Caixa Andorrana de Seguretat Social

Polítiques de certificació

Caixa Andorrana de Seguretat Social – Polítiques de certificació

Caixa Andorrana de Seguretat Social

Telèfon: +376 870870

Fax: +376 860986

Web: www.cass.ad

A/e: cass@cass.ad

CONTINGUT

Introducció

Estàndards aplicables

[X.509] ISO/IEC 9594-8/ITU-T RECOMMENDATION X.509: Information Technology – Open Systems Interconnection: The Directory: Public-key and attribute certificate frameworks, 2000.

[X.501] ITU-T Recommendation X.501: Information Technology – Open Systems Interconnection - The Directory: Models, 2001.

[X.520] ITU-T Recommendation X.520: Information Technology – Open Systems Interconnection - The Directory: Selected attribute types, 2001.

[X.680] ITU-T Recommendation X.680: Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation, 2002

[X.690] ITU-T Recommendation X.690 : Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER) , 2002

[TS 101862] European Telecommunications Standards Institute, "Qualified Certificate Profile", ETSI TS 101 862 v 1.2.1, 2001.

[TS 101 456] European Telecommunications Standards Institute, "Policy Requirements for Certification Authorities Issuing Qualified Certificates," ETSI TS 101 456, v 1.2.1, 2002.

[RFC 3280] HOUSLEY, FORD, POLK, SOLO, "IETF RFC 3280, Internet X.509 Public Key Infrastructure, Certificate and CRL Profile", 2002. Obsoleta RFC 2459.

[RFC 2510] C. Adams, S. Farrell "IETF RFC 2510, Internet X.509 Public Key Infrastructure, Certificate Management Protocols", 1999

[RFC 1738] Berners-Lee, T., L. Masinter and M. McCahill, "Uniform Resource Locators (URL)", RFC 1738, December 1994.

Objecte del document

Aquest document presenta la definició dels perfils de certificació i les llistes de revocació definits dins de l'entorn de la PKI de la Caixa Andorrana de Seguretat Social.

No s'especifiquen els perfils dels certificats necessaris per a l'operació pròpia de la PKI. Aquests es requereixen per al funcionament intern dels diferents elements de la PKI, com ara la signatura de registres de la BD, servidors SSL dels diferents mòduls, etc.

En l'apèndix A s'enumeren els certificats d'aquest tipus necessaris en les configuracions KeyOne®.

Aquest document, un cop aprovat pel cap del projecte i els responsables tècnics de la Caixa Andorrana de Seguretat Social, servirà com a marc de treball per a totes les tasques relatives a la implantació operativa de la PKI de la Caixa Andorrana de Seguretat Social.

CAPÍTOL 1

Descripció de les polítiques

Nom de la CP	OID assignat	Descripció
Política de CA arrel	1.3.6.1.4.1.20696.1.1.1	Certificat de l'autoritat de certificació arrel. El certificat emès sota aquesta política és autosignat i s'utilitza per a la signatura de certificats d'autoritat de certificació (CA) i de les llistes de revocació (ARL) corresponents.
Política de CA subordinada	1.3.6.1.4.1.20696.1.1.2	Certificat de l'autoritat de certificació subordinada. Els certificats emesos sota aquesta política estan signats per l'autoritat de certificació arrel i s'utilitzen per a la signatura de certificats d'autoritat de registre (RA), d'entitat final (EF) i de les llistes de revocació (CRL) corresponents.
Política d'RA	1.3.6.1.4.1.20696.1.2.1.1	Certificat de l'autoritat de registre. Els certificats emesos sota aquesta política estan signats per l'autoritat de certificació subordinada i s'utilitzen per a la signatura de lots de peticions. Aquest tipus de certificats s'ha de donar d'alta en l'autoritat de certificació subordinada com a RA reconeguda.
Política d'EF tramitador d'empresa	1.3.6.1.4.1.20696.1.2.2.1	Certificat dels tramitadors d'empreses. Els certificats emesos sota aquesta política estan signats per l'autoritat de certificació subordinada i s'utilitzen per a l'autenticació davant d'una aplicació web de la Caixa Andorrana de Seguretat Social, accessible a través d'Internet, i per a la signatura dels formularis HTML enviats a aquesta.
Política d'EF personal CASS	1.3.6.1.4.1.20696.1.2.2.2	Certificat del personal de la Caixa Andorrana de Seguretat Social. Els certificats emesos sota aquesta política estan signats per l'autoritat de certificació subordinada i s'utilitzen per a l'autenticació davant d'aplicacions web de la Caixa Andorrana de Seguretat Social, accessibles a través d'una intranet. A més, alguns dels certificats emesos sota aquesta

		política s'utilitzen com a certificats d'aprovadors de registre per a l'autenticació davant de l'autoritat de registre, per a la signatura d'aprovacions, denegacions i modificacions de peticions de certificat i per a la signatura de peticions de revocació, suspensió i habilitació de certificats. Aquests certificats s'han de donar d'alta en l'autoritat de registre com a aprovadors d'RA reconeguts.
Política d'EF dispositiu físic de servidor web	1.3.6.1.4.1.20696.1.2.3.1	Certificat dels servidors web Internet/intranet de la Caixa Andorrana de Seguretat Social. Els certificats emesos sota aquesta política estan signats per l'autoritat de certificació subordinada i s'utilitzen per establir canals segurs SSL/TLS amb els navegadors client que accedeixin als servidors web Internet/intranet de la Caixa Andorrana de Seguretat Social.

