



Eesti postkvant-krüptograafia ülemineku riiklik teekaart

Aruanne

Version 1.0

30.04.2026

D-16-1248

Avalik

©2026 Cybernetica AS

Sisukord

Annotatsioon	6
1 Sissejuhatus	7
1.1 Motivatsioon.....	7
1.2 Teekaart	7
1.3 Ülevaade hetkeolukorrast.....	8
1.3.1 Kvantalgoritmid ja postkvant-krüptograafia	8
1.3.2 Kvantkindla krüptograafia kasutust reguleerivad õigusaktid.....	8
1.4 Tegevuste, ajakava ja ressursside kirjeldamine	9
1.4.1 Riskianalüüs.....	9
1.4.2 Üleminekuks vajalikud tegevused.....	9
1.4.3 Krüptoinventuur	9
1.4.4 Tegevuste ajakava.....	10
1.4.5 Ülemineku finantseerimine	10
1.5 Mõjuanalüüs.....	10
2 Ajakava olulisemad punktid	12
2.1 Üleminekuprotsessi osalised	12
2.2 Prioriteedikategooriad	14
2.3 Tegevused.....	14
2.3.1 Kategoriseerimine.....	14
2.3.2 Ettevalmistused.....	15
2.3.3 Alustavad tegevused.....	16
2.3.4 Inventuur	16
2.3.5 Üleminek	17
2.3.6 Aruandlus ja seire	18
2.3.7 Madala prioriteedikategooriaga organisatsioonide tegevused.....	18
2.3.8 Suurtarnijad.....	18
3 Riigi tegevused	20
3.1 Peamised tegevused ja ajakava	20
3.1.1 Esmased tegevused	20

3.1.2	Teisesed tegevused	20
3.2	Ministeeriumide ja pädevate asutuste soovituslikud tegevused	21
3.2.1	Kiireloomulisemad tegevused	21
3.2.2	Kõrgete prioriteedikategooriatega organisatsioonide tuvastamine	22
3.2.3	Organisatsioonide tegevuskavade võrdlemine	22
3.2.4	Tehtud otsuste dokumenteerimine	23
3.3	Kontrollimine ja seire	23
3.4	Teadlikkuse tõstmine	23
3.4.1	Koolitumisvõimaluste loomine	23
3.4.2	Kommunikatsioonitegevused	24
3.5	Üle-Euroopaline ja ülemaailmne koordineerimine	25
3.6	Eelarveliste vahendite leidmine	25
3.6.1	Rahastusvoorude korraldamine	25
3.6.2	Avalik sektor	26
3.6.3	Erasektor	27
4	Nõuete kehtestamine	28
4.1	Nõuete kehtestamise ajend	28
4.2	Nõuded	29
4.2.1	Peamised nõuded subjektidele	29
4.2.2	Aruandlus	30
4.2.3	Ajakava	31
4.2.4	Nõuded krüptograafilistele algoritmidele	31
5	Organisatsioonide tegevused	33
5.1	Allikad	33
5.2	Üleminekutegevuste jaotus	33
5.3	Kategoriseerimine	34
5.3.1	SC.1: organisatsiooni kategooria määratlemine	35
5.3.2	SC.2: ülemineku edasilükkamisega seotud riskide analüüs	36
5.3.3	SC.3: tutvumine väljapakutud ülemineku ajakavaga	36
5.4	Üleminekutegevused madala prioriteedikategooria (IV kategooria) jaoks	36
5.4.1	LP.1: tarnijate tuvastamine	38
5.4.2	LP.2: tarnijate teavitamine	39
5.4.3	LP.3: alternatiivide kaalumine	39

5.5 Üleminekutegevused teiste prioriteedikategooriate jaoks (OP)	39
5.5.1 Ettevalmistused	40
5.5.2 Krüptoinventuur	44
5.5.3 Elluviimine	48
5.5.4 Seire	52
5.6 Väljast tellimine	54
6 Tähelepanekud eduka ülemineku saavutamiseks.....	56
6.1 Piirangud	56
6.1.1 Heterogeensus	56
6.1.2 Keerulisemate infosüsteemidega organisatsioonid	56
6.1.3 Erasektor	57
Lisa A Ülevaade postkvant-krüptograafia hetkeseisust.....	67
A.1 Kvantarvutus	67
A.1.1 Kvantalgoritmid	67
A.1.2 Kvantarvutuse arengusuunad	68
A.2 Postkvant-krüptograafia	69
A.2.1 Kaasaegne krüptograafia	69
A.2.2 Postkvant-krüptograafia	71
A.2.3 Hübriidskeemid	74
A.2.4 Standardiseerimine	75
A.3 Postkvant-krüptograafia teostused	76
A.3.1 Krüptoteegid	76
A.3.2 Krüptograafilised protokollid	78
A.3.3 Postkvant-krüptograafia riistvaralistes komponentides	79
A.4 Lüngad tehnoloogia arengus ning edasine uurimistöö	79
Lisa B Ülevaade krüptoinventuuri võimalikest meetoditest	81
B.1 Terminoloogia	81
B.1.1 Eri tüüpi varad	81
B.1.2 Krüptograafiliste varade avastamise ja inventuuri protsessid	82
B.1.3 CADI	83
B.2 Olemasolevate allikate ülevaade	83
B.2.1 Läbivad jutupunktid	83

B.2.2	Täiendavad tähelepanekud ja märkused	85
B.3	Infotehnoloogilised vahendid CADI jaoks	90
B.3.1	Krüptograafiliste varade loend (CBOM)	91
B.3.2	CADI-t toetavate IT-vahendite kategooriad	92
B.3.3	CADI töövahendite funktsionaalsused	93
B.3.4	Olemasolevad töövahendid CADI jaoks	93
B.4	Olemasolev (teadus)kirjandus / Kuidas edasi?	96
B.4.1	CADIle fookuseeruvad allikad	96
B.4.2	Üldised PQCle ülemineku tegevuskavad ja juhised	97
Lisa C	Üleminekut toetav inimressurss Eestis	99
C.1	Metoodika	99
C.2	Tulemused	100
C.2.1	Olemasolev inimressurss	100
C.2.2	Inimressursi kasvatamise võimalused	100
Lisa D	Riskianalüüs	102
D.1	Uuendatud organisatsioonide kategooriad	103
D.2	Riskid	104

Annotatsioon

Kvanttehnoloogia kiire arengu tõttu muutuvad lähitulevikus tänased krüptograafilised lahendused ebatavaliseks. See ei ohusta üksnes tänaste krüptograafiliste võtmete turvalisust, vaid mõjutab laiemalt ka paljude praegu kasutusel olevate krüptoalgoritmide turvahinnanguid ning andmete pikaajalise konfidentsiaalsuse garantiisid. Euroopa Liit on seadnud eesmärgi viia kõrge riskiga infosüsteemid hiljemalt 2030. aastaks ning kõik süsteemid hiljemalt 2035. aastaks üle postkvant-krüptograafia. Kuigi need tähtajad võivad näida kauged, on riiklike infosüsteemide arendus- ja uuendustsüklid pikad ning tegelik ettevalmistusaeg seetõttu oluliselt lühem.

