9. Allkirjastamisseade ja selle valik

Õpikeskkond: Riigi Infosüsteemi Ameti juhendid
Kursus: X-tee turvaserveri administraatori õppematerjal
Raamat: 9. Allkirjastamisseade ja selle valik
Printija: Jan Raik
Kuupäev: kolmapäev, 26. august 2020, 11.29

Sisukord

9.1. Sissejuhatus

Käesolevas õppetükis kirjeldatakse nõudeid ja kriteeriume, mille alusel valida X-tee toodangukeskkonda sobiv allkirjastamisseade (kvalifitseeritud sertifikaadi aluseks olevate privaatvõtmete haldamise ja e-templite moodustamise seade). Õppetüki lõpus on toodud viited allikatele, millest leiad rohkem infot allkirjastamisseadmete kohta.

Õppetüki lõpetamise järel suudad Sa hinnata turul olevate allkirjastamisseadmete vastavust X-tee nõuetele ja nende sobivust enda vajadustele.

Õppetüki läbimiseks kulub Sul umbes 15 minutit.

9.2. Allkirjastamisseade

Iga X-tee liige peab toodangukeskkonnas e-templi moodustamiseks kasutama kvalifit-seeritud sertifikaate. Sertifikaatide ja nendega seotud privaatvõtmete käsitlemiseks vaja allkirjastamisseadet.

Allkirjastamisseade võimaldab tarkvaralise allkirjastamisega (nn *soft token*) võrreldes tagada e-templi moodustamiseks kasutatavate privaatvõtmete turvalisemat ja lihtsamat haldust.

Allkirjastamisseade on toodangukeskkonnas vajalik kõigil turvaserveritel ning seda rakendatakse väljuvate sõnumite e-tembeldamiseks. Test- ja arenduskeskkonnas ei ole riistvaraline seade kohustuslik, kuna seal ei ole vaja ka kvalifitseeritud sertifikaate.

Allkirjastamisseadet on vaja e-templi sertifikaadi privaatvõtme hoidmiseks. Turvaserveri autentimissertifikaadi privaatvõtit hoitakse *soft token*'il.

9.3. eIDAS määrus ja nõuded allkirjastamisseadmele

X-teel kasutatav e-tempel ei eelda põhimõtteliselt allkirjastamisvahendi kasutamist. Euroopa Parlamendi ja Nõukogu määrus nr 910/2014 (eIDAS määrus), mis sätestab tingimused usaldusteenustele ja digiallkirjastamise aspektidele, ei sätesta otsest nõuet X-teel kasutatavatele allkirjastamisseadmetele. eIDAS määrus kehtestab nõuded allkirjastamisseadmele juhul, kui tegemist on kvalifitseeritud e-templiga.

Kvalifitseeritud e-templi loomiseks tuleb kasutada kvalifitseeritud e-templi loomise vahendit (*qualified signature creation device, QSCD*), st füüsilist seadet, millel on **Common Criteria (CC) sertifikaat „Protection Profile SSCD jaoks“** (Standard EN 419 211, *Protection Profiles for secure signature creation and other related devices part 1–2*). Paraku on seadusandlus kvalifitseeritud e-templi moodustamise osas veel loomejärgus ning napib ka selleks sobilikku riistvara. Põhimõtteliselt sobib X-teel kasutamiseks ka kvalifitseeritud e-templi sertitifkaat.

X-tee v6 e-tempel on eIDAS määruse mõttes täiustatud e-tempel kvalifitseeritud sertifikaatidega. Levinud praktika kohaselt väljastavad kvalifitseeritud usaldusteenuste osutajad seda tüüpi sertifikaate seadmetele, mis on mõeldud privaatvõtmete haldamiseks. Täpsemad nõuded on ära toodud **sertifitseerimisteenuse osutaja e-templi sertifitseerimise poliitikas** (*Certification Policy, CP*). Näiteks AS Sertifitseerimiskeskuse puhul on tarvilik kasutada seadet, mis omab kas:

- Common Criteria sertifitseeringut vastavalt EN standardile 419 211 võI
- FIPS 140-2 teise või kõrgema taseme sertifitseeringut.

Kuna seadmeid ja tootjaid on erinevaid ning eri seadmed vastavad eri standarditele, siis tuleks enne ostu veenduda, et allkirjastamisvahend toetaks valitud usaldusteenuste osutaja poolt kehtestatud nõudeid.