Clàusules aplicables

Comunitat d'aplicació

Nom de la CP	OID assignat	Comunitat d'aplicació
Política de CA arrel	1.3.6.1.4.1.20696.1.1.1	Aquest tipus de certificat correspon a l'entitat de certificació que proveeix la confiança en la infraestructura de la Caixa Andorrana de Seguretat Social. El certificat emès sota aquesta política ha d'estar present en tot l'àmbit d'ús de la infraestructura de la Caixa Andorrana de Seguretat Social, ja que és estrictament necessari per dur a terme les operacions de verificació associades a l'ús de la signatura digital. Aquest certificat és utilitzat per l'autoritat de certificació arrel de la infraestructura de la Caixa Andorrana de Seguretat Social per a la signatura de certificats d'autoritat de certificació (CA) i de les llistes de revocació (CRL) corresponents. L'ús d'aquest certificat fora de l'àmbit previst i descrit en aquest apartat està estrictament prohibit.
Política de CA subordinada	1.3.6.1.4.1.20696.1.1.2	Els certificats emesos sota aquesta política són utilitzats per les autoritats de certificació subordinades de la infraestructura de la Caixa Andorrana de Seguretat Social per a la signatura de certificats d'autoritat de registre (RA) i d'entitat final (EF) i de les llistes de revocació (CRL) corresponents. L'ús d'aquest certificat fora de l'àmbit previst i descrit en aquest apartat està estrictament prohibit.
Política d'RA	1.3.6.1.4.1.20696.1.2.1.1	Els certificats emesos sota aquesta política són utilitzats per les autoritats de registre de la infraestructura de la Caixa Andorrana de Seguretat Social per a la signatura de lots de peticions. A més, aquests certificats poden ser utilitzats internament per KeyOne® RA per signar registres a la seva base de dades i3D (*veg. apèndix A*). L'ús d'aquest certificat fora de l'àmbit previst i descrit en aquest apartat està estrictament prohibit.

Política d'EF tramitador d'empresa	1.3.6.1.4.1.20696.1.2.2.1	Els certificats emesos sota aquesta política són utilitzats pels tramitadors d'empreses, inicialment, per a l'autenticació davant d'una aplicació web de la Caixa Andorrana de Seguretat Social, accessible a través d'Internet, que ofereix serveis d'alta i de baixa d'assegurats, i per a la signatura dels formularis HTML enviats a aquesta. En el futur, podrà estendre's l'ús d'aquests certificats a altres aplicacions que requereixin l'ús d'un certificat d'autenticació i/o signatura digital d'un tramitador d'empresa. L'ús d'aquest certificat fora de l'àmbit previst i descrit en aquest apartat està estrictament prohibit.
Política d'EF personal CASS	1.3.6.1.4.1.20696.1.2.2.2	Els certificats emesos sota aquesta política són utilitzats pel personal de la Caixa Andorrana de Seguretat Social, inicialment, per a l'autenticació davant d'aplicacions web accessibles a través d'una intranet. Així mateix, aquests certificats poden ser utilitzats com a certificats d'aprovadors de registre de la Infraestructura de la Caixa Andorrana de Seguretat Social, per a l'autenticació davant de l'autoritat de registre, per a la signatura d'aprovacions, denegacions i modificacions de peticions de certificat i per a la signatura de peticions de revocació, suspensió i habilitació de certificats. En el futur, podrà estendre's l'ús d'aquests certificats a altres aplicacions que requereixin l'ús d'un certificat d'autenticació i/o signatura digital d'un usuari del personal de la Caixa Andorrana de Seguretat Social. L'ús d'aquests certificat fora de l'àmbit previst i descrit en aquest apartat està estrictament prohibit.
Política d'EF dispositiu físic de servidor web	1.3.6.1.4.1.20696.1.2.3.1	Els certificats emesos sota aquesta política són utilitzats pels servidors web Internet/intranet de la Caixa Andorrana de Seguretat Social per a l'establiment de connexions segures SSL/TLS amb clients web. L'ús d'aquest certificat fora de l'àmbit previst i descrit en aquest apartat està estrictament prohibit.

Obligacions

Nom de la CPS	OID assignat	Obligacions
Política de CA arrel Política de CA subordinada	1.3.6.1.4.1.20696.1.1.1 1.3.6.1.4.1.20696.1.1.2	La Caixa Andorrana de Seguretat Social, quan actua com autoritat de certificació arrel o subordinada, assumeix les obligacions següents: • Emetre els certificats sol·licitats seguint les normes establertes en aquest document. • Revocar, suspendre i habilitar els certificats sol·licitats. • Emetre una CRL que contingui els certificats que es troben en estat revocat o suspès abans que transcorri 1 any (autoritat de certificació arrel) o 1 setmana (autoritat de certificació subordinada) de l'emissió de l'última CRL o quan es revoca, suspèn o habilita un certificat. • Publicar les CRL emeses en les ubicacions indicades en aquest document. • Complir els requisits de seguretat física, de procediments, personals i tècnics definits en el pla de seguretat establert per la Caixa Andorrana de Seguretat Social. • Utilitzar sistemes i productes fiables que estiguin protegits contra tota alteració i que garanteixin la seguretat tècnica i, si escau, criptogràfica dels processos de certificació prestats. • Col·locar personal qualificat i degudament format en els processos que cal dur a terme per prestar el servei ofert. • Publicar una CPS (*Certificate Practice Stament*) que inclogui el contingut d'aquest document o una referència a aquest. • Mantenir un registre amb la informació relativa als certificats emesos que pugui ser consultat solament per personal autoritzat. • Complir tots els requisits de la normativa sobre protecció de dades de caràcter personal.

