KINNITATUD
Riigi Infosüsteemi Ameti peadirektori
02.06.2016. a
käskkirjaga nr 1.1-2/16-090

# Infosüsteemide andmevahetuskihi usaldusteenuste tingimused

Riigi Infosüsteemi Amet on välja töötanud tingimused, mida tuleb infosüsteemide andmevahetuskihi (edaspidi X-tee) usaldusteenuste pakkumisel järgida kasutades X-tee sõnumiprotokolli versioon 4 toetavat Eesti X-teed. Tingimused on kehtestatud ajatempliteenusele, turvaserveri autentimissertifikaadile, X-tee liikme e-templi sertifikaadile ja sertifikaadi kehtivuskinnituse (OCSP) teenusele.

Nende tingimuste järgimine on oluline, et andmete X-tee vahendusel liigutamisel oleks tagatud andmete käideldavus, terviklus ja konfidentsiaalsus.

## 1. Tingimused ajatempliteenusele

1.1. X-teel liikme poolt kasutatav ajatempliteenus peab väljastama kvalifitseeritud e-ajatempeleid Euroopa Parlamendi ja nõukogu 23. juuni 2014. a määruse nr 910/2014 „E-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93 EÜ“ tähenduses.

1.2. X-teel liikme poolt kasutatav ajatempliteenus:
- 1.2.1. peab toetama IETF standardis RFC 3161 kirjeldatud ajatempliprotokolli;
- 1.2.2. peab toetama transpordiprotokollina HTTP-d ning POST-päringut;
- 1.2.3. peab päringutes toetama SHA-256 või sellest tugevama räsialgoritmi kasutamist;
- 1.2.4. peab kasutama ajatemplite signeerimiseks sertifikaati, millel on seatud *key usage* väli *id-kp-timeStamping* (1.3.6.1.5.5.7.3.8);
- 1.2.5. ei tohi ajatempli päringutes nõuda ajatempli poliitika välja (*reqPolicy*) kasutamist;
- 1.2.6. peab vastuste signeerimiseks kasutama signatuurialgoritmi RSA võtmepikkusega vähemalt 2048 bitti ning vähemalt SHA-256 või sellest tugevama räsialgoritmi kasutamist;
- 1.2.7. tohib erineda UTC ajast kuni 1 sekund;
- 1.2.8. ei tohi olla järjestikuselt katkenud (planeeritult või planeerimata) rohkemaks kui neljaks tunniks.
- 1.2.9. Ajatembelduseks kasutatava sertifikaadi kehtivus tohib olla maksimaalselt viis aastat.

## 2. Tingimused turvaserveri autentimissertifikaadile

2.1. Turvaserveri autentimissertifikaat (*authentication sertificate of security server*) – kvalifitseeritud usaldusteenuse osutaja poolt väljastatud ja turvaserveriga seotud sertifikaat, mis tõendab turvaserveri autentsust ja mida kasutatakse turvaserverite autentimiseks turvaserverite vahelise ühenduse loomisel.
2.2. Sertifikaat peab vastama IETF standardile RFC 5280.
2.3. Sertifikaadi kehtivuse kontrollimine peab olema võimalik punktis 4 kirjeldatud nõuetele vastavalt.
2.4. Sertifitseerimisteenuse osutaja peab:

2.4.1. vastu võtma PKCS#10 sertifitseerimispäringuid (*.p10* või *pem* vormingus);
2.4.2. toetama sertifikaatide väljastamist RSA avalikele võtmetele pikkusega vähemalt 2048 bitti;
2.4.3. sertifikaatide allkirjastamiseks kasutama signatuurialgoritmi RSA võtmepikkusega vähemalt 2048 bitti ning SHA-256 või tugevamat räsialgoritmi.

2.5. Autentimissertifikaatide väljastamisel tuleb kasutusvaldkonnana märkida vähemalt üks järgmisest loetelust: *digitalSignature, keyEncipherment* või *dataEncipherment*. Alternatiivina võib laienduse *extended key usage* väärtuses sisalduda väärtuseid *ClientAuthentication* või *ServerAuthentication.* Autentimissertifikaatide väljastamisel ei tohi kasutada kasutusvaldkonda *nonRepudiation.*

2.6. Turvaserveri autentimissertifikaati võib kasutada sertifikaadi kehtivusaja lõpuni või sertifikaadi kehtetuks tunnistamiseni. Sertifikaadi kehtivuse peatamise korral on keelatud sertifikaadi kasutamine sertifikaadi kehtivuse peatatuse lõpetamiseni.

