RIIGI INFOSÜSTEEMI AMET

CYBERNETICA

smit

Eesti e-riigi alustaristu kvantarvutikindlaks muutmine Rahvastikuregistri näitel

Aruande kokkuvõte

Version 1.0
08.10.2026
D-16-1309
Avalik

Sisukord

1 Aruande kokkuvõte 3
1.1 Kvantoht ja rahvastikuregistri infosüsteem 3
1.2 Ülemineku põhjendatus 4
1.3 Kutse tegevusele 4
1.4 Tulemused 5
1.5 Õppetunnid 5

2 Tegevuskava 7

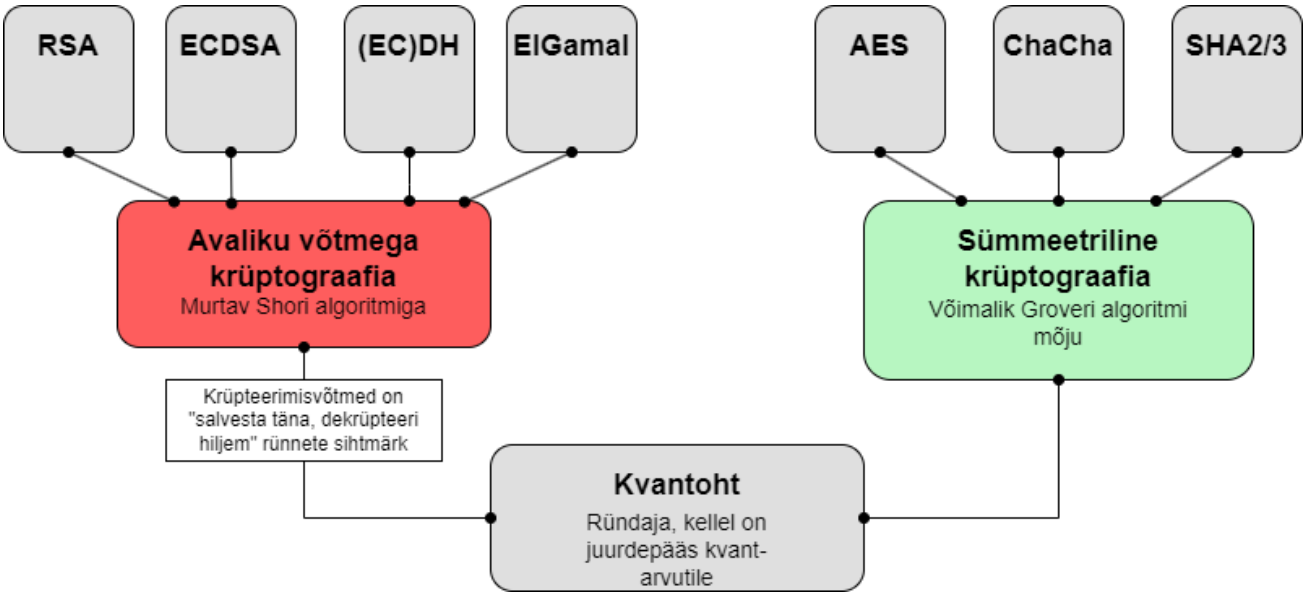
A Postkvant-krüptograafiale ülemineku käsiraamat 14
A.1 Kõrge riskiga komponentide tuvastamine 14
A.2 Olemasolevate postkvant-algoritmide sobivus 15
A.3 Tehnilised nõuded uutele postkvant-krüptograafilistele algoritmidele 16
A.4 Hübriidrežiimid 20
A.5 Üleminekumudelid 22
A.6 Postkvant-krüptograafiale üleminekut käsitlevad standardid ja juhised 24

1 Aruande kokkuvõte

See aruanne analüüsib Eesti rahvastikuregistri infosüsteemi, otsides vastust küsimusele, millisel viisil võivad seda tulevikus mõjutada kvantarvutuse arendamisest krüptograafiale tulenevad ohud.

1.1 Kvantoht ja rahvastikuregistri infosüsteem

Kvantarvutuse kiire areng tõotab tuua murrangulisi uuendusi valdkondades nagu ravimiarendus ja komplekssüsteemide optimeerimine, kuid kujutab samal ajal endast **olulist ohtu tänapäevasele küberturbele.** Kvantsüsteemidel on teoreeriline võime murda praeguseid sidet, finantstehinguid ja digitaalidentiteete turvavaid krüptograafilisi standardeid (vt joonis 1). Ehkki selleks võimelisi nn krüptograafiliselt märgilisi kvantarvuteid (*cryptographically relevant quantum computer*) seni veel ei eksisteeri, annab kvantbittide arvu järjepidev suurenemine kvantarvutites põhjust eeldada, et ohtlik lävi ületatakse juba lähiaastatel.



Joonis 1. Kvantohu ülevaade

Kujuneva olukorra lahendamiseks veab USA riiklik standardimis- ja tehnoloogiainstituut NIST 2016. aastast postkvant-krüptograafia väljatöötamisele ja juurutamisele suunatud ülemaailmset standardimistööd. Järgmise põlvkonna krüptoalgoritmid, mida nimetatakse postkvant-algoritmideks, on konstrueeritud selliselt, et need kaitseksid nii klassikaliste kui ka kvantarvutitega sooritatavate rünnete eest ning tagaks seeläbi digitaalse taristu pikaajalise turbe ja võltsimiskindluse ka küpse kvanttehnoloogia tingimustes.

Kuivõrd Rahvastikuregistri infosüsteem kasutab tundlike andmete kaitseks krüptograafilisi vahendeid, tuleb selle turvalisuse tagamiseks strateegiliselt hinnata üleminekuviise postkvant-krüptograafiale. Üleminek postkvant-standarditele peab olema põhjalikult läbi mõeldud, et tagada süsteemi maksimaalne turvalisus ning minimeerida samal ajal häiringuid selle toimimises.

1.2 Ülemineku põhjendatus

Ettevõtlus- ja avaliku sektori sidusrühmad peaks postkvant-krüptograafiale (*post-quantum cryptography*, PQC) üleminekut käsitlema mitte krüptograafiliste süsteemide teoreetilise parenduse, vaid pigem strateegilise kindlustuspoliitikana, mis aitab säilitada pikaajalises perspektiivis andmete konfidentsiaalsust ja vastavust õigusnormidele. Üleminekueelarve heakskiitmise eelduseks on, et otsustajad mõistavad järgmisi asjaolusid.

- **Eksisteeriv risk („salvesta täna, dekrüpteeri hiljem")**: kodanike registriandmete konfidentsiaalsus peab püsima aastakümneid. Postkvant-krüptograafia kasutuselevõtu edasilükkamine tähendab, et hästi korraldatud ülemineku asemel riskitakse viimasel minutil paanilise rapsimisega, mis seab ohtu nii ressursid kui ka maine.
- **Normatiivne ja vastavussurve**: nii riiklikud kui ka rahvusvahelised normatiivraamistikud (NIS-Ti standardid, ENISA suunised, ELi direktiivid) nõuavad järjest enam kvantkindluse tagamist. Proaktiivne lähenemine aitab vältida audititrahve, tagab piiriülese koostalitusvõime ning võimaldab postkvant-krüptograafiat käsitleda vastavuspõhise riskileevendusmeetmena.
- **Valdkondlik pretsedent**: postkvant-krüptograafia varane kasutuselevõtt võimaldab Rahvastikuregistril end positsioneerida riiklike digiteenuste vallas kerkse partnerina ning vältida tulevikus ühilduvusprobleeme väliste APIde ja partneritega.
- **Hetkeolukord tarnijate ja hangete vaatenurgast**: PQC-valmis vahetarkvara, füüsilised turvamoodulid ja protokollivirnad on peagi tootmisvalmis, kuid sertifitseerijate ja tarneahelate täitmisajad ulatuvad mitmest kuust mitme aastani. Varajased eelarveeraldised võimaldavad struktureeritud koostööd tarnijatega, aitavad vältida kiirustades koostatud hankeid ning vormistada lepingute kujul PQCle ülemineku tegevuskavad.
- **Ülemineku ajakavad**: ülemineku realistlik ajakava, mis hõlmab riskihindamist, hübriidrežiimis juurutamist, testimist ja lõplikku väljalaskmist, on mitmeaastane. Viivitused ülemineku rahastamisega kärbivad testimiseks jäävat aega, suurendavad lõimimisriske ning muudavad vältimatuks kulukate erakorraliste üleminekumeetmete kasutamise. *Rahvastikuregistri ülemineku ajakava on esitatud jaotises 2 konkreetsete tegevuste loendina.*

Rahvastikuregistri juhtkond peaks postkvant-krüptograafiale üleminekut käsitlema tegevuskestlikkusele suunatud algatusena, kehtestama konkreetseid verstaposte ja eelarvelisi vajadusi sisaldava kvantvalmisoleku tegevuskava ning määrama positsioonideülese migratsioonijuhi, kelle ülesanne on hallata koostööd infoturbe, hangete, vastavuse ja partnerluse valdkondade sidusrühmadega. Ülemineku varajane ja läbipaistev rahastamine võimaldab hallata uue süsteemi väljalaskmise riske ja süsteemi pidevalt valideerida.

1.3 Kutse tegevusele

Vastavalt jaotises 2 esitatud soovituslikule tegevusplaanile kutsume keskseid otsustajaid üles viivitamatult käivitama postkvant-krüptograafiale ülemineku protsessi (vt viidatud tegevusplaan). Tegevusplaani punkti R.0 soovituslik täitmisaeg on 2026. a. IV kvartal ja R.1 täitmisaeg – 2027. a. I kvartal.