Política d'RA	1.3.6.1.4.1.20696.1.2.1.1	La Caixa Andorrana de Seguretat Social, quan actua com a autoritat de registre, assumeix les obligacions següents: • Generar i signar els lots que contenen les peticions de certificat l'aprovació de les quals ha estat signada per un aprovador reconegut. • Generar i signar els lots que contenen les peticions de revocació, suspensió i habilitació de certificats signades per un aprovador reconegut. • Publicar cada certificat emès en una base de dades des d'on pugui ser descarregat pel subscriptor a través d'una adreça web. • Si el subscriptor del certificat ha indicat una adreça electrònica en la sol·licitud, enviar un missatge electrònic a aquesta adreça que contingui l'adreça web que li permeti de descarregar i instal·lar el certificat publicat. • Complir els requisits de seguretat física, de procediments, personals i tècnics definits en el pla de seguretat establert per la Caixa Andorrana de Seguretat Social. • Utilitzar sistemes i productes fiables que estiguin protegits contra tota alteració i que garanteixin la seguretat tècnica i, si escau, criptogràfica dels processos de certificació prestats. • Col·locar personal qualificat i degudament format en els processos que cal dur a terme per prestar el servei ofert. • Mantenir un registre amb la informació relativa als certificats sol·licitats que pugui ser consultat solament per personal autoritzat. • Complir tots els requisits de la normativa sobre protecció de dades de caràcter personal.

Política d'EF tramitador d'empresa Política d'EF personal CASS	1.3.6.1.4.1.20696.1.2.2.1 1.3.6.1.4.1.20696.1.2.2.2	**Subscriptor:** El subscriptor d'un certificat emès sota alguna d'aquestes polítiques assumeix les obligacions següents: • Garantir que tota la informació aportada en la petició del certificat és certa i correcta. • Sol·licitar, descarregar i instal·lar el certificat seguint el procediment establert per la Caixa Andorrana de Seguretat Social. • Acceptar que el certificat sigui publicat en un dipòsit comú, des d'on pot ser descarregat a través d'una adreça web. • Notificar immediatament als operadors de registre designats per la Caixa Andorrana de Seguretat Social qualsevol informació incorrecta que s'hagi inclòs en el certificat. • Custodiar de forma diligent el certificat sol·licitat i la seva clau privada, el suport d'aquests i els codis d'activació. • Utilitzar el certificat adequadament i per als usos especificats en aquest document. • Notificar immediatament als operadors de registre designats per la Caixa Andorrana de Seguretat Social la pèrdua, el robatori o qualsevol compromís potencial de la seva clau privada. **Terceres parts:** Les terceres parts que confien en un certificat emès sota alguna d'aquestes polítiques assumeixen les obligacions següents: • Complir la legislació aplicable a l'ús dels certificats. • Obtenir i verificar tots els certificats de la cadena de confiança dels certificats que se li presenten. • Verificar la validesa dels certificats que se li presenten a través de la CRL obtinguda amb una freqüència no superior a 1 setmana.

Política d'EF dispositiu físic de servidor web	1.3.6.1.4.1.20696.1.2.3.1	**Subscriptor:** El subscriptor d'un certificat emès sota alguna d'aquestes polítiques assumeix les obligacions següents: • Garantir que tota la informació aportada en la petició del certificat és certa i correcta. • Sol·licitar i obtenir el certificat seguint el procediment establert per la Caixa Andorrana de Seguretat Social. • Notificar immediatament als operadors de registre designats per la Caixa Andorrana de Seguretat Social qualsevol informació incorrecta que s'hagi inclòs en el certificat. • Custodiar de forma diligent el certificat sol·licitat i la seva clau privada, el suport d'aquests i els codis d'activació. • Utilitzar el certificat adequadament i per als usos especificats en aquest document. • Notificar immediatament als operadors de registre designats per la Caixa Andorrana de Seguretat Social la pèrdua, el robatori o qualsevol compromís potencial de la seva clau privada. **Terceres parts:** Les terceres parts que confien en un certificat emès sota alguna d'aquestes polítiques assumeixen les obligacions següents: • Complir la legislació aplicable a l'ús dels certificats. • Obtenir i verificar tots els certificats de la cadena de confiança dels certificats que se li presenten. • Verificar la validesa dels certificats que se li presenten a través de la CRL obtinguda amb una freqüència no superior a 1 setmana.

