REPUBLIKA E SHQIPËRISË
KËSHILLI I MINISTRAVE
AGJENCIA KOMBËTARE E SHOQËRISË SË INFORMACIONIT

Datë 14.12.2023

AKSHI

POLITIKA E CERTIFIKATËS
/
DEKLARATA E PRAKTIKËS SË CERTIFIKIMIT

për

CERTIFIKATAT E KUALIFIKUARA PËR NËNSHKRIMIN DHE VULËN ELEKTRONIKE

Versioni 2.1

Detajet e dokumentit

Emri i dokumentit	Politika e Certifikatës / Deklarata e Praktikës së Certifikimit për Certifikatat e Kualifikuara për Nënshkrimin dhe Vulën Elektronike
Pronari i dokumentit	AKSHI (Agjencia Kombëtare e Shoqërisë së Informacionit)
Kontakt	pki@akshi.gov.al

Historia e versionit

Versioni	**Data**	**Ndryshimi**
1.0	2016	Versioni i parë.
2.0	15.12.2022	Përmbajtja e CP/CPS u përditësua në përputhje me IETF RFC 3647.
2.1	14.12.2023	-Përkufizimi i LTV-Long Term Validation -Është shtuar përkufizimi në lidhje me përdorimin e saktë të karaktereve të vecanta, klauzola 3.1.2 . -Përmbajtja e CP/CPS u përditësua në klauzolën 4.9.7 për frekuencën e publikimit të CRL-së. -Është shtuar NAIS Root CA certs.akshi.gov.al/root.crl në klauzolë 4.10.1

Tabela e Përmbajtjes

1. HYRJE

1.1 Vështrim i përgjithshëm

Kjo Politikë e Certifikatës / Deklaratë e Praktikës së Certifikimit (në tekstin e mëtejmë referuar si 'CP/CPS') për Certifikatat e Kualifikuara për Nënshkrimin dhe Vulën Elektronike përshkruan politikën dhe praktikat e certifikimit që Agjencia Kombëtare e Shoqërisë së Informacionit (AKSHI) zbaton për lëshimin e certifikatave të kualifikuara për nënshkrimin elektronik dhe certifikatat e kualifikuara për vulën elektronike (në tekstin e mëtejmë referuar si certifikata për nënshkrim/vulë elektronike).

AKSHI PKI i referohet infrastrukturës PKI të ngritur tek AKSHI për ofrimin e shërbimeve të besuara. Shërbimet e besuara të ofruara nga AKSHI si Ofrues i Kualifikuar i Shërbimeve të Besuara në fushëveprimin e kësaj CP/CPS janë certifikatat për nënshkrimin elektronik dhe certifikatat për vulën elektronike.

AKSHI ka krijuar një arkitekturë PKI me tre nivele:

- Autoriteti i Certifikimit Root:
  - NAIS Root Certification Authority (NAIS Root CA)

- Autoriteti i Certifikimit të ndërmjetëm:
  - NAIS Certification Authority (NAIS CA)

- Autoritetet e Certifikimit të klasave:
  - NAIS Class 1 Certification Authority (NAIS Class 1 CA)
  - NAIS Class 2 Certification Authority (NAIS Class 2 CA)
  - NAIS Class 3 Certification Authority (NAIS Class 3 CA)
  - NAIS Class 4 Certification Authority (NAIS Class 4 CA)

NAIS Root CA ka lëshuar një certifikatë të vetë-nënshkruar si dhe një certifikatë për CA-në e saj vartëse (NAIS CA).

NAIS CA ka lëshuar katër certifikata të klasave: NAIS Class 1 CA, NAIS Class 2 CA, NAIS Class 3 CA, dhe NAIS Class 4 CA (së bashku të referuara si '**NAIS Class CAs**'). NAIS Class CAs lëshojnë certifikata për përdoruesit fundor. NAIS CA dhe NAIS Class CAs janë referuar kolektivisht si '**NAIS CAs**' në përmbajtjen e këtij dokumenti.

AKSHI ka krijuar gjithashtu një platformë për nënshkrimin elektronik në distancë (Platforma e Nënshkrimit Elektronik). Gjenerimi dhe menaxhimi i çelësave privatë për certifikatat e përdorura në Plaformën e Nënshkrimit Elektronik menaxhohet nga AKSHI në emër të Nënshkruesit.

Përmbajtja e kësaj CP/CPS është bazuar në "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" të Network Working Group (RFC 3647).

1.1.1 Certifikatat e lëshuara nga NAIS Class 1 Certification Authority

- Certifikatë për nënshkrimin elektronik për subjektet private
  Kjo certifikatë i lëshohet personave fizik në lidhje me një subjekt privat. Certifikata përdoret në Platformën e Nënshkrimit Elektronik për të mbështetur nënshkrimin elektronik të dokumenteve. Certifikata lëshohet në një QSCD remote.

- Certifikatë për nënshkrim elektronik për punonjësit qeveritar

Kjo certifikatë i lëshohet punonjësve qeveritar. Certifikata përdoret në Platformën e Nënshkrimit Elektronik për të mbështetur nënshkrimin elektronik të dokumenteve.
Certifikata lëshohet në një QSCD remote.

- Certifikatë për nënshkrim elektronik për punonjësit qeveritar për infrastrukturën kritike
  Kjo certifikatë i lëshohet punonjësve qeveritar që operojnë në infrastrukturë kritike ose aksesojnë sisteme ndërkombëtare, për autentifikim dhe nënshkrimin elektronik të dokumenteve. Certifikata lëshohet në një USB Token.

- Certifikatë për vulën elektronike
  Kjo certifikatë i lëshohet institucioneve publike në Shqipëri që ofrojnë shërbime në portalin qeveritar e-Albania. Certifikata përdoret në procesin e automatizuar të vulosjes elektronike të dokumenteve në portalin e-Albania.

1.1.2 Certifikatat e lëshuara nga NAIS Class 2 Certification Authority

- Certifikatë për nënshkrim elektronik për subjektet private për infrastukturën kritike
  Kjo certifikatë i lëshohet personave fizik në lidhje me një subjekt privat që operojnë në infrastrukturë kritike ose aksesojnë sisteme ndërkombëtare, për autentifikim dhe nënshkrimin elektronik të dokumenteve. Certifikata lëshohet në një USB Token.

1.1.3 Certifikatat e lëshuara nga NAIS Class 3 Certification Authority

- Certifikatë për projektin e fiskalizimit për institucionet publike
  Kjo certifikatë për vulën elektronike i lëshohet institucioneve publike në Shqipëri në mbështetje të projektit të fiskalizimit. Lëshohet si një certifikatë softuerike.

- Certifikatë për projektin e fiskalizimit për subjektet private
  Kjo certifikatë për vulën elektronike i lëshohet subjekteve private në Shqipëri në mbështetje të projektit të fiskalizimit. Lëshohet si një certifikatë softuerike.

- Certifikatë Test për projektin e fiskalizimit
  Kjo certifikatë për vulën elektronike i lëshohet subjekteve që zhvillojnë softuerë, për qëllime testimi, në mbështetje të projektit të fiskalizimit. Lëshohet si një certifikatë softuerike.

1.1.4 Certifikatat e lëshuara nga NAIS Class 4 Certification Authority

- Certifikatë për autentifikim për Platformën e Nënshkrimit Elektronik
  Kjo certifikatë për nënshkrimin elektronik përdoret si një komponent në Platformën e Nënshkrimit Elektronik.

1.2 Emri i dokumentit dhe identifikimi

Emri i Dokumentit: Politika e Certifikatës / Deklarata e Praktikës së Çertifikimit për Certifikatat e Kualifikuara për Nënshkrimin dhe Vulën Elektronike për AKSHI-n.

Versioni: 2.1

Data e miratimit: 14 Dhjetor 2023

1.3 Pjesëmarrësit e PKI

Pjesëmarrësit e PKI-së janë të gjithë personat juridik ose fizik që janë të përfshirë në aktivitetet e AKSHI-t si Ofrues i Shërbimeve të Besuara (TSP) ose që mund të ndikohen nga përdorimi i certifikatave të lëshuara nga AKSHI.

Pjesëmarrësit në AKSHI PKI janë:

- Autoritetet e Certifikimit
- Autoritetet e Regjistrimit
- Subjektet
- Pajtimtarët
- Palët e përfshira

1.3.1 Autoritetet e certifikimit

Një Autoritet Certifikues (CA) është një autoritet i besuar nga pajtimtarët, subjektet dhe palët e përfshira për krijimin dhe lëshimin e certifikatave me çelës publik.

Autoritetet e certifikimit brenda PKI të AKSHI-t në kuadër të kësaj CP/CPS janë:

- NAIS Root CA
- NAIS CA
- NAIS Class 1 CA
- NAIS Class 2 CA
- NAIS Class 3 CA
- NAIS Class 4 CA

1.3.2 Autoritetet e regjistrimit

Autoritetet e Regjistrimit (RA) janë entitetet që përcaktojnë procedurat e regjistrimit për aplikimet për certifikata, kryejnë identifikimin dhe autentifikimin e aplikantëve për certifikata, krijojnë ose kalojnë kërkesat për revokimin e certifikatave dhe miratojnë aplikimet për rinovimin ose re-key të certifikatave në emër të një CA-je.

Detyrat operacionale të RA-së kryhen nga funksioni i RA-së i ngritur pranë Sektorit të PKI në AKSHI.

1.3.3 Pajtimtarët

Pajtimtarët janë persona juridik ose fizik që kanë kërkuar lëshimin e një certifikate nga AKSHI për të cilën kanë nënshkruar një marrëveshje.

Subjekti është entiteti të cilit i është lëshuar një certifikatë dhe identifikohet në një certifikatë si mbajtësi i çelësit privat të lidhur me çelësin publik në certifikatë.

- AKSHI lëshon certifikata për vulën elektronike vetëm personave juridik që operojnë në Republikën e Shqipërisë.
- AKSHI lëshon certifikata për nënshkrim elektronik personave fizik në lidhje me një person juridik. Personi fizik mund të jetë:
    - Shtetas shqiptar, ose
    - Shtetas i huaj që operon një biznes në Republikën e Shqipërisë

1.3.4 Palët e përfshira

Një palë e përfshirë është një person fizik ose juridik që mbështetet në një identifikim elektronik ose një shërbim të besuar. Palët e përfshira përfshijnë palët që verifikojnë një nënshkrim elektronik duke përdorur një certifikatë me çelës publik.

Përgjegjësitë e palëve të përfshira përcaktohen në seksionin 9.6.4 të këtij dokumenti.

1.3.5 Pjesëmarrës të tjerë

- Sektorët brenda AKSHI-t me përgjegjësinë për zhvillimin, mirëmbajtjen dhe miratimin e politikave dhe praktikave që zbatohen në ofrimin e shërbimeve të certifikimit.
- Shërbimi i shpërndarjes dhe publikimit - ky rol (i cili kryhet nga AKSHI) i referohet publikimit të Politikave të Certifikatës, Deklaratave të Praktikës së Certifikimit, termave dhe kushteve të shërbimeve të certifikimit, certifikatave CA dhe informacionit përkatës për pajtimtarët dhe palët e përfshira.
- Shërbimi i menaxhimit të revokimit dhe statusit të revokimit - ky rol (i cili kryhet nga AKSHI) ka përgjegjësinë e shqyrtimit të kërkesave në lidhje me revokimin dhe dhënien e informacionit palëve të përfshira në lidhje me statusin e revokimit të certifikatës.
- Ofruesit e jashtëm të shërbimeve që suportojnë shërbimet e certifikimit sipas një marrëveshjeje të nënshkruar me AKSHI-n.

1.4 Përdorimi i certifikatës

1.4.1. Përdorimet e duhura të certifikatës

Certifikatat për nënshkrimin elektronik për subjektet private duhet të përdoren:

- *vetëm* për nënshkrimin elektronik të dokumenteve në Platformën e Nënshkrimit Elektronik
- *vetëm* nga subjekti, në këtë rast, personi fizik i lidhur me një subjekt privat

Certifikatat për nënshkrim elektronik për punonjësit qeveritar duhet të përdoren:

- *vetëm* për nënshkrimin elektronik të dokumenteve në Platformën e Nënshkrimit Elektronik
- *vetëm* nga subjekti, në këtë rast, punonjësi qeveritar

Certifikatat për nënshkrim elektronik për punonjësit qeveritar për infrastrukturën kritike duhet të përdoren:

- *vetëm* për autentifikim dhe nënshkrim elektronik të dokumenteve
- *vetëm* nga subjekti, në këtë rast, punonjës qeveritar që operon në infrastrukturë kritike ose akseson sisteme ndërkombëtare
- *vetëm* përmes USB Token të lëshuar nga AKSHI

Certifikatat për vulën elektronike duhet të përdoren:

- *vetëm* për procesin e automatizuar të vulosjes elektronike të dokumenteve në portalin e-Albania
- *vetëm* nga subjekti, në këtë rast, personi juridik që është një institucion publik që ofron shërbime në portalin qeveritar e-Albania

Certifikatat për nënshkrim elektronik për subjektet private për infrastukturën kritike duhet të përdoren:

- *vetëm* për autentifikim dhe nënshkrim elektronik të dokumenteve
- *vetëm* nga subjekti, në këtë rast, personi fizik i lidhur me një subjekt privat që operon në infrastrukturë kritike ose akseson sisteme ndërkombëtare
- *vetëm* përmes USB Token të lëshuar nga AKSHI

Certifikatat për projektin e fiskalizimit për institucionet publike duhet të përdoren:

- *vetëm* në mbështetje të ligjit 87/2019 "Për faturën dhe sistemin e monitorimit të qarkullimit", i ndryshuar
- *vetëm* nga subjekti, në këtë rast personi juridik që është një institucion publik në Republikën e Shqipërisë

Certifikatat për projektin e fiskalizimit për subjektet private duhet të përdoren:

- *vetëm* në mbështetje të ligjit 87/2019 "Për faturën dhe sistemin e monitorimit të qarkullimit", i ndryshuar
- *vetëm* nga subjekti, në këtë rast personi juridik që është një subjekt privat në Republikën e Shqipërisë

Certifikata Test për projektin e fiskalizimit duhet të përdoren:

- *vetëm* në mbështetje të ligjit 87/2019 "Për faturën dhe sistemin e monitorimit të qarkullimit", i ndryshuar
- *vetëm* nga subjekti, në këtë rast, personi juridik që është një subjekt privat në fushën e IT-së, i interesuar për zhvillim e softuerëve në kontekstin e projektit të fiskalizimit

Certifikata për autentifikim për Platformën e Nënshkrimit Elektronik duhet të përdoret vetëm nga AKSHI si një komponent i Platformës së Nënshkrimit Elektronik.

1.4.2 Përdorime të ndaluara të certifikatës

Çdo përdorim i një certifikate, i ndryshëm nga përdorimi i përcaktuar në seksionin 1.4.1 është i ndaluar.

1.5 Administrimi i politikave

1.5.1 Organizata që administron dokumentin

AKSHI është përgjegjës për hartimin, regjistrimin, mirëmbajtjen dhe përditësimin e kësaj CP/CPS-je.

Emri	Agjencia Kombëtare e Shoqërisë së Informacionit
Adresa	Rruga Papa Gjon Pali II, Nr.3, Kati 1, 1003, Tiranë, Shqipëri
NIPT	K72301452S
Telefon	+355(0)42277750
Fax	+355(0)42277764
Email	info@akshi.gov.al
Web	akshi.gov.al

1.5.2 Personi i kontaktit

Sektori i PKI-së në AKSHI është pika e kontaktit për administrimin dhe përmbajtjen e kësaj CP/CPS-je.

Kontakti Sektori i PKI

Email pki@akshi.gov.al

1.5.3 Personi që përcakton përshtatshmërinë e CPS për politikën

Sektori i PKI-së në AKSHI si dhe personeli i autorizuar që merr pjesë në zhvillimin, mirëmbajtjen dhe miratimin e politikave dhe praktikave që zbatohen në ofrimin e shërbimeve të çertifikimit janë kolektivisht përgjegjës për përcaktimin e përshtatshmërisë së CPS.

Vlerësimi i përshtatshmërisë së CPS mund të bazohet gjithashtu në rezultatet e raportit të një auditimi të pavarur të pajtueshmërisë.

1.5.4 Procedurat e miratimit të CPS

Sektori i PKI e dërgon CPS për miratim formal tek drejtuesit e lartë të AKSHI-t. Ndryshimet e bëra në CPS duhet të miratohen sipas procedurave të brendshme të AKSHI-t për krijimin dhe përditësimin e dokumentacionit. Versioni më i fundit i CPS do të jetë i disponueshëm në Direktorinë publike akshi.gov.al/repository në anglisht dhe në shqip.

