Certification Practice Statement

Version 1.0

Përmbajtja

1. HYRJE

Infrastruktura për menaxhimin e çelësave kriptografike të AKSHI (Agjencia Kombëtare për Shoqërinë e Informacionit) ka për qëllim të ofrojë zgjidhje (produkte dhe shërbime) për sigurinë e rrjeteve kompjuterike. Një pjese e kësaj infrastrukture është Infrastruktura me çelës publik - PKI.
PKI përbëhet nga produktet dhe shërbimet që ofrojnë dhe menaxhojnë certifikata dixhitale X.509 për enkriptim me çelës publik. Certifikatat identifikojnë një person ose pajisje të specifikuar në certifikatë dhe bashkëngjit këtë subjekt (entitet) me një çift të caktuar çelësash publik/privat.

Ky dokument paraqet *Certification Practice Statement* **Deklaratën e Praktikave te Certifikimit.**

Sistemet informative dhe aplikacionet që mbështetësin shërbimet dhe aktivitetet e AKSHI kërkojnë mekanizmat e mëposhtme të sigurisë:

- Autentifikim
- Autorizim
- Integritet
- Konfidencialitet
- mos-refuzim

Këto shërbime gjenden në shumicën e komponentëve të sigurisë të rrjetit të tilla si Workstations, pajisje si firewalls, routers, Web server, server data baze dhe server aplikimi. Veprimtaria e këtyre komponentëve është e siguruar dhe plotësuar duke përdorur kriptimin me çelës publik.

Shërbimet e sigurisë IT të ofruara nga PKI përfshijnë:
• Gjenerimin / magazinimin / rikuperimin e çelësave kriptografike,
• Krijimin, përditësimin, rinovimin dhe shpërndarjen e certifikatave,
• Gjenerimin dhe shpërndarjen e listave te revokimit te certifikatave (CRL)
• Menaxhimin e drejtorive të cilat publikojë materiale që lidhen me certifikatat,
• Përditësimin, rinovimin dhe ndryshimin e çelësit te një certifikate,
• Inicializimin/caktimin/menaxhimin e pajisjeve (tokens) që përmbajnë certifikatat
• Funksionet e sistemit të menaxhimit (P.sh. të auditimit të sigurisë, menaxhimin e konfigurimit, arkivimit, etj.)

Siguria e zgjidhjeve bazuar në çelës publik, ne zgjidhjen e sigurisë se IT është një rezultat i drejtpërdrejtë i funksionimit të sigurt dhe të besueshëm të PKI, duke përfshirë vendet, pajisjet, personelin dhe procedurat.

1.1 Të përgjithshme

Një Politike Certifikate është një grup rregullash i cili tregon fushat e përdorimit te një certifikate për një kategori të veçantë dhe/ose kategoritë e aplikimeve me kërkesat e caktuara të sigurisë. Politika e Certifikimit rregullon përdorimin e certifikatave në strukturat e ndryshme qe menaxhohen nga AKSHI, ajo përfaqëson një politikë të unifikuar për të gjithë veprimtarinë e CA(ofruesit te shërbimit) te AKSHI. CPS e AKSHI nuk përcakton një implementim të veçantë të një PKI as politikën e certifikimit për CA qe menaxhohen nga subjekte të jashtme, në emër të AKSHI.

Ky dokument përcakton krijimin dhe menaxhimin e certifikatave me çelës publik *X.509 Version 3* për përdorim në aplikimet që kërkojnë komunikimin midis sistemeve të bazuar në kompjuterët e lidhur ne rrjet. Aplikacionet e tilla përfshijnë, por nuk kufizohen vetëm në:

• e-mail,
• Transmetimi i informacionit të paklasifikuar,
• nënshkrimi i formave elektronike,
• nënshkrimin e dokumenteve elektronike dhe kontratave, dhe,
• autentifikimi i komponentëve të infrastrukturës të tilla si Web serverët, firewalls, routers dhe direktorite.

Llojet e rrjeteve të sigurisë për këto produkte janë:

• Rrjeti i pambrojtur (siç është Interneti)
• Rrjeti i brendshëm i AKSHI (Intranet AKSHI)
• Rrjeti i mbrojtur i AKSHI-t.

1.2 Identifikimi

Ka katër nivelet e besimit në këtë politikë, të përcaktuara në kapitujt në vijim. Çdo nivel i besimit është objekt identifikues (OID) për tu hedhur në të certifikatat e lëshuara nga CA.
OID janë të regjistruar si:

Id- NAIS-class1	ID :: = { 1.3.6.1.4.1.39148.10.1.1.1 }
id- NAIS -class2	ID :: = { 1.3.6.1.4.1.39148.10.1.1.2 }
id- NAIS -class3	ID :: = { 1.3.6.1.4.1.39148.10.1.1.3 }
id- NAIS -class4	ID :: = { 1.3.6.1.4.1.39148.10.1.1.4 }

1.3 Pjesëmarrësit në PKI

Paragrafët e mëposhtme tregojnë rolet të përfshirë në leshimin dhe ruajtjen e certifikatave dhe menaxhimin e PKI.

1.3.1 Autoritetet e PKI

1. Autoriteti i Certifikimit – CA është një entitet për:
   - krijimin,
   - nënshkrimin dhe
   - lëshimin

e certifikatave me çelës publik.

CA është përgjegjës për të gjitha aspektet e publikimit dhe menaxhimit te një certifikate, duke përfshirë kontrollin e:
   - Procesit te regjistrimit,
   - Identifikimit dhe procesit te vërtetimit,
   - Procesit te lëshimit te certifikatës,
   - Publikimit te certifikatës
   - Revokimit te certifikatave dhe
   - Ndryshimit te certifikatave me çelës publik,

për të siguruar që të gjitha aspektet e shërbimeve , veprimeve , si dhe infrastrukturën në lidhje me certifikatat e lëshuara sipas kësaj Politike janë në përputhje me kërkesat, përfaqësime dhe garanci e kësaj politike.
PKI i AKSHI është hierarkike. CA-ja duhet të jetë në vartësi të një Root-CA dhe maksimale dy të ndërmjetme CA. Nënshtrimi është përshkruar në CPS te krijuara për këtë hierarki dhe zbatohet duke përdorur procedurat dhe shtesën e certifikatës. CA e cila ka ne varësi një CA te dytë është quajtur "CA superiore".

2. Autoriteti i Regjistrimit – RA është entiteti i cili bashkëpunon me një CA për të marrë dhe verifikuar identitetin e Abonentëve (aplikuesit) dhe informacion që do të futen në certifikata me çelës publik. RA duhet të kryejë funksionet e veta në përputhje me CPS.

Te dyja CA dhe RA janë Autoriteti i Menaxhimit te Certifikatave-CMA. Termi RA përfshin subjekte të tilla si Autoritete Regjistrimi Lokale (LRA).

1.3.2 Subjektet fundor

1. Abonent (Aplikantët)

Abonent është entiteti emri i të cilit paraqitet si një subjekt në një certifikatë dhe pretendon për të përdorur çelësin e vet në përputhje me këtë politikë. Abonentët e AKSHI janë të ndarë në 3 kategori kryesore:

- Stafi i brendshëm: punonjesit i AKSHI;
- Stafi i jashtëm: punonjësit e institucioneve te administratës publike, punonjësit e organizmave te trete te kontraktuar nga institucionet;
- Komponentë te Infrastrukturës: workstations, firewalls, routers, pajisjet VPN, servera të besueshme (p.sh. web serverat, ftp, bazat e të dhënave, aplikacionet, proxy, e-mail) e rrjeteve te AKSHI. Këto komponentë duhet të operohet nga personat e autorizuar të cilët pranojnë certifikatën dhe janë përgjegjës për mbrojtjen dhe përdorimin e çelësit privat te lidhur me to.

Termi Abonent i përdorur në këtë dokument i referohet vetëm atyre që kërkojnë certifikata për përdorimin, përveç nënshkrimit dhe shpërndarjes se certifikatave. Prandaj CA te cilët kërkojnë certifikata nga CA superior nuk konsiderohen Abonent.

2. Marresi

Marresi duke përdorur shërbimet e AKSHI, mund të jetë çdo entitet (person) që merr vendime bazuar në saktësinë e lidhjes midis identitetit të Abonentit dhe çelësit publik (lidhje konfirmuar nga njëri prej Autoriteteve te Certifikimit ne varësi të Root CA).
Marresi është përgjegjës për mënyrën se si kontrollon statusin aktual të një certifikatë te nje abonenti per te vlerësuar pranimin ose jo te saj.
Marresi duhet të përdor informacionin në një certifikate (për shembull, identifikuesit dhe kualifikuesit e politikës se certifikimit) për të vendosur nëse certifikata është përdorur sipas qëllimit të deklaruar.

1.4 Përdorimi i Certifikatave

PKI i AKSHI duhet të mbështesë pesë shërbime themelore ndaj/per abonenteve:
kontrolli i aksesit,
konfidencialiteti,
integriteti,
autenticiteti
mos-refuzimi.

PKI mbështet këto shërbimeve nga nënshkrimet elektronike, vulat elektronike dhe mekanizmat e enkriptimit. Ne varësi te proceseve dhe procedurave ligjore e juridike

ku perdoret nënshkrimi elektronik apo vula elektronike mund te jete e nevojshme dhe përdorimi i vulës kohore te nënshkrimit. Psh ne rastet kur duhet te nënshkruhet një kontratë apo dokument elektronik, eshte e nevojshme te verifikohet firma per periudhën kohore.