Responsabilitat

Nom de la CP	OID assignat	Responsabilitat i límit
Política de CA arrel	1.3.6.1.4.1.20696.1.1.1	Tots i cadascun dels certificats emesos sota aquestes polítiques no admeten cap responsabilitat econòmica que es pugui derivar de l'ús d'aquests. La responsabilitat associada a l'ús dels certificats ve en tot cas imposada pel reglament disciplinari que pot ser d'aplicació en l'àmbit de la Caixa Andorrana de Seguretat Social.
Política de CA subordinada	1.3.6.1.4.1.20696.1.1.2	
Política de RA	1.3.6.1.4.1.20696.1.2.1.1	
Política d'EF tramitador d'empresa	1.3.6.1.4.1.20696.1.2.2.1	
Política d'EF personal CASS	1.3.6.1.4.1.20696.1.2.2.2	
Política d'EF dispositiu físic de servidor web	1.3.6.1.4.1.20696.1.2.3.1	

Publicació

Nom de la CP	Certificat	Llista de revocació
Política de CA arrel	https://online.cass.ad/pki/certs/cass_root_csrs.crl	http://www.cass.ad/pki/crls/cass_root_ca.crl
Política de CA subordinada	https://online.cass.ad/pki/certs/cass_subord_csrs.crt	http://www.cass.ad/pki/crls/cass_subord_ca.crl
Política d'EF tramitador d'empresa Política d'EF personal CASS	***Els certificats d'aquestes polítiques es publiquen en una base de dades des d'on poden descarregar-se a través d'una adreça web.***	
Política d'RA Política d'EF dispositiu físic de servidor web	***Els certificats d'aquestes polítiques no es publiquen.***	

Confidencialitat

Amb referència a la política de confidencialitat seguida per la Caixa Andorrana de Seguretat Social, s'estableixen els punts següents:

1. Les dades personals s'han obtingut directament dels subscriptors dels certificats.

2. Tota la informació necessària per emetre els certificats té caràcter confidencial i no pot ser revelada sense el consentiment exprés de la Caixa Andorrana de Seguretat Social.

3. La Caixa Andorrana de Seguretat Social adopta les mesures necessàries per evitar-ne l'alteració, la pèrdua, el tractament o l'accés no autoritzats.

4. La Caixa Andorrana de Seguretat Social no pot modificar un certificat que ja ha estat emès. En aquest sentit, els titulars de les dades que desitgen rectificar o cancel·lar qualsevol de les seves dades personals contingudes en el certificat han de posar-se en contacte amb els operadors de registre designats per ella. La Caixa Andorrana de Seguretat Social informa que per rectificar o cancel·lar qualsevol de les dades de caràcter personal és necessari revocar el certificat associat.

5. Malgrat allò que estableix el punt anterior, la Caixa Andorrana de Seguretat Social informa els subscriptors de les polítiques descrites que les dades rectificades o cancel·lades, relatives als certificats revocats, seran mantingudes per la Caixa Andorrana de Seguretat Social durant, almenys, 15 anys.

CAPÍTOL 3

Requisits operatius

Identificació i autenticació

Nom de la CP	OID assignat	Identificació i autenticació
Política de CA arrel	1.3.6.1.4.1.20696.1.1.1	El certificat de la CA arrel és generat en el moment de generació de les seves claus per la persona designada per la Caixa Andorrana de Seguretat Social com a administrador de la CA arrel. Aquest valida les dades contingudes en el certificat generat.
Política de CA subordinada	1.3.6.1.4.1.20696.1.1.2	La persona designada per la Caixa Andorrana de Seguretat Social com a administrador de la CA subordinada genera una petició de certificat, en format X.509 o PKCS#10, en un fitxer que fa arribar de forma off-line a l'administrador de la CA arrel. Aquest valida les dades contingudes en la petició i genera el certificat corresponent, que és lliurat en un fitxer en format X.509 a l'administrador de la CA subordinada.
Política d'RA	1.3.6.1.4.1.20696.1.2.1.1	La persona designada per la Caixa Andorrana de Seguretat Social com a administrador de l'RA genera una petició de certificat, en format X.509 o PKCS#10, en un fitxer que fa arribar de forma off-line a l'administrador de la CA subordinada. Aquest valida les dades contingudes en la petició i genera el certificat corresponent, que és lliurat en un fitxer en format X.509 a l'administrador de l'RA. Un cop generat el certificat de l'RA, l'administrador de la CA subordinada el dóna d'alta com a RA reconeguda i li assigna les polítiques de certificació permeses.
Política d'EF tramitador d'empresa Política d'EF personal CASS	1.3.6.1.4.1.20696.1.2.2.1 1.3.6.1.4.1.20696.1.2.2.2	Els subscriptors d'aquests certificats introdueixen les seves dades en un formulari web i generen una petició de certificat. Després, es presenten davant d'una de les persones designades per la Caixa Andorrana de Seguretat Social com a aprovadors de registre, amb la documentació necessària establerta per la Caixa Andorrana de Seguretat Social per a l'emissió del certificat. Els aprovadors de registre comproven en la