1.6 Përkufizime dhe akronime

Përkufizimet

Të dhënat e aktivizimit – Vlerat e të dhënave, përveç çelësave, që nevojiten për të operuar modulet kriptografike dhe që duhet të mbrohen (p.sh. një PIN, një frazë ose një key share e mbajtur manualisht).

Autoriteti i Certifikimit (CA) – Autoriteti i besuar nga një ose më shumë përdorues për të krijuar dhe lëshuar certifikata me çelës publik. Autoriteti i certifikimit mund të krijojë çelësat e subjekteve (opsionale).

Një autoritet certifikues mund të jetë:

1) një ofrues i shërbimit të besuar që krijon dhe lëshon certifikata me çelës publik; ose
2) një shërbim teknologjik për gjenerimin e certifikatave, që përdoret nga një ofrues i shërbimit të certifikimit që krijon dhe lëshon certifikata me çelës publik.

Deklarata e praktikës së certifikimit (CPS) – Një deklaratë e praktikave që një autoritet i certifikimit përdor në lëshimin, menaxhimin, revokimin dhe rinovimin të certifikatave.

Lista e revokimit të certifikatave (CRL) – listë e nënshkruar që tregon një grup certifikatash që nuk konsiderohen më si të vlefshme nga lëshuesi i certifikatës.

Politika e Certifikatës (CP) – grup i emërtuar rregullash që tregon zbatueshmërinë e një certifikate në një komunitet të caktuar dhe/ose klasë aplikimi me kërkesa të përbashkëta sigurie.

Certifikatë për nënshkrim elektronik – vërtetim elektronik i cili lidh të dhënat e vërtetimit të nënshkrimit elektronik me një person fizik dhe konfirmon së paku emrin ose pseudonimin e atij personi.

Certifikatë për vulë elektronike – vërtetim elektronik që lidh të dhënat e vërtetimit të vulës elektronike me personin juridik dhe konfirmon emrin e atij personi.

Krijuesi i vulës – Një person juridik që krijon një vulë elektronike.

e-Albania – i referohet portalit qeveritar (e-albania.al) i cili përdoret për ofrimin e shërbimeve elektronike dhe administrohet nga Agjencia Kombëtare e Shoqërisë së Informacionit.

FIPS 140-2 – Publikimi i Standardit Federal të Përpunimit të Informacionit 140-2 (FIPS PUB 140-2) është një standard i sigurisë kompjuterike i qeverisë amerikane që përdoret për të miratuar modulet kriptografike.

Certifikata me çelës publik – çelësi publik i një subjekti, së bashku me disa informacione të tjera, që nuk mund të falsifikohet, së bashku me çelësin privat të autoritetit certifikues që e ka lëshuar atë.

Shënim: në këtë dokument, përdorimi i termi "certifikatë" i referohet certifikatave me çelës publik.

Infrastrukturë me çelës publik (PKI) – infrastrukturë që suporton menaxhimin e çelësave publikë që mbështesin shërbimet e autentifikimit, enkriptimit, integritetit ose mos-refuzimit.

Platforma e Nënshkrimit Elektronik – i referohet platformës esign.akshi.gov.al të krijuar nga AKSHI që përdoret për nënshkrimin e dokumenteve.

Autoriteti i Regjistrimit (RA) – entitet që është përgjegjës për identifikimin dhe autentifikimin e subjekteve të certifikatave.

Palë e përfshirë – person fizik ose juridik që mbështetet në një identifikim elektronik ose një shërbim të besuar. Palët e përfshira përfshijnë palët që verifikojnë një nënshkrim elektronik duke përdorur një certifikatë me çelës publik.

Root CA – autoriteti certifikues i cili është në nivelin më të lartë brenda fushës së TSP-së, i cili përdoret për të nënshkruar CA-të vartëse.

Pajisja kriptografike e sigurt – Pajisja që mban çelësin privat të përdoruesit, e mbron këtë çelës nga kompromentimi dhe kryen funksione nënshkrimi ose dekriptimi në emër të përdoruesit.

Subjekti – subjekti i identifikuar në një certifikatë si mbajtësi i çelësit privat të lidhur me çelësin publik të përfshirë në atë certifikatë.

CA vartëse – Autoriteti i Certifikimit për të cilin certifikata është e nënshkruar nga CA-ja kryesore, ose një CA tjetër vartëse.

Pajtimtar – person juridik ose fizik i lidhur me marrëveshje me një ofrues të shërbimeve të besuara ndaj çdo detyrimi të pajtimtarit.

Nënshkrues – Personi fizik që krijon një nënshkrim elektronik.

Shërbimi i Besuar – shërbim elektronik i cili rrit besueshmërinë në transaksionet elektronike.

Ofruesi i Shërbimeve të Besuara – një person fizik ose juridik që ofron një ose më shumë shërbime të besuara.

Long Term Validation -ofron një regjistrim të gjendjes së certifikatës elektronike në kohën e nënshkrimit. Është e integruar tek nënshkrimi elektronik në platformën e nënshkrimit elektronik eSign.

Akronimet

CA Autoriteti i Certifikimit

CPS Deklarata e praktikës së certifikimit

CRL Lista e revokimit të certifikatës

OCSP Protokolli i statusit të certifikatës në internet

PKI Infrastruktura e çelësit publik

RA Autoriteti i Regjistrimit

TSP Ofruesi i Shërbimeve të Besuara

QSCD Pajisje e kualifikuar për krijimin e nënshkrimeve elektronike

HSM Moduli i Sigurisë së Hardware

LTV Long Term Validation

	Emri i shkurtër	**Emri i plotë**
Anglisht	NAIS	National Agency for Information Society
Shqip	AKSHI	Agjencia Kombëtare e Shoqërisë së Informacionit

2. PËRGJEGJËSITË E PUBLIKIMIT DHE TË DIREKTORIVE

2.1 Direktoritë

AKSHI operon dhe mirëmban një Direktori të PKI e cila përmban:

- Politikën e Certifikimit, Deklaratën e Praktikave të Certifikimit
- Certifikatat për NAIS Root CA, NAIS CA dhe NAIS Class CAs
- Listat e revokimit të certifikatave (CRL)
- Informacion mbi legjislacionin në fushën e shërbimeve të besuara
- Komunikimet me pajtimtarët dhe palët e përfshira në lidhje me ofrimin e shërbimeve të certifikimit
- Termat dhe kushtet për përdorimin e certifikatave

Informacioni i disponueshëm në këtë Direktori mund të gjendet në anglisht dhe në gjuhën shqipe në adresën akshi.gov.al/repository.

Adresa e direktorisë publike të LDAP: ldap://ldap.akshi.gov.al/.

2.2 Publikimi i informacionit të certifikimit

AKSHI është përgjegjës për publikimin dhe përditësimin e informacionit në lidhje me CP, CPS, certifikatat, statusin aktual të certifikatave, termat dhe kushtet si dhe informacione të tjera përkatëse në lidhje me shërbimet e besuara. AKSHI do ta vërë në dispozicion këtë informacion në Direktori. Disa informacione, për shkak të naturës sensitive, nuk mund të bëhen publike.

2.3 Koha ose shpeshtësia e publikimit

AKSHI shqyrton çdo vit (si dhe ne rastet kur ka ndryshime madhore) dokumentacionin në lidhje me shërbimet e besuara, për të siguruar që informacioni të jetë i përditësuar dhe i saktë. Ndryshimet publikohen në Direktori.

Frekuenca e publikimit të CRL-ve për certifikatat është përcaktuar në seksionin 4.9.7.

2.4 Kontrollet e aksesit në Direktori

I gjithë informacioni dhe dokumentacioni i publikuar nga AKSHI në Direktori është i disponueshëm për publikun në adresën akshi.gov.al/repository.

Për të mbrojtur integritetin e dokumentacionit, AKSHI ka implementuar kontrolle aksesi për të parandaluar modifikimet e paautorizuara dhe fshirjen e këtij informacioni.

Vetëm personeli i autorizuar në AKSHI mund të shtojë, modifikojë, përditësojë ose fshijë informacionin në Direktori, ndërsa përdoruesit e jashtëm mund vetëm të lexojnë dhe shkarkojnë informacionin e disponueshëm.

3. IDENTIFIKIMI DHE AUTENTIFIKIMI

Ky kapitull përshkruan procedurat e përdorura për të autentifikuar identitetin dhe atributet e tjera të një aplikuesi fundor për paisje me certifikatë, përpara lëshimit të certifikatës.

3.1 Emërtimi

3.1.1 Llojet e emrave

NAIS Class CAs lëshojnë certifikata për përdoruesit fundorë. Certifikatat e lëshuara nga NAIS Class CAs janë në përputhje me standardin X.509 V3. Fusha *Subject* është në përputhje me IETF RFC 5280.

- Për certifikatat e lëshuara për personat fizik të lidhur me një person juridik, fusha *Subject* duhet të përmbajë emrin dhe mbiemrin e personit, emrin e regjistruar të personit juridik dhe identifikuesin e tij .
- Për certifikatat e lëshuara për personat juridik, fusha *Subject* duhet të përmbajë emrin e plotë të regjistruar të personit juridik.
-

3.1.2 Nevoja që emrat të jenë kuptimplotë

Emrat që identifikojnë një person fizik ose juridik në fushën *Subject* duhet të jenë kuptimplotë.

- Për personat fizik, emri dhe mbiemri duhet të jenë të njëjtë me emrin në dokumentin zyrtar të identifikimit.
- Për personat juridik, emri i personit juridik duhet të jetë i njëjtë me emrin e regjistruar në Qendrën Kombëtare të Biznesit.
- Karakteret e veçanta ne CN nuk mund të përdoren në gjenerimin e certifikatave elektronike dhe zëvendësohen me karaktere alfanumerike. psh "&" me "and", "@" me "at".

Për shkak të disa kufizimeve softwerike, disa shkronja në alfabetin shqip zëvendësohen si më poshtë:

Shkronja	**Zëvendësohet me**
Ë/ë	E/e
Ç/ç	C/c

3.1.3 Anonimiteti ose pseudonimi i pajtimtarëve

AKSHI nuk suporton përdorimin e pseudonimeve ose identifikuesve të tjerë anonimë.

3.1.4 Rregulla për interpretimin e formave të ndryshme të emrave

Fusha *Subject* në certifikata duhet të interpretohet duke përdorur standardin X.520.

3.1.5 Veçantia e emrave

AKSHI siguron veçantinë e emrit të çdo Subjekti në mënyrat e mëposhtme:

- Për certifikatat për nënshkrim elektronik, fusha *Subject* përfshin atributin e numrit serial.
- Për certifikatat për projektin e fiskalizimit, fusha *Subject* përfshin atributin e numrit serial.
- Për çertifikatat për vulën elektronike, duhet të përfshihet emaili i institucionit publik.

3.1.6 Njohja, autentifikimin dhe roli i markave tregtare

Asnjë përcaktim.

3.2 Validimi fillestar i identitetit

Procesi i aplikimit për certifikatat më poshtë:

- Certifikatë për nënshkrim elektronik për subjektet private,
- Certifikatë për nënshkrim elektronik për subjektet private për infrastukturën kritike,
- Certifikatë për nënshkrim elektronik për punonjësit qeveritar,
- Certifikatë për nënshkrim elektronik për punonjësit qeveritar për infrastrukturën kritike,
- Certifikatë për projektin e fiskalizimit për institucionet publike,
- Certifikatë për projektin e fiskalizimit për subjektet private, dhe
- Certifikatë Test për projektin e fiskalizimit,

realizohet nëpërmjet portalit qeveritar e-Albania.

Të dhënat në portalin qeveritar e-Albania janë verifikuar më parë me të dhënat e Regjistrit Kombëtar të Gjendjes Civile për qytetarët dhe Regjistrit Kombëtar Tregtar për bizneset.

Pas marrjes së një aplikimi për certifikatë nga e-Albania, Oficeri i Regjistrimit pranë AKSHI-t verifikon të dhënat.

Aplikimet për certifikata për nënshkrim elektronik për punonjësit qeveritar duhet të kalojnë një hap shtesë verifikimi për validimin e identitetit.

Procesi i aplikimit për certifikatë për vulën elektronike kryhet nëpërmjet një kërkese zyrtare të paraqitur pranë AKSHI-t nga institucionet publike që ofrojnë shërbime në portalin e-Albania.

3.2.1 Metoda për të vërtetuar posedimin e çelësit privat

Çelësi privat shoqërues që korrespondon me një çelës publik për të cilin kërkohet lëshimi i certifikatës, gjenerohet nga nënshkruesi, krijuesi i një vule ose nga AKSHI.

- **Kur çelësi privat gjenerohet nga AKSHI**, kërkesa për paraqitjen e provës për posedimin e çelësit privat nuk është e aplikueshme. Në këtë rast, nëpërmjet mjeteve të sigurta teknologjike, AKSHI siguron që çelësi privat të jetë i lidhur me nënshkruesin ose krijuesin e vulës.
- **Kur çelësi privat nuk gjenerohet nga AKSHI**, zotërimi i çelësit privat që korrespondon me çelësin publik për të cilin kërkohet gjenerimi i certifikatës do të vërtetohet duke dërguar kërkesën për nënshkrimin e certifikatës (CSR) (që do të përfshijë çelësin publik të nënshkruar. nga çelësi privat që lidhet me të) në përputhje me standardin PKCS#10.

3.2.2 Autentifikimi i identitetit të organizatës

Për certifikatat më poshtë:

- Certifikatë për projektin e fiskalizimit për institucionet publike,
- Certifikatë për projektin e fiskalizimit për subjektet private, dhe
- Certifikatë Test për projektin e fiskalizimit,

të dhënat në lidhje me organizatën gjenerohen automatikisht përmes portalit qeveritar e-Albania gjatë procesit të aplikimit. Ky informacion është verifikuar dhe validuar paraprakisht me informacionin zyrtar të Qëndrës Kombëtare të Biznesit.

Për këto lloj certifikatash kërkohet informacioni më poshtë rreth organizatës:

- NIPT
- Emri ligjor
- Përfaqësuesi ligjor
- Email dhe numri i telefonit
- Adresa

Për certifikatat për vulën elektronike, aplikimi për certifikatë dërgohet përmes një kërkese zyrtare drejtuar AKSHI-t. Gjatë procesit të aplikimit, kërkohet informacioni më poshtë:

- Certifikata e rregjistrimit dhe NIPT
- Emri ligjor
- Përfaqësuesi ligjor
- Email dhe numri i telefonit
- Adresa

3.2.3 Autentifikimi i identitetit të individëve

Gjatë procesit të aplikimit nga persona fizik, nevojitet informacioni më poshtë:

- Numri personal i letërnjoftimit (ID)
- Emri dhe mbiemri ligjor
- Numri i telefonit

Ky informacion gjenerohet automatikisht nga portali qeveritar e-Albania. Të dhënat janë verifikuar dhe validuar paraprakisht me informacionin zyrtar të Rregjistrit Kombëtar të Gjendjes Civile.

Për personat fizik të lidhur me një subjekt privat, nevojitet gjithashtu informacioni më poshtë:

- Email (që gjenerohet automatikisht nga e-Albania)
- Pozicioni i punës
- NIPT i subjektit privat
- Emri ligjor i subjektit privat

Për punonjësit qeveritar, nevojitet gjithashtu informacioni më poshtë:

- Email zyrtar
- Pozicioni i punës
- Emri i institucionit publik
- Departamenti

3.2.4 Informacioni i paverifikuar i pajtimtarit

Pajtimtari është tërësisht përgjegjës për dhënien e informacionit të saktë dhe të përditësuar gjatë procesit të aplikimit. Informacioni që gjenerohet automatikisht përmes e-Albania është verifikuar pas regjistrimit në portalin qeveritar dhe AKSHI nuk kryen verifikime të mëtejshme.

3.2.5 Validimi i autoritetit

Përpara lëshimit të certifikatave për punonjësit qeveritar dhe operatorët e infrastrukturës kritike, AKSHI verifikon nëse personi fizik ka të drejta ose autorizim specifik për t'u pajisur me certifikatë.

3.2.6 Kriteret për ndërveprim

Asnjë përcaktim.

3.3 Identifikimi dhe autentifikimi për kërkesat për 're-key'

3.3.1 Identifikimi dhe autentifikimi për kërkesat 're-key' rutinë

Kërkesa për 're-key' rutinë i referohet procesit të rinovimit të certifikatës që kryhet për certifikatat që janë afër skadimit dhe përfshin procedurën e gjenerimit të një çifti të ri çelësash për subjektet ekzistuese.

Procesi 're-key' për certifikatën përpunohet nga Oficeri i Regjistrimit pranë AKSHI-t pas marrjes së një kërkese nga subjekti në portalin qeveritar e-Albania. Subjektit i kërkohet të konfirmojë që të dhënat e paraqitura në procesin fillestar të aplikimit janë ende të vlefshme dhe të sakta.

Procesi 're-key' i certifikatës për certifikatat e lëshuara në pajisje kriptografike të sigurta kryhet përmes prezencës fizike të subjektit në zyrat qëndrore të AKSHI-t.