## 3. Tingimused X-tee liikme e-templi sertifikaadile

3.1. Liikme e-templi sertifikaat – kvalifitseeritud sertifitseerimisteenuse osutaja poolt täiustatud või kvalifitseeritud e-templi loomiseks väljastatud ja liikmega seotud e-templi kvalifitseeritud sertifikaat, mida kasutatakse vahendatavate sõnumite tervikluse tõendamiseks ning tõendamaks liikme seost sõnumiga.

3.2. E-templi sertifikaat peab vastama kvalifitseeritud sertifikaadi nõuetele Euroopa Parlamendi ja nõukogu 23. juuni 2014. a määruse nr 910/2014 „E-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93 EÜ“ tähenduses. Sertifikaat peab vastama IETF standardile RFC 5280.

3.3. Sertifikaadi kehtivuse kontrollimine peab olema võimalik vastavalt punktis 4 kirjeldatud nõuetele.

3.4. Sertifitseerimisteenuse osutamise poliitika peab:
3.4.1. võimaldama vastu võtta PKCS#10 sertifitseerimispäringuid (*.p10* või *pem* vormingus);
3.4.2. toetama sertifikaatide väljastamist RSA avalikele võtmetele pikkusega vähemalt 2048 bitti;
3.4.3. määrama sertifikaadi kasutusvaldkonnana *(key usage*) väärtuse *nonRepudiation.*
3.4.4. sertifikaatide allkirjastamiseks kasutama signatuurialgoritmi RSA võtmepikkusega vähemalt 2048 bitti ning SHA-256 või tugevamat räsialgoritmi.
3.4.5. tagama kvalifitseeritud e-templi loomiseks kasutatava sertifikaadi puhul privaatvõtme paiknemise riistvaralisel turvalisel allkirja andmise vahendil ehk *Qualified Signature Creation Device* Euroopa Parlamendi ja nõukogu 23. juuni 2014. a määruse nr 910/2014 „E-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93 EÜ“ tähenduses;
3.4.6. tagama täiustatud e-templi loomiseks kasutatava sertifikaadi puhul privaatvõtme turvalise haldamise;

3.5. Kui kasutatakse keskuse poolt pakutavat turvaserveri tarkvara, peab turvalise allkirja andmise vahendit olema võimalik turvaserveriga ühendada kasutades PKCS#11 protokolli.

3.6. E-templi sertifikaati võib kasutada sertifikaadi kehtivusaja lõpuni või sertifikaadi kehtetuks tunnistamiseni. Sertifikaadi kehtivuse peatamise korral on keelatud sertifikaadi kasutamine sertifikaadi kehtivuse peatatuse lõpetamiseni.

## 4. Tingimused sertifikaadi kehtivuskinnituse (OCSP) teenusele

4.1. Sertifikaadi kehtivuskinnituse teenus peab:
  4.1.1. vastama IETF standardile RFC 6960 või RFC 2560;
  4.1.2. kasutama signatuurialgoritmi RSA võtmepikkusega vähemalt 2048 bitti ning SHA-256 või tugevamat räsialgoritmi.

4.2. Sertifikaadi kehtivuskinnituse teenuse lubatud järjestikuse katkestuse maksimaalne kestus on 4 tundi ning summaarne seisak ööpäevas ei tohi ületada 12 tundi.

## 5. Üleminekusätted

5.1. Kuni 30.06.2016 väljastatud turvaserveri autentimissertifikaati või e-templi sertifikaati võib kasutada sertifikaadi kehtivusaja lõpuni või sertifikaadi kehtetuks tunnistamiseni.

5.2. Kuni 30.06.2016 võib X-teel kasutatav ajatempliteenus väljastada kvalifitseeritud ajatempleid digitaalallkirja seaduse tähenduses.