1.5 Vlera e informacionit

Informacioni mund të klasifikohet në përputhje me qëllimet dhe objektivat kryesore të lidhura me aktivitetet e AKSHI. Klasifikimi merr parasysh përparësinë e informacionit sekret (p.sh. sekret ose te ndjeshme), mprehtësinë e tij (p.sh. Vlerësim kategorie siç është përcaktuar nga dokumentet e AKSHI) ose vlera monetare për aplikimet e përdorura. Shembuj të vlerave të informacionit janë:

- informacion me vlerë të vogël (p.sh. të dhënat administrative)
- Informacioni vlera mesatare (p.sh. të dhënat për aktivitetet mbështetëse, të dhënat që mbrojnë transaksione të vogla dhe të mesme financiare - furnizime zyre, libra, pagat, etj.)
- Informacioni me vlere te larte (p.sh. të dhënat për aktivitete kritike, transaksionet financiare me vlerë të lartë).

1.6 Niveli i mbrojtjes për informacion

Rrjetet e të dhënave të AKSHI që do përdorin certifikatat e përshkruara në këtë politikë do të kenë nivele të ndryshme të mbrojtjes. Mekanizmat që sigurojnë mbrojtjen e rrjetit përfshijnë enkriptim te rrjetit, izolim fizik, sigurim te nivelit te larte (HAG) dhe firewalls. Këto mekanizma janë përdorur për të krijuar një koleksion të rrjeteve te mbyllur dhe me nivele te ndryshme.

OSHC do të përdore nivele të ndryshme të mbrojtjes për rrjetin:
• Mjediset informatike te mbrojtura ne nivel te larte , të cilat janë të mbrojtura me anë të pajisjeve te enkriptimit të miratuara që mbrojnë të dhënat sensitive edhe përmes izolimit fizik.
• Mjediset informatike te mbrojtura ne nivel te mesëm,te paklasifikuara fizikisht te izoluar dhe te pa enkriptuara me akses baze të kufizuar ose të rrjetit të mbrojtura nga enkriptimi.
• Mjediset informatike te pambrojtur (rrjete te hapura, Internet).

1.7 Përcaktimi i niveleve te sigurisë ne certifikata

Çdo certifikatë e lëshuar per nënshkrim elektrnik ose vule elektronike do të ketë një kod identifikimi i cili është formuar duke lidhur kodin identifikues te CA dhe numrin e serisë së certifikatës.

Niveli i sigurisë lidhur me një certifikatë me çelësa publik është një deklaratë e CA ne lidhje me shkallën e besimit që një palë e tretë mund të ketë në çelësin publik te Abonentit dhe identitetin dhe privilegjet e shënuara në certifikatë. Niveli i sigurisë varet nga regjistrimi i saktë i Abonentit dhe menaxhimin dhe gjenerimin të certifikatës se tij te lidhur me çelësin privat, sipas përcaktimeve të kësaj politike. Kontrolli mbi personelin, mjedisi fizik, procedurat dhe siguria teknike kontribuon në sigurinë e certifikatave të lëshuara nga një sistem i menaxhimit certifikatave.

PKI i AKSHI do të nxjerrë për mbrojtjen e informacionit të transmetuar në rrjetet kompjuterike publike ose private, klasifikuar apo jo, këto lloje të certifikatave dixhitale:
1. Certifikatat personale - e përdorur nga stafi/njësite brenda AKSHI për autentifikim në mënyrë për të aksesuar burime të ndryshme informative, për nënshkrimin elektronik të informacionit (dokumente, e-mail), per gjenerimin e vulës elektronike, për enkriptim me çelësa simetrike.
2. Certifikatat per pajisjeje - përdoret për trafik IPsec (VPN) dhe shkëmbimin e të dhënave në protokollet e Web.

Ka tre lloje të certifikatave personale të lëshuara për individë apo organizata:

1. Certifikatat për nënshkrimet elektronike të rekomanduara për:
• Shërbimet e nënshkrimit elektronik në aplikimet me postë elektronike;
• Shërbimet e nënshkrimit elektronik në aplikimet administrative dhe menaxhimin e dokumentit elektronik;
• Vërtetimi i klientëve nga një Web server;
• Autentifikimi për kontrollin e aksesit te shërbimeve mbështetëse të rrjeteve dhe aplikacioneve;
• Konfirmim pranimi dhe mos-refuzim shërbimesh për menaxhimin e dokumentit, transaksioneve financiare dhe tregtisë elektronike (furnizuesit e zyrave, libra, automjeteve, pagat, etj).

2. Certifikatat për vulat elektronike të rekomanduara për:
• Shërbimet vulës elektronike në aplikimet administrative dhe menaxhimin e dokumentit elektronik;
• Vërtetimi i klientëve nga një Web server;
• Autentifikimi për kontrollin e aksesit të shërbimeve mbështetëse të rrjeteve dhe aplikacioneve;
• Konfirmim pranimi dhe mos-refuzim shërbimesh për menaxhimin e dokumentit, transaksioneve financiare dhe tregtisë elektronike (furnizuesit e zyrave, libra, automjeteve, pagat, etj).

3. Certifikatat për enkriptimin me çelës publik të rekomanduar për:

• Këmbimi i çelësave për sigurimin e informacionit të dërguar me anë të e-mail.
• Këmbimi i çelësave në mënyrë që të sigurojë informacionin e shkëmbyer ndërmjet Web server dhe motorit te kërkimit.
• Këmbimi i çelësave në mënyrë që të sigurojë informacionin e dërguar me anë të aplikacioneve të ndryshme;
• Këmbimi i çelësave në mënyrë që të mbrojë dhe të sigurojë dokumentet elektronike;

Për certifikatat e pajisjeve , përcaktohen këto lloje të certifikatave:

1. Certifikatat për IPSec (quajtur Certifikatat VPN)
Ky lloj i certifikatave është i destinuar për routers / porta / firewalls që zbatojnë protokollin e sigurisë IPSec, për sigurimin dhe autentifikimin në rrjetet virtuale private (VPN). Është e rekomanduar për:
• Këmbim te çelësave për sigurimin e informacionit të dërguar nëpërmjet routers / porta / firewalls që zbatojnë protokollin e sigurisë IPSec
• Autentifikimin në rrjetet virtuale private që zbatojnë protokollin e sigurisë IPSec,

2. Certifikatat për serverat Web (te quajtura Certifikata Web)
Ky lloj i certifikatave është i destinuar për servera Web që zbatojnë protokollin e sigurisë SSL, për sigurimin e autentifikimit te Serverave Web - komunikimet Klienti Web. Është e rekomanduar për:
• Këmbim te çelësave për sigurimin e informacionit të dërguar në mes serverave Web dhe klientët Web që zbatojnë protokollin e sigurisë SSL,
• Autentifikimin e serverit në Web Server - komunikimet Klienti Web

Katër nivelet e sigurisë janë të përcaktuara për të gjitha certifikatat, të shprehura nga klasat e tyre:

1. Klasa 1 Certifikatat digjitale (Non-secret/Personal)
Ky nivel është për:
• Informacion jo sekret, në të gjitha llojet e rrjeteve (publike, Intranet, AKSHI, sekret)
• Të gjitha llojet e aplikimeve
• Për personelin e brendshëm / të jashtëm.

2**. KLASA 2 Certifikatat digjitale (Konfidenciale / Personal)**
Ky nivel është për:
• Informacioni Jo-sekret, por i ndjeshëm në të gjitha llojet e rrjeteve (publike, Intranet AKSHI, të siguruara)
• Informacioni Sekret transmetohet vetëm në intranet AKSHI dhe në rrjetet e sigurta
• Të gjitha llojet e aplikimeve
• Për personelin e brendshëm / të jashtëm

3. Klasa 3 Certifikatat digjitale (Non-secret/Devices)

Ky nivel është për:

• Informacioni Jo-sekret në të gjitha llojet e rrjeteve (publike, Intranet, AKSHI, siguruar).

• Të gjitha llojet e aplikimeve

• për pajisjet

3. KLASA 4 Certifikatat digjitale (Konfidenciale / Devices)

Ky nivel është për:

• Informacioni Jo-sekret, por e ndjeshme në të gjitha llojet e rrjeteve (publike, Intranet AKSHI, të siguruara)

• Informacioni sekret transmetohet vetëm në intranet AKSHI dhe në rrjetet e sigurta

• Të gjitha llojet e aplikimeve

• Për pajisjet

1.8 Pikat e kontaktit për CPS

CPS do të vihen në dispozicion të abonentëve në adresën e internetit në vijim: http://www.akshi.gov.al/pki

2. DISPOZITA TË PËRGJITHSHME

2.1 Detyrimet e palëve

2.1.1 Detyrimet e CA

Një CA që lëshon certifikata duke miratuar politikën e përcaktuar nga ky dokument ka detyrimet e mëposhtme kryesore:

1. Te krijoje një Deklaratë te Praktikave te Certifikimit - CPS
2. Te jete ne përputhje me dispozitat e miratuara ne ketë CPS;
3. Te ketë sistemet e besueshme për gjenerimin, lëshimin dhe publikimin e certifikatave;
4. Te siguroje që informacioni i regjistrimit te aplikantëve është pranuar vetëm nga CA që e kuptojnë dhe janë të detyruar ti binden këtyre politikave;
5. Të përfshijë vetëm informacionin e vlefshëm në certifikatë dhe të mbajë një rekord të aktiviteteve të kryera për vlerësimin e informacionit qe gjendet ne certifikate;
6. Të imponojë detyrime për abonentët në përputhje me CPS dhe te informoje ata në lidhje me pasojat e mosrespektimit të këtyre detyrimeve;
7. Te revokoj certifikatat për ato abonentë të cilët kanë vepruar ne kundërshtim me këto detyrime disa here;
8. te ofroj shërbime në një directory online që kënaq kërkesat e CPS;
9. Te verifikoj nëse çelësi privat dhe publik i një Abonenti përbën një çift funksional;
10. Te verifikoj nëse pajtimtari ka çelësin privat që korrespondon me çelësin publik te certifikatës.