Postkvant-krüptograafilised lahendused on juba täna olemas ning nende kasutuselevõttu on võimalik alustada kohe. Eesti digiriigi eripära on, et krüptograafia on kasutusel väga paljudes süsteemides ning on sageli sügaval peidus. Mitmete teenuste, näiteks identiteeditaristu ja teiste turvakriitiliste e-teenuste üleviimine nõuab märkimisväärset arendus- ja testimistööd. Ülemineku ajakava mõjutavad oluliselt ka riiklike infosüsteemide arendus- ja hanketsüklid: suurte süsteemide uuendamine, uute tehnoloogiate juurutamine ning lahenduste jõudmine kõigi kasutajateni toimub järk-järgult mitme aasta jooksul.

Oluline on, et postkvant-krüptograafia nõuded jõuaksid võimalikult kiiresti uutesse hangetesse, arendusprojektidesse ja süsteemide uuendamisse. Muidu tekib risk, et lähiaastatel luuakse või uuendatakse süsteeme, mida tuleb peagi uuesti ümber teha. Seetõttu peaksid uued lahendused olema kavandatud krüptograafiliselt paindliku arhitektuuriga, hõlmama kasutatud krüptograafiliste lahenduste dokumentatsiooni ning sobima postkvant-krüptograafiliste lahenduste kasutuselevõtuks.

Lisaks mõjutavad ülemineku edukust ka infosüsteemide tehniline ajakohasus ja õigusruum. Vananenud tarkvaraplatvormid võivad takistada uute krüptograafiliste lahenduste kasutuselevõttu. Samuti sõltub ülemineku tempo sellest, kas krüptograafia kehtestatakse normatiivraamistik, mis toetab ülemineku elluviimist kogu riigis. Riik saab mõjutada ülemineku tempot läbi riiklike arhitektuurinõuete, turvanõuete, hankepoliitika ning koostöö tehnoloogiapartneritega. Samal ajal vastutavad konkreetsete e-teenuste ja infosüsteemide üleviimise eest neid käitavad asutused. Seetõttu on vaja, et asutused planeeriksid üleminekutegevusi varakult ning määraksid selge vastutaja postkvant-krüptograafia ülemineku juhtimiseks.

Ülemineku planeerimise keskseks eelduseks on spetsiifilise infosüsteemi krüptoinventuuri läbi viimine. Paljudes süsteemides ei ole täpselt kaardistatud, millist krüptograafiat ja millistes süsteemi komponentides kasutatakse. Ilma sellise ülevaateta ei ole võimalik hinnata ülemineku mahtu ega seada realistlikke prioriteete. Süsteemide krüptoinventuur on seetõttu üks oluliseid samme kogu ülemineku käivitamisel.

Mitmetes valdkondades, näiteks tervishoius, hariduses ja finantssektoris, toimub infosüsteemide arendus koostöös erasektori arendajate ja rahvusvaheliste tarnijatega. Seetõttu on oluline, et postkvant-krüptograafiliste uuenduste nõuded esitataks varakult nii hangetes kui ka koostöösuhetes. Ilma selleta võib süsteemide uuendamine sõltuda tarnijate arendusplaanidest ja venida oluliselt pikemaks.

Kokkuvõttes tähendab postkvant-krüptograafia üleminek Eesti jaoks ulatuslikku ja pikaajalist tehnoloogilist muutust. Arvestades süsteemide hulka, nende keerukust ning arendus- ja juurutustsüklite pikkust, on oluline alustada üleminekuga viivitamata, et tagada riigi digiteenuste turvalisus ka tulevikus.

1 Sissejuhatus

1.1 Motivatsioon

Rahvusvahelises kontekstis on üleminek postkvant-krüptograafiale (PQC) juba alanud. USA Riiklik Standardi- ja Tehnikainstituut (NIST) on standardiseerimas kvantkindlaid algoritme, NATO ja Euroopa Liit on käivitanud vastavad rakendusprogrammid ning mitmed riigid liiguvad kiiresti edasi PQC üleminekuplaanidega. Eesti kui maailma üks digitaalsemaid riike peab püsima nendega samas tempos või sellest ees, et säilitada oma senist töökindlust, usaldusväarsust ja julgeolekut.

Üleminek kvantkindlatele tehnoloogiatele ei ole võimalik üleöö. Tegemist on tehniliselt keeruka mitmeaastase protsessiga, mis eeldab strateegilist planeerimist, oskusteabe arendamist, ressursside koordineerimist ning selgelt sõnastatud tegevuskava. Väljavahetamist vajavad algoritmid, protokollid, tarkvarakomponendid ja teenused kogu riigi digitaristus. Edukaks läbiviimiseks on vajalik terviklik tegevuskava, mis toob välja peamised tegevused ja alamtegevused, nende omavahelised sõltuvused, ajakava, ressursivajaduse ja võimalikud rahastusallikad.

Nende vajaduste lahendamiseks kuulutas Justiits- ja Digiministerium välja riigihanke „Postkvant-krüptograafia riiklik teekaart“ (viitenumber 292945), mille eesmärk on luua ühtne ja rakendatav strateegiline karkass kvantkindlate tehnoloogiate kasutuselevõtuks Eestis. Hanke tehniline kirjeldus [1] toob välja, et:

Terviklik postkvant-krüptograafia strateegiline teekaart ja tegevuskava on vajalikud, et:

1. kaitsta Eesti kriitilisi infosüsteeme (sh andmekogusid) (Eesti digiteenuste ja andmevahetuse kaitse kvantarvutite mõju eest);
2. juhtida tehnoloogilise muudatuse kasutuselevõttu (plaanides ja astudes praktilisi samme kvantkindlate tehnoloogiate kasutusele võtmiseks);
3. tõsta avaliku sektori spetsialistide teadlikkust.

Lähtudes hanke tehnilisest kirjeldusest on aruandes esitatud soovitused eelkõige suunatud avalikule sektorile. Samas on tõenäoline, et avalikus sektoris kehtestatud nõuded ja praktikad hakkavad tulevikus mõjutama ka erasektorit.

1.2 Teekaart

Aruande põhiosa moodustab teekaart – komplekt tegevusi erinevatele pooltele koos ajakavaga nende tegevuste jaoks ja tegevuste omavaheliste seoste kirjeldustega. Teekaart nimetab ka eeldatava ressursivajaduse nende tegevuste tegemiseks ning soovib võimalikke rahastusallikaid. Esitatud tegevuskava täitmise korral jäävad kvantarvutitest lähtuvad ohud Eestis kasutusel olevate infosüsteemide turvalisusele suure kindlusastmega realiseerumata. See usk põhineb mõjuanalüüsil, mille projekti viimase osana läbi viisime.

Postkvant-krüptograafiale üleminekuga seoses ette nähtavaid tegevusi ja ajakava kirjeldab peatükk 2. Samuti kirjeldab see peatükk tegevuste subjekte – organisatsioone, kellele teekaart annab konkreetseid tegevusjuhised. Organisatsioone on kolme liiki: ühed koordineerivad, teevad järelevalvet ja jaotavad ressursse, teised kehtestavad nõuded ja leiavad ressursid ja kolmandad viivad tegevused ellu. Juhised erinevat liiki organisatsioonidele on toodud vastavalt peatükki-

des 3, 4 ja 5. Peatükkide struktuur lähtub eesmärgist, et iga organisatsioon leiaks enda kohta käivad ülesanded ja soovitused ennekõike „oma“ peatükist; üldisemad ajakava seosed teistega on toodud peatükis 2. Organisatsiooni esindaja peaks lugema kõigepealt peatükki 2, mis kirjeldab tegevuskava põhialuseid, ja seejärel „oma“ peatükki.