Në këtë rast, subjektit i kërkohet të paraqesë informacionin më poshtë:

- Formular i kërkesës zyrtare të nënshkruar nga administratori i personit juridik
- Kopje e dokumentit zyrtar të identifikimit
- Paisjen e sigurt kriptografike (USB Token)

3.3.2 Identifikimi dhe autentifikimi për 're-key' pas revokimit

Identifikimi dhe autentifikimi për kërkesat 're-key' pas revokimit ndjek të njëjtin proces si procedura fillestare e identifikimit të përmendur në seksionin 3.2.

3.4 Identifikimi dhe autentifikimi për kërkesat për revokim

Për certifikatat për nënshkrim elektronik për punonjësit qeveritar dhe certifikatat për nënshkrim elektronik për punonjësit qeveritar për infrastrukturën kritike, kërkesa për revokim të certifikatës mund të bëhet:

- Nga Subjekti, duke paraqitur një kërkesë tek pki@akshi.gov.al duke përdorur adresën zyrtare të emailit që është përdorur në procesin fillestar të aplikimit
- Nga institucioni publik, me një kërkesë zyrtare të paraqitur në AKSHI

Për çertifikatat për vulën elektronike dhe certifikatat për projektin e fiskalizimit për institucionet publike, kërkesa për revokim mund të bëhet nga institucioni nëpërmjet një emaili të dërguar në adresën pki@akshi.gov.al ose një kërkese zyrtare pranë AKSHI-t.

Për certifikatat më poshtë:

- Certifikatë për nënshkrim elektronik për subjektet private
- Certifikatë për nënshkrim elektronik për subjektet private për infrastrukturën kritike
- Certifikatë për projektin e fiskalizimit për subjektet private
- Certifikatë Test për projektin e fiskalizimit

kërkesa për revokim mund të paraqitet në adresën pki@akshi.gov.al nga Subjekti duke përdorur të njëjtën adresë emaili që është përdorur në procesin fillestar të aplikimit. Kërkesa vërtetohet nga Sektori i PKI duke krahasuar të dhënat e paraqitura me të dhënat në RA. Nëse të dhënat përputhen, kërkesa për revokim pranohet.

4. KËRKESAT OPERACIONALE TË CIKLIT TË CERTIFIKATAVE

4.1 Aplikimi për certifikatë

4.1.1 Kush mund të paraqesë një kërkesë për certifikatë

Aplikimi për certifikatat më poshtë:

- Certifikatë për nënshkrim elektronik për subjektet private mund të paraqitet nga Subjekti i certifikatës që është një shtetas shqiptar i lidhur me një subjekt privat në Shqipëri ose një shtetas i huaj që zotëron një biznes në Shqipëri.
- Certifikatë për nënshkrim elektronik për punonjësit qeveritar mund të paraqitet nga Subjekti i certifikatës që është një punonjës qeveritar në Shqipëri.
- Certifikatë për nënshkrim elektronik për subjektet private për infrastrukturën kritike mund të paraqitet nga Subjekti i certifikatës që është një shtetas shqiptar i lidhur me një subjekt privat në Shqipëris që operon në infrastrukturën kritike ose akseson sisteme ndërkombëtare.
- Certifikatë për nënshkrim elektronik për punonjësit qeveritar për infrastrukturën kritike mund të paraqitet nga Subjekti i certifikatës që është një punonjës qeveritar në Shqipëri që operon në infrastrukturën kritike ose akseson sisteme ndërkombëtare.
- Certifikatë për vulën elektronike mund të paraqitet nga institucioni publik në Shqipëri që ofron shërbime në portalin e-Albania.
- Certifikatë për projektin e fiskalizimit për institucionet publike mund të paraqitet nga institucioni publik në Shqipëri.
- Certifikatë për projektin e fiskalizimit për subjektet private mund të paraqitet nga subjekti privat në Shqipëri.
- Certifikatë Test për projektin e fiskalizimit mund të paraqitet nga subjekti privat në fushën e IT-së në Shqipëri, i interesuar për të zhvilluar softuerë në kontekstin e projektit të fiskalizimit.

4.1.2 Procesi i regjistrimit dhe përgjegjësitë

Procesi i aplikimit për certifikatat më poshtë:

- Certifikatë për nënshkrim elektronik për subjektet private,
- Certifikatë për nënshkrim elektronik për subjektet private për infrastukturën kritike,
- Certifikatë për nënshkrim elektronik për punonjësit qeveritar,
- Certifikatë për nënshkrim elektronik për punonjësit qeveritar për infrastrukturën kritike,
- Certifikatë për projektin e fiskalizimit për institucionet publike,
- Certifikatë për projektin e fiskalizimit për subjektet private, dhe
- Certifikatë Test për projektin e fiskalizimit,

realizohet nëpërmjet portalit qeveritar e-Albania.

Pajtimtari do të nënshkruajë një marrëveshje me AKSHI-n në formë elektronike përpara dorëzimit të aplikimit. Me nënshkrimin e marrëveshjes, Pajtimtari pranon termat dhe kushtet e marrëveshjes si dhe kushtet e kësaj CP/CPS. Është përgjegjësia e Pajtimtarit të sigurojë që informacioni në formularin e aplikimit është i plotë dhe i saktë.

Detyrimet dhe përgjegjësitë e CA-së, RA-së dhe Pajtimtarit janë përcaktuar në seksionin 9.6.

Procesi i aplikimit për certifikatat për vulë elektronike kryhet përmes një kërkese zyrtare dërguar AKSHI-t. Pajtimtari do të nënshkruajë një marrëveshje me AKSHI-n gjatë procesit të aplikimit. Me

nënshkrimin e marrëveshjes Pajtimtari pranon termat dhe kushtet e marrëveshjes si dhe kushtet e kësaj CP/CPS.

4.2 Shqyrtimi i aplikimit për certifikatë

4.2.1 Kryerja e funksioneve të identifikimit dhe autentifikimit

Pas marrjes së një aplikimit, Oficeri i RA shqyrton aplikimin dhe të dhënat e dorëzuara brenda afatit të shqyrtimit të aplikimit që përshkruhet në seksionin 4.2.3. Identifikimi dhe autentifikimi i identitetit të personave fizik dhe juridik është përshkruar në kapitullin 3.

4.2.2 Miratimi ose refuzimi i kërkesave për paisje me certifikatë

Oficeri i RA-së vërteton të dhënat që aplikanti ka dorëzuar. Nëse të dhënat janë të sakta, aplikimi pranohet dhe përcillet në CA. Nëse ka ndonjë mospërputhje ose informacion të pasaktë, aplikimi refuzohet.

4.2.3 Koha për të procesuar aplikimet për certifikatë

Koha normale për procesimin e aplikimeve për paisje me certifikatë është 10 ditë pune.

4.3 Lëshimi i certifikatës

4.3.1 Veprimet e CA-së gjatë lëshimit të certifikatës

CA do të procesojë kërkesat për paisje me certifikatë dhe do të vazhdojë me lëshimin e certifikatës vetëm pas marrjes së kërkesës për certifikatë nga RA. CA dhe RA janë sisteme të besuara, të integruara së bashku. Fusha *Serial Number* në certifikatë siguron që certifikatat të jenë unike.

4.3.2 Njoftimi i pajtimtarit nga CA për lëshimin e certifikatës

Oficeri i RA tek Sektori i PKI njofton Pajtimtarët për lëshimin e certifikatës.

- Për certifikatat për nënshkrimin elektronik në Platformën e Nënshkrimit Elektronik:
    - Certifikatë për nënshkrim elektronik për subjektet private
    - Certifikatë për nënshkrim elektronik për punonjësit qeveritar

  Sektori i PKI i dërgon një email Pajtimtarit duke ofruar udhëzime për logim në Platformën e Nënshkrimit Elektronik. Certifikata gjenerohet kur Subjekti nënshkruan për herë të parë.

- Për certifikatat që lëshohen në USB Token:
    - Certifikatë për nënshkrim elektronik për subjektet private për infrastukturën kritike
    - Certifikatë për nënshkrim elektronik për punonjësit qeveritar për infrastukturën kritike

  Sektori i PKI i dërgon një email Pajtimtarit duke e njoftuar për lëshimin e certifikatës. Pajtimtari duhet të paraqitet fizikisht pranë zyrave të AKSHI-t për të tërhequr USB Token.

- Për certifikatat për vulën elektronike, Sektori i PKI i dërgon një email Pajtimtarit duke e njoftuar atë për lëshimin e certifikatës.

- Për certifikatat për projektin e fiskalizimit:
    - Certifikatë për projektin e fiskalizimit për institucionet publike
    - Certifikatë për projektin e fiskalizimit për subjektet private
    - Certifikatë Test për projektin e fiskalizimit

Sektori i PKI i dërgon një email Pajtimtarit duke e njoftuar atë për lëshimin e certifikatës. Certifikata mund të shkarkohet nga llogaria e tyre në poralin e-Albania.

4.4 Pranimi i certifikatës

4.4.1 Sjellja që përbën pranimin e certifikatës

Certifikata konsiderohet e pranuar nga Subjekti me nënshkrimin e deklaratës mbi termat dhe kushtet si dhe pas përdorimit për herë të parë të certifikatës nga Subjekti.

Subjekti ka të drejtë të refuzojë certifikatën, përpara përdorimit të parë, me kusht që të zbatohet të paktën një nga kushtet më poshtë:

- Informacioni në certifikatë është i pasaktë.
- Informacioni në certifikatë nuk është më i vlefshëm (nga data e aplikimit).
- Subjekti nuk ka më të drejta mbi certifikatën (për shembull kur personi fizik i lidhur me personin juridik ka ndërprerë marrëdhënien me personin juridik).

4.4.2 Publikimi i certifikatës nga CA

Nëse Pajtimtari ka autorizuar publikimin e certifikatës, AKSHI do ta vërë në dispozicion certifikatën për palët e përfshira në Direktori. Publikimi i certifikatave përshkruhet në kapitullin 2.

4.4.3 Njoftimi për lëshimin e certifikatës nga CA tek entitetet e tjera

Njoftimi për lëshimin e certifikatës tek entitetet e tjera bëhet nëpërmjet publikimit të certifikatës në Direktori siç përshkruhet në kapitullin 2.

4.5 Përdorimi i çiftit të çelësave dhe certifikatës

4.5.1 Përdorimi i çelësit privat të pajtimtarit dhe certifikatës

a. Çelësi privat i Subjektit gjenerohet dhe kontrollohet nga AKSHI

Kur AKSHI gjeneron dhe kontrollon çelësin privat, AKSHI është përgjegjës për:

- Sigurimin e përdorimit të çiftit të çelësave të Subjektit në përputhje me rregullat e specifikuara në këtë CP/CPS.
- Vendosjen e kontrolleve teknike dhe të sigurisë për të siguruar që përdorimi i çelësit privat është nën kontrollin e vetëm të nënshkruesit ose krijuesit të vulës.

b. Subjekti zotëron dhe menaxhon çelësin privat

Kur Subjekti është në posedim dhe menaxhon çelësin privat, Subjekti është përgjegjës për sa vijon:

- Përdorimi i çelësit privat dhe certifikatës vetëm për përdorimin e synuar siç përcaktohet në këtë CP/CPS dhe në deklaratën për kushtet e përdorimit të certifikatës.
- Certifikata duhet të përdoret në përputhje me fushën e përdorimit të çelësit.
- Mbrojtja e çelësit privat nga vjedhja, humbja, kompromentimi ose përdorimi i paautorizuar.
- Sigurimi që çelësi privat të jetë nën kontrollin e vetëm të nënshkruesit ose krijuesit të vulës.
- Njoftimi i AKSHI-t për të kërkuar revokimin e certifikatës në rast se çelësi privat është humbur, vjedhur, kompromentuar ose kur nënshkruesi ose krijuesi i një vule nuk është më në posedimin e vetëm të çelësit privat.

- Sigurimi i konfidencialitetit të të dhënave sekrete të aktivizimit dhe t'i ndajë ato me një palë tjetër.
- Njoftimi i AKSHI-t në rast se të dhënat e certifikatës janë të pasakta ose për ndonjë arsye bëhen të pavlefshme pas procesit të regjistrimit.
- Përdorimi korrekt i pajisjes kriptografike të sigurt në rast se Subjekti ka marrë një pajisje kriptografike nga AKSHI.

4.5.2 Përdorimi i çelësit publik dhe certifikatës nga pala e përfshirë

Pala e përfshirë që synon të mbështetet në certifikatat të cilat janë lëshuar sipas kësaj CP/CPS duhet të:

- Mbështetet në certifikatat vetëm për përdorim të duhur siç përcaktohet në këtë CP/CPS dhe në përputhje me fushën e përdorimit të çelësit të certifikatës.
- Përdorimi i certifikatës për qëllim të nënshkrimit/vulës elektronike dhe të çelësit publik përkatës vetëm për të validuar nënshkrimin/vulën elektronike.
- Marrë përsipër të kontrollojë statusin e një certifikate duke përdorur mekanizmat e përcaktuar në këtë CP/CPS.

Nëse certifikata është revokuar ose ka skaduar, pala e përfshirë nuk duhet t'i besojë certifikatës. Duke u mbështetur në një certifikatë të skaduar ose të revokuar, pala e përfshirë humbet garancitë e ofruara nga AKSHI si ofrues i shërbimeve të besuara.

4.6 Rinovimi i certifikatës

Rinovimi i certifikatës nënkupton lëshimin e një certifikate të re për pajtimtarin, pa ndryshuar çelësin publik të pajtimtarit ose të një pjesëmarrësi tjetër ose ndonjë informacion tjetër në certifikatë.

AKSHI nuk rinovon certifikatat ekzistuese për çelësat ekzistues. Mënyra e vetme e rinovimit është krijimi i një çifti të ri çelësash dhe lëshimi i një certifikate të re për një subjektet ekzistuese, certifikata e të cilit skadon së shpejti.

Referojuni seksionit 4.7 për informacion mbi rinovimin e certifikatës.

4.6.1 Rrethanat për rinovimin e certifikatës

Referojuni seksionit 4.7.

4.6.2 Kush mund të kërkojë rinovim

Referojuni seksionit 4.7.

4.6.3 Përpunimi i kërkesave për rinovimin e certifikatës

Referojuni seksionit 4.7.

4.6.4 Njoftimi i pajtimtarit për lëshimin e certifikatës së re

Referojuni seksionit 4.7.

4.6.5 Sjellja që përbën pranimin e një certifikate të rinovuar

Referojuni seksionit 4.7.

4.6.6 Publikimi i certifikatës së rinovuar nga CA

Referojuni seksionit 4.7.

4.6.7 Njoftimi për lëshimin e certifikatës nga CA tek subjektet e tjera

Referojuni seksionit 4.7.

4.7 Re-key i certifikatës

Ky seksion përshkruan rinovimin e certifikatës në rastet e gjenerimit të një çifti të ri çelësash dhe një certifikate të re për subjektet ekzistuese.

4.7.1 Rrethanat për re-key të certifikatës

AKSHI kryen procesin e re-key të certifikatave për subjektet ekzistuese për certifikata dixhitale të vlefshme të cilat nuk kërkojnë ndryshime të të dhënave të certifikatës ose shtesa. Procesi i re-key konsiston në ri-lëshimin e një certifikate me një çift të ri çelësash për të shtyrë datën e skadencës, pa ndryshuar identitetin e subjektit ose shtesa të tjera të certifikatës.

AKSHI njofton pajtimtarët nëpërmjet të njëjtit email të përdorur në procesin e regjistrimit në lidhje me datën e vlefshmërisë së certifikatës 30 ditë para skadimit.

4.7.2 Kush mund të kërkojë certifikimin e një çelësi të ri publik

Re-key i certifikatës mund të kërkohet nga Subjekti ose Pajtimtari, sipas rastit, duke dërguar një kërkesë në Sektorin e PKI të AKSHI-t.

4.7.3 Përpunimi i kërkesave për re-key të certifikatës

Re-key i certifikatës përpunohet nga Oficeri i RA-së në Sektorin e PKI pas marrjes së një kërkese nga Subjekti përmes të njëjtit email të përdorur në procesin e regjistrimit fillestar. Subjektit i kërkohet të konfirmojë që të dhënat e paraqitura në procesin fillestar të aplikimit janë ende të vlefshme dhe të sakta.

4.7.4 Njoftimi i pajtimtarit për lëshimin e certifikatës së re

Zbatohet procesi që përdoret për lëshimin fillestar të certifikatës.

4.7.5 Sjellja që përbën pranimin e një certifikate për të cilën është bërë re-key

Zbatohet procesi që përdoret për lëshimin fillestar të certifikatës.

4.7.6 Publikimi i certifikatës që është bërë re-key nga CA

Zbatohet procesi që përdoret për lëshimin fillestar të certifikatës.