2.1.2 Detyrimet e RA

Një RA që kryen funksionet e regjistrimit, siç përshkruhet në këtë politikë, do të pajtohet me dispozitat e kësaj politike dhe do të jetë subjekt i CPS. Një RA që ka vepruar ne kundërshtim me këto detyrime është subjekt për revokimin e përgjegjësive RA.

CA është përgjegjës për të siguruar se certifikatat janë të krijuara dhe menaxhohen në përputhje me këtë politikë dhe se gjeneruesi i certifikatave, administratori dhe ndarja e funksioneve janë bërë vetëm nga ata që e kuptojnë dhe pajtohen me kërkesat e lidhura me politikat e certifikimit. Kërkesat e sigurisë qe imponojnë CA janë të ngjashme me ato të vendosura për RA, sepse RA është përgjegjës për informacionin e mbledhur. RA është përgjegjës për:

• Shpërndarjen e çelësave dhe / ose certifikatave tek abonentëve;

• Dërgimi i kërkesave te CA për lëshimin, pezullimin, revokimin ose rinovimin e certifikatave;
• Verifikimi paraprak i të dhënave të paraqitura nga abonentët për këto kërkesa, në përputhje me kërkesat CPS;
• Sigurimin që certifikatat (ose pajisjet kriptografike) aksesi, fjalëkalimi dhe çelësi privat që janë të shpërndarë në abonentit nuk janë kapur nga ndonjë palë e tretë.
• Transmetimit e një kopje të CP, CPS dhe një marrëveshje që do të nënshkruhet, për çdo abonent.

2.1.3 Detyrimet e Abonentit

Abonentët, të cilët mund të jene te punësuar si personel i AKSHI, personeli i institucioneve te administratës publike ose te trete qe kane kontrata me institucionet te administratës dhe qe duhet te marrin shërbimin PKI ne kuptim te atyre kontratave:

- Do të jenë të përfaqësuara saktë në të gjitha komunikimet me PKI;
- Do të mbajnë përgjithmonë çelësin e tyre privat, në përputhje me këtë politikë, siç përcaktohet në marrëveshjen e pranimit te certifikatës se tyre.
- Do te përmendin ne CA qe certifikatat e lëshuara, në kohën e duhur dhe nëpërmjet mekanizmave në përputhje me CPS nga ngjarjet e mëposhtme që mund të ndodhin gjatë periudhës së vlefshmërisë:
    - Çelësat e tyre private kanë qenë të kompromentuar, vjedhur apo humbur; Kontrolli mbi çelësat private ka qenë e prekur, duke humbur apo kompromentuar të dhënat e aktivizimit (p.sh fjalëkalimin);
    - Mungesat ose ndryshime në përmbajtjen e certifikatave të tyre
- Do të respektojë të gjitha afatet, kushtet dhe kufizimet e imponuara në përdorimin e çelësat private dhe certifikatave të lidhura me to;
- Do të përdorin certifikatat e ofruara nga AKSHI vetëm për transaksionet që lidhen me aktivitetet e AKSHI.

2.1.4 Detyrimet e Marresit

Marresit që përdorin dhe bazojnë veprimet e tyre në certifikatat e lëshuara në përputhje me një politikë të përcaktuar në këtë dokument:
• do të përdorin certifikatat për qëllimin për të cilin ato janë lëshuar, siç është specifikuar në informacionin e certifikatës
• do të verifikojë çdo certifikatë para përdorimit, bazuar në procedurat e përshkruara në standardin e X. 509, duke analizuar vlefshmërinë ose revokimin;
• do të përcaktojë nivelin e besimit për CA që ka lëshuar certifikatën nëpërmjet verifikimit te rrugës se certifikatës në përputhje me parimet e përcaktuara nga standardi X. 509, version 3;

• do të mbaj të dhënat origjinale të nënshkruara, aplikacionet e nevojshme për të lexuar dhe përpunimin e këtyre të dhënave dhe aplikacionet kriptografike të nevojshme për të verifikuar nënshkrimet digjitale e përmbajtura në këto të dhëna për sa kohë që ajo mund të jetë e nevojshme për të verifikuar nënshkrimet nga këto të dhëna.

2.2 Publikimi dhe depozita

2.2.1 Publikimi i informacionit për CA

CA do të sigurojë një directory on-line, në rrjetin e brendshëm AKSHI, në dispozicion për abonentët dhe marresit, e cila përmban:
• Certifikatat e lëshuara që korrespondojnë me këtë politikë;
• Listat revokimit të certifikatave (CRL);
• Certifikatën që korrespondon me çelësin i cili përdoret për nënshkrimin e certifikatave;
• Një kopje e Deklaratës se Praktikave te Certifikimit.

2.2.2 Frekuenca e publikimit

Certifikatat janë botuar pas pranimit të abonentëve sipas verifikimeve dhe provave qe posedojnë çelësin privat. CRL është publikuar në përputhje me specifikimet në CP. Të gjitha informatat do të publikohen menjëherë pasi ata të bëhen të disponueshem për CA.

2.2.3 Qasja e kontrollit

CA do të mbrojë çdo informacion ne direktori që duhet të shpërndahet apo modifikuar.

2.3 Niveli i Pajtueshmërisë verifikimit (auditimit)

2.3.1 Frekuenca e auditimeve të pajtueshmërisë

CA ka te drejte te kryej auditime periodike.

2.3.2 Identiteti / kualifikimi i auditorëve

Auditorët duhet të provojnë kompetencën e tyre në fushën e vërtetimit të konformitetit dhe duhet të jenë të familjarizuar plotësisht me CPS qe i paraqitet.

2.3.3 Marrëdhënia e audituesеve me palën e audituar

Personeli i kontrollit i takon AKSHI dhe do të jete i ndare për te siguruar një vlerësim te paanshëm dhe te pavarur.

2.3.4 Temat e mbuluara nga auditimi

Qëllimi i auditimit është që të verifikojë një:
• CA ka një sistem që garanton cilësinë e shërbimit të ofruar;
• CA është në përputhje me të gjitha CP dhe kërkesat e CPS.
Të gjitha aspektet e veprimeve te CA që lidhen me këtë CP do të jetë subjekt i inspektimit te testeve të pajtueshmërisë.

2.3.5 Veprimet e ndërmarra në rastin e të metave

Kur personi që verifikon nivelin e pajtueshmërisë gjen një mospërputhje në mes të një CA ose veprimeve te RA dhe dispozitat e CPS saj, duhet të merren masat e mëposhtme:
• Niveli i auditorit të pajtueshmërisë do të ve re mospërputhje;
• Niveli i auditorit të pajtueshmërisë do të informojë në lidhje me mospërputhjen ndodhur;
• CA do të propozojë një zgjidhje, duke përfshirë edhe kohën e nevojshme për zgjidhjen.
Zgjidhja e duhur do të përcaktoj, kohë për rregullimin e çështjes, duke përfshirë pezullimin dhe revokimin e mundshme certifikatës se CA-së.

2.3.6 Komunikimi i rezultateve të auditimit

Personat që vërtetojnë nivelin e konformitetit do të raportojë rezultatet. Rezultatet do të raportohen si për AK audituar dhe të CA saj superiore. Mjetet e zbatimin e masave do t'i komunikohet autoritetit përkatës. Një verifikim të veçantë të nivelit të pajtueshmërisë mund të kërkohet për përputhje zbatimin dhe efektivitetin e korrigjuar.

2.4 Konfidencialiteti

2.4.1 Llojet e informacionit që duhet të mbrohen

Një certifikatë duhet të përmbajë vetëm informacionin që është i rëndësishëm dhe i nevojshëm për të bërë transaksione të sigurta me certifikatë. Në mënyrë që të menaxhoj certifikata, një CA apo RA mund të kërkojnë informacion specifik të certifikatës, në mënyrë që të përdorin atë për menaxhimin e certifikatave (p.sh. numrat e identifikimit, adresat e punës apo shtëpisë si dhe numrat e telefonit). Të gjitha informatat ruhen në nivel lokal në pajisjet e CA-së, dhe jo në regjistrin publik, ato do të trajtohen si të ndjeshme dhe qasja (aksesi) në to do të kufizohet, në mënyrë që vetëm ata që kanë nevojë për të kryer detyrat zyrtare do të jetë në gjendje për ti aksesuar.

2.4.2 Shpërndarja e informacionit

Një CA nuk do të zbulojë informacione në lidhje me certifikatat e një pale të tretë, përveç rasteve kur ajo është e autorizuar nga ky CPS, kërkohet me ligj ose me rregulla ose rregullore te tjera. Çdo kërkesë për zbulimin e informacionit do të legalizohen.

3. IDENTIFIKIMI DHE AUTENTIFIKIMI

3.1 Regjistrimi i kërkesës fillestare për certifikate

3.1.1 Llojet e emrave

Të gjitha CA duhet të jenë në gjendje për të gjeneruar, nënshkruar dhe vulosur certifikata që përmbajnë një emër të veçantë (DN X.500). Certifikatat e shpërndara nga CA duhet të përdorë formularin e DN. CA nuk do të caktojë emra te veçante. Abonentët do të kenë DN të lidhur përmes organizatave, me pëlqimin e një autoriteti të caktuar. Në varësi të situatës, disa certifikata do të ketë gjithashtu një formë alternative te emrit.
Emrat e përdorura brenda AKSHI do të identifikojnë personin ose objektin që ata janë të lidhur me të. RA do të sigurojë ekzistencën e një përkatësie ndërmjet Abonentit dhe organizimin që është identifikuar nga një komponent në emër brenda certifikatës se tij. Kur DN është përdorur, emri i përbashkët do të përfaqësojë Abonentin në një mënyrë që mund të kuptohet lehtë nga njerëzit e tjerë. Për individët, kjo është zakonisht emri i tyre ligjor. Për pajisje, kjo do të jetë adresa e rrjetit të pajisjes.