Teekaardi koostamine koosnes kahest põhilisest osast: olemasoleva olukorra ülevaate loomisest ning sellest lähtuvalt tegevuste soovitamisest (ühes protsessi osaliste, sõltuvuste, ajakava ja vajaminevate ressursside kirjeldamisega). Selline jaotus oli ette nähtud juba projektiplaanis ja enne seda riigihanke kirjelduses, kus teine osa oli küll veel jagatud omakorda kaheks: „strateegilise suuna määratlemine“ ning „tegevuskava ja elluviimine“.

1.3 Ülevaade hetkeolukorrast

Töö käigus koostasime ülevaate postkvant-krüptograafia hetkeseisust ning sellega seotud regulatsioonidest ja rahvusvahelistest arengutest. Kõigepealt käsitletakse tehnoloogilist tausta ja peamisi kontseptsioone, seejärel analüüsitakse Eesti õiguslikku raamistikku ning lõpus tutvustatakse teiste riikide tegevuskavasid ja strateegiaid, mis võivad mõjutada Eesti avaliku sektori üleminekut postkvant-krüptograafiale.

1.3.1 Kvantalgoritmid ja postkvant-krüptograafia

Lisa A annab ülevaate sellest, kuidas kvantarvutid mõjutavad kasutuselolevate krüptoalgoritmide turvataset. Siin esitatav kirjeldus kvantarvutite mõjust põhineb küll eelkõige teadusartiklidel, kuid krüptoalgoritmide töö kohta on olemas ka populaarteaduslikke kirjeldusi.

Järgmiseks refereerib sama lisa kvantarvutite valdkonna spetsialistide arvamust sellest, millal võiksid valmida krüptograafiliselt märkimisväärsed kvantarvutid. Lugeja leiab sealt teadusartiklidel põhineva ülevaate olemasolevatest eeldatavalt kvantarvutikindlatest asümmeetrilise krüpteerimise ja signeerimise algoritmidest. Samuti refereeritakse avalikke allikaid nende algoritmide realiseerimise ja standardimise hetkeseisu kohta.

Ülevaade lõpeb aruteluga, millistes valdkondades esialgu veel puuduvad täielikult rahuldavad (piisav efektiivsus, mõistlikud turva(arhitektuuri)eeldused) kvantarvutikindlad krüptoalgoritmid või -protokollid. Kirjeldus põhineb teadmistel postkvant-krüptograafia-alase teadustegevuse hetkeseisust ning Eesti e-riigi komponentidest.

1.3.2 Kvantkindla krüptograafia kasutust reguleerivad õigusaktid

Euroopa Liidul on ootus, et liikmesriigid tegelevad postkvant-krüptograafiaga ja sellele minnakse õigeaegselt üle. Sellest annavad märku mitmed poliitikadokumendid ja õigusaktid, sh:

- **Komisjoni soovitus (EL) 2024/1101**, 11. aprill 2024, postkvant-krüptograafiale ülemineku koordineeritud rakendamise tegevuskava kohta [2] (**komisjoni soovitus**);
- **postkvant-krüptograafiale ülemineku koordineeritud rakendamise tegevuskava** (ingl *A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography*) [3] (**liidu tegevuskava**), mis koostati komisjoni soovituse EL 2024/1101 järelmina;
- Küberturvalisuse strateegia 2024–2030 „Läbivalt IT-vaatlikum Eesti“ [4];
- jaanuaris 2026 avaldatud **küberturvalisuse 2. määruse ettepanek** (ingl *k Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and ICT supply chain security*

and repealing Regulation (EU) 2019/881; CSA2) [5] ja sellega seondult **küberturvalisuse 2. direktiivi muudatuste panek** (ingl k *Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2022/2555 as regards simplification measures and alignment with the [Proposal for the Cybersecurity Act 2]*) [6].

Peatükk 4 esitab põhjendused postkvant-krüptograafia ülemineku puudutavate seadusmuudatuste kavandamiseks.

1.4 Tegevuste, ajakava ja ressursside kirjeldamine

Olukorrast ülevaate loomisele järgnes analüüs ja tegevuskava koostamine.

1.4.1 Riskianalüüs

Lisa D esitab analüüsi riskidest, mis on seotud postkvant-krüptograafia üleminekuuga. See lisa pakub kõigepealt välja organisatsioonide jaotuse vastavalt nende riskitasemele. Riskitase sõltub organisatsiooni töödeldavate andmete tundlikkusest, organisatsiooni pakutavate teenuste olulisusest ja organisatsioonide vastastikustest sõltuvustest. See kategoriseering on olulisel kohal ka väljapakutud tegevuskavades.

Organisatsioonide kategoriseerimisele järgneb riskide endi kirjeldus. Loetletud riskid pärinevad nii kirjandusest kui ka aruande autorite teadmistest ja kogemustest. Organisatsiooni avatus mingile ohule sõltub tema kategooriast. Riskitase sõltub ka sellest, milliseks ajaks organisatsioon püüab postkvant-krüptograafia üle minna. Osad riskid kasvavad ajas, osad kahanevad, olenevalt sellest, kas nad lähtuvad põhiliselt väliskeskkonnast või sisemisest, kontrollitud keskkonnast.

1.4.2 Üleminekuks vajalikud tegevused

Paljud olemasolevad tegevuskavad ja juhised kirjeldavad tegevusi, mida üks organisatsioon peaks tegema, et krüptograafiliselt märkimisväärsed kvantarvutid teda ei ohustaks (vähemalt mitte rohkem kui klassikalised arvutid). Ka siin välja pakutavad tegevused ei erine neist oluliselt.

Tegevuste nimekirja koostamise käigus sai selgeks, et organisatsioonid on need, kes tegevusi läbi viivad, aga nõudeid ja tähtaegu neile tegevustele ja saavutatavatele tulemusele esitavad teised institutsioonid. Seetõttu on üleminekuks vajalike tegevuste nimekiri koostatud kahes liinis. Üks neist nimekirjadest kirjeldab, mida tuleb üleminekuks ära teha. Teine kirjeldab, kuidas üleminek käib. Peatükid 3 ja 4 sisaldavad nii saavutatavate tulemuste kirjeldusi kui ka kontrollimeetmeid. Peatükk 5 annab juhiseid üleminekuks.

1.4.3 Krüptoinventuur

Postkvant-krüptograafia ülemineku võtmetegevus on ülevaate koostamine sellest, kus ja milliseid krüptoalgoritme organisatsiooni infosüsteemides kasutatakse. Krüptoinventuuri põhjalikuma kirjelduse leiab lisast B ja see on soovitatav lugemismaterjal neile, kes mingi organisatsiooni ülemineku eest hea seisma peavad. Kuna olemasolevad süsteemid ei ole sageli loodud viisil, mis toetaks krüptoinventuuri lihtsat läbiviimist, tuleb selle etapi jaoks plaanida ja varuda piisavalt aega.