Allkirjastamisseadme ühendamiseks turvaserveriga kasutatakse PKCS#11 protokolli.

Suhtlus toimib üldjuhul küll PKCS#11 protokolli järgi, kuid selle kohta, kas seade on X-teega ühendatav, on kõige kindlam küsida kinnitust tootjalt või edasimüüjalt.

9.4. Allkirjastamisseadme sobivuse hindamine

Allkirjastamisseade tuleb ise valida. Turul on mitmeid allkirjastamisseadmeid. Neid on kolme tüüpi:

- USB siinil töötavad seadmed (kõige odavam, madala või keskmise jõudlusega),
- PCI siinil töötavad seadmed (keskmise hinnaga, ent kõrge jõudlusega; ei sobi virtualiseeringu korral),
- NetHSM ehk võrgupõhised allkirjastamisseadmed (kõige kallim, mugav kasutada mitme turvaserveri või mitme kliendi korral).

PCI

USB

NETHSM

Valiku tegemisel hinda toote sobivust järgmiste parameetrite lõikes:

1. Turvaserverite arv
2. Seadmes hoitavate võtmete arv
3. Latents
4. Seadme sobivus virtuaalkeskkonnaga
5. Seadme klassifikatsioon FIPS standardile vastavalt

Allpool käsitletakse nimetatud parameetreid ükshaaval põhjalikumalt.

9.5. Turvaserverite arv

Kas soovite seadet kasutada paralleelselt mitme turvaserveri tarbeks?

Kui osapooli, kellega infot vahetatakse, on vähe, kui turvaservereid on vähe või kui käideldavusnõuded ei eelda kiiret reageerimist, siis on lihtsamate konfiguratsioonide puhul otstarbekas kasutada USB-siinil töötavaid seadmeid. Võimalik on ühendada iga turvaserveriga oma USB-token ning kõigile turvaserveritele soetada oma autentimissertifikaat.

Suure arvu turvaserverite puhul võib olla otstarbekas kasutada võrguseadet.

9.6. Seadmes hoitavate võtmete arv

Kui mitu sertifikaati ja privaatvõtit soovite allkirjastamisseadmes hoida?

Seadmes hoitavate võtmete arv sõltub turvaserveris majutatud klientide arvust. Iga turvaserverit kasutava X-tee liikme kohta peab hoidma üht e-templi sertifikaadi privaatvõtit.

Mitme turvaserveri kasutamise puhul on sama e-templi sertifikaati võimalik kasutada mitmel turvaserveril samaaegselt. Sama käib NetHSM seadme kohta.

Turvaserveri autentimissertifikaat peab olema tarkvara seifis (*soft token*). Seda ei ole võimalik hoida allkirjastamisvahendil.

9.7. Latents

Kui suur on allkirjastamisel lubatav lisanduv viivitusaeg ehk latents?

Optimaalseima seadme valikule aitab kaasa see, kui analüüsite, milline latents on teie andmeteenuste jaoks aktsepteeritav.

Keskmine latents on eri tüüpi seadmetel järgmine:

- USB siinil töötavad seadmed: 0,5 sekundit
- PCI siinil töötavad seadmed: 0,1 sekundit
- NetHSM seadmed: 0,01 sekundit

Oluline on mõista latentsi tähtsust nii oma infosüsteemi kui ka selle kasutajate seisukohast. Inimkasutajast sõltumatult toimuva täisautomaatse andmevahetuse puhul (näiteks päringu puhul lemmikloomade registrisse) ei juhtu ilmselt midagi, kui vastuse laekumiseks kulub sekundites mõõdetav aeg. Piiriületusel passikontrollis võib aga juba sekundiline latents mõjutada väga paljusid kasutajaid. Ka infosüsteemidel võivad olla oma nõuded selle kohta, mis aja jooksul peab vastus kohale jõudma.

9.8. Seadme sobivus virtuaalkeskkonnaga

Kas seade töötab virtuaalkeskkonnaga (kui plaanite turvaserveri paigaldada virtuaalkeskkonda)?