4.7.7 Njoftimi për lëshimin e certifikatës nga CA tek subjektet e tjera

Zbatohet procesi që përdoret për lëshimin fillestar të certifikatës.

4.8 Modifikimi i certifikatës

Modifikimi i certifikatës i referohet lëshimit të një certifikate të re për shkak të ndryshimeve në informacionin në certifikatë, përveç çelësit publik të Pajtimtarit.

AKSHI nuk kryen modifikime të certifikatave të lëshuara. Subjekti ose Pajtimtari, sipas rastit, duhet të paraqesë një kërkesë për revokimin e certifikatës në rast se informacioni i përfshirë në certifikatë nuk është më i vlefshëm.

4.8.1 Rrethanat për modifikimin e certifikatës

Nuk aplikohet.

4.8.2 Kush mund të kërkojë modifikimin e certifikatës

Nuk aplikohet.

4.8.3 Përpunimi i kërkesave për modifikimin e certifikatës

Nuk aplikohet.

4.8.4 Njoftimi i pajtimtarit për lëshimin e certifikatës së re

Nuk aplikohet.

4.8.5 Sjellja që përbën pranimin e certifikatës së modifikuar

Nuk aplikohet.

4.8.6 Publikimi i certifikatës së modifikuar nga CA

Nuk aplikohet.

4.8.7 Njoftimi për lëshimin e certifikatës nga CA tek subjektet e tjera

Nuk aplikohet.

4.9 Revokimi dhe pezullimi i certifikatës

Certifikatat e revokuara i referohen certifikatave që nuk konsiderohen më të vlefshme nga lëshuesi i certifikatës. Certifikatat e lëshuara nga AKSHI mund të revokohen. Procesi i revokimit të certifikatës është i pakthyeshëm. Ky seksion përshkruan procesin e revokimit të certifikatës.

4.9.1 Rrethanat për revokimin

Kushtet e mëposhtme përshkruajnë rrethanat në të cilat një certifikatë revokohet:

- Subjekti kërkon revokimin e certifikatës.
- Informacioni që përmban certifikata ka ndryshuar ose nuk është më i vlefshëm.
- Çelësi privat i lidhur me çelësin publik ose është kompromet uar ose ka arsye të forta për të besuar se ai është kompromet uar.

- Në rastin e certifikatave të lëshuara për personat fizik të lidhur me një person juridik (p.sh. certifikatat e lëshuara për nënshkrim elektronik), marrëdhënia ndërmjet personit fizik dhe personit juridik ka përfunduar (psh. është ndërprerë marrëdhënia e punës).
- Pajtimtarët nuk pajtohen dhe nuk pranojnë termat dhe kushtet e specifikuara në një CPS që është përditësuar.
- AKSHI ndërpret veprimtarinë e tij. Në këtë rast, të gjitha certifikatat e lëshuara nga CA-të do të revokohen së bashku me certifikatat e CA-ve.
- Çelësi privat i CA-ve të AKSHI-t, përmes të cilave janë lëshuar certifikata të subjekteve fundore, është kompromentar.
- Subjekti nuk i respekton rregullat e kësaj CP/CPS ose deklaratës së pajtimtarit mbi termat dhe kushtet.
- Pajisja e sigurt kriptografike është humbur, vjedhur ose kompromentuar.

4.9.2 Kush mund të kërkojë revokimin

Një kërkesë për revokim mund të kërkohet nga:

- Subjekti i cili identifikohet si mbajtësi i çelësit privat të lidhur me çelësin publik të dhënë në certifikatë.
- Autoriteti i Regjistrimit i cili mund të kërkojë revokimin në emër të një subjekti ose nëse ka informacion që justifikon revokimin e certifikatës sipas rrethanave të përshkruara në seksionin 4.9.1.

4.9.3 Procedura e kërkesës për revokim

Procesi i paraqitjes së një kërkese për revokimin e certifikatës dhe procesi për identifikimin dhe autentifikimin e kërkesave për revokim përshkruhet në seksionin 3.4.

Pasi Oficeri i Revokimit ka pranuar kërkesën për revokim, kërkesa i përcillet NAIS Class CA përkatëse.

Informacioni për certifikatat e revokuara vendoset në Listën e Revokimit të Certifikatave (CRL) të lëshuar nga NAIS Class CAs.

4.9.4 Koha e lejuar për kërkesat për revokim

Kërkesa për revokim duhet të paraqitet sapo të shfaqet një rrethanë për revokim.

4.9.5 Koha brenda së cilës CA duhet të përpunojë kërkesën për revokim

AKSHI kryen revokimin e certifikatës brenda 24 orëve nga marrja e kërkesës për revokim.

4.9.6 Kërkesat për kontrollin e statusit të revokimit për palët e përfshira

Palët e përfshira duhet të përdorin mekanizmat e ofruar nga AKSHI për të kontrolluar statusin e certifikatave në të cilat dëshirojnë të mbështeten. Informacioni rreth revokimit publikohet duke përdorur CRL dhe OSCP.

4.9.7 Frekuenca e publikimit të CRL

NAIS Class CAs publikojne listat përkatëse të revokimit të certifikatave. CRL-të publikohen brenda 24 orëve pas marrjes së një kërkese për revokim dhe përditësohen automatikisht çdo 48 orë.

4.9.8 Vonesa maksimale për CRL-të

Frekuenca e publikimit të CRL-ve është në përputhje me seksionin 4.9.7. CRL-të publikohen pa vonesë.

4.9.9 Disponueshmëria e kontrollit të statusit/revokimit online

NAIS Class CAs mbështesin verifikimin online të statusit të revokimit të certifikatës së lëshuar nëpërmjet shërbimit OCSP të AKSHI-t.

Adresa e shërbimit të OCSP të AKSHI-t është ocsp.akshi.gov.al dhe shënohet në shtesën *Authority Information Access* në të gjitha certifikatave të lëshuara nga NAIS Class CAs.

4.9.10 Kërkesat mbi kontrollin e revokimit online

Për të përdorur shërbimin e OCSP të AKSHI-t, pala e përfshirë duhet të ketë një aplikacion që mund të përdorë shërbimin OCSP duke përdorur metodën GET ose POST.

4.9.11 Forma të tjera të disponueshme për njoftimin e revokimit

Asnjë përcaktim.

4.9.12 Kërkesa të veçanta për kompromentimin re key

Asnjë përcaktim.

4.9.13 Rrethanat e pezullimit

AKSHI nuk kryen pezullime të certifikatave.

4.9.14 Kush mund të kërkojë pezullim

Nuk aplikohet.

4.9.15 Procedura e kërkesës për pezullim

Nuk aplikohet.

4.9.16 Kufijtë për periudhën e pezullimit

Nuk aplikohet.

4.10 Shërbimet e statusit të certifikatës

4.10.1 Karakteristikat operacionale

Mekanizmat e përdorur nga AKSHI për shërbimet e statusit të certifikatës janë CRL dhe OCSP.

CRL-të publikohen në serverin e AKSHI-t dhe në direktori. Adresat e publikimit të CRL-ve gjenden gjithashtu në shtesën *CRL Distribution Points* të çdo certifikate të lëshuar.

- NAIS Root CA certs.akshi.gov.al/root.crl
- NAIS CA certs.akshi.gov.al/ca.crl
- NAIS Class 1 CA certs.akshi.gov.al/class1.crl

- NAIS Class 2 CA certs.akshi.gov.al/class2.crl
- NAIS Class 3 CA certs.akshi.gov.al/class3.crl
- NAIS Class 4 CA certs.akshi.gov.al/class4.crl

Adresa e shërbimit të OCSP është ocsp.akshi.gov.al dhe shënohet në shtesën *Authority Information Access* për të gjitha certifikatat e lëshuara nga CA-të e AKSHI-t.

4.10.2 Disponueshmëria e shërbimit

Shërbimet e statusit të certifikatës janë të disponueshme 24 orë në ditë, 7 ditë në javë.

4.10.3 Karakteristikat opsionale

Asnjë përcaktim.

4.11 Përfundimi i abonimit

Përfundimi i abonimit ndodh nëse:

- Certifikata e subjektit ka skaduar dhe Subjekti nuk kërkon rinovimin e certifikatës.
- Pajtimtari përfundon marrëveshjen përpara datës së skadimit të certifikatës. Në këtë rast AKSHI revokon certifikatën që është pjesë e kësaj marrëveshjeje.

4.12 'Key escrow' dhe rikuperimi

'Key escrow' i çelësave privatë të pajtimtarëve nuk lejohet.

4.12.1 Politika dhe praktikat kryesore të 'key escrow' dhe rikuperimit

Asnjë përcaktim.

4.12.2 Politika dhe praktikat e enkapsulimit dhe rikuperimit të sesionit të çelësit

Asnjë përcaktim.

5. KONTROLLE FIZIKE, TË MENAXHIMIT DHE OPERACIONALE

5.1 Kontrollet fizike

5.1.1 Vendndodhja dhe ndërtimet

AKSHI performon funksionet operacionale të CA dhe RA në një vendndodhje parësore me disa nivele të kontrolleve fizike dhe teknike të sigurisë.

Një vendndodhje dytësore përdoret si qendër rikuperimi nga fatkeqësitë, me qëllim rikuperimin dhe rivendosjen e shërbimeve në rast fatkeqësie natyrore ose mosfunksionim të sistemit. Kjo vendndodhje mbrohet me kontrolle të sigurisë fizike që kanë të njëjtin nivel sigurie me kontrollet e implementuara në vendndodhjen parësore.

5.1.2 Aksesi fizik

AKSHI ka vendosur një sistem kontrolli fizik të aksesit për të siguruar që vetëm personeli i autorizuar mund të ketë akses në vendin e prodhimit. AKSHI mban rregjistra të aksesit fizik.

Masat e kontrollit fizik janë vendosur për të mbrojtur pajisjet kritike nga aksesi i paautorizuar dhe për të zvogëluar rrezikun e ndërhyrjes në pajisje.

Zonat e sigurisë së lartë mund të aksesohen vetëm nga personeli i autorizuar të cilit i janë caktuar role të besuara dhe vetëm sipas parimit të kontrollit të dyfishtë.

Aksesi fizik kontrollohet dhe monitorohet nga sistemet e alarmit të sigurisë dhe ambientet mbikëqyren me video 24/7.

5.1.3 Energjia elektrike dhe kondicionimi

Ambientet në të cilën kryhen funksionet operacionale CA/RA dhe ndodhen sistemet dhe pajisjet, janë të pajisura me furnizime primare dhe dytësore energjie për të siguruar akses të vazhdueshëm dhe të pandërprerë të energjisë elektrike.

Këto ambiente përdorin sisteme HVAC për ngrohjen, ftohjen dhe ventilimin e ajrit për të parandaluar mbinxehjen dhe për të ruajtur nivelet e duhura të lagështisë.

5.1.4 Ekspozimet ndaj ujit

Ambientet ku janë vendosur pajisjet janë të siguruara kundër përmbytjeve dhe vendosen në dysheme të ngritura.

5.1.5 Parandalimi dhe mbrojtja nga zjarri

AKSHI ka implementuar një mekanizëm alarmi dhe shuarje zjarri në ambientet ku ndodhet infrastruktura e PKI në përputhje me standardet dhe rregulloret e mbrojtjes nga zjarri.

5.1.6 Ruajtja e mediave

Mediat që përmbajnë të dhëna të PKI të AKSHI-t ruhen në mënyrë të sigurt në vendndodhjen parësore në një mënyrë që siguron mbrojtje nga dëmet aksidentale dhe aksesi fizik i paautorizuar. Skedarët rezervë mbahen në një vend tjetër, të ndarë nga vendndodhja parësore.

5.1.7 Asgjesimi i mbetjeve

Dokumentacioni dhe të dhënat e PKI të AKSHI-t që nuk nevojiten më ose që kanë arritur periudhën e ruajtjes asgjësohen në mënyrë të sigurt. Asgjesimi i pajisjeve të veçanta si HSM-të bëhet duke ndjekur rekomandimet e dhëna nga prodhuesi.

5.1.8 Backup në lokacion të jashtëm

AKSHI performon backup në lokacion të sigurt të jashtëm. Frekuenca, mbajtja dhe niveli i backup, përcaktohet nga politika e brendshme e AKSHI-t mbi backup.

5.2 Kontrollet proceduriale

5.2.1 Rolet e besuara

Rolet e besuara në PKI-në e AKSHI-t ndjekin rekomandimet e përshkruara në ETSI EN 319 401 dhe ETSI EN 319 411-1. Në përputhje me këto rekomandimeve, AKSHI ka caktuar rolet e mëposhtme të besuara për kryerjen e detyrave në lidhje me ofrimin e shërbimeve të besuara:

1. **Oficer i Sigurisë** me përgjegjësinë e përgjithshme të administrimit të zbatimit të praktikave të sigurisë.
2. **Administrator i Sistemit** i cili është i autorizuar të instalojë, konfigurojë dhe mirëmbajë sistemet e besuara të AKSHI-t për menaxhimin e shërbimeve.
3. **Operator i Sistemit** i cili është përgjegjës për funksionimin e sistemeve të besuara të AKSHI-t në përditshmëri. Ky rol është gjithashtu i autorizuar për të kryer backup të sistemit.
4. **Auditues i Sistemit** i cili është i autorizuar për të parë arkivat dhe regjistrat e auditimit të sistemeve të besuara të AKSHI-t.
5. **Oficer i Regjistrimit** me përgjegjësinë e përgjithshme të verifikimit të informacionit për lëshimin e certifikatës dhe miratimin e kërkesave për certifikatë.
6. **Oficer i Revokimit** me përgjegjësinë e përgjithshme të kryerjes së ndryshimeve të statusit të certifikatës.

5.2.2 Numri i personave të nevojshëm për detyrë

Për operacionet kritike në të cilat nevojitet kontroll i dyfishtë, duhet të jenë të pranishëm të paktën dy persona të cilëve u janë caktuar role të besuara.

5.2.3 Identifikimi dhe autentifikimi për çdo rol

Punonjësit e AKSHI-t, të cilëve u është caktuar një rol i besuar, duhet të identifikohen dhe të autentifikohen për të hyrë në ambientet e AKSHI-t, për të aksesuar sistemet kritike dhe zonat e sigurisë së lartë. Çdo punonjës është i pajisur me një kartë të kontrollit të aksesit. Për të hyrë në sistemet kritike për kryerjen e operacioneve CA/RA, kërkohet autentifikim me shumë faktorë.

5.2.4 Rolet që kërkojnë ndarjen e detyrave

AKSHI ka vendosur kontrolle sigurie për të siguruar ndarjen e detyrave për rolet e besuara të përshkruara në seksionin 5.2.1. Në veçanti, rolet e administratorit, operatorit dhe auditorit nuk mund të kryhen nga një person.

5.3 Kontrollet e personelit

5.3.1 Kërkesat për kualifikimin, përvojën dhe verifikimin

AKSHI ndjek procedurat e brendshme organizative për të siguruar që punonjësit që janë të përfshirë në ofrimin e shërbimeve të besuara të kenë njohuritë, përvojën dhe ekspertizën e duhur.

Për personelin e caktuar në role të besuara, aplikohen kërkesa shtesë për të siguruar integritetin, besueshmërinë dhe angazhimin e tyre në mbrojtjen e informacionit të klasifikuar.

Të gjithë punonjësit e AKSHI-t janë të detyruar të pajisen me certifikatën e sigurisë nga Drejtoria e Sigurimit të Informacionit të Klasifikuar në Shqipëri.

5.3.2 Procedurat e verifikimit

Në kuadër të procesit të aplikimit për t'u pajisur me certifikatën e sigurisë nga Drejtoria e Sigurimit të Informacionit të Klasifikuar, punonjësit duhet të plotësojnë një pyetësor të detajuar të sigurisë dhe të nënshkruajnë një deklaratë për mbrojtjen e informacionit të klasifikuar.

Procedurat e verifikimit kryhen nga Drejtoria e Sigurimit së Informacionit të Klasifikuar në përputhje me ligjin për informacionin e klasifikuar.

5.3.3 Kërkesat për trajnim

AKSHI siguron që punonjësit e përfshirë në ofrimin e shërbimeve të certifikimit të jenë të pajisur me njohuritë e nevojshme për kryerjen e detyrave të tyre.

Personeli i përfshirë në ofrimin e shërbimeve të besuara është trajnuar në fushat e mëposhtme:

- Kërkesat e politikave të brendshme të AKSHI-t rreth sigurisë së informacionit,
- Kërkesat e deklaratës së praktikës së certifikimit,
- Softuerët e PKI që përdoren në ofrimin e shërbimeve të certifikimit,
- Rimëkëmbja nga fatkeqësitë dhe procedurat e vazhdimësisë së biznesit,
- Kryerja e operacioneve ditore dhe detyrave individuale në bazë të rolit të caktuar.