1.4.4 Tegevuste ajakava

Aruandes esitatud tegevused ja nende ajastus põhinevad peatükis 2 kirjeldatud lähenemisel. Selles peatükis tuuakse välja üleminekuprotsessi olulisemad verstapostid, osalised ning prioriteedikategooriad, samuti tegevuste loogiline järjestus alates ettevalmistavatest sammudest ja inventuurist kuni ülemineku ning sellele järgneva seire ja aruandluseni. Ajakava kirjeldab, kuidas erinevad tegevused on omavahel seotud ning millises järjekorras on neid otstarbekas ellu viia. Riiklikud tegevused lähtuvad sellest raamistikust ning täpsustavad, milliseid samme on vaja ülemineku toetamiseks riigi tasandil astuda.

Tegevuste ajakavas on määratud tähtjad, millal vastavad tegevused peaksid olema lõpule viidud. Tähtaegade määratlemisel on lähtutud mitmest allikast. Üheks oluliseks sisendiks oli eespool kirjeldatud riskianalüüs. Lisaks arvestati Euroopa Liidu postkvant-krüptograafia ülemineku koordineeritud rakendamise tegevuskava [3]. Kolmanda lähtekohana võeti arvesse rahvusvahelisi arenguid ja tähtaegu, mida Eesti mõjutada ei saa, näiteks suurte tehnoloogiaettevõtete plaanid ja tegevuskavad.

Pärast nende lähtekohtade määratlemist hinnati tegevuste omavahelisi ajalisi sõltuvusi ning ajakulu, mida erinevate sammude elluviimine eeldab. Nende hinnangute põhjal kujunes aruandes esitatud ülemineku ajakava.

1.4.5 Ülemineku finantseerimine

Ülemineku finantseerimise juures on kaks põhilist küsimust: ülemineku maksumus ja võimalikud finantseerimisallikad. Samas ei piirdu kulud ainult ülemineku elluviimisega. Ka pärast postkvant-krüptograafia üleminekut on vajalik tagada süsteemide pidev ajakohasus, mis hõlmab näiteks lahenduste uuendamist, litsentside haldamist ja tehniliste komponentide uuendamist. Seetõttu ei tohiks tekkida arusaama, et pärast ülemineku lõpetamist sellega seotud kulud kaovad.

Pikemas vaates peaks krüptograafiliste lahenduste uuendamine kujunema loomulikuks osaks infosüsteemide regulaarse hoolduse ja arenduse tsüklist. See tähendab, et süsteemid peaksid olema krüptoagiilsed ning nende kasutatavat krüptograafiat tuleb regulaarselt hinnata ja vajadusel uuendada. Selline lähenemine ei ole seotud ainult postkvant-krüptograafiaga, vaid krüptograafia elutsükli juhtimisega laiemalt, mistõttu tuleb ka tulevikus planeerida vahendeid krüptolahenduste ajakohastamiseks.

Tegevuskava sisaldab autorite prognoosi ülemineku maksumuse kohta. See prognoos tugineb autorite hinnangutele (suhteliselt) sarnaste üleminekute maksumuse kohta ning oletustele selle kohta, kui mitu korda on kõik üleminekut vajavad süsteemid suuremad neist süsteemidest, millega autoritel on kokkupuuteid olnud. Esitatud hinnangud on indikatiivse iseloomuga, kuivõrd tegevuskava koostamise raames ei olnud eesmärgiks koostada detailset ülevaadet kõigist riiklikest infosüsteemidest. Täpsema maksumushinnangu andmine eeldaks eraldi ja põhjalikumat analüüsi, mis hõlmaks infosüsteemide detailset kaardistamist ning tihedamat koostööd nende omanikega.

1.5 Mõjuanalüüs

Tegevuskava loomise viimane samm on mõjuanalüüsi koostamine. Mõjuanalüüs põhjendab, miks siin esitatav tegevuskava „töötab“, st mis annab alust uskuda, et seda järgides jõuab tõepoolest postkvant-krüptograafia juurutamiseni kõikjal Eestis. Mõjuanalüüsi aluseks on võetud Justiits- ja Digiministeriumi ning Riigikantselei metoodika [7], mida on kohandatud vastavalt projekti

oludele.

Kuigi aruanne on koostatud eelkõige Eesti avaliku sektori organisatsioonidele suunatuna, arvestatakse nii mõjuanalüüsis kui ka tegevuskava eri osades ka erasektori rolli ja võimalikke mõjusid. Avaliku ja erasektori süsteemid, teenused ning tarnesuhted on tihedalt seotud ning paljud avalikus sektoris kasutatavad lahendused pärinevad erasektori tarnijatelt, sealhulgas rahvusvahelistelt ettevõtetest. Samuti on tõenäoline, et pikemas vaates puudutab postkvant-krüptograafia üleminek ka erasektorit laiemalt.

2 Ajakava olulisemad punktid

Põhipunktid:

- Euroopa Liidu soovitus on 2030. aastaks muuta kvantarvutikindlaks kõrge riskiga süsteemid ning 2035. aastaks kõik riigi süsteemid.
- Infosüsteemide, sideturbe- ja salvestussüsteemide jaoks on postkvant-krüptograafilised lahendused olemas ning üleminekuga saab alustada kohe täna.
- Eesti ei saa üleminekuga venitada, sest krüptograafia on meie süsteemides sügaval ning mõnede e-teenuste (nt e-hääletamine) üleviimine nõuab palju tööd.

Postkvant-krüptograafia üleminekut näevad ette ja soovivad järgmised poliitikadokumendid:

- **Komisjoni soovitus (EL) 2024/1101**, 11. aprill 2024, postkvant-krüptograafia ülemineku koordineeritud rakendamise tegevuskava kohta [2] (**komisjoni soovitus**);
- **postkvant-krüptograafia ülemineku koordineeritud rakendamise tegevuskava** (ingl *A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography*) [3] (**liidu tegevuskava**).

Liidu tegevuskava (p 4.1) soovib rakendada järgmist ajakava:

1. **31.12.2026** – riik on ellu viinud **esmased tegevused**.
2. **31.12.2030** – riik on ellu viinud **teiseseid tegevused**.
3. **31.12.2035** – riik on valmis kvanttohtudega silmitsi seisma.

Esmased tegevused:

- käivitatud PQC ülemineku planeerimine ja piloodid
- koostatud esmane riiklik teekaart

2026

Teiseseid tegevused:

- **kõrge riskiga** kasutusjuhtude PQC-üleminek lõpetatud
- **keskmise riskiga** kasutusjuhtude PQC-planeerimine ja piloodid lõpetatud,
- Kvantturvalised tarkvara- ja püsivara uuendused vaikumisi lubatud

2030

Lõpptähtaeg:

- **keskmise riskiga** kasutusjuhtude üleminek lõpetatud
- **madala riskiga** kasutusjuhtudes on üleminek mõistlikus ulatuses tehtud

2035

Joonis 1. Soovituslik ajaraam Euroopa Komisjoni järgi: kõrge riskiga organisatsioonide ülemineku lõpuleviimine 2030. aastaks ning kõigi organisatsioonide puhul 2035. aastaks

2.1 Üleminekuprotsessi osalised

Siin esitatavad soovitusel on suunatud kolme olulist liiki organisatsioonidele või nende klassidele.

