Certificate Policy

Version 1.0

Përmbajtja

1 Hyrje

Infrastruktura me çelës publik e AKSHI (Agjencia Kombëtare për Shoqërinë e Informacionit) ka për qëllim të ofrojë zgjidhje (produkte dhe shërbime) për aplikime te sigurta kompjuterike dhe te rrjetit. Infrastruktura me çelës publik (PKI) përbëhet nga produkte dhe shërbime që ofrojnë dhe menaxhojnë certifikata dixhitale X. 509 për enkriptimin e çelësit publik.
Ky dokument paraqet Politikat e Certifikimit te cilat aplikohen ne Infrastrukturën me Çelës Publik te AKSHI.

2 Certifikatat

Certifikata identifikon personin e përcaktuar ne certifikate dhe i bashkëngjit këtij personi një çift çelësash publik/privat.
Ky dokument përcakton krijimin dhe menaxhimin e certifikatave me çelës publik X.509 Version 3 për përdorim në aplikimet që kërkojnë komunikim midis sistemeve të bazuar ne rrjetet kompjuterik. Aplikacione te tilla përfshijnë, por nuk kufizohen vetëm në:

- e-mail,
- transmetimi i informacionit të paklasifikuar,
- nënshkrimi i formave elektronike,
- nënshkrimin e dokumenteve elektronike dhe kontrata
- autentifikim i komponentëve të infrastrukturës të tilla si serverat Web, firewall, dhe routera.

Llojet e rrjeteve që përdorin këto produkte të sigurisë janë:

- Rrjetet e pambrojtur
- Rrjeti i brendshëm i AKSHI-t (Intranet AKSHI)
- Rrjeti i mbrojtur AKSHI-t

Autoriteti i Certifikimit AKSHI zbaton katër nivele besimi për certifikatat e lëshuara, në varësi të:

- Llojet e aplikimeve që mund të përdoren me këto certifikata.
- Lloji i entitet për të cilin certifikata është lëshuar (person ose pajisje)

- Metoda e mbajtjes së çelësit privat nga Abonenti - pajisje (SmartCard) ose skedar

2.1 Class 1 Digital Certificates

Certifikatat e lëshuara ne këtë nivel besimi janë të destinuara vetëm për individët. Ato mund të përdoren për të mbrojtur informacionin e paklasifikuar në të gjitha llojet e rrjeteve (publike, intranet AKSHI, të klasifikuara) në të gjitha llojet e aplikimeve. Çelësi privat krijohet ne pajisje (token) ose smartcard .

Politika e lëshimit te certifikatave me këtë nivel të besimit ka identifikuesin mëposhtme:
1.3.6.1.4.1.39148.10.1.1.1

2.2 Class 2 Digital Certificates

Certifikatat e lëshuara ne këtë nivel besimi janë të destinuara vetëm për individët. Ato mund të përdoren në të gjitha llojet e aplikimeve për të mbrojtur informacionin e ndjeshme, por te paklasifikuar në të gjitha llojet e rrjeteve (publike, intranet AKSHI, sekret), ose informacion sekret, por vetëm në rrjetet intranet te klasifikuar dhe rrjetin e brendshëm te organizatës. Çelësi privat krijohet në pajisje (token) ose smartcard.

Politika e lëshimit te certifikatave me këtë nivel të besimit ka identifikuesin mëposhtme:
1.3.6.1.4.1.39148.10.1.1.2

2.3 Class 3 Digital Certificates

Certifikatat e lëshuara në këtë nivel besimi janë të destinuara vetëm për pajisjet dhe serverat. Ato mund të përdoren në të gjitha llojet e aplikimeve për të mbrojtur informacionin e paklasifikuar në të gjitha llojet e rrjeteve (publike, intranet AKSHI, sekret).

Politika e lëshimit te certifikatave me këtë nivel të besimit ka identifikuesin mëposhtme:
1.3.6.1.4.1.39148.10.1.1.3

2.4 Class 4 Digital Certificates

Certifikatat e lëshuara në këtë nivel besimi janë të destinuara vetëm për pajisjet dhe serverat. Ato mund të përdoren në të gjitha llojet e aplikimeve për të mbrojtur informacionet e ndjeshme, por te paklasifikuara në të gjitha llojet e rrjeteve (publike, intranet AKSHI, sekret), ose me informacion sekret, por vetëm në rrjetet intranet te klasifikuar dhe rrjetin e brendshëm te organizatës.