3.1.2 Rregullat për interpretimin e formave të ndryshme te emrit

Rregullat për interpretimin e formave të ndryshme te emrit janë të përfshira në profilin e zbatueshmerise se certifikatës dhe janë vendosur nga CA.

3.1.3 Emrat e veçante

Uniciteti i emrit në kuadër të AKSHI-t është i detyrueshëm. Kur është e mundur, emrat e veçante X.500 DN te caktuar nga një autoritet i specializuar i AKSHI do të përdoren, dhe CA e RA dhe do të detyrojë emrin unik në hapësira X.500 që kanë qenë të autorizuar. CA do të specifikojë në CPS për llojet e emrave që mund të përdorin, si RA dhe CA do të ndërveprojnë me autoritetin ne fjale e AKSHI do të caktojë këto emra në komunitetin e Abonentit për të siguruar veçantinë e emrit midis Abonentit aktual dhe të kaluar.

3.1.4 Zgjidhja e mosmarrëveshjeve për pronësinë e emrit

CA do të hetojë dhe saktësoje, nëse është e nevojshme, të gjitha konfliktet për emrin te sjella në vëmendjen e tij.

3.1.5 Prova e posedimit te çelësit privat

Çelësi gjenerohet direkt në pajisjen e Abonentit, ose në një software për gjenerimin e çelësave i cili mund të transferojë pajisjen e çelësit për tek Abonenti. Nëse Abonenti nuk ka pajisje, kur çelësi është krijuar, atëherë pajisja do t'u shpërndahet përmes një procedure administrative.

Kur certifikatat shpërndahen për abonentët ose në një pajisje ose ne skedar ne formatin PKCS # 12, shpërndarja do të bëhet në një mënyrë që siguron faktin se certifikatat përkatëse dhe të dhënat e aktivizimit u janë dhënë personave të duhur. RA do të mbajë një rekord vlefshmërie të marrjes se certifikatës nga Abonenti.

3.1.6 Vërtetimi i identitetit të organizatës

Kërkesat për certifikata për një organizate do të përfshijë emrin e organizatës dhe dokumentacionin në lidhje me ekzistencën e organizatës. RA do të verifikojë këtë informacion, përveç verifikimit të te deleguarit dhe autorizimin që personi ne fjale vepron në emër të organizatës.

3.1.7 Vërtetimi i identitetit të personave brendshëm dhe të jashtëm

RA do të sigurojë faktin se informacioni i identitetit te kandidatit (abonentit) dhe çelësat e tyre publike janë të lidhur përkatësisht. CA do të regjistrojë procesin për çdo certifikatë. Dokumentacioni i procesit duhet të përfshijë:

- Identiteti i operatorit te RA-së që kontrollon identitetin e avokatit;
- Deklarata e nënshkruar e operatorit e cila dëshmon faktin se ai verifikon identitetin e përfaqësuesit në përputhje me kërkesat e CPS te pranishëm;
- Një numër identifikimi;
- Verifikim i datës dhe orës;

Përveç kësaj, ne dokumentacion duhet të përfshihet edhe një deklaratë e identitetit. Deklarata duhet të jetë firmosur me dore nga përfaqësuesi në praninë e operatorit që kryen vërtetimin e identitetit.

KLASA 1 dhe 2 KLASA kërkojnë qe aplikantët të vërtetojnë identitetin e tyre, duke siguruar të paktën një dokument zyrtar të identifikimit vizual.

Kur çelësat private janë transmetuar për abonentët nëpërmjet pajisjeve hardware, të abonuarit mund te shkojnë personalisht tek RA për të marrë pajisjet apo të dhënave të tyre për aktivizimin.
Për një pajisje (KLASA 3 dhe KLASA 4), me përjashtim të identitetit të administratorit të pajisjes, të dhënat në lidhje me pajisjen përkatëse janë kontrolluar gjithashtu.

KLASA 1	Duhet të paraqitet personalisht tek Agjenti i besuar (operatori LRA) dhe të paraqesë një dokument zyrtar identifikimi. Nëse është e mundur, kontrolloni do të bëhet në vend.
KLASA 2	Duhet të paraqitet personalisht tek Agjenti i besuar (operatori LRA) dhe të paraqesë një dokument zyrtar identifikimi. Kontrolloni do të bëhet pas
KLASA 3	Administratori duhet të paraqitet personalisht tek Agjenti i besuar (Operatori LRA) dhe të paraqesë një dokument zyrtar identifikimi, si për te dhe për pajisjen. Verifikimi është bërë në vend.
KLASA 4	Administratori duhet të paraqitet personalisht tek Agjenti i besuar dhe të paraqesë një dokument zyrtar identifikimi, si për te dhe për pajisjen. Verifikimi behet me pas.

3.1.8 Vërtetimi i identitetit të elementeve të infrastrukturës

Disa komponentë te infrastrukturës, kompjuterët dhe komunikimit (routers, firewalls, etj) mund të jene subjekt i certifikimit. Në raste të tilla, pajisja duhet të ketë një operator njerëzor që është përgjegjës në RA ose agjente te besuar te aprovuar nga RA për disa informata të sakta në lidhje me:

- Identifikimin e pajisjeve,
- Çelësat publik te pajisjeve,
- Autorizimet dhe karakteristikat e pajisjeve (nëse ndonjë është për t'u përfshirë në certifikatë),
- Informacionet në kontratë që lejojnë RA për të komunikuar me operatorin kur është e nevojshme.

RA apo agjentët e tyre te besuar do të dëshmojnë vlefshmërinë e të gjitha autorizimeve të nevojshme në certifikatë dhe do të verifikojë burimin dhe integritetin e të dhënave të mbledhura në nivel sigurie që korrespondon me klasën e certifikatës se kërkuar. Metodat e aplikuara për kryerjen e këtyre autentifikimeve dhe për verifikimin e integritetit nuk kufizohen vetëm në:

• Verifikimin e mesazheve te nënshkruara elektronikisht te dërguara nga operatorët (duke përdorur certifikata me një nivel të sigurisë të barabartë ose më të madhe se ajo kërkuara)

• Regjistrimi personal nga operatori, me identitetin e konfirmuar te operatorit.

3.2 Modifikimi i certifikatave

3.2.1 Çelës i ri për certifikatën

Sa me shumë përdoret një çelës, aq me shume gjasa ka për te humbur ose për tu kompromet uar. Kjo është arsyeja pse është e rëndësishme që Abonenti te marr çelësa te rinj periodikisht dhe te rivendos identitetin e tij/saj. Ndryshimi i çelësit te një certifikate do të thotë krijimi i një certifikatë të re, të ngjashme me të parën, por që përmban një çelës publik të ri, një serial të ri dhe një periudhë të re vlefshmërie.

Vërtetimi i kërkesave për ndryshim çelësi behet me ane te certifikatës se vjetër qe Abonenti përdor për autentifikim përpara se te lëshoje kërkesën. Kërkohet qe behet ndryshimi i çelësit here pas here, për te shmangur dështimin e raportimeve te rasteve te humbjes se çelësit privat.

3.2.2 Rinovimi i certifikatës

Rinovimi i një certifikate do te thotë te krijosh një certifikate te re, me te njëjtin emër, çelës dhe autorizime si e vjetra, por me një periudhë të re të zgjatur të vlefshmërisë dhe një numër serial të ri. Rinovimi vlen vetëm për certifikatat që edhe pse kane arritur fundin e periudhës së vlefshmërisë, çelësat e tyre privat nuk janë kompromet uar.

4. KËRKESAT OPERATIVE

4.1 paraqitjes së aplikacionit

Çdo person që dëshiron qe një CA të lëshojë një certifikatë dixhitale duhet të:

- Te siguroje informacionin e nevojshëm për llojin e certifikatës dëshiruar;
- Marrjen e një çifti çelësash private/publike;
- Te demonstrojë funksionalitetin e çiftit te çelësave privat /publike;
- Te mbroje çelësin privat nga vjedhja, dëmtimi, modifikimi i përmbajtjes etj. Është e ndaluar duplikimi i çelësit privat;
- Të propozojë një emër të veçantë për identifikim;
- Në bazë të ekzaminimit CA-së (përmes RA): Kërkesa për të siguruar një certifikatë, marrëveshja për të respektuar detyrimet si një subjekt dhe te çiftit te çelësave në qoftë se ata nuk është e gjeneruar në CA.

Kur një subjekt kërkon te lëshohet një certifikatë, hapat e mëposhtme duhet të mbulohen:

- Verifikimin dhe regjistrimin e identitetit të Subjektit,
- Marrja e një çifti çelësash, publike dhe private,
- Vërtetimin e faktit se çelësi publik është çifti i çelësit private në pronësi nga Subjekti,
- Sigurimi i pikave të kontaktit për verifikimin e të gjitha roleve ose autorizimeve e kërkuara nga Subjekti.

Transmetimi i çelësi publik të Subjektit ndaj RA

Çelësat publike do ti dorëzohen atij që lëshon certifikatën në një mënyrë që siguron korrespondencën midis identitetit te verifikuar tashmë të Subjektit dhe çelësit publik që do të certifikohet.

4.2 Lëshimi i certifikatës

Pas marrjes së kërkesës, RA duhet të:

- Verifikoje identitetin e aplikantit
- Verifikoje autoritetin e kërkuesit dhe integritetin e informacionit në kuadër të kërkesës
- Dërgoje certifikatën Subjektit.