Seadme valiku juures võib olla määrav see, kuidas operatsioonisüsteem pääseb seadmele ligi. Kui soovid virtualiseerimist kasutada, veendu, et see toetab soovitud seadet. PCi seadmel töötavaid seadmeid pole virtuaalkeskkondades võimalik kasutada. USB-seade ei pruugi olla virtuaalkeskkonna jaoks mugavaim, ehkki see on kasutatav. Üle võrgu ligipääsetav seade ei sea piiranguid, kuid on kõige kulukam lahendus.

9.9. Seadme klassifikatsioon FIPS standardile vastavalt

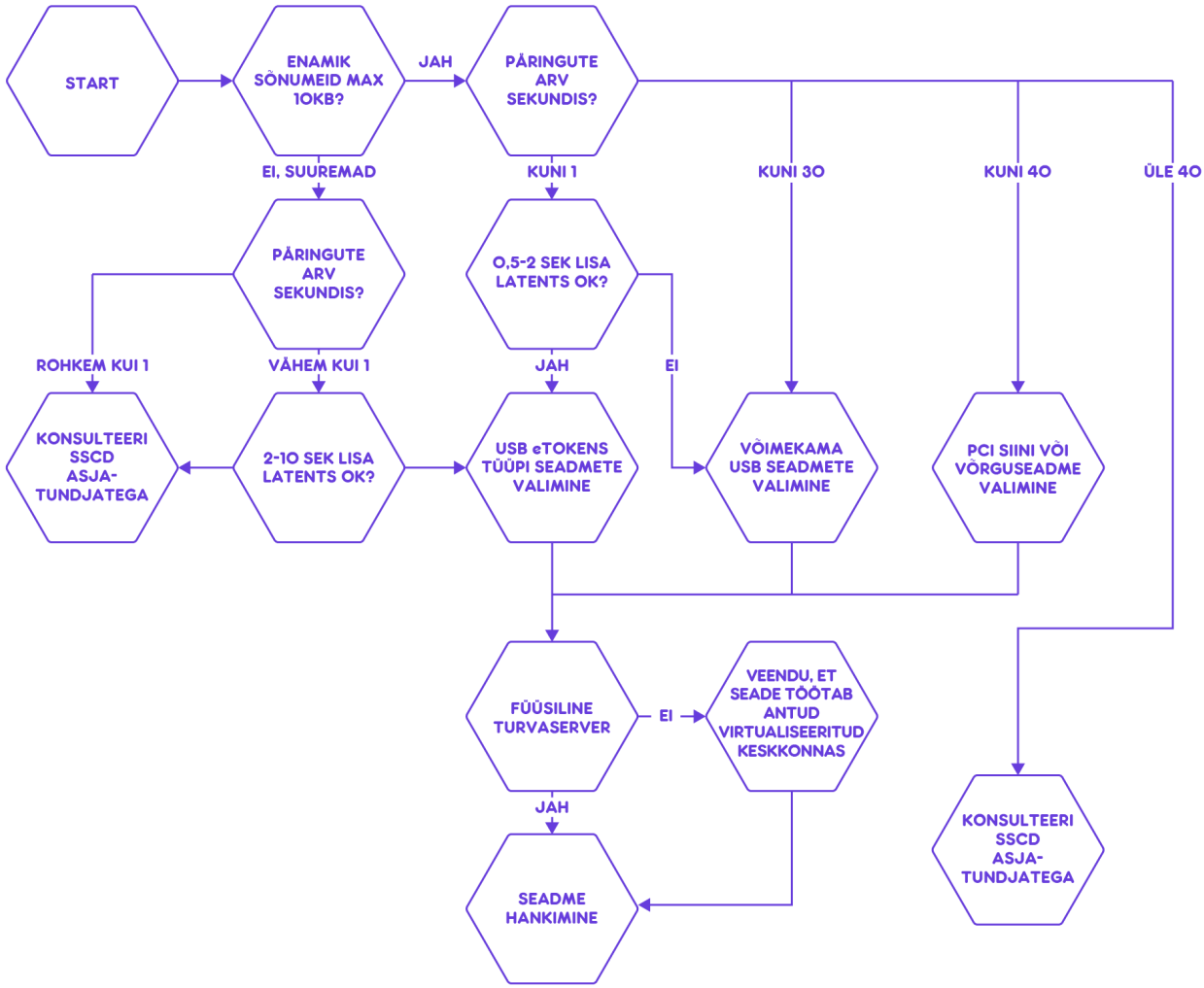
Kuigi X-tee ei nõua e-templi sertifikaadi saamiseks otseselt allkirjastamisseadet, tuleneb see nõue sertifitseerimisteenuse osutajate igapäevasest praktikast. Eestis registreeritud sertifitseerimisteenuse osutaja, AS Sertifitseerimiskeskuse sertifitseerimispoliitika järgi peab privaatvõti paiknema selleks mõeldud seadmel. Seadme nõuetekohasust näitab Common Criteria sertifitseering vastavalt standardile EN 419 211 või FIPS 140-2 Level 2 taseme sertifitseering.