> ***R.0: aruande kokkuvõtte läbilugemine.*** *Posktvant-krüptograafiale ülemineku protsessi käivitamiseks peavad kesksed otsustajad lugema läbi aruande jaotise 1.*
>
> ***R.1: üleminekujuhi määramine.*** *Postkvant-krüptograafiale üleminekut peab koordineerima selleks määratud üleminekujuht. Leidke selleks oma organisatsioonist üks või mitu piisavate tehniliste, ostu- ja juhtimisalaste võimetega (ja õigustega) isikut.*

Tegevusplaani järgmised punktid peab ellu viima määratud üleminekujuht (vajaduse korral koos meeskonnaga) ajavahemikus 2027–2030 ning jätkama seejärel ajavahemikus 2031–2035 pideva seiretegevusega.

1.4 Tulemused

Selle projekti eesmärk oli tuvastada Rahvastikuregistri infosüsteemis postkvant-krüptograafiale ülemineku peamised objektid. Järgmises alajaotises (jaotis 1.5) käsitletavad asjaolud

ei võimalda meil aga garanteerida, et komponentide loetelu on täielik. Eeldame siiski, et Rahvastikuregistri süsteemiadministraatorid suudavad asutusesisesele teadmusele tuginedes infosüsteemi täielikult ja süstemaatiliselt üle viia postkvant-krüptograafiale. Seetõttu on siinse aruande fookuses pigem üldised postkvant-krüptograafiale üleminekuga seotud juhised, üleminekustrateegia valikuga seotud kaalutlused ning ülemineku tegevusplaani koostamine leidude ja muude soovituste põhjal.

Aruande põhiline järeldus on siiski, et Rahvastikuregistri üleviimisega postkvant-krüptograafiale tuleb alustada niipea kui võimalik; esimeseks sammuks peab seejuures olema üleminekujuhi määramine. Enamik süsteemis tuvastatud krüptograafilisi komponente põhineb kolmandate tarnijate lahendustel. Seetõttu on eduka ülemineku eelduseks ennetav kommunikatsioon tarnijatega ja selge uuendusplaani kehtestamine.

1.5 Õppetunnid

See alajaotis võtab kokku töörühmasisesed järeldused mahukate süsteemide postkvant-krüptograa-fiale üleminekuks ette valmistamise kohta.

- Ehkki väline postkvant-ülemineku spetsialist võib täita olulist rolli protsessi suunamisel, vigade vältimisel ja riskide leevendamisel, vastutab ülemineku eest siiski spetsialisti kaasanud organisatsioon. See tähendab, et ülemineku jaoks tuleb moodustada eraldi meeskond, kellele tagatakse vajalikud vahendid, sh piisavad aja- ja finantsressursid.
- Teadlikkus postkvant-krüptograafia olemusest on seni veel algjärgus. Tulevastesse projektidesse tuleb seda arvesse võttes lülitada sissejuhatavad seminarid postkvant-krüptograafiast ja kvantohust. Niisugused algatused aitavad luua ühist teadmusbaasi ja sõnavara ning tagada kogu projekti vältel informatsiooni sujuvama liikumise.
- Motivatsioon üleminekuks postkvant-krüptograafiale on siiani kasin. Selle puudujäägi likvideerimine kattub üldisemate postkvant-krüptograafia alaste teadmiste levitamise sihiga, mis suurendab veelgi sissejuhatavate seminaride ja õppematerjalide väärtust. Siiski tuleb selgelt eristada kahe teema sihtauditooriume. Tippjuhte ja olulisi sidusrühmi motiveerivad teised ajendid kui üleminekut kokkuvõttes läbi viivaid arendajaid, administraatoreid ja tehnikuid. Oluline on mõlemate rühmade kaasamine ning ülemineku vajalikkuse ja aktuaalsuse selge põhjendamine.
- Täieliku krüptovarade loendi koostamine nõuab juurdepääsu organisatsiooni infosüsteemidele ja koodihoidlatele, aga ka põhjalikke teadmisi organisatsiooni IT-taristust. See nõuab tõenäoliselt koostööd mitme töörühmaga, kes vastutavad erinevate teenuste eest.
- Organisatsiooni teadmised oma infosüsteemidest võivad olla üllatavalt piiratud. Seetõttu võib andmete kogumine süsteemi arhitektuuri kohta – isegi väljaspool puhtalt krüptograafia valdkonda – nõuda oodatust rohkem aega.
- Postkvant-krüptograafia alase teadlikkuse kasvades hakatakse seda järjest enam ära kasu-

tama turunduslikes huvides. Organisatsioonid peavad seetõttu hoolikalt hindama kõiki tarnijate väiteid, kuivõrd postkvant-krüptograafiaga seotud teabe hulk kasvab järjepidevalt – ja mitte kogu teave ei ole alati täpne. Toetumine kontrollimata või väärale teabele võib tekitada tõrkeid üleminekuprotsessis.

2 Tegevuskava

See jaotis esitab üleminekuplaani koos konkreetsete tegevussammudega. Sammud on üle võetud otse riiklikust postkvant-krüptograafiale ülemineku tegevuskavast [1] ja kohandatud Rahvastikuregistri süsteemile.

> **NB:** *allpool esitatud ajakava järgib üldjoontes riiklikku teekaarti. Hiljutised edusammud kvantarvutuse vallas on aga ajendanud suuri tehnoloogiaettevõtteid kiirendama üleminekut postkvant-krüptograafiale.*[1] *Seetõttu soovitame lugejatel tutvuda valdkonna hetkeseisuga ning kaaluda oma ajakavade kohandamist, arvestades võimalusega, et krüptograafiliselt märgiline kvantarvuti võib ilmuda prognoositust varem.*

Tabel 1 toob välja ja võtab kokku tegevussammud koos iga sammu läbiviimiseks tuvastatud ajaraami ja vastutajaga. Samme kirjeldatakse veelgi üksikasjalikumalt allpool.

Tabel 1. Rahvastikuregistri postkvant-krüptograafiale ülemineku tegevuskava

ID	Tegevussamm	Ajavahemik	Vastutaja
R.0	Lugeda läbi selle aruande kokkuvõte	IV 2026	Kesksed otsustajad
R.1	Määratleda üleminekurollid	I 2027	Kesksed otsustajad
R.2	Määratleda üleminekukategooria	I 2027	PQC-ülemineku juht
R.3	Tutvuda ajakavaga seotud riskidega	I 2027	PQC-ülemineku juht
R.4	Tutvuda riikliku tegevuskavaga	I–II 2027	PQC-ülemineku juht
R.5	Hinnata krüptograafilist küpsust	II 2027	PQC-ülemineku juht
R.6	Võtta ühendust allsüsteemide tarnijatega	2027	PQC-ülemineku juht
R.7	Koostada krüptoinventuur	2027–2028	PQC-ülemineku juht
R.8	Viia ellu lühiajalised meetmed	2028	IT ja infoturbe meeskonnad
R.9	Postkvant-krüptograafia lõimimine	2029–2030	Arendajad ja süsteemiadministraatorid
R.10	Pidev seire ja uuendamine	2031–2035	PQC-ülemineku juht

R.0. Lugeda läbi selle aruande kokkuvõte. Üleminekuprotsessi käivitamiseks peavad kesksed otsustajad lugema läbi selle aruande kokkuvõtte.

R.1. Määratleda üleminekujuht. PQCle üleminekuks on vaja selget juhtisikut. Leidke oma organisatsioonist üks või mitu piisavate tehniliste, ostu- ja juhtimisalaste võimetega (ja volitustega) isikut. Rollide kirjeldusi vt riiklikust tegevuskavast.

paragraphR.2. Määratleda organisatsiooni üleminekukategooria. Organisatsiooni administraatorid ja/või kesksed otsustajad võiksid läbida enesekategoriseerimisprotsessi, kuna nemad tunnevad oma süsteemi kõige paremini. Juhiseid selle kohta vt riikliku teekaardi samm SC.1.

[1] Google: https://blog.google/innovation-and-ai/technology/safety-security/cryptography-migration-timeline/; Cloudflare: https://blog.cloudflare.com/post-quantum-roadmap/

R.3. Tutvuda ajakavaga ja ülemineku viibimisega seotud riskidega. Lähemalt vt riikliku tegevuskava samme SC.2 ja SC.3.

R.4. Tutvuda riikliku tegevuskavaga. Üleminekujuht peaks tutvuma riikliku tegevuskavaga tervikuna.

R.5. Hinnata krüptograafilist küpsust. Igal organisatsioonil on palju organisatsioonilisi kitsaskohti. Üleminekujuht peaks mõtlema krüptograafia halduse praegusele tasemele. Täpsemalt vt riikliku tegevuskava samm OP.2.