5.3.4 Frekuenca dhe kërkesat e rikualifikimit

Punonjësit e rinj duhet të trajnohen në fushat përmendura në seksionin 5.3.3. Gjatë periudhës së punësimit, AKSHI siguron që personeli i përfshirë në ofrimin e shërbimeve të certifikimit të marrë trajnime, mentorim dhe suport sa herë është e nevojshme.

Në rast të ndryshimeve në ofrimin e shërbimeve të besuara, ndryshime në funksionim ose përshtatje të një teknologjie të re, është e nevojshëm kryerja e trajnimeve.

Trajnimi i ndërgjegjësimit për sigurinë e informacionit kryhet të paktën një herë në vit për të gjithë punonjësit.

5.3.5 Frekuenca dhe sekuenca e rotacionit të roleve të punës

Asnjë përcaktim.

5.3.6 Sanksionet për veprime të paautorizuara

Sanksionet për veprimet e paautorizuara dhe zbulimin e informacionit konfidencial përcaktohen në rregulloren e brendshme të AKSHI-t. Këto sanksione mund të variojnë nga masat disiplinore, përfundimi i marrëdhënies së punës deri te procedime civile ose penale.

5.3.7 Kërkesat e kontraktorëve të pavaruar

Kërkesat për kontraktorët e pavarur përcaktohen në marrëveshjen kontraktuale me AKSHI-n. Organizatat që ofrojnë shërbime për PKI-në e AKSHI-t duhet të jenë të certifikuara me ISO 27001. Puna e kontraktorëve të pavarur në ambientet e AKSHI mbikëqyret nga punonjës të AKSHI-t të cilëve u janë caktuar role të besuara. Të njëjtat kërkesa për mbrojtjen e informacionit konfidencial që zbatohen për punonjësit e AKSHI-t zbatohen edhe për kontraktorët e pavarur.

5.3.8 Dokumentacioni që i ofrohet personelit

AKSHI i siguron personelit të gjithë dokumentacionin e nevojshëm për kryerjen e detyrave. Kjo përfshin politikat e sigurisë së informacionit, procedurat e brendshme operacionale, manualet dhe udhëzimet e punës. Dokumentacion tjetër ofrohet në bazë të nevojës në varësi të funksioneve specifike të punës.

5.4 Procedurat për loget e auditit

5.4.1 Llojet e ngjarjeve të regjistruara

AKSHI siguron që të rregjistrohet informacioni përkatës në lidhje me funksionimin e shërbimeve të besuara.

Ngjarjet e mëposhtme regjistrohen (manualisht ose në mënyrë automatike):

- Ngjarjet e menaxhimit të CA dhe të ciklit të certifikatës si gjenerimi i çelësave, backup, ruajtja dhe rikuperimi, përditësimet e CRL, etj.
- Certifikata e pajtimtarit dhe ngjarjet kryesore të menaxhimit të ciklit të certifkatës si aplikimet e certifikatave, lëshimi, rinovimi dhe revokimi, si dhe gjenerimi, rezervimi, ruajtja dhe rikuperimi i çelësave.
- Ngjarjet e lidhura me sigurinë, të tilla si ndërprerje të sistemit, mosfunksionim i harduerit, veprimet e sistemit të kryera nga personeli i AKSHI-t në role të besuara, aksesi në zona të sigurisë së lartë, etj.

Këto regjistra përfshijnë informacion mbi datën dhe kohën e hyrjes dhe identitetin e entitetit që bën regjistrimin në regjistër.

5.4.2 Frekuenca e procesimit të logeve

AKSHI monitoron sistemet në mënyrë të vazhdueshme për të dhënë alarme në kohë reale për ngjarjet e sigurisë. Këto ngjarje rishikohen në baza periodike nga personeli i AKSHI-t të caktuar në role të besuara.

5.4.3 Periudha e ruajtjes për loget e auditit

Periudha e ruajtjes për regjistrin e auditimit përshkruhet në procedurën e brendshme.

5.4.4 Mbrojtja e logeve të auditit

Loget e auditit mbrohen nga mekanizma dhe procedura që sigurojnë konfidencialitetin dhe integritetin e logeve si dhe mbrojtjen nga zbulimi, modifikimi, fshirja ose veprime të tjera të paautorizuara.

5.4.5 Procedurat për backup të logeve të auditit

Backup shtesë të logeve të auditit dhe backup-et e plota kryhen në baza periodike siç përcaktohet nga procedura e brendshme për backup.

5.4.6 Sistemi i mbledhjes së logeve (të brendshëm kundrejt të jashtëm)

Procesi i automatizuar i mbledhjes së logeve të auditit kryhet në nivel aplikacioni, rrjeti dhe sistemi operativ. Të dhënat e auditimit të krijuara manualisht regjistrohen nga personeli i AKSHI-t i caktuar në role të besuara.

5.4.7 Njoftimi për subjektin që shkaktoi ngjarjen

Për ngjarjet që regjistrohen nga sistemi i mbledhjes së logeve të auditit nuk është e nevojshme që të njoftohet pjesëmarrësi që shkaktoi ngjarjen, përveç rastit kur një njoftim i tillë është i detyrueshëm sipas ligjit.

5.4.8 Vlerësimet e vulnerabiliteteve

AKSHI kryen vlerësime të rregullta të vulnerabiliteteve për të identifikuar dhe vlerësuar kërcënimet e brendshme dhe të jashtme që mund të rezultojnë në akses të paautorizuar, zbulim, keqpërdorim, ndryshim ose shkatërrim të aseteve, përfshirë shërbimet e certifikimit si dhe të dhëna sensitive. Testi i penetrimit në baza periodike, siç përshkruhet në procedurë të brendshme. AKSHI punëson palë të jashtme për kryerjen e testimeve të penetrimit.

5.5 Arkivimi i të dhënave

5.5.1 Llojet e të dhënave të arkivuara

AKSHI arkivon të dhënat e mëposhtme në format elektronik ose në letër:

- Politika e certifikatës/Deklarata e praktikës së certifikimit
- Deklaratë mbi termat dhe kushtet e shërbimeve të besuara
- Aplikimet për certifikatë dhe të dhënat e mbledhura gjatë këtij procesi
- Informacioni i ciklit të jetës së certifikatës
- Të dhëna që lidhen me gjenerimin e çifteve të çelësave të NAIS CAs dhe certifikatat e NAIS CAs
- Politikat e brendshme, procedurat dhe udhëzimet e punës
- Informacioni i logeve të përmendur në seksionin 5.4.1

5.5.2 Periudha e ruajtjes së arkivave

Periudha e ruajtjes së arkivave përcaktohet në procedurën e brendshme.

5.5.3 Mbrojtja e arkivave

AKSHI mbron të dhënat dhe informacionin e arkivuar në mënyrë që vetëm personeli i autorizuar të ketë akses në arkivë. Arkivat mbrohen nga mekanizma dhe procedura që sigurojnë konfidencialitetin dhe integritetin e regjistrave dhe mbrojtjen nga zbulimi, modifikimi, fshirja ose veprime të tjera të paautorizuara.

5.5.4 Procedurat e backup për arkivat

Backup shtesë të logeve të auditit dhe backup e plota kryhen në baza periodike siç përcaktohet nga procedura e brendshme për backup.

5.5.5 Kërkesat për vulën kohore të të dhënave

Asnjë përcaktim.

5.5.6 Sistemi i grumbullimit të arkivave (i brendshëm ose i jashtëm)

Dokumentacioni në format fizik mblidhet manualisht dhe arkivohet brenda në ambientet e mbrojtura të AKSHI-t. Të dhënat në formë elektronike mblidhen automatikisht dhe arkivohen së brendshmi.

5.5.7 Procedurat për marrjen dhe verifikimin e informacionit të arkivuar

Vetëm personeli i autorizuar mund të ketë akses në arkiva. Integriteti i informacionit verifikohet kur ai rikthehet.

5.6 Ndërrimi i çelësit

Për të siguruar vazhdimësinë e shërbimeve të certifikimit, AKSHI do të gjenerojë një çift çelësash të rinj për CA-të përpara skadimit të një prej certifikatave të CA-ve të AKSHI-t.

Gjenerimi i një çifti çelësash për CA-të përshkruhet në seksionin 6.1. Certifikata e re me çelësin publik të ri, do të nënshkruhet nga NAIS Root CA.

AKSHI do të njoftojë paraprakisht pjesëmarrësit e PKI në lidhje me modifikimin e çelësit.

5.7 Kompromentimi dhe rikuperimi nga fatkeqësitë

5.7.1 Procedurat për trajtimin e incidenteve dhe kompromentimit

AKSHI ka implementuar një procedurë për përgjigjen ndaj incidenteve si pjesë e Sistemit të Menaxhimit të Sigurisë së Informacionit për trajtimin e incidenteve, reduktimin e risqeve ndaj sistemeve dhe të dhënave si dhe rikthimin e sistemeve në gjendjen operacionale sa më shpejt të jetë e mundur.

AKSHI ka caktuar personel me rol të besuar për të ndjekur alertet e sistemeve kritike, për të siguruar që incidentet përkatëse të raportohen në përputhje me procedurën e implementuar.

Brenda 24 orëve nga identifikimi i incidentit, AKSHI duhet të njoftojë Autoritetin Kombëtar për Çertifikimin Elektronik dhe Sigurinë Kibernetike në Shqipëri.

Nëse shkelja e sigurisë ka pasur efekt negativ ndaj një personi fizik ose juridik të cilit i është ofruar shërbimi i besuar, AKSHI do të njoftojë gjithashtu personin fizik ose juridik.

5.7.2 Resurset kompjuterike, softueri dhe/ose të dhënat korruptohen

Nëse burimet, programet kompjuterike ose të dhënat korruptohen, AKSHI merr masat e duhura, siç përshkruhet në procedurën e brendshme, për hetimin e incidentit, përshkallëzimin e duhur dhe reagimin ndaj incidentit.

Si pjesë e Sistemit të Menaxhimit të Sigurisë së Informacionit, AKSHI ka implementuar një politikë të vazhdimësisë së biznesit.

5.7.3 Procedurat në rast komprometimi të çelësit privat të entitetit

Në rast se çelësi privat i ndonjë prej CA-ve të AKSHI-t është kompromentuar, AKSHI do të revokojë certifikatën e CA që është e lidhur me çelësin e komprometuar. AKSHI do të njoftojë pjesëmarrësit e prekur të PKI për kompromentimin e celësit dhe revokimin e certifikatës.

Pasi të vlerësohet shkaku kryesor i kompromentimit të çelësit dhe të merren masa për të parandaluar që ngjarja të ndodhë në të ardhmen, AKSHI do të gjenerojë një çift të ri çelësash për CA dhe NAIS Root CA dhe do të lëshojë një certifikatë të re. CA-ja e re do të lëshojë certifikata për Pajtimtarët e prekur.

5.7.4 Aftësia për vazhdimësinë e biznesit pas një fatkeqësie

AKSHI përdor një vendndodhje dytësore si një qendër rikuperimi nga fatkeqësitë dhe do të zhvendosë operacionet në këtë vend dytësor në rast fatkeqësie. Politika e brendshme e vazhdimësisë së biznesit përshkruan hapat që do të ndërmerren në mënyrë më të detajuar.

5.8 Përfundimi i CA ose RA

Përpara përfundimit të aktiviteteve të CA-së, AKSHI do të:

- Njoftojë Autoritetin Kombëtar për Çertifikimin Elektronik dhe Sigurinë Kibernetike në Shqipëri.
- Informojë të gjithë pajtimtarët, palët e përfshira dhe pjesëmarrësit e tjerë të PKI në lidhje me përfundimin e shërbimeve të certifikimit.
- Transferojë vazhdimësinë e ofrimit të shërbimit të certifikimit tek një Ofrues tjetër i Kualifikuar i Shërbimit të Besuar. Gjatë këtij procesi, AKSHI do të dorëzojë tek ofruesi i kualifikuar i shërbimit të besuar të ri të gjithë dokumentacionin e mbledhur gjatë procesit të regjistrimit të Pajtimtarëve dhe dokumentacionin për certifikatat e lëshuara. Gjithashtu, AKSHI do t'i kalojë ofruesit të kualifikuar të shërbimit të besuar të ri të gjitha detyrimet për të vazhduar funksionimin pa probleme të shërbimeve të certifikimit.
- Revokojë të gjitha certifikatat e lëshuara dhe shkatërrojë çelësat privatë të Pajtimtarit (kur AKSHI menaxhon çelësat privatë në emër të Pajtimtarit).
- Revokojë certifikatat e CA-së dhe shkatërrojë çelësat privatë të CA-ve të AKSHI-t që nuk do të vazhdojnë më funksionimin e tyre.

6. KONTROLLET TEKNIKE TË SIGURISË

Ky kapitull përshkruan masat e sigurisë të marra nga AKSHI për të mbrojtur çelësat kriptografikë të NAIS CA dhe të dhënat e aktivizimit. Kapitulli përshkruan gjithashtu kontrolle të tjera teknike të sigurisë të përdorura nga CA-të e AKSHI-t për të kryer në mënyrë të sigurt funksione të tilla si gjenerimi i çelësave, autentifikimi i përdoruesit, regjistrimi i certifikatës, revokimi i certifikatës, auditimi dhe arkivimi.

6.1 Gjenerimi dhe instalimi i çifteve të çelësave

6.1.1 Gjenerimi i çiftit të çelësave

Gjenerimi i çiftit të çelësave të CA-ve të AKSHI-t

Gjenerimi i çiftit të çelësave të AKSH-t kryhet në përputhje me procesin e brendshëm të dokumentuar, në një zonë të sigurisë së lartë. Ky proces kryhet nga personel i përshtatshëm në përputhje me alkokimin në rolet të besuara, të paktën nën kontroll të dyfishtë dhe dëshmohet nga persona të autorizuar pranë PKI-së së AKSHI-t.

Algoritmet kriptografike të përdorura për gjenerimin e çelësave dhe gjatësinë e çelësit për NAIS CAs bazohen në rekomandimet e specifikuara në ETSI TS 119 312.

Gjenerimi i çiftit të çelësave të pajtimtarëve

a. Gjenerimi i çiftit të çelësave të pajtimtarëve brenda HSM

HSM e përdorur për gjenerimin e çelësave është në përputhje me kërkesat e përshkruara në seksionin 6.2. Në këtë rast, gjenerimi i çiftit të çelësave kryhet në një zonë të sigurisë së lartë. Kjo aplikohet për gjenerimin e çifteve të çelësave për certifikatat të cilat përdoren në Platformën e Nënshkrimit Elektronik:

- Certifikatë për nënshkrim elektronik për subjektet private
- Certifikatë për nënshkrim elektronik për punonjësit qeveritar

b. Gjenerimi i çiftit të çelësave të pajtimtarëve në një pajisje kriptografike të sigurt (USB Token)

Pajisja e sigurt kriptografike e përdorur për gjenerimin e çelësave është në përputhje me kërkesat e përshkruara në seksionin 6.2. Çifti i çelësave mund të gjenerohet nga Oficeri i RA në Sektorin e PKI, në një zonë të sigurisë së lartë. Kjo aplikohet për certifikatat më poshtë:

- Certifikatë për nënshkrim elektronik për subjektet private për infrastrukturën kritike
- Certifikatë për nënshkrim elektronik për punonjësit qeveritar për infrastrukturën kritike

c. Gjenerimi i çiftit të çelësave të pajtimtarëve në një modul softuer

Gjenerimi i çiftit të çelësave kryhet brenda një moduli të sigurt softueri në formatin PKCS#12. Në këtë rast çifti i çelësave gjenerohet nga Oficeri i RA. Kjo aplikohet për certifikatat më poshtë:

- Certifikatë për vulën elektronike
- Certifikatë për projektin e fiskalizimit për institucionet publike
- Certifikatë për projektin e fiskalizimit për subjektet private

- Certifikatë Test për projektin e fiskalizimit

6.1.2 Dorëzimi i çelësit privat tek pajtimtari

Në rastet kur AKSHI gjeneron dhe menaxhon çelësin privat në emër të nënshkruesit ose krijuesit të vulës, AKSHI siguron ruajtjen e sigurt të çelësit privat. AKSHI zbaton kontrolle sigurie për mbrojtjen e çelësit privat nga zbulimi, korruptimi dhe riprodhimi i paautorizuar.

Nëse çifti i çelësave gjenerohet nga pajtimtari, çelësi privat konsiderohet se është në zotërim të pajtimtarit.

Në rastet kur AKSHI i dorëzon pajtimtarit çelësin privat:
- Nëse AKSHI gjeneron çelësin privat në një modul softuer, çelësi privat i dorëzohet pajtimtarit përmes një kanali të sigurt në formatin PKCS#12.
- Nëse AKSHI gjeneron çelësin privat në një pajisje kriptografike të sigurt, çelësi privat i dorëzohet pajtimtarit nëpërmjet pajisjes së sigurt kriptografike në zyrat e AKSHI-t.