Seadusandlikud institutsioonid on institutsioonid, mis kehtestavad siintoodud soovitusel tegevuste ja tähtaegade kohta õigusaktidega. Peatükk 4 sisaldab konkreetseid soovitusi, milliseid õigusakte tuleks täiendada või muuta, et tagada efektiivne üleminek postkvant-krüptograafia.

Lisaks nõuete kehtestamisele, mis panevad paika postkvant-krüptograafiale ülemineku tegevuste oodatavad tulemused ja tähtajad, annavad seadusandlikud institutsioonid välja ka õigusakte, mis võimestavad täidesaatvaid institutsioone üleminekut korraldama ja seirama. Seadusandlike institutsioonide tegevuste hulka võib kuuluda ka eelarvevahendite leidmine, mida postkvant-krüptograafiale ülemineku täiendavalt vajab, võrreldes infosüsteemide regulaarse hooldusega.

Täidesaatvad institutsioonid korraldavad ja koordineerivad organisatsioonide postkvant-krüptograafiale üleminekut. Nad tuvastavad väga kõrge ja kõrge prioriteediga organisatsioonid ning toetavad ja kontrollivad neid infosüsteemide korrastamisel ja uuendamisel. Nad seisavad hea selle eest, et täiendavad eelarvevahendid jõuaksid õigel ajal sinna, kus neid on vaja kasutada, ning korraldavad informatsiooni liikumist nii Eestis kui ka väljaspool, sealhulgas ülemineku puudutatud isikute teadlikkuse ja teadmiste taseme tõstmist.

Organisatsioonid peavad seisma hea selle eest, et nende infosüsteemides kasutatavad krüptograafilised algoritmid saaksid välja vahetatud kvantturvaliste algoritmide vastu. Nad peavad seejuures silmas pidama väljavahetamise lõpp- ja vahetähtaegu, mille nende jaoks kehtestavad seadusandlikud institutsioonid. Üleminekul toetavad ja kontrollivad neid täidesaatvad institutsioonid.

Lisaks neile kolmele protsessiosaliste klassile on ülemineku protsessis oma roll ka mõningatel teistel organisatsioonidel. See roll on aga pisut reaktiivsem: tegutsema hakatakse eeldatavasti siis, kui mõni eelmainitud osalistest seda palub. Sellised organisatsioonid on näiteks:

- **koolitajad.** Infosüsteemides krüptoalgoritme tegelikult välja vahetavad arendajad ja administraatorid, samuti väljavahetamisprojekte vedavad projektijuhid vajavad ilmselt täiendavaid teadmisi, et see vahetus lihtsamini läheks. Kuna inimesi, kes uusi oskusi vajavad, on üsna palju, siis on mõttekas panna paika koolitustegevuste struktuur ja kaasata neisse organisatsioone, mille põhitegevus on teadmiste ja oskuste andmine;
- **teavitajad.** Näeme ette, et kvantarvutitest lähtuvate ohtude teadvustamine potentsiaalselt ohustatud infosüsteemide haldajate seas vajab selgelt piiritletud teavitustegevusi. Nende elluviimine võib jääda avalikke suhteid korraldavatele organisatsioonidele;
- **tarnijad ja haldajad.** Teekaardis avaldatav tegevuskava on formaalselt suunatud avaliku sektori organisatsioonidele. Need organisatsioonid tellivad aga IT-süsteemide arendust (sh karbitooteid), haldamist jms eraettevõtelt, sh nii Eestist kui ka väljastpoolt. Oluline osa algoritmide vahetusest jääb ilmselt tarkvara tootja ettevõtete teha;
- **Euroopa Liidu institutsioonid.** Teekaarti koostades on tegevuste ja tähtaegade juures lähtutud Euroopa Liidu postkvant-krüptograafiale ülemineku tegevuskavast [3]. Selle tegevuskava järgi peab ülemineku postkvant-krüptograafiale toimuma koostöös teiste liikmesriikide ja Euroopa Liidu institutsioonidega, eriti võrgu- ja infoturbe koostöörühmaga;
- **Suured rahvusvahelised ettevõtted.** Nemad teekaardis kirjeldatud tegevustes ei osale, st neilt osalemist ei paluta. Neil ettevõtetel on aga omad postkvant-krüptograafiale ülemineku tegevuskavad, milles ette nähtud ajakavaga peab Eesti teekaart ühilduma. Suurte rahvusvaheliste ettevõtete kavade mõjutamine on Eesti institutsioonide jaoks ilmselt keeruline, kuigi mitte täiesti võimatu¹.

¹ – Internetis: <https://ria.ee/uudised/ria-valmistab-ette-id-kaardi-tarkvara-kauguuenduse-voimalust>

2.2 Prioriteedikategooriad

Siin esitatav tegevuskava näeb ette, et organisatsioonile rakenduv ajakava sõltub sellest, kui oluline on organisatsiooni infosüsteemides välja vahetada kvantmurtavad krüptoalgoritmid. Iga organisatsioon on kategoriseeritav ühte neljast prioriteedikategooriast, mida siin tähistavad rooma numbrid I–IV või sõnad „väga kõrge“, „kõrge“, „keskmine“ ja „madal“. Kõrgemasse kategooriasse kuuluvatel organisatsioonidel tuleb üleminekutegevused (vähemalt osaliselt) kiiremini läbi viia, samuti on meie soovitusel neile põhjalikumad.

Kategooriatesse jagamisest järeldeb kohe, et organisatsioonid peavad varakult teada saama, kas nad kuuluvad kõrge(ima)sse kategooriasse; see teave peab jõudma kõigi organisatsioonideeni enam-vähem samal ajal. Tegevuskava pakub välja küsimustiku, mille alusel organisatsioon (või ka erasektoris kuuluv organisatsioon) saab otsustada, millisesse kategooriasse ta kuulub. Organisatsioonidel ei ole hetkel seadusest ega muust õigusaktist tulenevat kohustust oma prioriteedikategooria hindamiseks. Kuivõrd 2026. aasta jooksul sellist seadusemuudatust vastu võtta ei jõutaks ning kuivõrd tegevuskava subjektidele oleks ka seadusemuudatuse vastuvõtmise ja jõustumise järel vaja anda mõistlikult aega vajalike ettevalmistuste tegemiseks, võiks väga kõrgesse või kõrgesse kategooriasse kuuluvaid organisatsioone nende prioriteedikategooriast teavitada pigem täidesaatev institutsioon. Samas ei vabastaks see kokkuvõttes organisatsioone vastutusest õigeaegselt oma prioriteedikategooria välja selgitada.