R.6: Tuvastada ja võtta ühendust allsüsteemide tarnijatega. Organisatsioon peaks tuvastama oma allsüsteemide tarnijad. Vajaduse korral peaks üleminekujuht nende tarnijatega ühendust võtma ning uurima nende postkvant-krüptograafiale ülemineku tegevus- ja ajakavade kohta. Täpsemalt:

1. uurida võimalikke postkvant-krütpograafia toega HSMide variante ja algatada hankeprotsess;
2. kontrollida tarnijate tegevuskavasid, et hinnata tarnija toote või teenuse postkvant-krüptograafilist küpsust. Kasulik metoodika tarneahela kvantriski haldamiseks on PKI Consortiumi välja töötatud postkvant-krüptograafilise küpsuse mudel[2] See kirjeldab teenuste jaoks järgmisi küpsustasemeid:

Tase	Nimetus	Kirjeldus
Tase 0 (puudub)	PQC teostus puudub	PQC võib olla ettevalmistusfaasis, kuid ühtki kvantkindlat algoritmi ei ole tootele lisatud
Tase 1 (esmane)	Kasutatav testimiseks	PQC-algoritmid on olemas, kuid ainult testimiseks ja hindamiseks. Ei ole tootmisküps
Tase 2 (baastase)	Tootmisküps	Vähemalt üks PQC-algoritm on tootmises ja vastab asjakohastele standarditele
Tase 3 (edasijõudnud)	Inventuur ja paindlikkus	Krüptograafiline inventuur (SBOM/CBOM) on olemas ning toode toetab krüptograafilist paindlikkust
Tase 4 (hallatud)	Pärandalgoritmivaba	Pärandalgoritmid on kõrvaldatud või isoleeritud. Olemas hübriidrežiimi tugi
Tase 5 (optimeeritud)	Vaikimisi PQC	Kvantkindlus on vaikimisi valik; jõudlus on mõõdetud ja teostus sõltumatult verifitseeritud

Selle hindamise lähteandmed on esitatud jaotises **??**. PQCMMi eeskujul soovitame lisaks vastata järgmistele küsimustele:

[2] https://pkic.org/wg/pqc/pqcmm/

Küsimus	Nõutav vastus
Milline toode või teenus kuulub käsitlusalasse?	Toote/teenuse nimi, versioon, väljaanne, juurutusmudel ja hinnatud konfiguratsioon
Millist PQCMM taset selle toote või teenuse puhul deklareeritakse?	Tase 0/tase 1/tase 2/tase 3/tase 4/tase 5
Milline kinnitusmeetod väidet toetab?	Tarnija enesehinnang, kolmandapoolne hinnang või PKI Consortiumi sertifitseering
Milline teave on hindamise kohta olemas?	Hindamise kuupäev ja aruande versioon, hindaja või sertifitseerija isik, kui see on kohaldatav
Millised tõendid väidet toetavad?	Viited okumentatsioonile, väljalaskemärkmed, tarkvarakomponentide inventuur (SBOM), krüptograafiliste komponentide inventuur (CBOM), valideerimistulemused, testiaruanded või häälestusjuhised
Millised järgmise taseme kriteeriumid on osaliselt täidetud või kavandatud?	Lünkade loetelu, sihtkuupäevad, sõltuvused ja vastutav isik
Millised sündmused nõuavad uut hindamist?	Suuremad versioonimuudatused, krüptograafiliste teekide muudatused, algoritmimuudatused, juurutusviisi muudatused või turvaintsidendid

Selle sammu eesmärk on tuvastada süsteemi tarnijate postkvant-krüptograafilise küpsuse hetkeseis ning määrata kuupäev ML-KEMi (või ML-KEMiga hübriidi) toe ja ML-DSA (või ML-DSA-ga hübriidi) toe jaoks;

3. suhelda riiklike sertifitseerimisasutustega, et selgitada välja, millal nad suudavad välja anda hübriidseid postkvant-sertifikaate. Veenduda, et kõik sisemised mehhanismid (CRL/OCSP) suudavad töödelda suuremaid sertifikaate;
4. lisada kõikidele eelseisvatele süsteemiuuendustele ja tarnijavahetustele hanke tingimusena postkvant-krüptograafia toetuse nõue. Lisaks soovitame nõuda tarnijalt postkvant-krüptograafia küpsusmudeli (PQCMM) hindamis- või sertifitseerimisaruannet. Aruanne peab esitama deklareeritava PQCMM-taseme, kinnitusmeetodi, hindamise kuupäeva, hindaja või sertifitseerija (kui on kohaldatav) ning tõendid, mis toetavad deklareeritava taseme ja kõigi madalamate tasemete kriteeriume;
5. tarnijatega suhtlemisel peaksid järgmiste asjaoludega kaasnema selgituse nõudmine, parandusmeetmete nõudmine või vastuse tagasilükkamine:

Nr	Kirjeldus
1	Tarnija deklareerib postkvant-krüptograafilise küpsuse taseme, kuid keeldub esitamast hinnangut, sertifitseerimisaruannet või muid tõendeid selle kohta (nt viiteid dokumentatsioonile)
2	Tarnija esitab dokumentatsioonipõhiste tõendite asemel turundusmaterjali
3	PQC-küpsuse hindamise käsitlusala ei vasta organisatsiooni poolt hangitavale/kasutatavale konkreetsele tootele või versioonile, või väide on liiga ebamäärane
4	Tarnija tugineb kirjeldustes ja dokumentatsioonis vananenud või mittestandardsetele algoritminimedele (nt ML-KEMi asemel Kyber, ML-DSA asemel Dilithium)
5	Tarnija esitab tõendamata väiteid hübriidrežiimi kohta, ilma järgitava standardi või valitud kombineerija kirjelduseta

R.7. Koostada asutusesisene krüptoinventuur. Üleminekujuht peaks koostama oma versiooni krüptoinventuurist ning hoidma seda kogu üleminekuprotsessi vältel ajakohasena. Soovitame lähtealusena kasutada PQCC koostatud postkvant-krüptograafia inventuuri töövihikut[3]. Lähemalt vt riikliku tegevuskava sammud OP.5, OP.6 ja OP.7.

R.8. Viia ellu lühiajalised meetmed. Kuni tarnijad lähevad üle postkvant-krüptograafiale, peaks organisatsioonid uurima riikliku tegevuskava sammus OP.9 loetletud olemasolevaid lühiajalisi meetmeid.

R.9. Postkvant-krüptograafia lõimimine. Niipea kui see võimalus avaneb, tuleb Rahvastikuregistri tarnijatarkvara uuendada, et lisada postkvant-krüptograafia tugi nin kõrvaldada samal ajal kõik tekkida võivad uued koostalitlusvõime probleemid. See kehtib ka postkvant-krüptograafia kasutuse kohta andmevahetusprotokollides. Krüptograafiliste algoritmide üleviimine postkvant-krüptograafiale on järkjärguline protsess, kõiki süsteeme ei ole võimalik korraga üle viia. Seetõttu peaks täieliku ülemineku ajahinnang arvestama mitme teenuste postkvant-krüptograafiale ülemineku mitmes etapis. See tegevussamm hõlmab:

1. postkvant-krüptograafia suutega riistvara hankimist ja kasutuselevõttu (juhul kui see on vajalik) enne teiste komponentide uuendamist või sellega paralleelselt. Valideerida, et uued HSMid toetavad täpselt samu hübriidalgoritme, mis on valitud (vajaduse korral) X-tee autentimis-/signeerimisvõtmete (ja kõigi teiste HSMis hoitavate komponentide võtmete) jaoks, ning tagada platvormideülene koostalitlusvõime;
2. komponentide uuendamist, et võimaldada TLSi kasutamist hübriidrežiimis (X25519ML-KEM-768); niipea kui need on kättesaadavad, võtta kasutusele hübriidsed X.509 sertifikaadid autentimiseks/signeerimiseks;
3. niipea kui need on kättesaadavad, (vajaduse korral) X-tee autentimiseks/signeerimiseks hübriidsete X.509 sertifikaatide juurutamist ning hübriid-TLS (X25519ML-KEM-768) kasutuselevõttu.

R.10. Pidev seire ja uuendamine. Üleminekujuhi tööd tuleb käsitleda pideva tegevusena, kuivõrd süsteemi üleviimisega postkvant-krüptograafiale tema vastutus veel ei lõppe. Üleminekujuht peaks järjepidevalt uuendama krüptoinventuuri, tagama krüptograafia halduse küpsuse

[3] https://pqcc.org/pqc-inventory-workbook/

püsivalt kõrge taseme ning teavitama ametivõime edusammudest. See samm hõlmab:

1. RIA krüptograafiliste algoritmide elutsükli aruannete jälgimist, et olla kursis ML-KEM/ML-DSA standardite kasutust ja soovitatud võtmepikkusi puudutavate uuendustega;
2. puhta postkvant-krüptograafia nõuet süsteemi mittepärandkomponentide puhul, juhtudel kus see on teostatav, ning kvantnõrkade algoritmide (RSA, ECDSA, (EC)DH) kasutuselt kõrvaldamist. Süsteemidele postkvant-krüptograafia toe lisamisest üksi jääb väheks. Madaldusrünnete vastu turvalisuse tagamiseks peavad süsteemid keelama kvantnõrkade krüptograafiliste algoritmide kasutuse;
3. kõigi varem kvantnõrkades süsteemides paljastatud paroolide, pääsutõendite ja mandaatide rotatsiooni.

Bibliograafia

[1] Cybernetica AS. *Eesti postkvant-krüptograafiale ülemineku riiklik teekaart*. Estonian. Aruanne D-16-1248. Versioon 1.0. Riigihange "Postkvantkrüptograafia riiklik teekaart" (viitenumber 292945), tellija Justiits- ja Digiministeerium. Cybernetica AS, apr 2026. URL: https://www.justdigi.ee/sites/default/files/documents/2026-05/2026_ROAD2PQ_final_report__avalik_v1.0.pdf (vaadatud 19.06.2026).

[2] Michele Mosca ja Marco Piani. *Quantum Threat Timeline Report 2025*. Published March 9, 2026. Global Risk Institute, märts 2026. URL: https://globalriskinstitute.org/publication/quantum-threat-timeline-report-2025b/.

[3] National Institute of Standards and Technology (US). *Module-lattice-based key-encapsulation mechanism standard*. Tehniline aruanne NIST FIPS 203. Washington, D.C.: National Institute of Standards ja Technology (U.S.), aug 2024, NIST FIPS 203. DOI: 10.6028/NIST.FIPS.203. URL: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.pdf (vaadatud 29.09.2025).

[4] National Institute of Standards and Technology (US). *Module-lattice-based digital signature standard*. Tehniline aruanne NIST FIPS 204. Washington, D.C.: National Institute of Standards ja Technology (U.S.), aug 2024, NIST FIPS 204. DOI: 10.6028/NIST.FIPS.204. URL: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.204.pdf (vaadatud 29.09.2025).