RA pranon si te vertete dhe te verifikuar informacionin e sjelle nga administrata shteterore.

Koha për të verifikuar informacionin ne kërkesë dhe për lëshimin e certifikatës nuk mund, në rrethana normale, kaloje:

- 3 (tre) ditë pune, për certifikatat e CLASS 1 dhe CLASS 3;
- 7 (shtatë) ditë pune, për certifikatat e CLASS 2 dhe CLASS 4,

nga momenti qe LRA fjalë merr të gjitha informatat e nevojshme për këtë qëllim.

4.2.1 Dorëzimi i çelës privat Subjektit

Një çelës privat do të gjenerohet duke përdorur një software ose modul hardware kriptografike. Nëse çelësi është gjeneruar në CA, moduli duhet ti dorëzohet Subjektit. Autoriteti që gjeneron çelësin privat te nënshkrimit të një Subjektit nuk duhet të mbajë asnjë kopje të çelësit. Vetëm çelësat e nënshkrimeve private te CA mund të jenë subjekt operacionesh backup te sigurte. Gjithashtu, një procedurë rikuperimi për çelësat private enkriptimit që u përkasin përdoruesve të bazuar në skemat e tipit (k nga n).

Kur çifti i çelësave është krijuar për Subjektin nga CA, CA duhet të zbatojë mekanizma të sigurta për ti dërguar Subjektit:
• Pajisjen/skedarin me çiftin e çelësave
• Metoda e aktivizimit.

4.2.2 Shpërndarja e certifikatave te CA përdorueseve

Gjithë "filozofia" e PKI është bazuar në certifikatat e ashtuquajtura ”Trusted Certificates “që përfaqësojnë pikat e përbashkëta te besimit mes përdorueseve. Për shpërndarjen e këtyre certifikatave te besuara, metodat e mëposhtme do të përdoren:

- shpërndarja e sigurt për përdoruesit përmes mjeteve jo-elektronike
- shpërndarja elektronike dhe krahasimin e disa vlera hash ose gjurme gishtash, të dërguara nëpërmjet mjeteve jo-elektronike
- shkarkimit certifikatën nga faqet Web të siguruara

4.3 Pranimi i Certifikatës

Përpara se CA ti dorezoje Abonentit çelësin privat, duhet të:
• Shpjegoje cilat janë përgjegjësitë e abonentit
• Informoje abonentin në lidhje me kërkesën dhe përmbajtjen e certifikatës
• te kërkoje nga abonenti te aprovoje duke nënshkruar me shkrim ose elektronikisht detyrimet e tij dhe certifikatën e lëshuar
• Përfundojnë një marrëveshje te pranimit për detyrimet dhe certifikatën.

Pranimi i certifikatës nga Subjekti do te thotë se Subjekti pajtohet me te mëposhtmet:
• Çdo nënshkrim dixhital i krijuar duke përdorur çelësin privat i cili korrespondon me çelësin publik të listuar në certifikatë është nënshkrimi dixhital i subjektit dhe certifikata

e pranuar është operacionale (nuk ka skaduar, pezulluar ose revokuar) në datën dhe orën kur nënshkrimi dixhital eshte krijuar;
• Asnjë person i paautorizuar nuk ka qasje në çelësin privat të Subjektit;
• Informacionet që përmbahen në certifikatë janë të vërteta;
• Certifikata mund të përdoret vetëm për qëllime të autorizuara nga AKSHI;
Pajtimtari, si një përdorues fundor, nuk mund të përdorë çelësin privat i cili korrespondon me çelësin publik e shënuar në certifikatë për nënshkrimin e certifikatave të tjera ose listave te revokimit, përveç rasteve kur kjo është e përcaktuar shprehimisht në kontratën me tij me CA. Duke pranuar certifikatën, Subjekti merr përgjegjësinë mbi kontrollin e çelësit te tij private dhe mbi marrjen e masave parandaluese për të parandaluar, humbje, zbulimin, modifikim ose të përdorimit te paautorizuar te tij.

4.4 Revokimi i Certifikatës

4.4.1 Revokimi

Certifikata revokohet kur:
• Informacioni brenda certifikatës ka ndryshuar (personi ka lënë institucionin, vdiq, u vu nën ndalim, është shkëputur për periudha të gjata, etj)
• Privilegjet e dhëna për Subjektin nëpërmjet certifikatës janë anuluar apo kufizuar
• Është vërtetuar se Subjekti ka shkelur detyrimet e marrëveshjes me RA.
• Çelësi private apo të dhënat e aktivizimit janë kompromet uar (humbur ose vjedhur)
• Subjekti ose në një tjetër njësi e autorizuar kërkon revokimin e certifikatës.
Certifikatat revokuara janë te vendosura në CRL deri sa të përfundojnë.

Procedura e kërkesës për revokim përfshin metoda elektronike apo letër. RA duhet të vërtetoj kërkesën në mënyrë për të parandaluar sulmet dashakeqe. Nëse është kështu, RA do te revokoj certifikatën duke vendosur numrin e saj serial në CRL. RA do të informojnë mbajtësin certifikatës për revokimin.

4.4.2 Listat e Certifikatave te Revokuara (CRL)

CA nxjerrë dhe publikon CRL periodikisht. Publikimi do të bëhet në dosje, në intervale të caktuara kohore, edhe në qoftë se nuk ka përditësime me versionet e mëparshme. CA duhet të publikoje mënyrat në të cilat mund të merret informacion mbi CRL dhe të shpjegojë pasojat e përdorimit të certifikatave tashme të publikuara në CRL. Është përgjegjësi e palëve të treta që përdorin certifikata për të marrë listat e përditësuara te CRL në kohën e duhur.

Frekuencat e mëposhtme për publikimin e CRL janë te rekomanduara:

• Class 1 - CA do të publikojë CRL të paktën një herë në çdo shtatë ditë dhe një certifikatë qe njoftohet si e kompromet uar do të shfaqet në CRL brenda 48 orëve.
• Class 2 - CA do të publikojë CRL të paktën një herë në çdo dy ditë dhe një certifikatë qe njoftohet si e kompromet uar do të shfaqet në CRL brenda 24 orëve.
• Class 3 - CA do të publikojë CRL të paktën një herë në çdo dy ditë dhe një certifikatë qe njoftohet si e kompromet uar do të shfaqet në CRL brenda 48 orëve.
• Class 4 - CA do të publikojë CRL të paktën një herë në çdo dy ditë dhe një certifikatë qe njoftohet si e kompromet uar do të shfaqet në CRL brenda 24 orëve.

4.4.3 Verifikimi i statusit te certifikatës Online

Verifikimi statusit te certifikatës Online do të bëhet në mënyrë që të sigurojë:
• Treguesit e vlefshmërisë së certifikatës apo një rrugë që çon në një certifikimit CA te besuar (zakonisht ROOT CA)
• Secila certifikatë në rrugën e vlefshmërisë është kontrolluar për revokimin
• Përgjigja për statusin e saj duhet të jetë subjekt i masave të vërtetimit,
• Duhet të jetë e qartë në përgjigjen e statusit te certifikatës se cilat atribute janë vërtetuar nga autoriteti verifikimit

4.5 Procedurat e auditimit te sigurisë

Ky seksion përshkruan regjistrimin dhe kërkesat e auditimit të sigurisë të vendosura për sistemet dhe pajisjet e përdorura për:
• Regjistrimi i kërkesave për certifikatë,
• Gjenerimin, nënshkrimin dhe menaxhimin e certifikatave,
• Gjenerimin, nënshkrimin dhe menaxhimin e CRL.

4.5.1 Llojet e ngjarjeve të regjistruara

Regjistrimi i ngjarjeve që ndodhin në RA ose CA është e nevojshme:
• Qasja fizike, nisja, transferimi, back-up i çelësave për/nga modulet kriptografike te CA ose për të marrë apo të shkatërruar modulet kriptografike te RA ose CA;
• Transporti i hardware kriptografik;
• Vendosja e informacionit në dosje;
• Kushtet e gabimeve, gabimet e verifikimit te integritetit te software, lista e mesazheve të gabuara të marra;
• Çdo shkelje e njohur apo e pretenduar e sigurisë fizike, përpjekjet për të sulmuar CA apo pajisje te RA nëpërmjet rrjetit, gabimet ne pajisje, ndërprerjet e energjisë ose shkelje e kësaj politike te certifikimit.

Pajisjet e CA do të regjistrojnë instalimet e serverëve, qasje dhe ndryshimet (duke përfshirë ndryshimet në skedarët e konfigurimit, profilet e sigurisë, si dhe privilegjet e administratorit). Regjistrimi i operacioneve te mëposhtëm te CA është e nevojshme:
• Qasja në pajisjet e CA;
• trajtimi i skedarëve dhe menaxhimi i përdorueseve;
• vendosjen e çfarëdo lloji të informatave në dosje;
• aksesi i bazës se të dhënave CA;
• çdo përdorim i çelësave te nënshkrimit të CA.

Për çdo rast te hasur te përcaktuar në këtë seksion, regjistrimi i auditimit të sigurisë CA duhet të përfshijë informacionin e mëposhtëm
• Lloji ngjarjes;
• Data dhe koha e ndodhjes së ngjarjes;
• Përpjekje te CA për të nënshkruar një certifikatë ose revokimin, një tregues suksesi apo dështimi;
• Veprimet e operatorit, identiteti i personit që nisi veprimin

Te dhënat e auditimit te sigurisë do të mblidhen automatikisht dhe nëse nuk është e mundur, për log-et do të përdoret dhe format letër, ose mekanizma të tjera fizike.