6.1.3 Dorëzimi i çelësit publik tek lëshuesi i certifikatës

Në rastet kur AKSHI gjeneron dhe menaxhon çiftin e çelësave në emër të nënshkruesit ose krijuesit të vulës, dorëzimi i çelësit publik tek AKSHI nuk është i nevojshëm.

Në rastet kur çifti i çelësave gjenerohet nga pajtimtari, pajtimtari do të paraqesë një kërkesë për nënshkrimin e certifikatës (CSR) (e cila do të përfshijë çelësin publik të nënshkruar nga çelësi privat i lidhur) në përputhje me standardin PKCS#10.

6.1.4 Dorëzimi i çelësit publik të CA-së tek palët e përfshira

Çelësat publikë të NAIS CA janë të disponueshme për palët e përfshira në certifikatat e NAIS CA të lëshuara nga NAIS Root CA për të siguruar integritetin dhe verifikimin e zinxhirit të certifikatave.

AKSHI ka vënë në dispozicion të publikut certifikatat në direktorinë akshi.gov.al/repository. Kontrollet e aksesit të direktorive përshkruhen në seksionin 2.4.

Linqet për aksesin direkt të certifikatave të NAIS Root CA, NAIS CA, NAIS Class CAs janë:

Certifikata Root:

- NAIS Root CA: certs.akshi.gov.al/root.crt

Certifikata vartëse:

- NAIS CA: certs.akshi.gov.al/ca.crt

Certifikatat e klasave:

- NAIS Class 1 CA: certs.akshi.gov.al/class1.crt
- NAIS Class 2 CA: certs.akshi.gov.al/class2.crt
- NAIS Class 3 CA: certs.akshi.gov.al/class3.crt
- NAIS Class 4 CA: certs.akshi.gov.al/class4.crt

6.1.5 Madhësitë e çelësave

Madhësitë e çelësave janë si më poshtë:

- NAIS Root CA përdor algoritmin sha256WithRSA me madhësi çelësi 4096-bit
- NAIS CA përdor algoritmin sha256WithRSA me madhësi çelësi 2048-bit
- NAIS Class CAs përdorin algoritmin sha256WithRSA me madhësi çelësi 2048-bit
- Certifikatat e pajtimtarëve përdorin çifte çelësash RSA 2048-bitësh

6.1.6 Gjenerimi i parametrave të çelësit publik dhe kontrolli i cilësisë

Gjenerimi i çiftit të çelësave për të gjitha CA-të e AKSHI-t kryhet duke përdorur parametrat e gjenerimit të rekomanduara në ETSI TS 119 312.

AKSHI siguron kontrollin e cilësisë duke përdorur module HSM dhe pajisje kriptografike të sigurta që janë në përputhje me standardet e referuara në seksionin 6.2.

6.1.7 Qëllimet e përdorimit të çelësit (sipas fushës së përdorimit të çelësit X.509 v3)

Seksioni 7.1.2 jep informacion mbi fushën *KeyUsage* të certifikatave të lëshuara nga AKSHI në përputhje me standardin X.509 V3.

Bitet e vendosur në fushën *KeyUsage* përdoren si më poshtë:

- digitalSignature bit (0) vendoset kur çelësi publik i subjektit përdoret për verifikimin e nënshkrimeve dixhitale, përveç nënshkrimeve në certifikata (bit 5) dhe CRL (bit 6), si ato të përdorura në një shërbim autentifikimi të një entiteti, një shërbim autentifikimi i origjinës së të dhënave dhe/ose një shërbim integriteti.
- nonRepudiation bit (1) vendoset kur çelësi publik i subjektit përdoret për të verifikuar nënshkrimet dixhitale, përveç nënshkrimeve në certifikata (biti 5) dhe CRL-ve (biti 6), të përdorura për të ofruar një shërbim mos-refuzimi që mbron kundër mohimit të rremë të subjektit nënshkrues për veprimet e kryera.
- keyEncipherment bit (2) vendoset kur çelësi publik i subjektit përdoret për shifrimin e çelësave privatë ose sekretë, p.sh., për transportin e çelësave.
- dataEncipherment bit (3) vendoset kur çelësi publik i subjektit përdoret për shifrimin e drejtpërdrejtë të të dhënave të papërpunuara të përdoruesit pa përdorimin e një shifrimi simetrik të ndërmjetëm.
- keyAgreement bit (4) vendoset kur çelësi publik i subjektit përdoret për marrëveshjen e çelësit.
- keyCertSign bit (5) vendoset kur çelësi publik i subjektit përdoret për verifikimin e nënshkrimeve në certifikatat me çelës publik.
- cRLSign bit (6) vendoset kur çelësi publik i subjektit përdoret për verifikimin e nënshkrimeve në listat e revokimit të certifikatave.
- encipherOnly bit (7) - kur biti *encipherOnly* është vendosur dhe biti *keyAgreement* është vendosur gjithashtu, çelësi publik i subjektit mund të përdoret vetëm për shifrimin e të dhënave gjatë kryerjes së marrëveshjes së çelësit.
- decipheOnly bit (8) - kur biti *decipherOnly* është vendosur dhe biti *keyAgreement* është vendosur gjithashtu, çelësi publik i subjektit mund të përdoret vetëm për deshifrimin e të dhënave gjatë kryerjes së marrëveshjes së çelësit.

6.2 Mbrojtja e çelësit privat dhe kontrollet inxhinierike të modulit kriptografik

6.2.1 Standardet dhe kontrollet e modulit kriptografik

HSM-të e përdorura për mbrojtjen e çelësave privatë për NAIS CA dhe NAIS Class CAs plotësojnë kërkesat e FIPS 140-2 Niveli 3.

Mbrojtja e çelësave privatë të pajtimtarëve për:

- Certifikatat e përdorura në Platformën e Nënshkrimit Elektronik, kryhet nga një QSCD remote duke përdorur HSM në përputhje me standardin FIPS 140-2 Niveli 3.
- Certifikatat për operatorët e infrastrukturës kritike, kryhet nga pajisje kriptografike të sigurta që plotësojnë kërkesat e nivelit 2 ose 3 të FIPS 140-2.
- Certifikatat e lëshuara si certifikata softuerike, çelësi privat mbrohet nga një software token.

6.2.2 Çelësi privat (n nga m) kontroll me shumë persona

HSM-të, të cilat përdoren për mbrojtjen e çelësave privatë për NAIS CA dhe NAIS Class CA, janë të vendosura në një zonë të sigurisë së lartë, e cila mund të aksesohet vetëm nën kontrollin e dyfishtë të personelit të autorizuar, të cilëve u janë caktuar role të besuara në PKI-në e AKSHI-t.

Gjenerimi i çiftit të çelësave të NAIS Class CA përshkruhet në seksionin 6.1.1.

6.2.3 'Escrow' i çelësit privat

'Escrow' i çelësit privat të NAIS CA dhe NAIS CAs nuk lejohet. Çelësat privatë të pajtimtarëve nuk janë në ruajtje.

6.2.4 Backup i çelësit privat

AKSHI kryen backup të çelësave privatë për të siguruar rikuperimin në rast urgjence. Backup i çelësit privat për NAIS CA dhe NAIS Class CAs kryhet nga role të besuara, sipas parimit të kontrollit të dyfishtë, në një zonë të sigurisë së lartë. Kur përdoren jashtë HSM, çelësat privatë janë gjithmonë të enkriptuar.

6.2.5 Arkivimi i çelësit privat

Çelësat privatë të NAIS CA, NAIS Class CA dhe të Pajtimtarëve, nuk arkivohen.

6.2.6 Transferimi i çelësit privat në ose prej një moduli kriptografik

Transferimi i çelësit privat në ose nga HSM-ja mund të kryhet vetëm nga personeli i autorizuar, të cilit i janë caktuar role të besuara, sipas parimit të kontrollit të dyfishtë, në një zonë të sigurisë së lartë.

Transferimi i çelësit privat në ose nga një HSM kryhet në një mënyrë që siguron të njëjtin nivel sigurie si në rastin kur çelësi është brenda HSM. Në raste të tilla, çelësi privat mbrohet gjithmonë me enkriptim.

Transferimi i çelësit privat mund të ndodhë gjatë procedurave backup ose në rastet e mosfunksionimit të modulit.

6.2.7 Ruajtja e çelësit privat në modulin kriptografik

AKSHI përdor HSM për të mbrojtur çelësat privatë. HSM-të janë të vendosura në një zonë të sigurisë së lartë, që mund të aksesohet vetëm nga personeli i autorizuar, të cilit i janë caktuar role të besuara. Çelësat privatë të përdorur në certifikatat për nënshkrim elektronik në Platformën e Nënshkrimit Elektronik, mund të përdoren vetëm kur janë aktivizuar siç duhet.

6.2.8 Mënyra e aktivizimit të çelësit privat

Aktivizimi i çelësave privatë të NAIS CA në modulet kriptografike harduerike kryhet nën kontroll të dyfishtë nga personeli i autorizuar, të cilëve u janë caktuar role të besuara në AKSHI.

Kur çelësi privat i subjektit ruhet në një pajisje kriptografike të sigurt, çelësi privat është nën kontrollin e vetëm të subjektit. Çelësi mund të aksesohet vetëm duke përdorur të dhënat sekrete të aktivizimit.

Për certifikatat për nënshkrimin elektronik që do të përdoren në Platformën e Nënshkrimit Elektronik, moduli i aktivizimit të nënshkrimit i lejon Subjektet të mbajnë kontroll ekskluziv mbi çelësat e tyre.

6.2.9 Metoda e çaktivizimit të çelësit privat

Çaktivizimi i çelësave privatë të NAIS CAs së kryhet në përputhje me procedurën e përshkruar në manualin për HSM-të. Ky proces kryhet nën kontroll të dyfishtë nga personeli i autorizuar, të cilëve u janë caktuar role të besuara në AKSHI.

Për certifikatat e përdorura në Platformën e Nënshkrimit Elektronik, çelësat privatë çaktivizohen pasi të ketë përfunduar procesi i nënshkrimit.

Për certifikatat e ruajtura në një pajisje kriptografike të sigurt, Subjekti mund të çaktivizojë çelësin privat duke hequr ose shkëputur fizikisht pajisjen.

6.2.10 Metoda e shkatërrimit të çelësit privat

Çelësat privatë të CA-ve të AKSHI-së asgjesohen nga personeli i AKSHI-t, të cilëve u janë caktuar role të besuara, në prani të një përfaqësuesi nga menaxhimi i AKSHI-t për të siguruar që çelësat privatë nuk mund të merren ose të përdoren përsëri. Procesi kryhet në përputhje me hapat e përshkruar në manualin e HSM.

6.2.11 Vlerësimi i modulit kriptografik

Referojuni seksionit 6.2.1.

6.3 Aspekte të tjera të menaxhimit të çifteve kryesore

6.3.1 Arkivimi i çelësit publik

Të gjitha çelësat publik të NAIS CAs dhe çelësat publikë të pajtimtarëve janë arkivuar. Seksioni 5.5 përshkruan procesin e arkivimit.

6.3.2 Kohëzgjatja operacionale e certifikatës dhe periudhat e përdorimit të çiftit të çelësave

Periudha e përdorimit të çelësave publik vendoset në fushën e vlefshmërisë së çdo certifikate me çelës publik. Periudha e vlefshmërisë së çelësit privat është e barabartë me periudhën e vlefshmërisë së certifikatës përkatëse.

- Afati i vlefshmërisë për NAIS CA është 15 vjet.
- Periudha e vlefshmërisë NAIS Class CAs është 7 vjet.
- Periudha e vlefshmërisë së një certifikate të pajtimtarit është një vit.

6.4 Të dhënat e aktivizimit

6.4.1 Gjenerimi dhe instalimi i të dhënave të aktivizimit

Të dhënat e aktivizimit që lidhen me çelësat privatë të NAIS CAs gjenerohen dhe instalohen gjatë gjenerimit të çiftit të çelësave.

Të dhënat e aktivizimit që përdoren për të mbrojtur pajisjet kriptografike të sigurta që përmbajnë çelësat privatë të subjektit krijohen në përputhje me manualin e pajisjes kriptografike.

Të dhënat e aktivizimit për çelësat privatë të përdorur në Platformën e Nënshkrimit Elektronik përbëhen nga të dhënat e aktivizimit të lidhura me HSM, të cilat gjenerohen në përputhje me manualin e HSM.

6.4.2 Mbrojtja e të dhënave të aktivizimit

Të dhënat e aktivizimit në lidhje me çelësat privatë të NAIS CAs ruhen në mënyrë të sigurt, duke përdorur një kombinim mekanizmash kontrolli për t'i mbrojtur ata nga zbulimi i paautorizuar.

Të dhënat e aktivizimit të pajisjeve kriptografike të sigurta i dorëzohen Pajtimtarit në mënyrë të sigurt, nga një kanal i veçantë. AKSHI rekomandon pajtimtarin të ndryshojë të dhënat e aktivizimit në pajisjen kriptografike përpara përdorimit të parë. Pas disa përpjekjeve të pasuksesshme për të hyrë në modulin kriptografik, kjo do të rezultojë në bllokimin e tij.

6.4.3 Aspekte të tjera të të dhënave të aktivizimit

Asnjë përcaktim.

6.5 Kontrollet e sigurisë kompjuterike

6.5.1 Kërkesat teknike specifike të sigurisë kompjuterike

Vetëm personat e autorizuar të cilëve u janë caktuar role të besuara mund të kenë akses në sistemet dhe aplikacionet që përdoren në ofrimin e shërbimeve të certifikimit. Qasja në këto sisteme jepet në bazë të funksioneve specifike të punës. Ndarja e detyrave kryhet për rolet e besuara të caktuara që përshkruhen në seksionin 5.2.1.

Procedurat e monitorimit të sistemit janë implementuar për të zbuluar dhe për t'iu përgjigjur aktivitetit të pazakontë ose aksesit të paautorizuar.

AKSHI ka implementuar zgjidhje teknike për të mbrojtur sistemet e besuara kundër malware.

Një procedurë e brendshme për menaxhimin e fjalëkalimeve kërkon nga përdoruesit përdorimin e fjalëkalimeve komplekse dhe ndryshimin e këtyre fjalëkalimeve në mënyrë të rregullt.

Të gjitha mediat që përmbajnë të dhëna sensitive, të logeve të auditit, arkivimit ose backup mbrohen përmes kontrolleve të përshtatshme fizike dhe logjike të aksesit.

6.5.2 Vlerësimi i sigurisë së kompjuterit

Asnjë përcaktim.

6.6 Kontrollet teknike të ciklit jetësor

6.6.1 Kontrollet e zhvillimit të sistemit

AKSHI përdor sisteme të besuara për ofrimin e shërbimeve të certifikimit të cilat i janë nënshtruar një procesi të gjerë testimi sigurie përpara se të miratohen për përdorim brenda një mjedisi PKI.

Softueri që zhvillohet në emër të AKSHI-t kalon nëpër procedura të sigurta zhvillimi përpara se të kalojë në mjedisin e prodhimit.

AKSHI ka implementuar një procedurë për menaxhimin e ndryshimeve. Ndryshimet e bëra në softuerë implementohen në përputhje me këtë procedurë.

6.6.2 Kontrollet e menaxhimit të sigurisë

AKSHI ka politika dhe mekanizma për të kontrolluar dhe monitoruar konfigurimin e sistemeve të përdorura për ofrimin e shërbimeve të certifikimit. AKSHI verifikon integritetin e sistemeve të tij në mënyrë të rregullt.

6.6.3 Kontrollet e sigurisë së ciklit jetësor

AKSHI kryen rishikime periodike të politikave, sistemeve dhe aseteve të tjera për të siguruar që ato të jenë të përshtatshme dhe për të siguruar efektivitetin e tyre të vazhdueshëm. AKSHI ka implementuar një proces të brendshëm të menaxhimit të kapaciteteve për të monitoruar dhe vlerësuar kërkesat e kapaciteteve të sistemeve që përdoren në ofrimin e shërbimeve të certifikimit.

6.7 Kontrollet e sigurisë së rrjetit

AKSHI kryen të gjitha funksionet e CA dhe RA duke përdorur rrjete të sigurta në përputhje me Sistemin e Menaxhimit të Sigurisë së Informacionit për të parandaluar aksesin e paautorizuar dhe aktivitete të tjera keqdashëse.

AKSHI kryen segmentimin e sistemeve të certifikimit në rrjete/zona bazuar në marrëdhëniet e tyre funksionale, logjike dhe fizike. Zonat e rrjetit ndahen nga firewalls dhe implementohen masa të njëjta sigurie për sistemet që ndodhen brenda të njëjtës zonë rrjeti.

AKSHI monitoron nivelin e sigurisë së rrjetit të brendshëm dhe lidhjeve të jashtme.