[5] National Institute of Standards and Technology (US). *Stateless hash-based digital signature standard*. Tehniline aruanne NIST FIPS 205. Washington, D.C.: National Institute of Standards ja Technology (U.S.), aug 2024, NIST FIPS 205. DOI: 10.6028/NIST.FIPS.205. URL: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.205.pdf (vaadatud 29.09.2025).

[6] *ISO/IEC 18033-2:2006/DAM 2:2025(en); Information technology - Security techniques - Encryption algorithms - Part 2: Asymmetric ciphers; Amendment 2*. https://www.iso.org/standard/86890.html. 2025.

[7] Daniel Commey *et al. Performance Analysis and Deployment Considerations of Post-Quantum Cryptography for Consumer Electronics*. 2025. arXiv: 2505.02239 [cs.CR]. URL: https://arxiv.org/abs/2505.02239.

[8] *Agreed Cryptographic Mechanisms*. 2025. URL: https://certification.enisa.europa.eu/document/download/a845662b-aee0-484e-9191-890c4cfa7aaa_en?filename=ECCG%20Agreed%20Cryptographic%20Mechanisms%20version%202.pdf.

[9] NIST. *Post-Quantum Cryptography: FAQs*. https://csrc.nist.gov/Projects/post-quantum-cryptography/faqs. 2026.

[10] BSI and European Partner Agencies. *Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography*. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/PQC-joint-statement.pdf?__blob=publicationFile&v=3. Joint statement from cybersecurity authorities of 18 EU member states. Accessed: 2025-09-03. Nov 2024.

[11] European Commission. *A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography*. https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography. 2024.

[12] German Federal Office for Information Security (BSI). *Migration to Post-Quantum Cryptography*. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Migration_to_Post_Quantum_Cryptography.pdf?__blob=publicationFile&v=2. 2024.

[13] German Federal Office for Information Security (BSI). *Quantum-safe cryptography – fundamentals, current developments and recommendations*. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.pdf?__blob=publicationFile&v=6. 2022.

[14] TNO. *TNO-2024-pqc-en*. https://publications.tno.nl/publication/34643386/fXcPVHsX/TNO-2024-pqc-en.pdf. 2024.

A Postkvant-krüptograafiale ülemineku käsiraamat

A.1 Kõrge riskiga komponentide tuvastamine

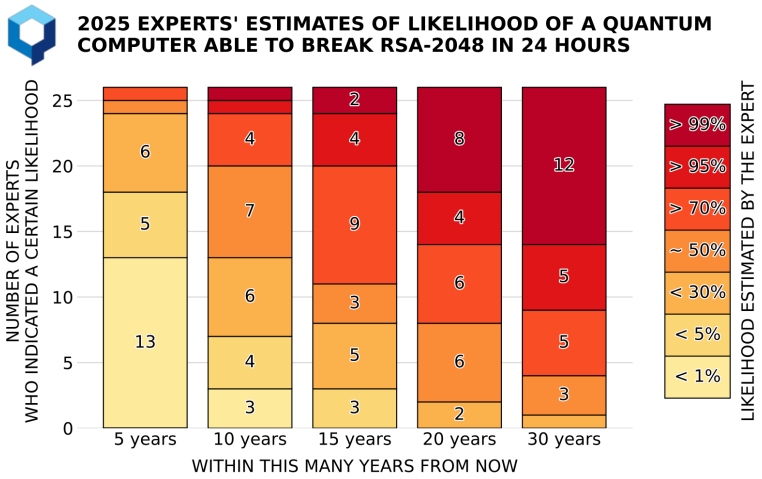
Krüptograafiliselt märgiliste kvantarvutite väljatöötamise edenedes muutub klassikalise avaliku võtmega krüptograafia ohumaastik. Ehkki suuremastaabiline ja veakindel kvantarvuti, mis suudaks murda laialdaselt kasutatavaid algoritme nagu RSA ja ECC, on veel aastate kaugusel, on kvantoht juba praegu olemas „salvesta täna, dekrüpteeri hiljem“ (*harvest-now-decrypt-later*, HNDL) rünnete kujul. Selliste rünnete puhul koguvad ründajad juba täna krüpteeritud andmeid, talletavad neid ning dekrüpteerivad tulevikus, kui kvantarvutid on selleks piisavalt küpsed. Arvestades, et paljud süsteemid peavad kaitsma andmeid aastakümneid, on ennetav üleminek kvantkindlale krüptograafiale hädavajalik.

Üleminek postkvant-krüptograafiale ei ole lihtne protsess. Kaasaegsete süsteemide keerukuse ja mastaabi tõttu on ebapraktiline ja ebaefektiivne uuendada kõiki krüptograafilisi komponente üheaegselt. Seetõttu on vajalik prioriseeritud lähenemine. Selle prioriseerimise suunamiseks vaatleme kolme põhinäitajat, mis aitavad tuvastada süsteemis kõrge riskiga komponente.

1. **„salvesta täna, dekrüpteeri hiljem“ rünnete oht**
   See näitaja väljendab riski, et ründajad võivad tundlikke andmeid, mis on praegu krüpteeritud klassikaliste algoritmidega kehtestatud võtmega, koguda ja talletada tulevikus dekrüpteerimiseks kvantarvutit kasutades.

   Eriti ohustatud on pikaajalise konfidentsiaalsusnõudega andmed (nagu isikutuvastusandmed, ajaloolised rändeandmed ning sünni- või surmatunnistused). Neid andmeid tuleb sageli kaitsta aastakümneid, mis ületab kvantohu eeldatavat ajakava. Kvantohu ajakava saab hinnata, tuginedes aruande „Quantum Threat Timeline Report 2025“ [2] tulemustele. Selles aruandes on kvantarvutuse ekspertidel palutud hinnata krüptograafiliselt märgilise kvantarvuti tõenäosust, koondatuna tõenäosuse ja ajaraami järgi. Uuringu tulemused on esitatud joonisel 2.

Joonis 2. Ekspertide hinnangud krüptograafiliselt märgilise kvantarvuti kättesaadavusele



Kõik selliseid andmeid töötlevad komponendid peavad konfidentsiaalsuse pikaajaliseks ta-

gamiseks olema ülemineku prioriteediks.

2. **Pikad üleminekuperioodid**
   Mõnel süsteemil ja seadmel on pikk kasutusiga, mistõttu on neid olemuslikult raske uuendada. Sellised on näiteks:
   - avaliku võtme taristud (PKI), mis väljastavad ja haldavad digitaalseid sertifikaate;
   - isikutuvastuseks kasutatavad sardseadmed ja kiipkaardid;
   - pärandriistvara (nt valijate registreerimissüsteemid, eID-kaardid või riiklikud andmekogud), mida ei pruugi olla lihtne uuendada.

   Need süsteemid võivad jääda kasutusse pikaks ajaks. Kui postkvant-krüptograafiale üleminekut edasi lükatakse, on need süsteemid pikka aega avatud kvantrünnetele, isegi kui oht ei ole vahetu. Seega on pika elueaga ja piiratud uuendatavusega komponendid kõrge prioriteediga varaseks üleminekuks.
3. **Organisatsiooni missioonikriitilised varad**
   Kuigi see näitaja ei ole otseselt seotud kvantriskiga, rõhutab see mõningate andmete või teenuste strateegilist tähtsust organisatsiooni põhifunktsioonide jaoks. Nende süsteemide rikkumine võib põhjustada tõsiseid tegevushäireid, avaliku usalduse kadu või riikliku julgeoleku riske. Teisisõnu, isegi kui need komponendid ei ole võimalike „salvesta täna, dekrüpteeri hiljem“ rünnete ega üleminekuaja vaatenurgast kõige suurema riskiga, õigustab nende missioonikriitilisus neile kõrge prioriteedi andmist üleminekukavas.

Oluline on märkida, et komponentide kõrge riski staatus ei määra ära ülemineku ulatust, vaid pigem teostuse järjekorda ja kiireloomulisust. Postkvant-krüptograafiale ülemineku lõppeesmärk on tagada, et kõik kvantnõrgad krüptograafilised komponendid vahetatakse välja. Kuid eespool nimetatud kolme näitaja alusel prioriseerides saab organisatsioon suunata oma piiratud ressursid esmalt kõige kriitilisematele ja haavatavamatele valdkondadele, minimeerides riski üleminekufaasi jooksul.

Käsitletud näitajaid rakendades saab organisatsioon välja töötada riskipõhise tegevuskava postkvant-krüptograafia lõimimiseks, tagades, et kõige nõrgemate ja strateegiliselt olulisemate komponentidega seotud küsimused lahendatakse kõige esimesena, luues samal ajal aluse täielikuks süsteemiüleseks üleminekuks.

A.2 Olemasolevate postkvant-algoritmide sobivus

Järgnev jaotis hindab postkvant-krüptograafiliste algoritmide hetkeseisu, nende standardimisstaatust ja sobivust klassikaliste krüptograafiliste komponentide asendamiseks või täiendamiseks.

A.2.1 Olemasolevad postkvant-algoritmid

Postkvant-krüptograafia väli on viimastel aastatel oluliselt arenenud, seda suuresti USA riiklik standardimis- ja tehnoloogiainstituudi (NIST) eestvedamisel. 2016. aastal käivitas NIST mitmeaastase standardimisprotsessi kvantkindlate krüptograafiliste algoritmide leidmiseks, mis võiksid asendada laialdaselt kasutatavaid klassikalisi skeeme, nagu RSA, (EC)DSA ja EC(DH). See algatus kulmineerus esimese standarditud PQC-algoritmide komplekti väljavalimisega 2024. aasta augustis.