4.5.2 Frekuenca e procesimit te logeve

• Për CLASS 1 dhe CLASS 3, të paktën 2 përpunime te logeve në vit janë të nevojshme, me të paktën 25% të të dhënave të auditimit të sigurisë të krijuara nga analiza e fundit të sigurisë.
• Për CLASS 2 dhe CLASS 4, të paktën 5 përpunime te logeve në vit janë të nevojshme, me të paktën 33% të të dhënave të auditimit të sigurisë të krijuara nga analiza e fundit të sigurisë.
CA ose RA ose duhet të zbatojnë procedurat për të siguruar se të dhënat e auditimit të sigurisë janë transferuar para se ata janë mbishkruar me të dhëna të reja ose para se skedarët te janë plotë.

4.5.3 Periudha e ruajtjes se te dhënave te auditimit

Informacioni i gjeneruar nga pajisjet e CA apo RA duhet të ruhet ne pajisjet e CA ose RA deri sa informacioni te jete zhvendosur në një arkiv. Fshirja e të dhënave të auditimit të sigurisë nuk duhet të bëhet nga RA ose CA.

4.5.4 Mbrojtja e te dhënave te auditi

Për klasat 1, 2, 3 dhe 4 të dhënat e auditimit të sigurisë nuk duhet të jetë në dispozicion për lexim apo modifikim nga ana e ndonjë personi apo procesi, përveç atyre që kryejnë

auditimin e sigurisë. Konfigurimet e sistemit dhe procedurat e RA ose CA duhet të sigurojnë që vetëm personat e autorizuar mund te arkivojnë ose fshijnë të dhënat e auditimit të sigurisë. Entiteti që arkivon të dhënat e auditimit të sigurisë nuk duhet te ketë të drejtën për ti fshire ato dhe këto procedura duhet të zbatohen në mënyrë që të mbrojnë të dhënat e arkivuara nga fshirja ose shkatërrimi, deri në fund të periudhës së ruajtjes. Te dhënat e auditimit te sigurisë duhet të zhvendosen në një vend të sigurt magazinimi, të ndryshme nga vendndodhja e pajisjeve te RA ose CA.

4.5.5 Proceset e auditimit te sigurisë

Procesi i auditimit te sigurisë duhet të ekzekutohet i pavarur dhe nuk duhet të jetë nën kontrollin e stafit te RA ose CA. Proceset e auditimit të sigurisë duhet të fillojnë me ndezjen e sistemit dhe të mbyllen me fikjen e sistemit. Nëse rezultojnë parregullsi nga procesi i auditimit të sigurisë, CA apo RA duhet te mbyllin të gjitha operacionet (përveç revokimit) derisa proceset e auditimit të rivendosen.

4.5.6 Vlerësimi i vulnerabilitetit

CA ose RA duhet te jene te vëmendshëm ndaj shkeljeve në integritetin e sistemit të menaxhimit te certifikatës, duke përfshirë pajisjet, vendndodhjen fizike, dhe stafin. Te dhënat e auditimit te sigurisë do të rishikohen nga audituesi i sigurisë për të zbuluar veprimet te përsëritura gabimesh, kërkesat për informacion të privilegjuar, përpjekjet për të hyrë në skedarët e sistemit dhe përgjigjet e pa verifikuara. Auditorët e sigurisë do të verifikojnë vazhdimësinë e te dhënave te auditimit të sigurisë.

4.6 Arkivimi i rekordeve

4.6.1 Tipi i të dhënave të arkivuara

Të dhënat arkivuar nga CA ose RA do të detajohen mjaftueshme për të lejuar përcaktimin e vlefshmërisë së operacioneve brenda infrastrukturës. Të dhënat e mëposhtme do të arkivohen:

- Gjatë initializimit të sistemit te CA:
    - Konfigurimin e sistemit.
- Gjatë operacioneve te RA ose CA:
    - Kërkesat për certifikata dhe revokim;
    - Dokumentet për verifikimin e identitetit te abonentit;
    - Dokumentet e marrjes dhe pranimit te certifikatës;
    - Dokumentacioni i marrjes se pajisjes;
    - Te gjitha certifikatat dhe CRL te lëshuara;
    - Te dhënave e auditimit te sigurisë;
    - të gjitha gjërat që lidhen me komunikimin me të tjera CA dhe auditorë.

4.6.2 Periudha e mbajtjes se arkives

Arkivi dhënat do të mbahen për një periudhë:
• Së paku dhjetë vjet, për klasën 1 dhe klasën 3
• Së paku njëzet vjet, për klasën 2 dhe klasën 4.

Aplikacionet e nevojshme për të lexuar arkivat duhet të ruhen për një periudhë të paktën të barabartë me periudhën më të vogël të përshkruar më sipër. Para periudhës se skadimit te ruajtjes, CA do të ofrojë të dhënat e arkivuara dhe aplikacionet e nevojshme për leximin arkivave te AKSHI-t, i cili do të mbajë aplikacionet e nevojshme për leximin e këtyre të dhënave te arkivuara.

4.6.3 Mbrojtja e arkivit

Asnjë operator i paautorizuar i pajisjeve te CA nuk duhet të jetë në gjendje të modifikojë ose fshije arkivat. Nëse mediumi origjinal i ruajtjes se te dhënave nuk mund të mbajë të dhënat për periudhën e kërkuar, një mekanizëm do të përcaktohet, përmes të cilit të dhënat e arkivuara do të transferohen në një medium të ndryshëm ruajtje.

4.7 Ndryshimi i çelësit te CA

CA përdor një çelës privat për nënshkrimin e certifikatave; palët e treta përdorin certifikatat e CA gjatë gjithë jetës së certifikatave te abonentëve, pasi ato janë nënshkruar. Kështu, CA nuk duhet të lëshojë certifikata që shtrihen përtej datës së skadimit të certifikatës së tyre dhe periudha e vlefshmërisë së CA duhet të zgjasë periudhën e vlefshmërisë së certifikatave te abonentëve përtej përdorimit të fundit të çelësit privat CA.
Për të minimizuar rrezikun e dëmtimit te PKI duke kompromentuar çelësin privat te CA-së, Çelësi privat i nënshkrimin te CA do të duhet të ndryshohet më shpesh, dhe vetëm çelësi i ri do të përdoret që të nënshkruajë certifikatat nga ai moment e në vazhdimësi. Certifikatat e vjetra, por ende të vlefshme, do të jenë në dispozicion për të verifikuar çelësin e vjetër, derisa të gjitha certifikatat e abonentëve te nënshkruara me këtë çelës do të kenë skaduar.

Jetëgjatësia e certifikatave do të jetë si më poshtë:

• Certifikata e abonentëve: 1 (një) vit
• Certifikatat e klasave: 7 (shtatë) vjet
• SUB CA: 15 (pesëmbëdhjetë) vjet
• ROOTCA: 25 (njëzet e pesë) vjet

4.8 Komprometimi dhe rimëkëmbja

4.8.1 Ringritje ne rast komprometimi

Nëse siguria e një çelësi te CA është komprometuar, një CA superiore do te revokoj certifikatën dhe informacioni i revokimit do te publikohet menjëherë. Më pas, instalimi i CA do të rikthehet si më poshtë. Nëse CA është një ROOT CA, certifikata e vetë-nënshkruar duhet të fshihen nga çdo aplikim i përdorur nga palët e treta dhe pastaj një e re duhet të shpërndahet nëpërmjet mekanizmave jo-elektronike.

4.8.2 Ringritja

CA duhet të zbatoje procedurat ne rast fatkeqësish (disaster recover procedure). Në rastin e një fatkeqësie në të cilën pajisjet CA janë dëmtuar ose behën joaktive, operacionet e CA duhet të rikthehen sa më shpejt të jetë e mundur, bazuar ne prioritetin për revokimin certifikatave te abonentëve. Nëse CA nuk mund të rivendos aftësitë e saj për revokimin brenda një jave, atëherë ai duhet të raportoje se çelësat e saj janë kompromet uar. Më pas, CA ka për të rivendosur çelësat dhe certifikatat e saj dhe përfundimisht certifikatat abonentëve.

Në rastin e një fatkeqësie në të cilën është dëmtuar fizikisht CA dhe të gjitha kopjet e çelësave te CA janë shkatërruar, CA duhet të kërkojë qe të gjitha certifikatat e saj të revokohen. Instalimi i CA përfshin riparimin e pajisjeve, gjenerimin e çelësave te rinj publike dhe private, duke ri-lëshuar certifikatat dhe ri-nënshkrimin e të gjitha ndër-certifikatave. Së fundmi, certifikatat e të gjithë abonentëve do të ri-lëshohen.

4.8.3 Përfundimi i Autoritetit te Certifikimit

Ne rast mbyllje shërbimi te CA zgjidhja behet në përputhje me seksionin 4.8. Nëse ndërprerja është rezultat i riorganizimit apo të çështjeve te tjera jo-sigurie dhe nuk ka pasur dispozita për të vazhduar veprimtarinë e rivendosjes se çelësave te kompromentuar, të auditimeve të sigurisë dhe arkivave, atëherë as certifikatat e CA dhe as certifikatat e nënshkruar nga CA nuk do të duhet të revokohet. Nëse dispozitat për vazhdimin e mëtejshëm të këtyre shërbimeve nuk mund të përcaktohen, atëherë ndërprerja e CA do të bëhet si një kompromis i CA me te tjere, në përputhje me nenin 4.8.1. Para përfundimit te CA, autoriteti duhet të dorëzojë të dhënat e arkivuara në një strukturë brenda AKSHI.

