les CRLs es correspon amb el proposat en les Polítiques de certificació corresponents però en tot cas d'acord amb l'especificació tècnica IETF RFC 5280. Les CRLs són firmades per l'AC que ha emès els certificats.

7.2.1. Número de versió

Les CRL emeses per Camerfirma són de la versió 2.

7.2.2. CRL i extensions

Les imposades per les polítiques de certificació corresponents.

7.2.3. Perfil d'OCSP

Segons l'estàndard RFC 5677 i l'especificació tècnica IETF RFC 5019.

8. Especificació de l'Administració

8.1. Autoritat de les polítiques

L'àrea jurídica de Camerfirma es constitueix l'autoritat de les polítiques (PA) i és responsable de l'administració de les Polítiques i CPS

8.2. Procediments d'especificació de canvis.

Aquesta CPS es modificarà quan es produïsquen canvis rellevants en la gestió de qualsevol tipus de certificats subjectes a ella. Es produiran almenys revisions biennals en el cas que no es produïsquen canvis en aquest temps. Aquestes revisions quedaran reflectides en el quadre de versions a l'inici del document.

8.2.1. Elements que poden canviar sense necessitat de notificació

Els canvis que poden realitzar-se a esta CPS no requereixen notificació excepte que afecte de forma directa als drets dels Signants/Subscriptors dels certificats, i en aquest cas deuran a fi de que puguin presentar els seus comentaris a l'organització de l'administració de les polítiques dins dels 15 dies següents a la publicació.

8.2.2. Canvis amb notificació

8.2.2.1. Llista d'elements

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

8.2.2.2. Mecanisme de notificació

Tots els canvis proposats d'esta política seran immediatament publicats en la Web https://pki.govern.ad

En aquest mateix document hi ha un apartat de canvis i versions on es pot conèixer els canvis produïts des de la seua creació i la data de les dites modificacions.

8.2.2.3. 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 **15 dies** següents a la recepció de la notificació.

8.2.2.4. Mecanisme de tractament dels comentaris

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

8.2.3. Publicació i còpia de la política

Una còpia d'aquesta CPS estarà disponible en format electrònic en l'adreça d'Internet https://pki.govern.ad

8.2.4. Procediments d'aprovació de la CPS

La publicació de les revisions d'esta CPS haurà d'estar aprovada per la Gerència de Camerfirma.

AC Camerfirma publica al seu pàgina web cada nova versió. La CPS està publicada format PDF signat electrònicament amb el certificat digital de persona jurídica d'AC Camerfirma SA.