Värskeimate uuenduste tulemusena on NIST praeguseks lõplikult kinnitanud kolm põhialgoritmi:

- **ML-KEM** (Module-Lattice Key Encapsulation Mechanism) [3]: valitud peamiseks võtmekapseldusmehhanismiks (KEM) turvalise võtmevahetuse jaoks. Selle aluseks on moodulipõhine vigadega (*module learning with errors*, MLWE) probleemi arvutuslik keerukus ning see tagab tugeva turvalise suhteliselt tõhusa jõudlusega.
- **ML-DSA** (Module-Lattice Digital Signature Algorithm) [4]: valitud peamiseks digisignatuuriskeemiks, tugineb samale matemaatilisele struktuurile kui ML-KEM. ML-DSA pakub tasakaalu turvalisuse, signatuuri suuruse ja arvutusliku tõhususe vahel.
- **SLH-DSA** (Stateful Hash-based Digital Signature Algorithm) [5]: valitud teiseseks signatuuriskeemiks, tugineb Winternitzi ühekordsel signatuuriskeemil (WOTS) ning mõnekordsel signatuuriskeemil FORS. SLH-DSA paistab eriti silma oma vastupidavuse poolest kvantrünnetele, kuna skeemi turvalisus tugineb selle aluseks oleva räsifunktsiooni turvalisusele, mida peetakse kvantkindlaks.

Loetletud algoritmid esindavad standarditud postkvant-krüptograafiliste primitiivide esimest lainet ja on mõeldud vaikimisi valikuks tulevaste süsteemide kaitsmiseks. Standardimisprotsess on siiski endiselt käimas ning lähiaastatel oodatakse täiendavate standardite avaldamist. Näiteks:

- **Falcon** (FN-DSA): võrepõhine signatuuriskeem, mis pakub väiksemaid signatuure kui ML-DSA ning sobib seetõttu piiratud läbilaskevõimega keskkondadesse. Skeemi keerukama olemuse tõttu on seda aga raskem turvaliselt teostada. NISTi standard on praegu mustandi staadiumis, mis lõplikult kinnitatakse eeldatavasti 2026. aasta suvel. Kui FN-DSA standardimine edeneb samas tempos kui ML-DSA (mille esimene mustand avaldati 2026. aastal), siis võib eeldada, et varajane tarkvaratugi saab kättesaadavaks alles 2029. aasta alguses. See tähendab, et FN-DSA ei sobi 2030. aastaks postkvant-krüptograafiale ülemineku kavadesse.
- **HQC** (Hybrid Quadratic Residue-based Key Encapsulation): koodipõhine võtmevahetusmehhanism, mis pakub teistsugust turvaalust ning võib mõningate kasutusmallide puhul pakkuda jõudlusega soetud eeliseid. NIST on selle valinud teiseks KEMiks.
- **FrodoKEM** ja **Classic McEliece**: FrodoKEM on (struktureerimata) võrepõhine KEM ning Classic McEliece on koodipõhine KEM. Mõlemad skeemid olid NISTi konkursi varajaste kandidaatide seas. Kuigi NIST ei standardiseerinud, on mõlemad leidnud koha ISO/IEC standardites [6] ning võivad leida kasutust niši- või kõrge turvalisusega rakendustes.

NIST on väljendanud ka huvi täiendavate, teistsugustesse krüptograafilistesse perekondadesse kuuluvad digisignatuuriskeemide standardimise vastu, et suurendada algoritmide mitmekesisust ja vähendada riski, et üks ründevektor õõnestab kõiki postkvant-krüptograafia teostusi. Täiendavate esitatud kandidaatide analüüs on praegu käimas.

A.3 Tehnilised nõuded uutele postkvant-krüptograafilistele algoritmidele

Postkvant-krüptograafia lõimimine mistahes süsteemi nõuab märkimisväärsete tehniliste probleemide lahendamist, eelkõige seoses süsteemi ühilduvuse, ressursikasutuse ja jõudlusega. Järgnev jaotis hindab, kas olemasolev süsteem (sh protokollid, tarkvara ja taristu) suudab võtmesuuruste ja jõudluse vaatenurgast toetada postkvant-krüptograafiat.

A.3.1 Postkvant-krüptograafiliste objektide suurus

Postkvant-krüptograafilised algoritmid nõuavad reeglina rohkem tehnilisi ressursse kui klassikalised algoritmid; eelkõige puudutab see võtmesuurust, mälukasutust ja läbilaskevõimet. Tabel 2 annab ülevaate valitud postkvant-algoritmide võtmepikkustest ning võrdleb neid klassikaliste vastetega, kõik ligikaudu 128-bitisel (klassikalisel) turvatasemel.

Tabel 2. Postkvant-krüptograafiliste ja traditsiooniliste algoritmide objektisuuruste võrdlus (~128-bitised turvaparameetrid)

Digitaalsignatuuriskeem	Signatuuri pikkus [B]	Võtmepikkused [B]	
		Avalik võti	Privaatvõti
RSA 2048	256	256	256
ECDSA P-256	64	64	32
ML-DSA-44	768	1312	2528
SLH-DSA-128s	7856	32	64
SLH-DSA-128f	170888	32	64
FN-DSA (512)	666	897	1281
Võtmekapseldusmehhanism	**krüptogrammi pikkus [B]**	**Võtmepikkused [B]**	
		Avalik võti	Privaatvõti
ECDH P-256	65	32	65
ML-KEM 512	768	800	1632
HQC-128	4433	2249	2305
FrodoKEM-640-AES	9720	9616	19888
Classic McEliece (348864)	96	261120	6492

Olulisemad tähelepanekud tabeli 2 kohta

- **Avalikud võtmed ja signatuurid:** postkvant-algoritmidel on klassikaliste skeemidega võrreldes oluliselt suuremad avalikud võtmed ja signatuurid. Näiteks ML-DSA-44 avalik võti on 1312 baiti ja signatuur 768 baiti, samas kui ECDSA P-256 kasutab avaliku võtme jaoks vaid 64 baiti ja signatuuri jaoks 64 baiti.
- **Privaatvõtmed:** privaatvõtmed on samuti suuremad, eriti ML-DSA puhul (2528 baiti), mis võib mõjutada salvestus- ja mäluruumi kasutust.
- **Krüptogrammid:** võtmekapseldusmehhanismid (KEMid) nagu ML-KEM väljastavad umbes 768-baidiseid krüptogramme, mis on suuremad kui ECDH 65 baiti.
- **Äärmuslikud juhud:** SLH-DSA-128f-i signatuur on erakordselt suur (170 888 baiti), mis muudab selle enamiku rakenduste jaoks ebapraktiliseks. Classic McEliece'il on väga suur privaatvõti (261 120 baiti), mis on samuti enamiku süsteemide jaoks liiga suur.

Mõju süsteemiressurssidele

- **Läbilaskevõime ja võrgumaht:** suuremad krüptograafilised objektid suurendavad edastusaega ja andmemahtu. Suure läbilaskevõimega süsteemides, nagu X-tee, võib see põhjustada suuremat latentsust või võrgu ülekoormust.

- **Salvestusruum:** suuremad võtmed ja signatuurid nõuavad rohkem kettaruumi, eriti süsteemides, millel on palju kasutajaid või milles võtmed sageli roteeruvad.
- **Mälukasutus:** postkvant-toimingud vajavad ajutiste andmestruktuuride jaoks sageli rohkem RAMi, mis võib olla piiravaks teguriks sardsüsteemides või vähese mäluga keskkondades.

A.3.2 Postkvant-krüptograafia jõudlusnäitajad

Kuigi postkvant-algoritmid nõuavad üldiselt rohkem ressursse, varieerub nende arvutusjõudlus märkimisväärselt sõltuvalt algoritmist ja toimingust. Hiljutised jõudlusanalüüsid (nt [7]) näitavad, et mõned postkvant-skeemid ületavad mõningate toimingute puhul siiski klassikalisi algoritme.

- **Võtmeloome:** postkvant-krüptograafiline võtmeloome on tavaliselt kiirem kui klassikalistel algoritmidel üleüldiselt. Näiteks ML-KEM ja ML-DSA võtmeloome on sageli kiirem kui RSA või ECDSA puhul.
- **Kapseldus ja lahtikapseldus:** ML-KEM töötab nii võtmekapselduse kui ka lahtikapselduse puhul oluliselt kiiremini kui ECDH ja RSA, mis teevad sellest tugeva kandidaadi turvalise võtmevahetuse jaoks. Ka FrodoKEMi jõudlus on võtmeloome ja lahtikapselduse kontekstis konkurentsivõimeline, kuid suured krüptogrammid muudavad selle piiratud läbilaskevõimega keskkondade jaoks sobimatuks.
- **Signeerimine ja verifitseerimine:** ML-DSA on kõigis kolmes toimingus (võtmeloome, signeerimine ja verifitseerimine) pisut kiirem kui ECDSA ja RSA, mis teeb sellest hea valiku digisignatuuride jaoks.

A.3.3 Peamised raskuskohad postkvant-krüptograafia lõimimisel

Üleminek postkvant-krüptograafiale tähendab olulist nihet turvaliste süsteemide kavandamises, juurutamises ja haldamises. Kuigi krüptograafiakogukond on teinud suuri edusamme postkvant-algoritmide standardimisel, seda eelkõige NISTi käimasoleva PQC standardimisprotsessi kaudu, on nende praktiline lõimimine olemasolevatesse süsteemidesse endiselt keerukas. Raskused ei ole ainult tehnilised, vaid ka organisatsioonilised ja strateegilised, ning paljudele neist peavad esmalt lahendusi otsima krüptograafialahenduste tarnijad, taristupakkujad ja protokollide arendajad, mitte lõppkasutajad. Allpool kirjeldame peamisi raskuskohti, mida tuleb postkvant-krüptograafia lõimimisel süsteemidesse arvesse võtta.