5. KONTROLLET E SIGURISE FIZIKE, PROCEDURIALE DHE PERSONELIT

5.1 Kontrollet e sigurisë fizike

Pajisjet e CA nuk do të kryejnë funksione të tjera. Përdorimi i paautorizuar i pajisjeve te CA është e ndaluar. Kontrollet fizike të sigurisë do të zbatohen për të mbrojtur hardware dhe software te CA ndaj përdorimit të paautorizuar. Modulet kriptografike te CA duhet të mbrohen kundër vjedhjeje, humbjeje dhe përdorimit të paautorizuar.

5.1.1 Vendndodhja dhe konstruksioni

Vendndodhja dhe konstruksioni i një objekti për vendosjen e pajisjeve te CA do të bëhet në përputhje me rregulloren e AKSHI për mbrojtjen e informacionit me të njëjtën vlerë ose klasifikim me materialet që do të mbrohen me çelësat publike të nxjerra ose të administruara nga AKSHI.

5.1.2 Qasja fizike

Pajisjet e CA do të jenë te mbrojtur gjithmonë kundër qasjes së paautorizuar.
Heqja e paautorizuar e pajisjeve nga dhoma e CA duhet të ndalohet dhe gjithashtu largimin e mediave të magazinimit dhe software te lidhur me CA.

5.1.3 Furnizimi me energji elektrike dhe ajri i kondicionuar

Dhomë ku janë vendosur pajisjet e CA do të kenë qasje në rrjet elektrike dhe do të jenë me ajër të kondicionuar në mënyrë që të sigurojë një mjedis të favorshëm. Një pajisje e CA do të duhet të jetë në gjendje për të siguruar backup të mjaftueshme për të përfunduar ndonjë nga operacionet ne proces dhe të regjistrojë gjendjen e pajisjeve përpara se energjia elektrike dhe ajri i kondicionuar te ndërpriten.

5.1.4 Ekspozimet ndaj ujit

Pajisjet e CA do të instalohen ne një dysheme te ngritur, në mënyrë që te mos jene në rrezik për t'u ekspozuar ndaj ujit. Detektorë lagështi do të instalohen në zona të ndryshme. Operatorët e CA të cilët kanë aparatet zjarri duhet të veprojnë në bazë të një plani të paracaktuara, gjate përdorimit te tyre, në mënyrë që dëmet e shkaktuara nga uji të ndikojnë vetëm në zonën ku është vendosur zjarri.

5.1.5 Parandalimi dhe mbrojtja nga zjarri

Datacenter e AKSHI e ka një sistem te parandalimit dhe shuarjes se zjarrit në përputhje me standardet dhe rregulloret përkatëse në këtë fushë.

5.1.6 Magazinimi i mediave

Pajisjet e arkivimit duhet të vendosen në vende ku ata janë të mbrojtur kundër dëmtimeve aksidentale (uji, zjarri, fusha elektromagnetike). Mediat që përmbajnë të dhënat e auditimit të sigurisë, arkiva ose informacion rimëkëmbjes do të duhet të ruhen në pajisje të tjera jo te CA, ku ato duhet të transportohen të paktën një herë në javë.

5.1.7 Shkatërrimi i mbeturinave

Të gjitha kopjet e panevojshme të informacionit te ndjeshëm të shtypura shkatërrohen në vend. Të gjitha mediat elektronike janë zerohen.

5.1.8 Backup Off-site

AKSHI bën kopje backup të rregullt të çdo informacioni të nevojshëm për të rimëkëmbur nga një dështim i sistemit. Kopjet ruhen off-site ne një kasaforte.

5.2 Kontrollet proceduriale

5.2.1 Rolet e besuar

Një rol i besuar është personi i cili ekzekuton funksionet që, nëse nuk ekzekutohen sipas rregullave, mund të shkaktojnë probleme sigurie aksidentalisht ose me qëllim.

Njerëzit e përzgjedhur për të përmbushur këtë rol duhet të jenë kompetent dhe te besueshëm. Funksionet e kryera nga këto role janë baza e besimit për gjithë PKI.

Ka dy mënyra për të rritur gjasat që këto funksione te ekzekutohen me sukses:

- E para është që të sigurohet se personi i veshur me rolin është i besueshëm dhe të trajnuar mirë.
- E dyta është shpërndarja e funksioneve te një rol për sa më shumë njerëz të jetë e mundur, një aktivitet keqbërës kërkon një aleance (me pake gjasa) ndërmjet tyre.

Të gjitha certifikatat duhet të lëshohen nga një CA. Përgjegjësitë e CA supozojnë sigurimin e funksioneve te mëposhtme:

- Gjenerimi dhe revokimi i certifikatave;
- Publikimi i certifikatave dhe CRL;
- Funksionet administrative të tilla si raportimi i kompromiseve dhe mirëmbajtjen e bazës së të dhënave;

Përgjegjësitë kryesore të RA:

- Verifikimi i identitetit në përputhje me këtë politikë;
- Regjistrimi i informacionit te abonentëve dhe kontrolli i saktësisë se tyre;
- Transmetim i sigurte i kërkesave CA
- Marrjen dhe shpërndarjen e certifikatave Abonentëve.

Për të siguruar infrastrukturën, CA do të duhet të definojnë rolet e tjera të besuar përmes së cilës të caktojë përgjegjësitë për sigurimin e operacionale në kushte të sigurta dhe të mirë të pajisjeve dhe procedurave te CA. Këto përgjegjësi përfshijnë:

- Konfigurimi fillestar i sistemit, duke përfshirë instalimin e aplikacioneve, krijimin e llogarive të reja, konfigurimi i hosteve dhe ndërfaqeve fillestar të rrjetit.;
- Auditimet periodike;
- Krijimi i pajisjeve për rimëkëmbjen ne rast fatkeqësish;
- Te ekzekutoj backup, përditësime, dhe korrigjime te software;
- Te ruaje dhe shpërndajë ne rruge te sigurta backup dhe përditësimet ne një vendndodhje te jashtme;
- Ndryshimi konfigurimin hosteve dhe ndërfaqeve te rrjetit;
- Caktimi i privilegjeve të sigurisë dhe kontrollet qasjes për abonentët;
- Krijimi i arkivave dhe fshirjen e auditeve te sigurisë dhe të dhënave të tjera te arkivuara;
- Rishikimi i auditit të sigurisë.

5.3 Kontrolli i personelit

5.3.1 Kualifikimi, përvoja, dhe kërkesat për kualifikim

Personat për CA ose role te tjetër të besuar do të përzgjidhen pas:

- Besnikëria,
- Besimi dhe
- Kompetenca.
- Operacionet e CA duhet të administrohen nga një person ose organizatë. Ky person apo organizatë duhet të identifikohen si CA. Operatorët dhe pajisjet e nevojshme për instalimin e PKI duhet të jenë nën kontrollin administrativ të CA.

Personeli i CA duhet të ketë detyrat funksionale të përcaktuara, për të siguruar ndarjen e duhur të detyrave dhe përgjegjësive dhe përgjegjësi të qartë në rastin e incidenteve.

5.3.2 Procedurat e kontrollit te background

Kontrollet e background janë bërë për të përcaktuar përshtatshmërinë e një personi për të përmbushur një rol brenda PKI.

5.3.3 Kërkesat për trajnim

Gjithë personeli i përfshirë në operacionin CA duhet të jetë i trajnuar siç duhet. Temat duhet të përfshijë funksionimin hardware dhe software, procedurat operative dhe të sigurisë, ketë politikë dhe përcaktimet e sjelljes. Trajnim specifik do të varet nga pajisjet e përdorura dhe personeli i zgjedhur. Plani i trajnimit duhet të jetë vendosur në instalimin e CA dhe trajnimi i marrë nga personeli duhet të dokumentohet.

5.3.4 Frekuenca e rikualifikimit dhe kërkesat

Ata që janë përfshirë në rolet PKI duhet të informohen në lidhje me ndryshimet në operacionet e CA. Ndryshime të konsiderueshme ne operacionet e CA do të kenë një plan trajnimi dhe ekzekutimi i një plani të tillë do të duhet të dokumentohet. Shembuj të këtyre ndryshimeve janë përmirësimet hardware dhe software te CA, ndryshimet në sistemin e sigurisë dhe zhvendosja e pajisjeve te CA.

6. KONTROLLET TEKNIKE TË SIGURISË

6.1 Instalimi dhe gjenerimi i çiftit te çelësave

6.1.1 Gjenerimi i çiftit te çelësave

Çifti i çelësave duhet te gjenerohet nga një entitet PKI: një Abonent, një RA ose CA. Çelësi privat nuk duhet të qëndrojë jashtë modulit (hard apo soft), ku është gjeneruar derisa ai është enkriptuar për transmetim lokal ose për procesin e magazinimit të ekzekutohet nga një mekanizëm rikuperimi. Nëse çelësi është gjeneruar në format software, duhet të mbrohet me fjalëkalim.

6.1.2 Shpërndarja e çelësit privat Abonentit

Nëse njësia që ka gjeneruar çelësin privat është i ndryshëm nga Abonenti, ai duhet ti dorëzohet Abonentit ose në një pajisje (hard), ose në një skedarë (soft), të koduar dhe të mbrojtur me një fjalëkalim.

6.1.3 Madhësia e çelësave

Për RSA, çelësi publik i Abonentit duhet të jetë të paktën 1024 bit.

6.1.4 Përdorimi i çelësit

Çelësat publike që janë të vendosur në certifikata janë te caktuar për t'u përdorur për nënshkrimin dhe enkriptimin, por jo për të dy. Përdorimi i një çelësi është vendosur nga shtesa e përdorimit të çelësit ne certifikatat X. 509.