		documentació presentada pels subscriptors que les dades de les peticions corresponents són correctes, i si no ho són, poden modificar-les. Després, aproven les peticions de certificat. Un cop aprovades les peticions de certificat dels subscriptors, l'administrador de l'RA genera un lot en un fitxer que fa arribar de forma off-line a l'administrador de la CA subordinada. Aquest genera els certificats i el lot de resposta en un fitxer que fa arribar de forma off-line a l'administrador de l'RA. Aquest processa el lot de resposta i publica els certificats en una base de dades, des d'on són descarregats pels subscriptors a través d'una adreça web. En el cas dels certificats d'EF personal CASS utilitzats com a certificats d'aprovadors de registre, un cop generats, l'administrador de l'RA els dóna d'alta com a aprovadors d'RA reconeguts.
Política d'EF dispositiu físic de servidor web	1.3.6.1.4.1.20696.1.2.3.1	Els responsables d'aquests dispositius generen una petició de certificat, en format PKCS#10 o X.509, en un fitxer que fan arribar de forma off-line a l'administrador de la CA subordinada. Aquest valida les dades contingudes en les peticions i genera els certificats corresponents, que són lliurats en fitxers en format X.509 als responsables dels dispositius.

Requisits operacionals

Nom de la CP	OID assignat	Requisits
Política de CA arrel Política de CA subordinada Política d'RA	1.3.6.1.4.1.20696.1.1.1 1.3.6.1.4.1.20696.1.1.2 1.3.6.1.4.1.20696.1.2.1.1	Generació de claus i certificats: La generació de claus corresponents als certificats associats a aquestes polítiques és efectuada pels mecanismes proveïts pel mètode PSS en disc dels productes KeyOne® de Safelayer. La generació del certificat de la CA arrel es fa en el moment de generació de les seves claus. L'administrador de la CA arrel genera el certificat de la CA subordinada, Tan bon punt ha rebut la petició de certificat corresponent. L'administrador de la CA subordinada genera el certificat de l'RA, tan bon punt ha rebut la petició de certificat corresponent. Suspensió i revocació: La petició de suspensió o revocació d'un certificat associat a aquestes polítiques només pot venir determinada per: o Compromís del sistema o Discontinuïtat del servei La petició de revocació d'aquests certificats només pot ser duta a terme per petició expressa de la direcció de la Caixa Andorrana de Seguretat Social. La suspensió o la revocació d'un certificat de CA arrel o CA subordinada és efectuada per l'administrador de la CA arrel. La suspensió o la revocació d'un certificat d'RA és efectuada per l'administrador de la CA subordinada. Renovació: El certificat de la CA arrel pot ser renovat si no hi ha canvis rellevants en el seu entorn. El mecanisme de renovació de claus privades i, per tant, de certificats en aquesta política és el que es troba recollit en la RFC 2510, apartat 2.4 "Root CA Key Update". No es preveu la renovació per als certificats de CA subordinada i RA, per als quals després de la seva expiració o revocació cal fer-ne una nova emissió.
Política d'EF tramitador d'empresa	1.3.6.1.4.1.20696.1.2.2.1	Generació de claus i certificats: La generació de claus corresponents als certificats

Nom de la CP	OID assignat	Requisits
Política d'EF personal CASS	1.3.6.1.4.1.20696.1.2.2.2	associats a aquestes polítiques és efectuada pel navegador web dels subscriptors dels certificats. L'administrador de la CA subordinada genera els certificats, tan bon punt ha rebut el lot de peticions aprovades corresponent generat per l'administrador de l'RA. Un cop l'administrador de l'RA ha rebut el lot de resposta i publicat els certificats, aquests són descarregats i instal·lats pel navegador web dels subscriptors dels certificats. Suspensió i revocació: La petició de suspensió o revocació d'un certificat associat a aquestes polítiques pot ser efectuada per: o El subscriptor, comunicant-ho directament a un aprovador de registre. o Un aprovador de registre. o L'administrador de l'RA. o L'administrador de la CA subordinada. Renovació: S'exclou la possibilitat de renovació dels certificats associats a aquestes polítiques, per als quals després de la seva expiració o revocació cal fer-ne una nova emissió.

Nom de la CP	OID assignat	Requisits
Política d'EF dispositiu físic de servidor web	1.3.6.1.4.1.20696.1.2.3.1	Generació de claus i certificats: La generació de claus corresponents als certificats associats a aquestes polítiques és efectuada pels mecanismes propis que disposin els dispositius informàtics. L'administrador de la CA subordinada genera els certificats, tan bon punt ha rebut les peticions de certificat corresponents. Suspensió i revocació: La petició de suspensió o revocació d'un certificat associat a aquestes polítiques pot ser efectuada per: o El tramitador del dispositiu, comunicant-ho directament a l'administrador de la CA subordinada. o L'administrador de la CA subordinada. Renovació: S'exclou la possibilitat de renovació dels certificats associats a aquestes polítiques, per als quals després de la seva expiració o revocació cal fer-ne una nova emissió.