Jõudlusega seotud kompromissid. Üks vahetumaid probleeme on vajadus tasakaalustada turvalisust jõudluse ja ressursipiirangutega. Kuigi NIST on standardinud mitmeid paljulubavaid kandidaate, on neil algoritmidel erinevad jõudlusprofiilid. Näiteks pakub ML-KEM tugevat turvalisust ja suhteliselt tõhusaid toiminguid, mis muudab selle sobivaks paljude rakenduste jaoks. Piiratud arvutusvõimsusega keskkondades (nagu sardseadmed, esemevõrgu andurid või vähese energiakuluga süsteemid) võib jõudlus siiski osutuda kitsaskohaks.

Süsteemiarhitektid võivad sellistel juhtudel olla sunnitud valima kõrgema turvataseme ja väiksema jõudluse vahel, või kaaluma alternatiivseid algoritme, mis pakuvad väiksemaid võtmeid või kiiremaid toiminguid. See otsus ei ole kunagi lihtne ning nõuab tihti ohumudelite, latentsusnõuete ja riistvaravõimekuse hoolikat hindamist.

Andmevahetusmahud. Kõige olulisem praktiline probleem seoses postkvant-krüptograafia kasutuselevõtuga on ehk krüptograafiliste objektide suuruse märkimisväärne kasv. Traditsioonili-

sed RSA- või ECC-algoritmid loovad suhteliselt kompaktseid võtmeid, krüptogramme ja signatuure, samas kui postkvant-algoritmid vajavad tihti palju suuremaid andmestruktuure.

Suured krüptograafilisedlastid võivad oluliselt mõjutada võrgu läbilaskevõimet ja salvestusmahtu, eriti suure läbilaskevõimega keskkondades, nagu pilveliidesed, servarvutussõlmed või reaalaja-suhtlussüsteemid.

Selle tagajärjel ei sobi algoritmid nagu FrodoKEM või Classic McEliece (mille objektid on oluliselt suuremad kui nt ML-KEMil) piiratud läbilaskevõimega või latentsustundlikesse rakendustesse. Andmemahtude suurenemine mõjutab ka protokolle, mis tuginevad sagedastele võtmevahetustele või digisignatuuridele, nagu TLS, kus iga kätlus või sõnumiautentimine kasvatab summaarset edastatavat andmemahtu.

Hübriidrežiimidega seotud kaalutlused. Üks võtmelisi strateegilisi küsimusi postkvant-krüptograafia lõimimise juures on, kas võtta kasutusele hübriidne krüptograafiline lähenemine (klassikaliste ja postkvant-algoritmide kombineerimine) või minna otse üle täielikult postkvant-krüptograafia põhistele süsteemidele. NIST ja paljud turbeeksperdid ning riiklikud asutused soovitavad praegu optimaalse üleminekustrateegiana hübriidrežiime.

See lähenemine tagab, et süsteem jääb rünnete vastu kaitstuks ka siis, kui üks algoritmidest peaks hiljem osutuma nõrgaks. Näiteks kasutatakse hübriidse võtmevahetuse puhul nii klassikalist ECDHd kui ka PQC ML-KEMi, kus lõplik võti tuletatakse mõlemast.

Hübriidrežiimi valik mõjutab ka võtmehaldussüsteemide, sertifikaadistruktuuride ja protokollilaienduste kavandamist.

Ühilduvuse ja koostalitlusvõime probleemid. Postkvant-krüptograafia integreerimist olemasolevatesse süsteemidesse raskendab ka laialdase kasutuselevõtu puudumine ja pärandtaristu mitmekesisus. Paljud süsteemid (alates pärandandmebaasidest ja püsivarast ning lõpetades kolmandate poolte APIde ja füüsiliste turvamoodulitega) on kavandatud klassikalist krüptograafiat silmas pidades ning ei pruugi postkvant-primitiive hõlpsalt toetada.

Koostalitlusvõime tagamine eri tarnijate, platvormide ja protokollide (nt TLS, IPsec, S/MIME, PKI) vahel on keeruline ülesanne. Näiteks ei pruugi PQC-toega server suuta suhelda pärandkliendiga, millel postkvant-krüptograafia tugi puudub; selle tagajärjeks võib olla ühenduse katkemine või turvalisuse kahanemine.

Sellest kasvab omakorda välja järgmine probleem: tarnijad suhtuvad postkvant-krüptograafiasse investeerimisse suure ettevaatusega, kuni selle järele pole nõudlust, kuid lõppkasutajad kõhklevad postkvant-krüptograafiat kasutusele võtmast enne, kui sellel on olemas laialdane tugi. Standardimispüüetest on küll kasu, kuid täielik koostalitlusvõime nõuab koordineeritud uuendusi üle kogu ökosüsteemi, sealhulgas sertifitseerimisasutustes, operatsioonisüsteemides ja vahetarkvaras.

Võtmehalduse ja elutsükli keerukus. Postkvant-krüptograafia suurendab ka võtmehalduse keerukust. Suuremad võtmed ning potentsiaalselt erinevad võtmeloome, võtmete talletamise ja edastamise mehhanismid nõuavad võtmehaldussüsteemide (KMS), HSMide ja PKI taristute uuendamist.

Näiteks võivad postkvant-algoritmide võtmetalletusnõuded olla oluliselt suuremad, mis võib nõuda riistvarauuendusi või muudatusi võtmerotatsiooni poliitikates.

Lisaks tõstatab postkvant-krüptograafia küsimusi võtmete elutsükli poliitikate kohta: kas võtmeid tuleks roteerida sagedamini? Kas pikaajalisi võtmeid tuleks kasutada ainult signeerimiseks, krüpteerimise jaoks aga efemeervõtmeid? Uute võtmehaldusstrateegiate vajadus koos küpsete postkvant-krüptograafiale spetsiifiliste vahendite ja heade tavade puudumisega suurendab süsteemiadministraatorite ja turbemeeskondade töökoormust.

Teostuse ja auditeeritavusega seotud raskuskohad. Isegi standardiseeritud postkvant-algoritmid on sageli keerukad ja nõuavad eriotstarbelisi teostusi. Postkvant-süsteemi turvalisus ei sõltu ainult algoritmist endast, vaid ka selle teostuse õigsusest ja töökindlusest. Postkvant-krüptograafia teostuste õigsust on üldlevinud testimisraamistike ja etalonteostuste puudumise tõttu ühtlasi keerulisem verifitseerida.

Väljatöötusjärgus on küll vastavad avatud lähtekoodiga teegid, kuid need ei ole veel sama küpsed ega laialdaselt auditeeritud kui klassikalised krüptograafiateegid.

Regulatiiv- ja vastavusnõuetega seotud kaalutlused. Reguleeritud majandusharude organisatsioonid peavad tagama, et nende krüptograafilised valikud vastavad kehtivatele regulatsioonidele ja standarditele. Praegu ei tunnista paljud regulatiivsed raamistikud postkvant-krüptograafiat veel formaalselt nõuetele vastava lahendusena.

See sünnitab ebakindlust organisatsioonide jaoks, kes peavad täitma vastavusnõudeid ning valmistuma samal ajal kvantohtudeks.

Väljaõpe ja töötajaskonna valmisolek. Viimaks nõuab postkvant-krüptograafia edukas lõimimine kvalifitseeritud töötajaskonda, kes suudab mõista ja juurutada kvantkindlaid lahendusi. Paljud turbespetsialistid ei ole veel tuttavad postkvant-krüptograafia aluseks olevate matemaatiliste mõistetega ning selles kujunevas valdkonnas valitseb ekspertide puudus. Üks näide postkvant-krüptograafia tunnustamisest on ENISA tunnustatud krüptograafiliste mehhanismide loetelu [8]. Tunnustatud postkvant-signatuuriskeemide seas on ML-DSA, SLH-DSA, XMSS, LMS ning võtmekapseldusmehhanismide (KEM) hulgas ML-KEM ja FrodoKEM.

Selle teadmuslõhe ületamise jaoks on olulised koolitusprogrammid, dokumentatsioon ning tarnijate tugi.

A.4 Hübriidrežiimid

Postkvant-krüptgoraafiale üle minevad organisatsioonid peavad valima, kas minna vahetult üle puhtalt postkvant-krüptograafilistele lahendustele või kasutada hübriidkrüptograafiat hõlmavat vahestrateegiat. Järgnev jaotis analüüsib hübriidkrüptograafia sobivust, selle rakendamise mõjusid ja riske üleminekuperioodil.

A.4.1 Hübriidkrüptograafia

Hübriidkrüptograafia tähendab postkvant-krüptograafiale ülemineku kontekstis traditsiooniliste (klassikaliste) krüptograafiliste algoritmide kasutamist kõrvuti kvantkindlate algoritmidega. See lähenemine on mõeldud tagama seansi/andmete kaitse juhul, kui ükskõik milline hübriidkrüptograafia element peaks murtama:

1. traditsiooniline (klassikaline, kvant-eelne või kvantnõrk) komponent tagab turvalisuse potentsiaalsete, seni avastamata loogiliste, matemaatiliste või kõrvalkanalirünnete vastu, mis

võidakse uutes postkvant-algoritmides avastada. See toimib kaitsemehhanismina veel avalikustamata postkvant-algoritmi nõrkuste vastu;

2. postkvant-komponent tagab turvalisuse kvantohu vastu – see puudutab konkreetselt praegu aktuaalset „salvesta täna, dekrüpteeri hiljem“ ründevektorit. Isegi kui postkvant-algoritm hiljem murtakse, jääb klassikaline komponent praeguse klassikalise arvutusvõimsuse vastu turvaliseks.