Certifikata mund të përfshijë një çelës të vetëm për t'u përdorur për enkriptim dhe nënshkrim vetëm në aplikacionet S/MIME (Secure Multipurpose Internet Mail Extensions). Certifikatat duhet të gjenerohen dhe të administrohen në përputhje me kërkesat në lidhje me certifikatat për nënshkrim/ per vulosje.

6.2 Mbrojtja e çelësit privat dhe kontrolli i moduleve kriptografike

6.2.1 Standardet dhe kontrollet për modulet kriptografike

Standardi përkatës për modulet kriptografike është “Security Requirements for Cryptographics Modules [FIPS140-1]”. Modulet kriptografike do të vlerësohen sipas nivel FIPS 140-1.

Të gjitha modulet kriptografike (hardware ose software) duhet të veprojnë në mënyrë që çelësat asimetrike private nuk janë shfaqen në tekst të qartë. Asnjë çelës privat nuk duhet të paraqitet i pa enkriptuar jashtë pajisjeve CA. Askush nuk duhet të ketë qasje në çelësin privat për nënshkrimin/vulosjen me përjashtim të Abonentit. Menaxhimi i magazinës se çelësave privat çelësat nga CA (ripërtëritja e çelësave) do të mbahet nën konfidencialitetit të plotë.

6.2.2 Kontrolli i çelësit privat dhe backup

Qasja në çelësin privat te CA për nënshkrimin/vulosjen apo moduleve te saj kriptografike që përmbajnë çelësin privat te CA për nënshkrimin duhet të bëhet nën kontroll të dyfishtë.

Për CLASS 1, Abonenti merr përgjegjësinë për kontrollin e çelësit te tij privat dhe për të marrë masa për të parandaluar vjedhjen, zbulimin, ndryshimin apo përdorimit të paautorizuar.

Për CLASS 2, vetëm CA mund të bëjë backups te çelësit privat për enkriptim në modulet kriptografike në favor të abonentëve, as RA as abonenti mund të beje backup çelësave privat për CLASS 2.

Për CLASS 3 dhe 4 nuk është e nevojshme backup, pasi këto certifikata nuk janë përdorur për enkriptim.

Backup do të bëhet për çelësat e CA vetëm për nënshkrim nën kontrollin e dy personave. Emri i atyre që janë pjesë e grupit të kontrollit duhet të mbahen në një listë në dispozicion për inspektim gjatë auditimit të përputhshmërisë. CA mund të beje backup çelësat e menaxhimit dhe e nënshkrimit/vulosjes në modulet kriptografike të shumta pa praninë e të paktën dy personave të kontrollit, për aq kohë sa veprimet backup janë regjistruar për auditimin e sigurisë.

Çelësat e menaxhimit te asociuar me çelësat private mund të nxirren nga baza e të dhënave të rimëkëmbjes (key recovery) vetëm në praninë e të paktën dy njerëz të caktuar me miratimin e AKSHI.

6.2.3 Transferimi i çelësit privat nga/ne një pajisje kriptografike

Çelësat private mund të gjenerohen në një modul kriptografike (hardware ose software - PKCS # 12). Nëse një çelës privat duhet të transportohet nga një modul kriptografike në tjetrin, çelësi privat duhet të jetë i enkriptuar gjatë transportit; çelësat private nuk duhet të nxirren në tekst të qartë në modul kriptografike.

Çelësat private ose simetrike të përdorura për enkriptim te çelësave të tjerë private për transport duhet të mbrohen. Mbrojtja e këtyre çelësave duhet të behet përputhje me nivelin e mbrojtjes së të dhënave të mbrojtura me certifikatën e lidhur me këtë çelës privat.

6.2.4 Metoda e aktivizimit te çelësit privat

Për aktivizimin e çelësit privat në modulet kriptografike, fjalëkalimet dhe kodet PIN mund të përdoren. Të dhënat e aktivizimit mund të shpërndahen personalisht ose dërgohen me postë abonentëve, te ndarë nga modulet kriptografike që ata aktivizojnë. Hyrja e të dhënave aktivizimit duhet të mbrohet nga zbulimi (nuk duhet të shfaqet).

6.2.5 Metoda e shkatërrimit te çelësit privat

Çelësat private duhet të shkatërrohen, kur ata nuk janë më të përdorur ose kur certifikatat e tyre përkatëse kanë skaduar apo janë shfuqizuar. Për modulet kriptografike software, kjo mund të bëhet duke shkruar mbi të dhënat ekzistuese. Për modulet kriptografike hardware, kjo do të thotë ekzekutimin e një komande për fshirje fizike (zerim). Shkatërrimi fizik i hardware nuk është e nevojshme.

6.3 Aspektet te tjera te menaxhimit te çiftit te çelësave

6.3.1 Arkivimi i çelësave publik

Çdo autoritet i cili lëshon certifikata arkivon çelësat publik te abonentëve të cilëve certifikata iu është lëshuar.

6.3. Periudha e përdorimit te certifikatës dhe çiftit te çelësave

Periudha për të përdorur çelësat është përshkruar në kapitullin 3.

6.4 Te dhënat e aktivizimit

6.4.1 Gjenerimi i te dhënave te aktivizimit dhe instalimi

Për të mbrojtur qasje në përdorimin e çelësit privat, duhen përdorur fjalëkalime dhe kode PIN.
Nëse të dhënat e aktivizimit duhet të transmetohen, kjo duhet të bëhet nëpërmjet një mjeti të mbrojtur siç duhet, dhe të ndryshme në hapësirë dhe kohë e transmetimit te pajisjes kriptografike. Abonenti duhet të jetë i informuar në lidhje me transportin e aktivizimit të të dhënave, metoda e transportit dhe datën e pritur te dorëzimit. Përveç kësaj, Abonentët duhet të marrin edhe një deklaratë në mënyrë që të kuptojnë përgjegjësitë në përdorimin dhe kontrollin e moduleve kriptografike.

6.4.2 Mbrojtja e te dhënave te aktivizimit

Cdo informacion duhet te ruhet i sigurt dhe jo mbajtur shenim. Informacioni per aktivizimin e moduleve kriptografike nuk duhet te ruhen ne te njëjtin vend me to.

Të dhënat për aktivizimin e çelësave private të shoqëruara me certifikata që deklarojnë identitetet individuale nuk duhet të ndahet me njerëz të tjerë. Të dhënat për aktivizimin e çelësit private të shoqëruara me certifikata që deklarojnë identitetin e organizatës do të duhet të jetë i kufizuar për ato të cilët janë të autorizuar nga organizata për të përdorni çelësat private

6.5 Kontrollet e sigurisë kompjuterike

Pajisje e CA te përdorur për sigurimin e infrastrukturës për CLASS 1,2,3 dhe 4 do të duhet të përdorin sistemet operative të cilët:
• Vërtetohen hyrjet;
• Mundësojnë kontroll te aksesit;
• Mundësojnë kapacitete audituese te sigurisë.

6.6 Kontrollet teknike te ciklit jetësor

Pajisje (hard dhe soft) të siguruara për të operuar një PKI do të blihen në mënyrë që te zvogëlojnë probabilitetin e depërtimit.

Hardware dhe software i zgjedhur si mbështetje për PKI duhet të dërgohet ose shpërndahet nëpërmjet metodave të kontrolluara që ofrojnë siguri dhe përgjegjësi, nga ku ai u identifikua si mbështetje për funksionet e CA në objektin e përdorimit.

7. POLITIKA E MENAXHIMIT TË CERTIFIKIMIT

7.1 Procedurat për ndryshimin e specifikimeve

Këto praktika do të rishikohen te paktën një herë në vit. Gabimet, të rejat dhe sugjerime për ndryshime për këto dokumente do të dorëzohen personat e kontaktit të caktuara nga ky dokument. Çdo njoftim do të duhet të përfshijë një përshkrim të modifikimit të nevojshme, arsyet e saj dhe informatat kontaktuese për personin që kërkon ndryshimin.

Të gjitha ndryshimet CPS do të shpërndahen palëve të interesuara për një periudhë prej të paktën një muaji.

7.2 Publikimi dhe politikat e paralajmërimit

Informacionin e kërkuar (përfshirë politiken) do të publikohen në një faqe Web. Një listë e CAS aktivizimin në përputhje me këto praktika do të mbahen.

7.3 Procedurat e miratimit te CPS

DO të përcaktohet nëse një CPS është në përputhje me këtë politikë për një nivel të caktuar të sigurisë. Para se të bëhet funksional, CA duhet të respektojë të gjitha kërkesat e CPS te miratuar.

Akronime dhe Shkurtime

- CA — Autoriteti i Certifikimit (Certification Authority)
- CMA — Autoriteti i Menaxhimit te Certifikatave (Certificate Management Authority)
- CP — Politika e Certifikates (Certificate Policy)
- CPS — Deklarata e Praktikave te Certifikimit (Certification Practice Statements)
- CRL — Lista e Certifkatave te Revokuara (Certificate Revocation List)
- DN — Emri i Vecante (Distinguished Name)
- DSS — Standarte te nënshkrimeve elektronike (Digital Signature Standard)
- FIPS — Federal Information Processing Standard
- FTP — File Transfer Protocol
- I&A — Identifikim dhe Autentifikim (Identification and Authentication)
- OID — Identifikuesi i Objektiti (Object Identifier)
- PIN — Numer Personal Identifikimi (Personal Identification Number)
- PKCS — Standarde te Certifiaktave me Celes Publik
- PKI — Infrastruktura me celes Publik (Public Key Infrastructure)
- RA — Autoriteti i Regjsitrimit (Registration Authority)
- LRA — Autoritet lokal Regjistrimi (Local Registration Authority)
- RSA — Rivest, Shamir, Adleman (algoritëm enkriptimi)
- S/MIME — Secure Multipurpose Internet Mail Extensions
- VPN — Virtual Private Network