Krüptoalgoritmide väljavahetamise prioriteedikategooria ei ole sama, mis organisatsiooni staatus elutähtsa teenuse tarnijana (või tarnimise korraldajana). Samuti ei tähenda tundlike andmetega opereerimine veel automaatselt kõrgesse kategooriasse liigitumist, ehkki mingi korrelatsioon nende vahel kindlasti on. Tõepoolest, elutähtis teenus ei pruugi olla infotehnoloogiline, või siis sisaldab see üksnes väikest infotehnoloogilist ja krüptograafiast sõltuvat komponenti. Samuti võib andmeid töödelda viisil, mis krüptograafia rakendamist ei nõua. Prioriteedikategooria muudab kõrgeks ennekõike see, kui tundlikke andmeid töödeldakse viisil, kus nende konfidentsiaalsuse säilimine sõltub avaliku võtmega krüptograafia turvalisusest.

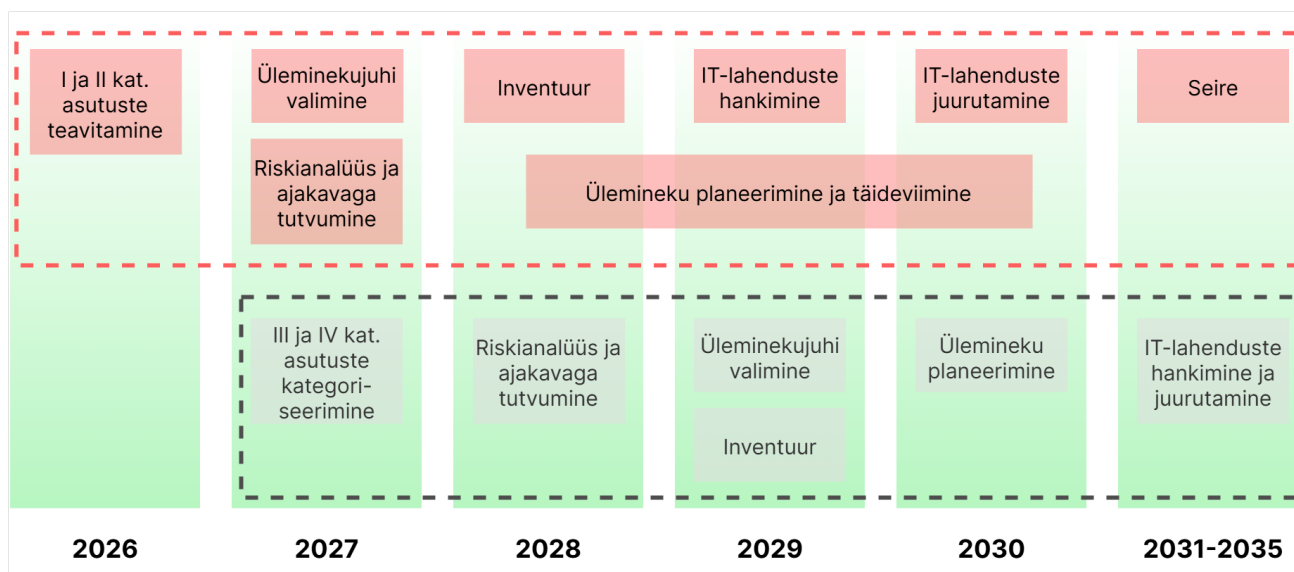
Organisatsioonil võib olla mitu funktsiooni, mõned neist põhilised, mõned toetavad. Mõistlik võib olla prioriteedikategooria omistada igale funktsioonile eraldi; organisatsiooni kategooria on sellisel juhul kõigi funktsioonide kategooriatest kõrgeim. Organisatsiooni prioriteedikategooria määrab omakorda tähtsused ja protseduurid selle organisatsiooni konkreetsete funktsioonide üleminekuks postkvant-turvalisele krüptograafiale. Teiste funktsioonide üleviimiseks võib aega olla rohkem. Täpse(ma)d plaani(d) iga funktsiooni jaoks koostab organisatsioon ülemineku käigus.

2.3 Tegevused

2.3.1 Kategoriseerimine

Nagu eespool märgitud, algab organisatsiooni ülemineku postkvant-krüptograafiale tema prioriteedikategooria leidmisest. „Väga kõrgesse“ või „kõrgesse“ kategooriasse kuuluvad organisatsioonid tuleks välja selgitada 2026. aasta 3. kvartali jooksul. Prioriteedikategooria tuvastamine on organisatsiooni enda vastutusel, aga täidesaatvad institutsioonid peaksid siin ka ise näitama initsiatiivi, püüdes tuvastada ja informeerida kõrge ja väga kõrge prioriteediga organisatsioone. Riskipõhine ülemineku ajakava on esitatud joonisel 2.

Juhul kui organisatsioon ei kuulu kõrgesse või väga kõrgesse prioriteedikategooriasse, tuleb tal endal välja selgitada, kas ta kuulub kategooriasse „keskmine“ või „madal“. Täidesaatvate institutsioonide initsiatiivile nemad loota ei saa. Küll aga peaksid täidesaatvad institutsioonid kor-



Joonis 2. Riskipõhine ülemineku ajakava: väga kõrge ja kõrge riskiga organisatsioonid peavad ülemineku varem, keskmise ja madala riskiga organisatsioonidel on pikem ajaraam

raldama teavituskampaania, mis hoolitseks selle eest, et õiged inimesed kõigis organisatsioonides teaksid, et kvantarvutid võivad nõrgendada kasutuselolevaid krüptograafilisi algoritme. See kampaania võiks jõuda ainult mitte nende organisatsioonideni, vaid ka teiste organisatsioonide ja ettevõteteni, mis oma infosüsteemide uuendamise eest hoolt peavad kandma. Kampaania võiks toimuda 2026. aasta viimases ja 2027. aasta esimeses kvartalis. „Keskmisesse“ ja „madalasse“ prioriteedikategooriasse kuuluvad organisatsioonid võiksid sel juhul oma kategooria tuvas-tada 2027. aasta teises kvartalis. Kui selle käigus selgub, et nende kategooria peaks ikkagi olema „(väga) kõrge“, siis on neil veel võimalus teistele kõrgematesse kategooriatesse kuuluvatele organisatsioonidele järele jõuda.

„Väga kõrge“, „kõrge“ ja „keskmise“ prioriteedikategooria organisatsioonide ülemineku tegevused on oma struktuurilt pigem sarnased, ehkki detailides erinevad. Järgmised alapeatükid kirjeldavad neid tegevusi ja nende soovitatavat ajakava. „Madala“ prioriteedikategooria organisatsioonidele on ette nähtud eraldi loetelu tegevustest, mida kirjeldab peatükk 2.3.7.

2.3.2 Ettevalmistused

Ettevalmistavad toimingud võivad järgneda vahetult kategoriseerimisele, sest need analüüsivad põhjalikumalt, millistel põhjustel kuulub organisatsioon just sellesse prioriteedikategooriasse. Organisatsioon peaks enda jaoks välja selgitama, mis juhtub siis, kui ülemineku tegevused jäävad tegemata või hakkavad venima. Samuti tuleks oma organisatsiooni jaoks läbi mõelda ülemineku tõenäoline ajakava, pidades silmas siin soovitatavaid tähtaegu. Need toimingud võiksid olla tehtavad kolme kuu jooksul pärast kategoriseerimist (st 2026. aasta 4. kvartali jooksul organisatsioonides, mille kategooria on „(väga) kõrge“, ja 2027. aasta 3. kvartali jooksul organisatsioonides, mille kategooria on „keskmise“).