A.4.2 Kompromissid ja riskid

Kuigi hübriidkrüptograafia pakub tugevaid turvagarantiisid, kaasnevad selle lähenemise rakendamisega taristus mõningad kompromissid ja probleemkohad.

1. **Teostuse keerukuse kasv**
   Hübriidrežiim sisuliselt kahekordistab algoritmi teostamiseks, võtmehalduseks ja lõimimiseks vajalikku tööd. See hõlmab täiendavate algoritmiidentifikaatorite haldamist, sertifitseerimisasutuste uuendamist hübriidsertifikaatide väljastamiseks ning tagamist, et võtmehaldussüsteemid suudavad talletada ja käidelda kahte eraldi võtmekomplekti. Suurenenud keerukus suurendab ka teostusvigade või konfiguratsioonivigade tõenäosust.
2. **Andmevahetus- ja talletusmaht**
   Puhta postkvant-krüptograafiaga kaasnevad juba oluliselt suuremad võtmed, krüptogrammid ja signatuurid võrreldes klassikaliste skeemidega. Suhteliselt väikese traditsioonilise võtme (nt ECDSA avaliku võtme suurus on ~64 baiti) lisamise mõju palju suuremale postkvantvõtmele (nt ML-KEMi avaliku võtme suurus on ~64 baiti800 baiti) tähendab aga protsentuaalselt tihti tühist lisamahtu. Suure läbilaskevõimega stsenaariumide korral võib see lisaandmemaht latentsust pisut suurendada, kuid see on üldiselt kaasaegsete võrguseadmetega hallatav.
3. **Arvutuskulu**
   Kahe krüptograafilise toimingu kombineerimine tähendab kõigi krüptograafiliste toimingute (võtmeloome, krüpteerimine, signeerimine) topeldamist. Kuigi mõned postkvant-algoritmid (nagu ML-KEM) võivad olla klassikalistest vastetest kiiremad, on mõlema virna paralleelse kasutamise kombineeritud kulu suurem. Kaasaegse serveririistvara jaoks on arvutuskulu suurenemine tavaliselt tühine. Piiratud ressurssidega seadmete puhul, nagu esemevõrgu andurid, kiipkaardid või isikutuvastuseks kasutatavad sardmikrokontrollerid, võib see aga muutuda kitsaskohaks.
4. **Ajutine lahendus**
   Hübriidkrüptograafia juurutamine pikendab põhimõtteliselt üleminekuperioodi. Organisatsioon peab kokkuvõttes läbima teise üleminekuetapi, mille käigus kõrvaldatakse klassikalised krüptograafilised komponendid ja minnakse täielikult üle postkvant-lahendustele. See tähendab kahe turvatehnoloogiavirna haldamist määramata aja vältel, mis suurendab pikaajalist tegutsemiskoormust.
5. **Regulatiivne mõju**
   Olemasolevad NISTi standardid ja juhised toetavad hübriidsignatuuride kasutamist (kaks või enam signatuuri ühel sõnumil), tingimusel et vähemalt üks komponentsignatuurialgoritm on NISTi heakskiiduga. See muudab sujuvamaks selliste süsteemide ülemineku postkvantkrüptograafiale, mis peavad vastama standarditele ja regulatsioonidele ning kasutama samal ajal NISTi heakskiiduga traditsioonilisi signatuuriskeeme. Sarnaselt kavatseb NIST toetada hübriidse võtmekehtestusrežiimi kasutamist FIPS 140 nõuetele vastava valideerimise puhul, eeldusel et see on sobivalt kombineeritud NISTi heakskiiduga skeemiga [9].

A.4.3 Valdkondlik konsensus ja soovitused

Arutelud parima üleminekustrateegia üle ei ole kaugeltki lõppenud. Mõned turbevaldkonna eestkõnelejad ja spetsiifilised allikad (ajalooliselt sh mõned tõlgendused NISTi varastest juhistest) on argumenteerinud hübriidkrüptograafia kasutamise vastu, soovitades organisatsioonidel juurutada kohe puhtalt postkvant-krüptograafilisi lahendusi. See seisukoht põhineb argumendil, et hübridiseerimine toob kaasa keerukuse tarbetu suurenemise ja potentsiaalsete ründepindade arvu kasvu.

Kõigest sellest hoolimata valitseb suuremate küberturbeasutuste seas hetkel konsensus, et keskenduda tasub esmalt hübriidrežiimidele. Näiteks 18 ELi riigi ühisavaldus postkvant-krüptograafia kasutuselevõtu kohta [10], aga ka Saksamaa BSI (Föderaalne Infoturbe Amet) soovitused toetavad üleminekuperioodil hübridiseerimist peamise riskileevendusstrateegiana. Seda põhjendatakse asjaoluga, et hübridiseerimise eelised kaaluvad selgelt üles suurenenud keerukusest tulenevad probleemid.

A.5 Üleminekumudelid

Postkvant-krüptograafiale ülemineku strateegia kavandamisel tuleb tasakaalustada kahte peamist eesmärki: **tagasiühilduvus pärandsüsteemidega** ning **„salvesta täna, dekrüpteeri hiljem“ ohu leevendamine**. Mõlema samaaegne saavutamine on olemuslikult keeruline, kuna klassikalise krüptograafia tagasiühilduvuse laiendamine avab sageli süsteemid madaldusrünnetele või lükkab edasi kvantvalmisolekut. Valdkonna ettevõtted ja standardimisasutused on välja pakkunud mitmeid üleminekumudeleid. Neid käsitletakse allpool.

A.5.1 Tagasiühilduvusega seotud kompromissid

Enne konkreetsete üleminekumudelite hindamist on elutähtis teadvustada pinget tagasiühilduvuse ja kvantturvalisuse vahel. Paljud olemasolevad infosüsteemid peavad jääma ühilduvaks väliste partnerite, pärandklientide või uuendamata taristuga. Nende ühenduste toetamine postkvant-krüptograafiale ülemineku perioodil nõuab põhimõttelist kompromissi: **tagasiühilduvuse säilitamine mitte-postkvantsüsteemidega õõnestab sageli postkvant-krüptograafia turvagarantiisid**, seda eelkõige läbi madaldusrünnete võimaldamise, mille käigus ründaja sunnib süsteemi kätluse või kooskõlastuse käigus kasutama klassikalisi algoritme.

Selle probleemi lahendamiseks uurivad mitmed IETFi ja valdkondlikud aalgatused krüptograafilise järjepidevuse mehhanisme. Näiteks TLS PQC Continuity Extension [1] toob sisse mehhanismi, millega kontrollida, et postkvant-võtmevahetust ei ole kooskõlastuse käigus eemaldatud, samas kui Certificate Hosting Continuity [2] eesmärk on siduda sertifikaadid kvantkindlate parameetritega, et vältida tagasiulatuvaid madaldusi. Ehkki need laiendused on paljulubavad, suurendavad nad märkimisväärselt protokolli keerukust, nende toimimine eeldab laialdast kasutuselevõttu ning need ei ole veel küpsed ega universaalselt kasutuses.

Praktikas otsustavad paljud organisatsioonid pragmaatilise kompromissi kasuks: nad taluvad ajutist avatust „salvesta täna, dekrüpteeri hiljem“ rünnetele, mis aga tagab neile operatsioonilise järjepidevuse ja ühilduvuse olemasoleva ökosüsteemiga. Üks levinud lähenemine on kehtestada ajaliselt piiratud koostalitlusvõime aken, mille jooksul säilitatakse pärandprotokollide tugi, kuid seda kommunikeeritakse avalikult koos kindla üleminekutähtajaga. Pärast tähtaja möödumist ta-

[1] https://datatracker.ietf.org/doc/draft-sheffer-tls-pqc-continuity/
[2] https://datatracker.ietf.org/doc/html/draft-reddy-lamps-x509-pq-commit-00

gasiühilduvus lõpetatakse ning süsteemid töötavad eranditult hübriidses või puhtas postkvant-režiimis. See strateegia pakub riski aktsepteerimise hinnaga selget teed täieliku kvantvalmisolekuni.

A.5.2 Näitlikud üleminekumudelid

1. Kohene väljavahetamine. See mudel näeb ette postkvant-algoritmide kohese juurutamise, jättes klassikalise krüptograafia täielikult vahele. Kuigi see lähenemine pakub tugevaimat ja vahetuimat kaitset nii praeguste kui ka tulevaste kvantohtude vastu, on see suuremahuliste, omavahel seotud süsteemide puhul harva teostatav. Kohene asendamine katkestab tavaliselt koostalitlusvõime uuendamata klientide, serverite ja protokollidega, muutes süsteemi kasutuskõlbmatuks, kuni kõik pooled lähevad üheaegselt üle postkvant-krüptograafiale. See sobib kõige paremini uute juurutuste, sisemiste mittesuhtluskomponentide või keskkondade jaoks, mis juba algusest toetavad krüptograafilist paindlikkust. Piirangutest hoolimata jääb kohene asendamine ainsaks mudeliks, mis kõrvaldab juurutamise korral täielikult „salvesta täna, dekrüpteeri hiljem" ohu.

2. Järkjärguline üleminek. See lähenemine võtab postkvant-krüptograafia kasutusele järk-järgult, tavaliselt kolmes etapis:

1. **klassikaline** – praegune olukord, tugineb üksnes RSAle, ECCle või sümmeetrilistele algoritmidele;
2. **hübriidne** – paralleelselt kasutatakse nii klassikalisi kui ka postkvant-algoritme. Võtmevahetus või signatuuri valideerimine õnnestub ainult siis, kui mõlemad kihid on rahuldatud, mis tagab turvalisuse isegi ühe algoritmi murdmise korral;
3. **ainult PQC** – klassikalised komponendid kõrvaldatakse kasutuselt, süsteem töötab eranditult standarditud postkvant-primitiividega.