Seetõttu on oluline tuvastada toode spetsifikatsioonis tase, millele toode FIPS standardi järgi vastab. Kui hindate oma asutuse vajadusi seoses võtmete haldamisega ja leiate, et allkirjastamisvahendit on võimalik kasutada ka muude oluliste funktsioonide täitmiseks, siis tasub nende võimaluste osas konsulteerida seadmete maaletoojate ja edasimüüjatega. FIPS tasemed aitavad teil valida seadet vastavalt teie organisatsiooni vajadustele ja teenuste kriitilisusele.

Loe FIPS standardi 140-2 kohta lähemalt siit.

9.10. Allkirjastamisseadme valiku protsess

Alltoodud skeem aitab Sul teha valikut allkirjastamisseadme kohta sõnumite suuruse, päringute arvu ja latentsi alusel.



Allkirjastamisseadme valik sõnumite suuruse, päringute arvu ja latentsi alusel

9.11. Hind

Allkirjastamisseadme kasutamise kulud sõltuvad mitmetest teguritest.

Omaenda turvaserverit kasutav X-tee liige saab üldjuhul hakkama USB-tokeni laadse allkirjastamisseadmega, mis maksab 50-100 eurot.

Kui plaanite kasutada mitut turvaserverit, hoida mitme liikme sertifikaate või vahendada teenuseid üliväikese latentsusega, siis on teil otstarbekas kasutada NetHSM kategooria seadmeid, mille hinnad jäävad vahemikku 10 000 kuni 50 000 eurot.

9.12. Abimaterjal

Allkirjastamise seadmete kohta põhjalikuma info saamiseks konsulteerige tootjate kasutusjuhenditega.

Allkirjastamise seadmed, mida on hinnatud X-tee kasutatavuse osas on loetletud siin. Enne konkreetse seadme hankimist palume kontrollida seadme tarnija ja sertifikaadi väljastaja käest seadme sobivust.

Mõningate seadmete osas on ära toodud näpunäiteid nende X-tee turvaserveriga ühendamiseks. Materjalid on leitavad siit.

Kui olete otsustanud paigaldada seadme, mida seal ei ole veel kirjeldatud, siis palume teil edastada info oma paigaldamiskogemuse kohta ka RIAle (help@ria.ee), et teistelgi oleks enda valiku tegemisel rohkem informatsiooni.

9.13. Küsimused

Õppetüki lõpetamiseks otsusta palun, kas alltoodud väited on tõesed või väärad.

A. Riistvaraline allkirjastamisseade tagab suurema turvalisuse kui tarkvaraline allkirjastamine.
B. Kui keskkonnas on mitu turvaserverit, siis tuleb valida võrguseade, mis suudab hoida enam kui kahte sertifikaati.
C. Virtuaalkeskkonna puhul tuleb vältida PCI siinil toimivaid seadmeid.

Õigeid vastuseid vaata siit (avanevad uues aknas).

9.14. Kokkuvõte

Toodangukeskkonnas on allkirjastamisseade vajalik kõigil turvaserveritel nii päringu- kui ka vastussõnumite e-tembeldamiseks. Test- ja arenduskeskkonnas ei ole riistvaraline krüptoseade kohustuslik.

Allkirjastamisseadme sobivust tuleks muuhulgas hinnata selle järgi, kui mitu võtit see mahutab, kui suur on allkirjastamisel lubatav viivitusaeg ehk latents ning kas seade sobib virtuaalkeskkonnaga.

Soovitud allkirjastamisseade peab vastama usaldusteenuste osutaja nõuetele, kui usaldusteenuse osutaja on oma sertifitseerimise poliitikas nõudeid täpsustanud.