Ettevalmistavate toimingute sekka kuulub ka ülemineku eest vastutava juhi ja/või meeskonna paikapanek. „Kõrge“ ja „väga kõrge“ kategooria organisatsioonid peaksid seda tegema paralleelselt eelmiste tegevustega või isegi enne seda. „Keskmise“ kategooria organisatsioonid võivad sellega ehk oodata 2029. aastani.

2.3.3 Alustavad tegevused

Alustavate tegevuste käigus tuvastatakse organisatsiooni asukoht tarneahelates ja luuakse sise-mised struktuurid ülemineku läbiviimiseks. Organisatsioon (st ülemineku eest vastutavad isikud) peaks saama ülevaate sellest, kes on nende tarnijad ja teenusepakkujad ning millised lepingud on nendega sõlmitud — kas postkvant-krüptograafia ülemineku toetamist saab tarnijalt juba eeldada või vajavad need suhted täiendavat korraldamist (seda kuni tarnijast loobumiseni või tema väljavahetamiseni).

Organisatsiooni juhtkond ja muud sidusrühmad tuleks hoida teadlikena ülemineku toimumisest, selle vajadusest ja vajadustest ning ülemineku hetkeseisuga tutvumise viisidest.

Organisatsioon peab tuvastama inimesed, kes ülemineku tegelikult läbi võiksid viia. See võib vajada organisatsiooni üldise krüptograafilise küpsuse hindamist, et mõista, kas need inimesed on organisatsioonis põhimõtteliselt olemas ja milline võiks neil olla asjakohane kogemus. Töötajate kompetentsuse tõstmiseks näeb sinne tegevuskava ette võimalust neid koolitada. Siin esitatud soovitude järgi võiksid valmida õpimoodulid või kursused, mis aitaksid tõsta nii tehniliste kui ka projektide juhtimisega tegelevate inimeste teadmiste taset postkvant-krüptograafia üleminekuuga seotud teemadel.

Kirjeldatud tegevused võiksid „väga kõrge“ ja „kõrge“ prioriteedikategooriaga organisatsioonides toimuda 2027. aasta jooksul. Krüptograafilise küpsuse hindamine ja tarnijate tuvastamine saavad seejuures toimuda juba talvel ja kevadel. Neile tegevustele saab järgneda juhtkonna ja muude sidusrühmade põhjalikum kaasamine.

Üleminekutegevuste mehitamine piisava oskusteabega töötajatega võib võtta kauem aega, sest siin soovitatud õppematerjale veel loodud ei ole. **Kui nende loomisega kohe alustada, võiks vajalikud õppematerjalid olemas olla 2027. aasta suve lõpuks.** Materjalide tellimist ja vastuvõtmist korraldaksid täidesaatvad institutsioonid. Pärast seda on võimalik neid materjale kasutada, nii et 2028. aasta veebruariks võiksid vajalikud inimesed olla varustatud vajalike teadmistega.

„Keskmise“ prioriteedikategooria organisatsioonides võivad alustavad tegevused jääda hilisemas aega, näiteks 2029. aasta algusesse. Meie nägemuses peaksid need olema läbi viidavad kolme kvartali jooksul, kuivõrd koolitusmaterjalid ja koolitatud inimesed on selleks ajaks juba olemas.

2.3.4 Inventuur

Krüptograafiliste varade tuvastamine ja inventeerimine on üks olulisemaid üleminekutegevusi. Selle käigus saab organisatsioon teada, milliseid tema varasid võib üleminek postkvant-krüptograafia mõjutada ja kuidas üleminek neist igaüht puudutab. Organisatsioon tuvastab riskianalüüsist lähtudes ülemineku jaoks kriitilised infovarad ja viib läbi kõigi krüptograafiliste varade inventuuri. Inventuuriga seotud tegevuste juurde kuulub ka tarnijate ja teenusepakkujatega ülemineku detailide osas kokkulepete saavutamine.

Inventuuriga seotud tegevused saavad alata siis, kui üleminekutegevused on mehitatud. „Väga kõrge“ ja „kõrge“ prioriteedikategooria organisatsioonides võiks inventuur toimuda alates 2028. aasta märtsist kuni 2029. aasta veebruarini. See algaks inventuuriplaaniga paikapanekest, mille juurde võib kuuluda eelarvestamine. Plaanimine võiks võtta umbes kolm kuud, millele järgneks inventuur ise. Kogu tegevuse käigus tuleks olla kontaktis oma tarnijatega, kelle tarkvara kasutatakse. Mingitel juhtudel võib olla mõistlik, kui organisatsioonidevahelist suhtlust korraldavad täidesaatvad institutsioonid.

„Keskmise“ prioriteedikategooria inventuur võiks siinse nägemuse kohaselt alata hiljem, 2029. aasta neljandas kvartalis. See võiks kesta lühemat aega kui kõrgematesse kategooriatesse kuuluvate organisatsioonide inventuur, sest inventeeritavaid varasid on ilmselt vähem ja selleks ajaks on olemas ka rohkem kogemusi inventuuri tegemisel. Leiame, et 2030. aasta maikuuks võiks „keskmise“ prioriteedikategooria organisatsioonide inventuur olla tehtud.

Krüptograafiliste varade inventuuri õnnestumine ja põhjalikkus on oluline eeldus ülemineku enda õnnestumisele. Seetõttu näeme me ette, et organisatsioonidel, vähemalt kõrgematesse prioriteedikategooriatesse kuuluvatel, tuleb lisaks inventuuri tegemisele ka aru anda sellest, kuidas neil tegemine õnnestub. Me oleme käesolevasse teekaarti plaaninud järelvalvetegevused. Inventuuri ja hiljem ülemineku üle järelvalve teostamine ja vajadusel abistamine on osa täidesaatvate institutsioonide tegevustest.

Krüptograafiliste varade inventuur tekitab organisatsioonidele eeldatavasti täiendavaid kulusid lisaks igapäevastele IT-süsteemide uuendamise ja hoolduse kuludele. Seetõttu peavad seadusandlikud institutsioonid leidma ja ette valmistama sobivad eelarvevahendid, mille organisatsioonide vahel jagamist korraldavad täidesaatvad institutsioonid. „Väga kõrge“ ja „kõrge“ prioriteedikategooriaga organisatsioonide krüptoinventuuri toetavad vahendid peaksid olemas olema 2028. aasta eelarves, „keskmise“ prioriteedikategooria organisatsioonide toetavad vahendid 2029. aasta omas. Ettevalmistustegevused peavad seega tehtud saama hiljemalt 2027. ja 2028. aastal.

2.3.5 Üleminek

Ülemineku põhiosa on kvantkindlate IT-lahenduste hankimine ja juurutamine. Hankimine võib endast kujutada nii lahenduste tarnijatelt tellimist kui ka sisemist arendust. Enne hankimist võib olla mõistlik koostada üleminekutegevuste eelarve. Olulisem aga on koostada üleminekuplaan ehk organisatsiooni isiklik teekaart.