> **Oluline märkus:** hübriidrežiimi peamine eesmärk ei ole mitte tagasiühilduvus, vaid pigem krüptograafiline liiasus. See kaitseb postkvant-algoritmide (mida ei ole nii põhjalikult kontrollitud kui klassikalisi skeeme) potentsiaalse tulevase murdmise eest, leevendades samal ajal üleminekuperioodil „salvesta täna, dekrüpteeri hiljem" riske. Hübriidrežiimi kasutamine peamiselt pärandühilduvuse säilitamiseks lükkab paratamatult edasi postkvant-krüptograafia kvantkindluse täieliku realiseerumise. Vt lähemalt selle kompromissi kohta jaotist A.5.1.

3. Paralleelne üleminek. See mudel kasutab kõrvuti kahte eraldiseisvat süsteemi: üks täielikult klassikaline ja tagasiühilduv, teine täielikult postkvant-krüptograafia toega. Andmeid ja teenuseid peegeldatakse mõlemas keskkonnas, võimaldades välistel pooltel suhelda klassikalise süsteemi kaudu, samas kui sisemised või turvatundlikud toimingud kasutavad postkvant-süsteemi. Niisugune lähenemine kahekordistab aga taristukulusid, suurendab võtmehalduse keerukust, nõuab rangelt sünkroniseeritud süsteeme ning avab süsteemi jällegi madaldusrünnetele.

4. Tarnija/platvormi veetav üleminek. Selle mudeli korral ei teosta lõppasutus postkvant-krüptograafiat ise, vaid tugineb selles vahetarkvarale, pilveteenuse andjatele, protokollitarnijatele või hallatud turbeplatvormidele, kelle ülesandeks on krüptograafilise uuenduse läbipaistev elluviimine. Organisatsioon tellib või häälestab postkvant-krüptograafia toega lõppseadmeid (nt TLS 1.3/PQC lüüsid, PQC-valmis HSMid või pilvepõhised KMS-teenused), säilitades vajalikes

kohtades klassikalise krüptograafia toe. See lähenemine delegeerib keerulisemad ülesanded tarnijatele ja ökosüsteemi osalistele, vähendades oluliselt teostuskoormust. Sellega kaasnevad aga sõltuvusriskid, krüptograafilise paindlikkuse vähenemine ning vajadus tarnijate põhjaliku taustakontrolli järele, tagamaks, et postkvant-krüptograafia teostused vastavad turvastandarditele ega sisalda varjatud madaldusvahendeid.

A.6 Postkvant-krüptograafiale üleminekut käsitlevad standardid ja juhised

Postkvant-krüptograafiliste lahenduste sobivuse ja turvalisuse hindamisel hangete ja juurutuse jaoks on peamine mõõdupuu lahenduste vastavus kehtestatud rahvusvahelistele ja riiklikele standarditele. Nende standardite järgimine tagab, et krüptograafia teostused on koostalitlusvõimelised, kontrollitud ja vastupidavad nii klassikalistele kui ka kvantohtudele.

Järgnev jaotis liigitab asjaomased standardid ja juhised kolme rühma: *algoritmistandardid*, *moodulite sertifitseerimisraamistikud* ning *ülemineku- ja evitusjuhised*.

A.6.1 Algoritmistandardid

Ametlikud postkvant-algoritmide standardid esitavad fundamentaalsed krüptograafilised primitiivid, mida lahendused peavad teostama. Nendele standarditele vastavus on turvahinnangu esimene samm.

- **NIST FIPS 203, 204 ja 205** on ametlikud USA föderaalsed infotöötlusstandardid (FIPS) postkvant-algoritmide jaoks: **ML-KEM** (Module-Lattice KEM), **ML-DSA** (Module-Lattice DSA) ja **SLH-DSA** (Stateless Hash-based DSA). 2024. aasta augustis avaldatud dokumendid määratlevad spetsifikatsioonid, parameetrid ja turvatasemed põhialgoritmide jaoks, mida enamik regulatiivasutusi praegu soovitab. Lähitulevikus on oodata täiendavaid standardeid, näiteks Falconi (FN-DSA) ja HQC jaoks.
- **ISO/IEC 18033-2** – see rahvusvahelise standardiorganisatsiooni ISO standard käsitleb krüpteerimisalgoritme. Seda on täiendatud postkvant-võtmekapseldusmehhanismidega, nagu **ML-KEM**, **FrodoKEM** ja **Classic McEliece**.
- **ISO/IEC 14888-3, 5 ja 6** – need dokumendid täpsustavad digisignatuuriskeemide standardimist. Konkreetselt käsitlevad tulevased dokumendid (ISO/IEC 14888-5 ja 14888-6) **ML-DSAd** ja **SLH-DSAd**, pakkudes üleüldist karkassi signatuuride valideerimiseks ja verifitseerimiseks postkvant-kontekstis.

A.6.2 Moodulite sertifitseerimisraamistikud

Standardid üksi ei suuda tagada turvalisust; rangetele turvanõuetele peab vastama ka rakenduskeskkond. See on eriti oluline füüsiliste turvamoodulite (HSM), kiipkaartide ja kriitilistes süsteemides ja taristus kasutatavate krüptograafiliste tarkvarateekide puhul. Tugev turberaamistik tagab, et postkvant-krüptograafia teostused ei ole mitte ainult algoritmiliselt õiged, vaid ka kaitstud füüsilise muutmise, kõrvalkanali rünnete ja halva operatiivjuhtimise eest.

- **FIPS 140-3** – Föderaalsete Infotöötlusstandardite (FIPS) sari määratleb krüptograafiamoodulite turvanõuded. Praegune redaktsioon FIPS 140-3 hõlmab juba ka uusi postkvant-krüptograafia standardeid. Mooduleid valideeritakse krüptograafiliste moodulite valideerimisprogrammi (CMVP) kaudu, mis hõlmab tarkvara, riistvara ja püsivara, andes kindlustunde,

et võtmed on kaitstud volitamata juurdepääsu eest ning moodul on vastupidav füüsilisele ja loogilisele muukimisele. Standardi nõuete täitmine on riiklike süsteemide puhul sageli kohustuslik.

- **Common Criteria (ISO/IEC 15408)** – Common Criteria on rahvusvaheline arvutiturbe sertifitseerimise standard. Tooteid saab hinnata vastavalt hindamistagatise tasemetele (*Evaluation Assurance Level*, EAL), alates EAL1-st (funktsionaalselt testitud) ja lõpetades EAL7-ga (formaalselt verifitseeritud disain ja testitud). Kõrge turvalisusega komponentide nagu riiklike identiteedivõtmete puhul tagab EAL4 või kõrgem hindamistagatise tase turvaomaduste range läbivaatamise. Ilmunud on juba esimesed postkvant-standarditega seotud kaitseprofiilidega sertifikaadid.

A.6.3 Ülemineku- ja evitusjuhised

Lisaks algoritmidele endile peavad organisatsioonid järgima juhiseid selle kohta, kuidas olemasolevaid süsteeme üle viia postkvant-krüptograafiale. Need dokumendid kirjeldavad riskijuhtimise, võtmehalduse ja protokollide lõimimise parimaid tavasid.

- **EL** – Euroopa Komisjon on avaldanud dokumendi „A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography“ [11], mis täpsustab ajakava ja soovitused, mida liikmesriigid peavad rakendama.
- **BSI** – Saksamaa Föderaalne Infoturbe Amet (Bundesamt für Sicherheit in der Informationstechnik) on avaldanud mitmeid põhjalikke juhendeid, sealhulgas „Migration to Post Quantum Cryptography“ [12] ja „Quantum-safe cryptography – fundamentals, current developments and recommendations“ [13].
- **TNO** – Madalmaade Rakendusteaduslike Uuringute Organisatsioon (TNO) avaldas postkvant-krüptograafiale ülemineku käsiraamatu, mis annab suurepärase ülevaate kõigistüleminekuga seotud küsimustest [14].
- **NIST SP 800-227** – see dokument sisaldab soovitusi võtmekapseldusmehhanismide jaoks ning pakub juhiseid KEM-ide kasutamiseks erinevates keskkondades. See kirjeldab, kuidas turvaliselt konfigureerida ja valideerida postkvant-võtmevahetusmehhanisme.
- **NIST IR 8547** – see dokumendikavand esitab NISTi eeldatava lähenemise postkvant-krüptograafiale üleminekuks ning erinevate ülemaailmsete asutuste ja organisatsioonide asjakohased ajakavad.
- **ETSI QSC WG** – Euroopa Telekommunikatsioonistandardite Instituudi (ETSI) kvantkindla krüptograafia töörühm keskendub postkvant-ülemineku praktilistele aspektidele. Nad avaldavad tehnilisi aruandeid, nagu **ETSI TR 103 619** (üleminekustrateegiad ja soovitused kvantkindlate skeemide jaoks) ja **ETSI TR 104 016** (korratav karkass kvantkindlate üleminekute jaoks), mis on Euroopa organisatsioonide jaoks väga aktuaalsed.
- **IETF PQUIP WG** – IETFi postkvant-krüptograafia kasutust protokollides uuriv töörühm töötab aktiivselt postkvant-krüptograafia lõimimisega argistesse internetiprotokollidesse, nagu TLS ja PKI. Nende dokumendikavandid määratlevad, kuidas postkvant-algoritmid suhestuvad olemasoleva taristuga, nagu sertifikaadid ja kätlused.[3]

[3] Complete list of RFC drafts is available at https://github.com/ietf-wg-pquip/state-of-protocols-and-pqc.