Controls de seguretat tècnics

Nom de la CP	OID assignat	Controls de seguretat
Política de CA arrel Política de CA subordinada Política de RA	1.3.6.1.4.1.20696.1.1.1 1.3.6.1.4.1.20696.1.1.2 1.3.6.1.4.1.20696.1.2.1.1	Salvaguarda de claus: Mitjançant els mecanismes de còpia de seguretat (*backup*) previstos per la Caixa Andorrana de Seguretat Social per als seus sistemes d'informació. Protecció de les claus: Mitjançant els mecanismes proveïts pel mètode PSS en disc dels productes KeyOne® de Safelayer. Aquest mètode deriva una clau simètrica a partir de la paraula de pas que dóna accés a l'objecte, xifrant-ne el contingut simètricament.
Política d'EF tramitador d'empresa Política d'EF personal CASS	1.3.6.1.4.1.20696.1.2.2.1 1.3.6.1.4.1.20696.1.2.2.2	Salvaguarda de claus: Mitjançant els mecanismes d'exportació de claus proporcionats pel navegador web on s'hagin generat les claus. Protecció de les claus: Mitjançant els mecanismes proveïts pel navegador web on s'hagin generat les claus o pel suport on s'han exportat.
Política d'EF dispositiu físic de servidor web	1.3.6.1.4.1.20696.1.2.3.1	Salvaguarda de claus: Mitjançant els mecanismes de còpia de seguretat (*backup*) previstos per la Caixa Andorrana de Seguretat Social per als seus sistemes d'informació. Protecció de les claus: Mitjançant els mecanismes proveïts pels dispositius informàtics associats.

CAPÍTOL 4

Perfils de certificats i CRL

NOTA: Les extensions ombrejades són CRÍTIQUES.

Perfils d'entitats de confiança

CA arrel

Perfil de certificat

Camp x509v3	Nom	Valor
Version	Versió de X509	Versió 3
SerialNumber	Número de sèrie	1
SignatureAlgorithm	Algoritme de signatura digital del certificat	pkcs1-sha1withRsaSignature
Issuer	Nom de la CA arrel emissora	Mateix valor que el Subject
Subject	C (País)	AD
	O (Organització)	Caixa Andorrana de Seguretat Social
	CN (Nom)	CASS Root CA
Validity	NotBefore	Data d'emissió del certificat
	NotAfter	NotBefore + 30 anys
subjectyPublicKeyInfo	Clau pública	Clau RSA – dimensió 2048
Extensions estàndard		
subjectKeyIdentifier	Ident. de clau pública del subjecte	Hash de la clau pública generat automàticament
keyUsage	Ús de la clau	keyCertSign, cRLSign
CertificatePolicies	Policy Identifier	1.3.6.1.4.1. 20696.1.1.1
	CPS Pointer	http://www.cass.ad/pki/cps/cps.html
	User Notice	Les limitacions de garanties d'aquest certificat es poden trobar a la CPS
BasicConstraints	CA	TRUE

Perfil de CRL

Camp CRL v2	Nom	Valor
Versió	Versió de CRL	Versió 2
signatureAlgorithm	Algoritme de signatura digital	pkcs1-sha1WithRsaSignature
Issuer	C (País)	AD
	O (Organització)	Caixa Andorrana de Seguretat Social
	CN (Nom)	CASS Root CA
thisUpdate	Data de la CRL	Calculat de forma automàtica
nextUpdate	Data de generació de la propera CRL	+ 1 any
CRL extensions		
authorityKeyIdentifier	Id. de clau pública de l'emissor	Calculat de forma automàtica – Mateix valor que l'extensió subjectKeyIdentifier del certificat de la CA arrel
cRLNumber	Número seqüencial de CRL	Calculat de forma automàtica
IssuingDistributionPoint	Punt de distribució de la llista.	http://www.cass.ad/pki/crls/cass_root_ca.crl
Certificats revocats (1 entrada per certificat)		
serialNumber	Número de sèrie	Número de sèrie dels certificats revocats
invalidityDate	Data de rev.	Fixat automàticament.
reasonCode	Raó	Raó subministrada per l'operador. Valors possibles: Unspecified (0), keyCompromise (1), cACompromise (2), affiliationChanged (3), superseded (4), cessationOfOperation (5), certificateHold (6)

CA subordinada

Perfil de certificat

Camp x509v3	Nom	Valor
Version	Versió de X509	Versió 3
SerialNumber	Número de sèrie	Seqüencial, assignat per la CA arrel
SignatureAlgorithm	Algoritme de signatura digital del certificat	Pkcs1-sha1withRsaSignature
Issuer	C (País)	AD
	O (Organització)	Caixa Andorrana de Seguretat Social
	CN (Nom)	CASS Root CA
Subject	C (País)	AD
	O (Organització)	Caixa Andorrana de Seguretat Social
	CN (Nom)	CASS Subordinate CA
Validity	NotBefore	Data d'emissió del certificat
	NotAfter	NotBefore + 25 anys
subjectyPublicKeyInfo	Clau pública	Clau RSA – mida 2048
Extensions estàndard		
subjectKeyIdentifier	Ident. de clau pública del subjecte	Hash de la clau pública generat automàticament
authorityKeyIdentifier	Identificador de la clau pública de l'emissor	Calculat de forma automàtica – Mateix valor que l'extensió subjectKeyIdentifier del certificat de la CA arrel
keyUsage	Ús de la clau	keyCertSign, cRLSign
CertificatePolicies	Policy Identifier	1.3.6.1.4.1. 20696.1.1.2
	CPS Pointer	http://www.cass.ad/pki/cps/cps.html
	User Notice	Les limitacions de garanties d'aquest certificat es poden trobar a la CPS
BasicConstraints	CA	TRUE
	PathLenConstraint	0
CRLDistributionPoints	Punt de distribució de la CRL	http://www.cass.ad/pki/crls/cass_root_ca.crl