6.8 Time-stamping (vula kohore)

Certifikatat, CRL-të dhe informacionet e tjera të revokimit përmbajnë informacion për kohën dhe datën. Koha në sistemet e certifikimit të AKSHI-t sinkronizohet me kohën UTC.

7. PROFILI I CERTIFIKATAVE, CRL DHE OCSP

7.1 Profili i Certifikatave

Profili për fushat bazë për certifikatën **NAIS Root CA** përshkruhet më poshtë:

Emri i fushës	Vlera	
Version	Version 3	
Serial Number	11530b05a0db73c682	
Signature Algorithm	sha256WithRSAEncryption	
Issuer	Organizational Unit (OU)	NAIS Root Certification Authority
	Organization Name (O)	NAIS
	Country (C)	AL
Valid from	Thursday, February 11, 2016 11:06:42 AM	
Valid to	Saturday, February 9, 2041 11:06:42 AM	
Subject	Organizational Unit (OU)	NAIS Root Certification Authority
	Organization Name (O)	NAIS
	Country (C)	AL
Subject Public Key Info	RSA (4096 Bits)	
Signature	sha256WithRSAEncryption	

Profili për fushat bazë për certifikatën **NAIS CA** përshkruhet më poshtë:

Emri i fushës	Vlera
Version	Version 3

Serial Number	1001352ea8aaad2022fd	
Signature Algorithm	sha256WithRSAEncryption	
Issuer	Organizational Unit (OU)	NAIS Root Certification Authority
	Organization Name (O)	NAIS
	Country (C)	AL
Valid from	Thursday, February 11, 2016 11:16:06 AM	
Valid to	Monday, February 10, 2031 11:16:06 AM	
Subject	Organizational Unit (OU)	NAIS Certification Authority
	Organization Nam+e (O)	NAIS
	Country (C)	AL
Subject Public Key Info	RSA (2048 Bits)	
Signature	sha256WithRSAEncryption	

Profili për fushat bazë për certifikatën **NAIS Class 1 CA** përshkruhet më poshtë:

Emri i fushës	Vlera	
Version	Version 3	
Serial Number	2001b464c5574b29f500	
Signature Algorithm	sha256WithRSAEncryption	
Issuer	Organizational Unit (OU)	NAIS Certification Authority
	Organization Name (O)	NAIS
	Country (C)	AL

Valid from	Thursday, February 11, 2016 11:19:53 AM	
Valid to	Friday, February 10, 2023 11:19:53 AM	
Subject	Organizational Unit (OU)	NAIS Class 1 Certification Authority
	Organization Name (O)	NAIS
	Country (C)	AL
Subject Public Key Info	RSA (2048 Bits)	
Signature	sha256WithRSAEncryption	

Profili për fushat bazë për certifikatën **NAIS Class 2 CA** përshkruhet më poshtë:

Emri i fushës	Vlera	
Version	Version 3	
Serial Number	2002d37d1fe47e327b1d	
Signature Algorithm	sha256WithRSAEncryption	
Issuer	Organizational Unit (OU)	NAIS Certification Authority
	Organization Name (O)	NAIS
	Country (C)	AL
Valid from	Thursday, February 11, 2016 11:23:43 AM	
Valid to	Friday, February 10, 2023 11:23:43 AM	
Subject	Organizational Unit (OU)	NAIS Class 2 Certification Authority
	Organization Name (O)	NAIS
	Country (C)	AL

Subject Public Key Info	RSA (2048 Bits)
Signature	sha256WithRSAEncryption

Profili për fushat bazë për certifikatën **NAIS Class 3 CA** përshkruhet më poshtë:

Emri i fushës	Vlera	
Version	Version 3	
Serial Number	20038b09625165fadf49	
Signature Algorithm	sha256WithRSAEncryption	
Issuer	Organizational Unit (OU)	NAIS Certification Authority
	Organization Name (O)	NAIS
	Country (C)	AL
Valid from	Thursday, February 11, 2016 11:26:17 AM	
Valid to	Friday, February 10, 2023 11:26:17 AM	
Subject	Organizational Unit (OU)	NAIS Class 3 Certification Authority
	Organization Name (O)	NAIS
	Country (C)	AL
Subject Public Key Info	RSA (2048 Bits)	
Signature	sha256WithRSAEncryption	

Profili për fushat bazë për certifikatën **NAIS Class 4 CA** përshkruhet më poshtë:

Emri i fushës	Vlera

Version	Version 3	
Serial Number	2004cd6bb1a82a33ce32	
Signature Algorithm	sha256WithRSAEncryption	
Issuer	Organizational Unit (OU)	NAIS Certification Authority
	Organization Name (O)	NAIS
	Country (C)	AL
Valid from	Thursday, February 11, 2016 11:27:26 AM	
Valid to	Friday, February 10, 2023 11:27:26 AM	
Subject	Organizational Unit (OU)	NAIS Class 4 Certification Authority
	Organization Name (O)	NAIS
	Country (C)	AL
Subject Public Key Info	RSA (2048 Bits)	
Signature	sha256WithRSAEncryption	

7.1.1 Versionet

Të gjitha certifikatat që lëshohen nga AKSHI janë në versionin X.509 Version 3.

7.1.2 Fushat shtesë të certifikatave

Fushat shtesë për certifikatën **NAIS CA** paraqiten më poshtë.

Fusha shtesë	Vlera	Kritike
Authority Info Access	[1] Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.akshi.gov.al [2] Authority Info Access Access Method=Certification Authority Issuer	Jo

	(1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://certs.akshi.gov.al/root.crt	
Basic Constraints	Subject type=CA Path Length Constraint=None	Po
Key Usage	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)	Po
Authority Key Identifier	KeyID= 53011db30451cb76ccb6a1a426aaeb80e5e2edda	Jo
Subject Key Identifier	eb1ed6948abdf0de2c812f9753b99b216b345db3	Jo
Certificate Policies	[1] Certificate Policy: Policy Identifier= 1.3.6.1.4.1.39148.10.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.akshi.gov.al/repository [2] Certificate Policy: Policy Identifier= 1.3.6.1.4.1.39148.10.1.1 [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.akshi.gov.al/repository	Jo
CRL Distribution Points	CRL Distribution Point: Distribution Point Name: Full Name: URL = http://crl.akshi.gov.al/root.crl URL = ldap://ldap.akshi.gov.al/OU=NAIS Root Certification Authority,O=NAIS,C=AL?certificateRevocationList;binary	Jo

Fushat shtesë për certifikatën **NAIS Class 1 CA** paraqiten më poshtë.

Fusha shtesë	Vlera	Kritike
Authority Info Access	[1] Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.akshi.gov.al [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://certs.akshi.gov.al/ca.crt	Jo
Basic Constraints	Subject type=CA Path Length Constraint=None	Po

Key Usage	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)	Po
Authority Key Identifier	KeyID= eb1ed6948abdf0de2c812f9753b99b216b345db3	Jo
Subject Key Identifier	42d78665150a4f63e5bffa820fbc3f72c5251d47	Jo
Certificate Policies	[1] Certificate Policy: Policy Identifier= 1.3.6.1.4.1.39148.10.1.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.akshi.gov.al/repository	Jo
CRL Distribution Points	CRL Distribution Point: Distribution Point Name: Full Name: URL = http://crl.akshi.gov.al/ca.crl URL = ldap://ldap.akshi.gov.al/OU=NAIS Certification Authority,O=NAIS,C=AL?certificateRevocationList;binary	Jo

Fushat shtesë për certifikatën **NAIS Class 2 CA** paraqiten më poshtë.

Fusha shtesë	Vlera	Kritike
Authority Info Access	[1] Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.akshi.gov.al [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://certs.akshi.gov.al/ca.crt	Jo
Basic Constraints	Subject type=CA Path Length Constraint=None	Po
Key Usage	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)	Po
Authority Key Identifier	KeyID= eb1ed6948abdf0de2c812f9753b99b216b345db3	Jo
Subject Key Identifier	5fd64efdbc49c5e27c1782ba4d483d9b76b961cb	Jo
Certificate Policies	[1] Certificate Policy: Policy Identifier= 1.3.6.1.4.1.39148.10.1.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS	Jo

	Qualifier: http://www.akshi.gov.al/repository	
CRL Distribution Points	CRL Distribution Point: Distribution Point Name: Full Name: URL = http://crl.akshi.gov.al/ca.crl URL = ldap://ldap.akshi.gov.al/OU=NAIS Certification Authority,O=NAIS,C=AL?certificateRevocationList;binary	Jo

Fushat shtesë për certifikatën **NAIS Class 3 CA** paraqiten më poshtë.

Fusha shtesë	Vlera	Kritike
Authority Info Access	[1] Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.akshi.gov.al [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://certs.akshi.gov.al/ca.crt	Jo
Basic Constraints	Subject type=CA Path Length Constraint=None	Po
Key Usage	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)	Po
Authority Key Identifier	KeyID= eb1ed6948abdf0de2c812f9753b99b216b345db3	Jo
Subject Key Identifier	8726a8fbdb2b519b39d098d6f4c63356475cd805	Jo
Certificate Policies	[1] Certificate Policy: Policy Identifier= 1.3.6.1.4.1.39148.10.1.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.akshi.gov.al/repository	Jo
CRL Distribution Points	CRL Distribution Point: Distribution Point Name: Full Name: URL = http://crl.akshi.gov.al/ca.crl URL = ldap://ldap.akshi.gov.al/OU=NAIS Certification Authority,O=NAIS,C=AL?certificateRevocationList;binary	Jo

Fushat shtesë për certifikatën **NAIS Class 4 CA** paraqiten më poshtë.

Fusha shtesë	Vlera	Kritike
Authority Info Access	[1] Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.akshi.gov.al [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://certs.akshi.gov.al/ca.crt	Jo
Basic Constraints	Subject type=CA Path Length Constraint=None	Po
Key Usage	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)	Po
Authority Key Identifier	KeyID= eb1ed6948abdf0de2c812f9753b99b216b345db3	Jo
Subject Key Identifier	947b502134c449dc19d29807e9b0d9f8ae777508	Jo
Certificate Policies	[1] Certificate Policy: Policy Identifier= 1.3.6.1.4.1.39148.10.1.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.akshi.gov.al/repository	Jo
CRL Distribution Points	CRL Distribution Point: Distribution Point Name: Full Name: URL = http://crl.akshi.gov.al/ca.crl URL = ldap://ldap.akshi.gov.al/OU=NAIS Certification Authority,O=NAIS,C=AL?certificateRevocationList;binary	Jo

7.1.3 OID e algoritmave

Algoritmat me numër identifikimi OID për të gjitha certifikatat të lëshuara nga NAIS CAs paraqiten më poshtë:

Algoritmi	OID
sha256WithRSAEncryption	1.2.840.113549.1.1.11
rsaEncryption	1.2.840.113549.1.1.1

7.1.4 Format e emrave

Referojuni seksionit 3.1.

7.1.5 Fusha 'Name constraints'

Fusha shtesë *Name Constraints* nuk përdoret.

7.1.6 OID për politikën e certifikatës

Tabela më poshtë përmbledh emrat e certifikatës dhe OID përkatëse.

Emri i Certifikatës	Lëshuar nga	OID
- Certifikatë për nënshkrimin elektronik për subjektet private - Certifikatë për nënshkrim elektronik për punonjësit qeveritar - Certifikatë për nënshkrim elektronik për punonjësit qeveritar për infrastrukturën kritike - Certifikatë për vulën elektronike	NAIS Class 1 CA	1.3.6.1.4.1.39148.10.1.1.1
- Certifikatë për nënshkrim elektronik për subjektet private për infrastukturën kritike	NAIS Class 2 CA	1.3.6.1.4.1.39148.10.1.1.2
- Certifikatë për projektin e fiskalizimit për institucionet publike - Certifikatë për projektin e fiskalizimit për subjektet private - Certifikatë Test për projektin e fiskalizimit	NAIS Class 3 CA	1.3.6.1.4.1.39148.10.1.1.3
- Certifikatë për autentifikim për Platformën e Nënshkrimit Elektronik	NAIS Class 4 CA	1.3.6.1.4.1.39148.10.1.1.4

7.1.7 Përdorimi i fushës shtesë 'Policy Constraints'

Fusha shtesë *Policy Constraints* nuk përdoret.

7.1.8 Semantika dhe sintaksa e 'Policy qualifiers'

'Policy qualifiers' në fushën shtesë *Certificate Policies* përmbajnë një tregues në formatin URI me adresën e faqes në web të direktorisë.

7.1.9 Semantika e procesimit për fushën kritike shtesë 'Certificate Policies'

Asnjë përcaktim.

7.2 Profili CRL

Profili CRL për **NAIS CA** përshkruhet në tabelën më poshtë:

Emri i fushës	Vlera	
Version	V2	
Signature Algorithm	sha256WithRSAEncryption	
Issuer	Organizational Unit (OU)	NAIS Certification Authority
	Organization Name (O)	NAIS
	Country (C)	AL
Effective date	Date of CRL issuance	
Next update	Date of next expected CRL update	
Revoked certificates	List of revoked certificates	

Profili CRL për **NAIS Class 1 CA** përshkruhet në tabelën më poshtë:

Emri i fushës	Vlera	
Version	V2	
Signature Algorithm	sha256WithRSAEncryption	
Issuer	Organizational Unit (OU)	NAIS Class 1 Certification Authority
	Organization Name (O)	NAIS
	Country (C)	AL
Effective date	Date of CRL issuance	
Next update	Date of next expected CRL update	
Revoked certificates	List of revoked certificates	

Profili CRL për **NAIS Class 2 CA** përshkruhet në tabelën më poshtë:

Emri i fushës	Vlera	
Version	V2	
Signature Algorithm	sha256WithRSAEncryption	
Issuer	Organizational Unit (OU)	NAIS Class 2 Certification Authority
	Organization Name (O)	NAIS
	Country (C)	AL
Effective date	Date of CRL issuance	
Next update	Date of next expected CRL update	
Revoked certificates	List of revoked certificates	

Profili CRL për **NAIS Class 3 CA** përshkruhet në tabelën më poshtë:

Emri i fushës	Vlera	
Version	V2	
Signature Algorithm	sha256WithRSAEncryption	
Issuer	Organizational Unit (OU)	NAIS Class 3 Certification Authority
	Organization Name (O)	NAIS
	Country (C)	AL
Effective date	Date of CRL issuance	
Next update	Date of next expected CRL update	
Revoked certificates	List of revoked certificates	

Profili CRL për **NAIS Class 4 CA** përshkruhet në tabelën më poshtë:

Emri i fushës	Vlera	
Version	V2	
Signature Algorithm	sha256WithRSAEncryption	
Issuer	Organizational Unit (OU)	NAIS Class 4 Certification Authority
	Organization Name (O)	NAIS
	Country (C)	AL
Effective date	Date of CRL issuance	
Next update	Date of next expected CRL update	
Revoked certificates	List of revoked certificates	

7.2.1 Versionet

Të gjitha CRL-të e lëshuara nga AKSHI janë në versionin X.509 Version 2.

7.2.2 CRL-të dhe fushat shtesë të CRL-ve

Fushat shtesë të CRL për **NAIS CAs** përshkruhen në tabelën më poshtë:

Emri i fushës	Kritike
Authority Key Identifier	Jo
CRL Number	Jo

7.3 Profili OCSP

OCSP (Online Certificate Status Protocol) përdoret për të kontrolluar statusin e revokimit të një certifikate dixhitale X.509.

Informacioni rreth statusit të certifikatës përfshihet në fushën *certStatus*. Mund të kthejë një nga vlerat e mëposhtme:

- "good" që tregon një përgjigje pozitive ndaj kërkesës për statusin e certifikatës. Minimalisht, kjo përgjigje pozitive tregon se certifikata nuk është revokuar, por nuk do të thotë

domosdoshmërisht se certifikata është lëshuar ndonjëherë ose se koha në të cilën është prodhuar përgjigja është brenda intervalit të vlefshmërisë së certifikatës.
- "revoked" tregon se certifikata është revokuar.
- "unknown" tregon se nuk ka informacion rreth certifikatës që kërkohet.

Ky shërbim zbatohet në përputhje me RFC 2560.

7.3.1 Versioni

Serveri OCSP lëshon konfirmime të statusit të certifikatës në përputhje me RFC 2560. Numri i verisonit është V1.

7.3.2 Fushat shtesë të OCSP

Serveri OCSP pranon prapashtesën *Nonce*.

8. AUDITIMI I PAJTUESHMËRISË DHE VLERËSIMET E TJERA

Si Ofrues i Kualifikuar i Shërbimeve të Besuara në Shqipëri, në bazë të ligjit nr. 107/2015, datë 1.1.2015 "Për identifikimin elektronik dhe shërbimet e besuara", i ndryshuar, AKSHI është i detyruar të përmbushë kërkesat e parashikuara në këtë ligj.