Politika e lëshimit te certifikatave me këtë nivel të besimit ka identifikuesin mëposhtme:
1.3.6.1.4.1.39148.10.1.1.4

3 Pranimi i Certifikatës

Pranimi i certifikatës nga ana e Abonentit nënkupton se ai është dakord me si më poshtë:

- çdo nënshkrim dixhital i krijuar duke përdorur çelësin privat përkatës me çelësin publik të listuar në certifikatën dixhitale përfaqësojnë nënshkrimin digjital te Abonentit dhe certifikata e pranuar është funksionale (jo skaduar, pezulluar ose revokuar) në datën dhe kohën qe është përdorur nënshkrimi dixhital;
- Ne çelësin privat te Abonentit nuk kane qasje persona te paautorizuar;
- informacioni që përmbahet në certifikatë është e vërtetë;
- certifikata mund të përdoret vetëm për qëllime të autorizuara nga AKSHI;
- abonenti, si një përdorues fundor nuk mund të përdorë çelësin privat të tij përkatës me çelësin publik të listuar në certifikatë për të nënshkruar certifikata

të tjera ose listat e revokimit veçse në rastet kur kjo është shprehimisht e përcaktuar në kontratën e nënshkruar me Autoritetin e Certifikimit.

Me pranimin e certifikatës, Abonenti merr përgjegjësinë për kontrollin e çelësit te tij privat dhe duke marrë masa paraprake për të parandaluar humbjen, zbulimin, ndryshimin apo përdorimin e paautorizuar.

4 Shërbimi i certifikimit

Regjistrimi i kërkesës për certifikatë për një abonent përbehet nga një numër hapash të përshkruara në Deklaratën e Praktikave te Certifikimit (CPS):
• Vërtetimi dhe regjistrimi i identitetit te Abonentit
• Marrjen e një çifti çelësash, publike dhe private
• Verifikimin që çelësi publik ka një çelës privat çift në pronësi nga Abonenti
• Sigurimi i pikave të kontaktit për verifikimin e të gjitha roleve ose të autorizimeve të kërkuara nga Abonenti.

Një Abonenti mund të rinovojë certifikatën e tij dhe ky proces është përshkruar në Deklaratën e Praktikave te Certifikimit (CPS).

Certifikata e një abonenti mund të revokohet. Kushtet në të cilat një certifikate revokohet i referohet kompromet imit te çelësit privat te abonentit, ndryshimi i identitetit te abonentit dhe rrethanat e tjera që janë paraqitur në CPS. Certifikatat revokuara vendosen në listat e revokimit të certifikatave (CRL) deri në skadimin e tyre.

Për revokimin një certifikatë, përdoruesi duhet të ndjeke disa procedura të caktuara që janë përshkruar në CPS.

5 Marrësi

Marresi është një entitet që është duke përdorur certifikatën e tjetrit për të verifikuar integritetin e një mesazhi elektronik të nënshkruar, për të identifikuar cili krijoi mesazhin, ose të krijojë komunikim konfidencial me pronarin e certifikatës.

Marresi ka te nevojshme të verifikoje nënshkrimin dixhital lidhur me një dokument që ka marrë. Në procesin e verifikimit te një nënshkrimi dixhital krijuar duke përdorur një certifikatë të lëshuar nga infrastruktura me çelës publik e AKSHI-t duhet të përdorë procedurat dhe resurset e AKSHI.

6 Abonenti

Abonenti është entiteti emri i të cilit paraqitet si një subjekt në një certifikatë dhe pretendimet për të përdorur çelësin e saj në përputhje me Politikat e Certifikimit.

Është e detyrueshme për Abonentin të mbroje çelësin e tij privat, në përputhje me Deklaratën e Praktikave te Certifikimit (CPS). Ata duhet të raportojnë për ngjarjet e mëposhtme që mund të ndodhin gjatë periudhës së vlefshmërisë së certifikatës së tyre:

- çelësi i tij privat është kompromet uar, vjedhur apo humbur;
- kontrolli i çelësit privat është humbur apo kompromentuar (PIN)
- një pamjaftueshmëri ose dyshime në përmbajtjen e certifikatës

Abonenti do të pajtohet me të gjitha termat, kushtet dhe kufizimet mbi përdorimin e çelësave privatë dhe certifikatave të lidhura me ta.

Ai do të përdorë certifikatat e ofruara nga AKSHI vetëm për transaksionet që lidhen me aktivitetet ne rrjetin dhe ne aplikimet qe menaxhohen nga AKSHI.

7 Përditësimi i politikave të certifikimit

Politika rishikohet periodikisht, të paktën një herë çdo vit. Gabime, përditësime apo sugjerime për ndryshimin e këtij dokumenti do t'i komunikohet personave të kontaktit të caktuara për këtë qëllim. Çdo komunikim do të përfshijë një përshkrim të ndryshimit të kërkuar, një arsyetim dhe informatat kontaktuese për personin i cili ka kërkuar ndryshimin.

Të gjitha ndryshimet që janë në studim do të shpërndahen palëve të interesuara për një periudhë të paktën dy mujore.