Perfil de CRL

Camp CRL v2	Nom	Valor
Versió	Versió de CRL	Versió 2
signatureAlgorithm	Algoritme de signatura digital	pkcs1-sha1WithRsaSignature
Issuer	C (País)	AD
	O (Organització)	Caixa Andorrana de Seguretat Social
	CN (Nom)	CASS Subordinate CA
thisUpdate	Data de la CRL	Calculat de forma automàtica
nextUpdate	Data de generació de la propera CRL	+ 1 setmana
CRL extensions		
authorityKeyIdentifier	Id. de clau pública de l'emissor	Calculat de forma automàtica – Mateix valor que l'extensió subjectKeyIdentifier del certificat de la CA subordinada
cRLNumber	Número seqüencial de CRL	Calculat de forma automàtica
IssuingDistributionPoint	Punt de distribució de la llista.	http://www.cass.ad/pki/crls/cass_subord_ca.crl
Certificats revocats (1 entrada per certificat)		
serialNumber	Número de sèrie	Número de sèrie dels certificats revocats
invalidityDate	Data de Rev.	Fixat automàticament.
reasonCode	Raó	Raó subministrada per l'operador. Valors possibles: Unspecified (0), keyCompromise (1), cACompromise (2), affiliationChanged (3), superseded (4), cessationOfOperation (5), certificateHold (6)

RA

Perfil de certificat

Camp x509v3	Nom	Valor
Version	Versió de X509	Versió 3
SerialNumber	Número de sèrie	Seqüencial, assignat per la CA subordinada
SignatureAlgorithm	Algoritme de signatura digital del certificat	Pkcs1-sha1withRsaSignature
Issuer	C (País)	AD
	O (Organització)	Caixa Andorrana de Seguretat Social
	CN (Nom)	CASS Subordinate CA
Subject	C (País)	AD
	O (Organització)	Caixa Andorrana de Seguretat Social
	CN (Nom)	CASS RA
Validity	NotBefore	Data d'emissió del certificat
	NotAfter	NotBefore + 20 anys
subjectyPublicKeyInfo	Clau pública	Clau RSA – mida 1024
Extensions estàndard		
subjectKeyIdentifier	Identificador de la clau pública del subjecte	Hash de la clau pública generat automàticament
authorityKeyIdentifier	Identificador de la clau pública de l'emissor	Calculat de forma automàtica – Mateix valor que l'extensió subjectKeyIdentifier del certificat de la CA subordinada
keyUsage	Ús de la clau	digitalSignature, nonRepudiation
extKeyUsage	Ús de clau estès	clientAuth
NetscapeCertType	Ús de clau estès	SSL_client
CertificatePolicies	Policy Identifier	1.3.6.1.4.1. 20696.1.2.1.1
	CPS Pointer	http://www.cass.ad/pki/cps/cps.html
	User Notice	Les limitacions de garanties d'aquest certificat es poden trobar a la CPS
BasicConstraints	CA	FALSE
CRLDistributionPoints	Punt de distribució de la CRL	http://www.cass.ad/pki/crls/cass_subord_ca.crl

Perfils d'entitat final

Perfil de certificat EF tramitador d'empresa

Camp x509v3	Nom	Valor
Version	Versió de X509	Versió 3
SerialNumber	Número de sèrie	Seqüencial, assignat per la CA subordinada
SignatureAlgorithm	Algoritme de signatura digital del certificat	pkcs1-sha1withRsaSignature
Issuer	C (País)	AD
	O (Organització)	Caixa Andorrana de Seguretat Social
	CN (Nom)	CASS Subordinate CA
Subject	C (País)	AD
	O (Organització)	Caixa Andorrana de Seguretat Social
	OU (Departament)	<Nom de l'empresa>
	DNQualifier	<Número de l'empresa>
	CN (Nom)	<Nom i cognoms del tramitador de l'empresa>
	SerialNumber	<Número de cens del tramitador de l'empresa>
	EA (Email) *<Opcional>*	<Adreça electrònica del tramitador de l'empresa>
Validity	NotBefore	Data d'emissió del certificat
	NotAfter	NotBefore + 3 anys
subjectyPublicKeyInfo	Clau pública	Clau RSA – mida 1024
Extensions estàndard		
subjectKeyIdentifier	Identificador de clau pública del subjecte	Hash de la clau pública generat automàticament
authorityKeyIdentifier	Identificador de la clau pública de l'emissor	Calculat de forma automàtica – Mateix valor que l'extensió subjectKeyIdentifier del certificat de la CA subordinada
keyUsage	Ús de la clau	digitalSignature, nonRepudiation
extKeyUsage	Ús de clau estès	clientAuth, emailProtection
NetscapeCertType	Ús de clau estès	SSL_client, SMIME_client
CertificatePolicies	Policy Identifier	1.3.6.1.4.1. 20696.1.2.2.1
	CPS Pointer	http://www.cass.ad/pki/cps/cps.html
	User Notice	Les limitacions de garanties d'aquest certificat es poden trobar a la CPS
BasicConstraints	CA	FALSE
SubjectAltName	rfc822Name (Email) *<Opcional>*	<Adreça electrònica del tramitador de l'empresa>
CRLDistributionPoints	Punt de distribució de la CRL	http://www.cass.ad/pki/crls/cass_subord_ca.crl