AKSHI i nënshtrohet vlerësimit periodik të konformitetit të shërbimeve të çertifikimit ndaj kritereve të Rregullores 910/2014, akteve zbatuese të saj dhe standardeve përkatëse ETSI.

AKSHI ka implementuar gjithashtu një sistem të integruar menaxhimi në përputhje me kërkesat e standardeve ISO 27001, ISO 9001 dhe ISO 20000-1, i cili vlerësohet nëpërmjet auditimeve të përputhshmërisë gjatë gjithë ciklit të certifikimit.

8.1 Frekuenca ose rrethanat e vlerësimit

Frekuenca dhe rrethanat përcaktohen nga lloji i vlerësimit, kërkesat e standardeve të industrisë dhe ligjet kombëtare në fuqi.

Auditimet e brendshme të pajtueshmërisë kryhen nga strukturat përkatëse në AKSHI për të verifikuar përputhshmërinë me politikat, procedurat dhe praktikat e brendshme si dhe me legjislacionin kombëtar, standardet ndërkombëtare dhe të industrisë. Në disa raste, AKSHI mund të vendosë të caktojë një organizatë ose organ të jashtëm për të kryer funksionet e auditimit të brendshëm.

8.2 Identiteti/kualifikimet e vlerësuesit

Në varësi të standardit ose rregullores, auditimet e jashtme të pajtueshmërisë kryhen nga një Organ i akredituar i Vlerësimit të Konformitetit.

Auditimet e brendshme të pajtueshmërisë kryhen nga ekspertë që njohin fushën e standardeve dhe legjislacionin e PKI, si dhe standardet ISO dhe ETSI në lidhje me shërbimet e besuara.

8.3 Marrëdhënia e vlerësuesit me subjektin që vlerësohet

Për të garantuar besueshmërinë, objektivitetin dhe paanshmërinë, auditimet e jashtme kryhen nga një Organ i pavarur i Vlerësimit të Konformitetit, i cili nuk është i lidhur drejtpërdrejt ose tërthorazi me AKSHI-n. Gjatë kryerjes së auditimeve të brendshme, personeli nuk do të auditojë fushat e tyre të përgjegjësisë.

8.4 Temat e mbuluara nga vlerësimi

Në varësi të fushëveprimit të secilit vlerësim, mund të mbulohen temat e mëposhtme:

- Politikat dhe praktikat e shërbimeve të besuara
- Siguria fizike dhe e ambientit
- Menaxhimi i sigurisë së informacionit
- Organizimi, proceset dhe procedurat e brendshme
- Pajtueshmëria me standardet ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2, ETSI EN 319 412-1, ETSI EN 319 412-2, ETSI EN 319 412-3, ETSI EN 319 412-5
- Tema të tjera mund të jenë pjesë e fushëveprimit të secilit vlerësim individual

8.5 Veprimet e ndërmarra si rezultat i mangësive

Nëse gjatë auditimeve të brendshme dhe të jashtme janë konstatuar mospërputhje, AKSHI do të ndërmarrë hapat e nevojshëm për eliminimin e mangësive të konstatuara. AKSHI do të implementojë një plan veprimi për korrigjimin e mangësive dhe një afat kohor për zgjidhjen e jo-konformiteteve. Rezultatet e zgjidhjeve do t'i komunikohen drejtuesve të lartë.

8.6 Komunikimi i rezultateve

Rezultatet e auditimit të brendshëm që përmbajnë informacion konfidencial do të komunikohen brenda AKSHI-t, vetëm me personelin e autorizuar.

Organi i vlerësimit të konformitetit do t'ia komunikojë rezultatin e auditimit drejtuesve të AKSHI-t. Këto raporte do t'i vihen në dispozicion organit mbikëqyrës.

Për shkak të ndjeshmërisë së informacionit, raportet e pajtueshmërisë nuk do të jenë të disponueshme publikisht në internet.

9. ÇËSHTJE TË TJERA DHE ÇËSHJE JURIDIKE

9.1 Tarifat

Tarifat për shërbimet e PKI përshkruhen në Vendimin e Këshillit të Ministrave nr. 35, datë 22.1.2020 "Për miratimin e tarifave për shërbimet elektronike të Agjencisë Kombëtare të Shoqërisë së Informacionit". Ky dokument është publikuar në faqen e AKSHI-T nën 'legjislacionin' akshi.gov.al/legjislacion.

9.1.1 Tarifat për lëshimin ose rinovimin e certifikatës

AKSHI aplikon tarifa për lëshimin dhe rinovimin e certifikatës për pajtimtarët, në përputhje me Vendimin e Këshillit të Ministrave.

9.1.2 Tarifat e aksesit të certifikatës

Nuk aplikohet asnjë tarifë për aksesin e certifikatës.

9.1.3 Tarifat e revokimit ose aksesit të statusit të informacionit

Nuk aplikohet asnjë tarifë për revokimin ose aksesin në informacionin e statusit të certifikatës.

9.1.4 Tarifat për shërbime të tjera

Tarifat e shërbimeve të tjera përshkruhen në Vendimin e Këshillit të Ministrave të publikuar në faqen e AKSHI-t.

9.1.5 Politika e rimbursimit

AKSHI nuk zbaton një politikë rimbursimi.

9.2 Përgjegjësia financiare

9.2.1 Siguracionet

AKSHI ka burime të mjaftueshme financiare dhe mban siguracione për mbulimin e detyrimeve ndaj pjesëmarrësve të tjerë.

9.2.2 Asetet e tjera

Asnjë përcaktim.

9.2.3 Sigurimi ose mbulimi i garancisë për subjektet fundore

Referojuni seksionit 9.2.1.

9.3 Konfidencialiteti i informacionit

9.3.1 Fushëveprimi i informacionit konfidencial

Informacioni konfidencial përfshin të gjithë informacionin në lidhje me ofrimin e shërbimeve të certifikimit që nuk vihen në dispozicion publikisht në direktori (referojuni seksionit 2.1) nga AKSHI.

Informacioni konfidencial përfshin:

- Çelësat privatë dhe të dhënat e aktivizimit të përdorura për të aksesuar çelësat privatë.
- Informacioni i mbajtur nga AKSHI si informacion privat i cili përshkruhet në seksionin 9.4.
- Procedurat e brendshme, manualet dhe dokumentet e tjera të përdorura nga rolet e besuara në kryerjen e detyrave të tyre.
- Infrastruktura PKI, topologjia e rrjetit, softuerët dhe informacion rreth harduerëve.
- Regjistrat dhe të dhënat e auditimit.
- Çdo informacion tjetër që mund të rrezikojë sigurinë e infrastrukturës së çelësit publik të implementuar tek AKSHI si dhe shërbimet e certifikimit.

9.3.2 Informacioni që nuk është brenda fushës së informacionit konfidencial

Informacioni që nuk klasifikohet si konfidencial konsiderohet informacion publik. Informacioni që AKSHI publikon në direktori (përshkruar në seksionin 2.1), duke përfshirë certifikatat e publikuara dhe të dhënat e revokimit, konsiderohet informacion publik.

9.3.3 Përgjegjësia për të mbrojtur informacionin konfidencial

Punonjësit e AKSHI-t janë përgjegjës dhe u kërkohet të mbrojnë konfidencialitetin e informacionit gjatë dhe pas përfundimit të punës. Organizatat e jashtme janë të detyruara kontraktualisht të ruajnë konfidencialitetin e informacionit të AKSHI-t.

9.4 Privatësia e informacionit personal

9.4.1 Plani i privatësisë

Gjatë procesit të regjistrimit, AKSHI mbledh informacion për pajtimtarët me qëllim ofrimin e shërbimeve të certifikimit. Të dhënat personale të pajtimtarëve trajtohen në përputhje me ligjin nr. 9887, datë 10.3.2008 “Për mbrojtjen e të dhënave personale”, i ndryshuar.

9.4.2 Informacioni i trajtuar si privat

Informacioni personal i pajtimtarit që dorëzohet gjatë procesit të regjistrimit dhe që nuk është i disponueshëm publikisht në përmbajtjen e një certifikate ose CRL trajtohet si informacion privat.

9.4.3 Informacioni që nuk konsiderohet privat

Certifikatat, CRL-të ose përmbajtja e tyre nuk konsiderohen si informacion privat.

9.4.4 Përgjegjësia për të mbrojtur informacionin privat

AKSHI është përgjegjës për mbrojtjen e informacionit privat të pajtimtarëve dhe trajtimin e të dhënave personale në përputhje me legjislacionin në fuqi siç përshkruhet në seksionin 9.4.1.

9.4.5 Njoftimi dhe pëlqimi për përdorimin e informacionit privat

Njoftimi për përdorimin e informacionit privat u jepet pajtimtarëve gjatë procesit të aplikimit. Me nënshkrimin e deklaratës për termat dhe kushtet e certifikatës, pajtimtarët japin pëlqimin për mbledhjen e informacionit privat për qëllimin e ofrimit të shërbimeve të certifikimit.

9.4.6 Vënia në dispozicion e të dhënave për procese gjyqësore ose administrative

AKSHI nuk vë në dispozicion të dhënat e përmendura në seksionin 9.4.2, me përjashtim të rasteve të kërkuara nga ligji ose organet kompetente administrative ose qeveritare.

9.4.7 Rrethana të tjera të vënies në dispozicion të informacionit

Asnjë përcaktim.

9.5 Të drejtat e pronësisë intelektuale

AKSHI zotëron të drejtat e pronësisë intelektuale të aplikacioneve të zhvilluara në emër të AKSHI-t, si Platforma e Nënshkrimit Elektronik. AKSHI nuk zotëron të drejtat e pronësisë intelektuale të softuerit të përdorur në PKI-në e AKSHI-t i cili është në pronësi të palëve të treta. Dokumentacioni dhe politikat e publikuara në akshi.gov.al janë në pronësi të AKSHI-t.

9.6 Përfaqësimet dhe garancitë

9.6.1 Përfaqësimet dhe garancitë e CA-së

Përfaqësimet dhe garancitë e AKSHI-t si Ofrues i Shërbimeve të Besuara janë si më poshtë:

- Pajtueshmëria me këtë CP/CPS si dhe me politikat dhe procedurat e brendshme të AKSHI-t.
- Lëshimi i certifikatave në mënyrë të sigurt, bazuar në identitetin e personit fizik ose juridik.
- Lëshimi i certifikatave në përputhje me profilet e certifikatave të përcaktuara në seksionin 7.1 dhe sipas llojit të certifikatës të dhënë gjatë aplikimit për certifikatë.
- Vepron në përputhje me ligjet dhe rregulloret përkatëse.

9.6.2 Përfaqësimet dhe garancitë e RA

Përfaqësimet dhe garancitë e funksionit të RA pranë AKSHI-t janë si më poshtë:

- Pajtueshmëria me këtë CP/CPS si dhe me politikat dhe procedurat e brendshme të AKSHI.
- Kryerja e procedurave të regjistrimit dhe identifikimit duke ndjekur procesin e përshkruar në këtë CP/CPS.

9.6.3 Përfaqësimet dhe garancitë e pajtimtarëve

Pajtimtari:

- Është përgjegjës për dhënien e informacionit të saktë gjatë procesit të regjistrimit.
- Lexon dhe pranon termat dhe kushtet e certifikatës.
- Merr masat e duhura për të mbrojtur pajisjen e tyre të sigurt kriptografike, çelësin privat dhe të dhënat e aktivizimit.
- Kërkon revokimin e certifikatës në rast të kompromentimit të çelësit privat.
- Përdor certifikatën në përputhje me rregullat e përcaktuara në seksionin 1.4.

9.6.4 Përfaqësimet dhe garancitë e palëve të përfshira

Palët e përfshira janë përgjegjëse për:

- Kryerjen e funksioneve operacionale të çelësit publik si një parakusht për t'u mbështetur në një certifikatë.

- Validimin e një certifikate duke përdorur CRL-të ose shërbimet e validimit të certifikatës.
- Nuk mbështetet në një certifikatë nëse ajo është revokuar ose kur ajo ka skaduar.

9.6.5 Përfaqësimet dhe garancitë e pjesëmarrësve të tjerë

Asnjë përcaktim.

9.7 Mohimet e garancive

AKSHI nuk është përgjegjës për dëmtimin, përfshirë dëmin indirekt, si dhe për çdo humbje fitimi, humbje të të dhënave apo dëme të tjera indirekte në rastet kur ky dëm shkaktohet:

- Për shkak të përdorimit të paautorizuar të çelësave dhe certifikatave të përdoruesit,
- Për përdorime të certifikatës që nuk lejohen nga ky dokument,
- Për përdorime në mënyrë mashtruese ose të pakujdesshme të certifikatës, shërbimit CRL ose OCSP,
- Si rezultat i informacionit të pasaktë ose jo të plotë të dorëzuar gjatë procesit të aplikimit.

9.8 Kufizimet e përgjegjësisë

Përgjegjësia ligjore është përcaktuar në ligjin nr.9880, datë 25.2.2008 “Për nënshkrimin elektronik”, i ndryshuar dhe ligjin nr. 107/2015 “Për identifikimin elektronik dhe shërbimet e besuara” i ndryshuar.

Përgjegjësia është e kufizuar në dëmet e vërtetuara ligjërisht. AKSHI nuk është përgjegjës për:

- Përgjegjësi që lidhen me mashtrimin ose sjelljen e pahijshme të Pajtimtarit.
- Përgjegjësi që lidhen me përdorimin e certifikatave përtej kufizimeve të përcaktuara në këtë CP/CPS.
- Përgjegjësi që lidhen me kompromet imin e çelësit privat të një Pajtimtari.

9.9 Dëmshpërblimet

Çdo pjesëmarrës është përgjegjës ndaj palës së dëmtuar për dëmet e shkaktuara nga moszbatimi i dispozitave të kësaj CP/CPS-je.

9.10 Afati dhe përfundimi

9.10.1 Afati

Afati i kësaj CP/CPS-je fillon me publikimin në Direktori dhe mbetet në fuqi derisa të zëvendësohet nga një CP/CPS e re.

9.10.2 Përfundimi

CP/CPS do të mbetet në fuqi derisa të zëvendësohet nga një version i ri.

9.10.3 Efekti i përfundimit dhe qëndrueshmërisë

Kur një CP/CPS e re publikohet në Direktori, dispozitat e CP/CPS zbatohen për të gjitha certifikatat e reja që lëshohen. Megjithatë, të gjitha marrëveshjet aktuale mbeten në fuqi derisa certifikata të revokohet ose të skadojë.

9.11 Njoftimet dhe komunikimet individuale me pjesëmarrësit

Komunikimi individual me pjesëmarrësit realizohet nëpërmjet adresës zyrtare të emailit: pki@akshi.gov.al.

9.12 Ndryshimet

9.12.1 Procedura për ndryshim

Kjo CP/CPS do të ndryshohet në rastet kur është e nevojshme. Pasi Sektori i PKI të ketë bërë ndryshimet e nevojshme, drejtuesit e lartë të AKSHI-t aprovojnë ndryshimet në mënyrë formale.

9.12.2 Mekanizmi dhe periudha e njoftimit

Të gjitha ndryshimet e bëra në këtë CP/CPS do të regjistrohen në tabelën e historisë së versionit. CP/CPS e përditësuar do të vihet në dispozicion në Direktori pas miratimit formal nga drejtuesit e lartë të AKSHI-t.

9.12.3 Rrethanat në të cilat OID duhet të ndryshohet

Ndryshimet e mëdha në politikën e certifikatës ose deklaratën e praktikës së certifikimit mund të kërkojnë një ndryshim në treguesin CP OID ose CPS. Sektori i PKI së bashku me drejtuesit e lartë të AKSHI-t do të përcaktojnë nëse OID do të duhet të ndryshohet.

9.13 Dispozitat për zgjidhjen e mosmarrëveshjeve

Në rast mosmarrëveshjeje, palët e përfshira inkurajohen ta zgjidhin mosmarrëveshjen në mënyrë miqësore. Nëse kjo nuk është e mundur, mosmarrëveshjet mund të zgjidhen nga gjykata kompetente në Shqipëri.

9.14 Ligji në fuqi

AKSHI si Ofrues i Shërbimeve të Besuara ndjek të gjitha ligjet dhe rregulloret në fuqi në Republikën e Shqipërisë.

9.15 Pajtueshmëria me ligjet në fuqi

Kjo CP/CPS është në përputhje me legjislacionin shqiptar dhe ligje përkatëse.

9.16 Dispozita të ndryshme

9.16.1 Marrëveshja e plotë

Asnjë përcaktim.

9.16.2 Detyra

Asnjë përcaktim.

9.16.3 Ndarshmëria

Asnjë përcaktim.

9.16.4 Përmbarimi (tarifat e avokatëve dhe heqja dorë nga të drejtat)

Asnjë përcaktim.

9.16.5 Forca madhore

Asnjë përcaktim.

9.17 Dispozita të tjera

Asnjë përcaktim.