Perfil de certificat EF personal CASS

Camp x509v3	Nom	Valor
Version	Versió de X509	Versió 3
SerialNumber	Número de sèrie	Seqüencial, assignat per la CA subordinada
SignatureAlgorithm	Algoritme de signatura del certificat	pkcs1-sha1withRsaSignature
Issuer	C (País)	AD
	O (Organització)	Caixa Andorrana de Seguretat Social
	CN (Nom)	CASS Subordinate CA
Subject	C (País)	AD
	O (Organització)	Caixa Andorrana de Seguretat Social
	OU (Departament)	CASS
	CN (Nom)	<Nom i cognoms de l'usuari del personal de CASS>
	SerialNumber	<Número de cens de l'usuari del personal de CASS>
	EA (Email)	<Adreça electrònica de l'usuari del personal de CASS>
Validity	NotBefore	Data d'emissió del certificat
	NotAfter	NotBefore + 3 anys
subjectyPublicKeyInfo	Clau pública	Clau RSA – mida 1024
Extensions estàndard		
subjectKeyIdentifier	Identificador de clau pública del subjecte	Hash de la clau pública generat automàticament
authorityKeyIdentifier	Identificador de la clau pública de l'emissor	Calculat de forma automàtica – Mateix valor que l'extensió subjectKeyIdentifier del certificat de la CA subordinada
keyUsage	Ús de la clau	digitalSignature, nonRepudiation
extKeyUsage	Ús de clau estès	clientAuth, emailProtection
NetscapeCertType	Ús de clau estès	SSL_client, SMIME_client
CertificatePolicies	Policy Identifier	1.3.6.1.4.1. 20696.1.2.2.2
	CPS Pointer	http://www.cass.ad/pki/cps/cps.html
	User Notice	Les limitacions de garanties d'aquest certificat es poden trobar a la CPS
BasicConstraints	CA	FALSE
SubjectAltName	rfc822Name (Email)	<Adreça electrònica de l'usuari del personal de CASS>
CRLDistributionPoints	Punt de distribució de la CRL	http://www.cass.ad/pki/crls/cass_subord_ca.crl

Perfil de certificat EF dispositiu – servidor web

Camp x509v3	Nom	Valor
Version	Versió de X509	Versió 3
SerialNumber	Número de sèrie	Seqüencial, assignat per la CA subordinada
SignatureAlgorithm	Algoritme de signatura digital del certificat	pkcs1-sha1withRsaSignature
Issuer	C (País)	AD
	O (Organització)	Caixa Andorrana de Seguretat Social
	CN (Nom)	CASS Subordinate CA
Subject	<El contingut en la petició>	
Validity	NotBefore	Data d'emissió del certificat
	NotAfter	NotBefore + 1 any
subjectyPublicKeyInfo	Clau pública	Clau RSA – mida 1024
Extensions estàndard		
subjectKeyIdentifier	Identificador de clau pública del subjecte	Hash de la clau pública generat automàticament
authorityKeyIdentifier	Identificador de la clau pública de l'emissor	Calculat de forma automàtica – Mateix valor que l'extensió subjectKeyIdentifier del certificat de la CA subordinada
keyUsage	Ús de la clau	digitalSignature, nonRepudiation, keyEncipherment
extKeyUsage	Ús de clau estès	serverAuth
NetscapeCertType	Ús de clau estès	SSL_server
CertificatePolicies	Policy Identifier	1.3.6.1.4.1. 20696.1.2.3.1
	CPS Pointer	http://www.cass.ad/pki/cps/cps.html
	User Notice	Les limitacions de garanties d'aquest certificat es poden trobar a la CPS
BasicConstraints	CA	FALSE
SubjectAltName	Nom alternatiu *<Opcional>*	<El contingut en la petició>
CRLDistributionPoints	Punt de distribució de la CRL	http://www.cass.ad/pki/crls/cass_subord_ca.crl

Apèndix A – Llista de certificats d'operació propis de productes KeyOne®

A continuació s'enumeren els certificats d'ús intern presents en la implementació de la PKI de la Caixa Andorrana de Seguretat Social amb KeyOne®.

CA arrel

Signatura i xifratge: Usat per signar registres en la base de dades i3D, signar lots interns i com a Master de la base de dades i3D.

SSL local: Usat com a certificat de servidor en l'aplicació d'administració.

CA subordinada

Signatura: Usat per signar registres en la base de dades i3D i per signar lots de resposta a les RA.

Xifratge: Usat com a Master de la base de dades i3D.

SSL local: Usat com a certificat de servidor en l'aplicació d'administració.

RA

NOTA: El certificat de l'RA usat per signar lots (política d'RA) també és usat per signar registres en la base de dades i3D

Xifratge: Usat com a Master de la base de dades i3D.

SSL local: Usat com a certificat de servidor en l'aplicació d'administració.

SSL online: Usat com a certificat de servidor en els serveis d'RA online aprovador.