Üleminekuplaanis on vaja fikseerida, millised kvantturvalised algoritmid kasutusele võetakse. Siinse tegevuskava järgi võiks seadusandja kehtestada algoritmide valiku kriteeriumid ning organisatsioonid järgiksid neid kriteeriumeid. Järgida tuleb neid nii organisatsioonisiseses arendustöös kui ka tarnijatele esitavates nõuetes.

Krüptoinventuur võib tuvastada krüptograafilisi varasid, näiteks kasutusel olevaid sertifikaate, mis on loodud kvanthaavatavaid algoritme kasutades ja mille väljavahetamine on osa postkvantkrüptograafia üleminekust. Kui üleminekuplaan fikseerib, millal kvantkindlad versioonid tarkvarast juurutatud saavad, siis tuleks teha ka nii, et need sertifikaadid aeguvad selle juurutamisega võrreldes mitte väga palju hiljem. Tõepoolest, enne kvanthaavatavate sertifikaatide väljavahetamist ei ole postkvantkrüptograafia üleminek lõpetatud. Sertifikaatide eluea määramine või lühendamine on aga midagi, mida on võimalik teha kohe, kui üleminekuplaan ühes oma kuupäevadega on fikseeritud. Ka sellised lühiajalise efektiga tegevused on osa üleminekust.

„Väga kõrge“ ja „kõrge“ prioriteedikategooria organisatsioonide üleminek võiks alata pärast inventuuri lõppu, st märtsis 2029, ja lõppeda septembriks 2030. **Plaanid ja eelarved võiksid olla olemas juuniks 2029**, pärast mida on selge, milliseid lühiajalise efektiga tegevusi teha. 2029. aasta lõpuks või 2030. aasta esimeste kuude jooksul võiks olla toimunud IT-lahenduste hankimine, millele saab järgneda nende juurutamine. Seejuures võivad hanke- ja juurutamistegevused suuresti ajaliselt kattuda. Kõigi nende tegevuste juures võib oluline olla täidesaatvate institutsioonide poolne järelvalve.

„Keskmise“ prioriteedikategooria üleminekutegevused algavad samuti pärast inventuuri lõppu, 2030. aasta suvel. Nende tegevuste lõpptähtaega sinne tegevuskava ei säteta, kuid need võiksid

siiski olla valmis 2035. aasta lõpuks.

Üleminekut finantseeritakse eeldatavasti osaliselt organisatsioonide tavapärasest IT-eelarvest, IT-süsteemide uuendamise kulude osana. Samas võib aga arvata, et ette nähtav tähtaegadega uuendamine tekitab täiendavaid kulusid, milleks tuleb leida eelarvelised vahendid. Neid vahendeid läheb vaja alates 2029. aastast ja eeltööd nende vahendite olemasoluks peavad olema selleks ajaks tehtud.

2.3.6 Aruandlus ja seire

Omaette tegevuste komplekti moodustavad aruandlus ja seire. Aruandlus on suunatud organisatsioonidelt täidesaatvatele institutsioonidele, kelle ülesanne on üleminekul silma peal hoida ja vajaduse korral aidata ning koordineerida. Suur osa aruandlusest toimub paralleelselt teiste tegevustega. Ühe olulise tegevusena tuleb seejuures veenduda, et kvantkindlate IT-süsteemide ja komponentide juurutamine on õnnestunud. „Väga kõrge“ ja „kõrge“ prioriteedikategooriaga organisatsioonid võiksid selle ära teha 2030. aasta lõpuks. „Keskmise“ kategooriaga organisatsioonid teevad seda pärast süsteemide juurutamist.

Võib kaaluda regulaarse aruandluse protsessi ühendamist mõne teise juba käimasoleva protsessiga nagu näiteks hukukindluse saavutamiseks. Samas peab arvestama sellega, et nii võib postkvant-krüptograafia üleminek jääda tahaplaanile. Lisaks hukukindluse temaatika ei puuduta nii paljusid organisatsioone kui postkvandile üleminek.

2.3.7 Madala prioriteedikategooriaga organisatsioonide tegevused

Madala prioriteedikategooriaga organisatsioonide üleminek on teekaardi autorite nägemuses lihtsam. Need organisatsioonid hangivad ilmselt oma IT-süsteemid kusagilt mujalt, samuti toetuvad nad süsteemide hooldusel välistele teenuseandjatele. Ülemineku oluline osa on nende tarnijate tuvastamine ja nende teavitamine, et infosüsteemid on tarvis panna kasutama kvantkindlaid krüptograafilisi algoritme. Märku ei pea andma neile tarnijatele, kes ilmselt juba isegi on märganud ülemineku vajadust. Juhul kui mõne tarnijaga kokkuleppele jõuda ei õnnestu, tuleb kaaluda tarnija vahetust.

Ka madala prioriteedikategooriaga organisatsioonid võiksid kaaluda, mis juhtub siis, kui nad postkvant-krüptograafia üleminekut ignoreerivad või sellega viivitavad. Samuti võiksid nad olla kursis teekaardis soovitatud ajakavaga, sh ka kõrgema kategooriaga organisatsioonidele sätestatud tähtaegadega, sest nende üleminek võib omakorda mõjutada madala kategooriaga organisatsioone. Need tegevused võiksid toimuda pärast kategoriseerimist, 2028. aasta esimese kvartali jooksul. Ka sellele järgnev tarnijate tuvastamine ja nende informeerimine võiks toimuda 2028. aasta jooksul. Kvant-turvaliste infosüsteemide kasutuselevõtt toimuks vastavalt tarnijate tegevuskavadele. Vajaduse korral (näiteks siis, kui tarnijate tegevuskavad omavahel kokku ei sobi) võib abi saamiseks pöörduda täidesaatvate institutsioonide poole. Samas tellijad peavad olema teadlikud, et kvant-turvalisi lahendusi oma tarnijatelt küsida.

2.3.8 Suurtarnijad

Suured rahvusvahelised ettevõtted, mis pakuvad tarkvara või IT-ressursse, on eeldatavasti kehtestanud oma tegevuskavad üleminekuks postkvant-krüptograafia. Need kavad on rohkem või vähem avalikud; mõni ettevõtetest nimetab mitme aasta pärast saabuval tähtaegu, aga sagedamini antakse aru sellest, mis juba ära tehtud. Eesti organisatsioonidel ei ole tõenäoliselt olulisi

hoobasid, millega suurte rahvusvaheliste ettevõtete tegemisi kiirendada. Meie ajakava peab see-
ga järgima nende välja kuulutatud kuupäevi (või aastaid).

Kuidas asetuvad loetletud tähtajad suurte rahvusvaheliste ettevõtete avalikustatud postkvant-
krüptograafia toega seotud tähtaegade konteksti? Käesolevas aruandes välja pakutav ajakava ei
ürita neist ettevõtetest kiirem olla. Kui suurettevõtted avaldatud ajakavadest kinni peavad, siis
sobituvad nad ka siinse tegevuskavaga.

3 Riigi tegevused

Põhipunktid:

- Riik saab otseselt juhtida enda teenuste arendust ning nõuda tehnoloogiapartneritelt nende teenuste üleviimist.
- Eesti turvakriitiliste e-teenuste kvantkindlaks muutmise eeldab teadus-arendustegevust, sest kõiki vajalikke tehnoloogiaid ja standardeid ei ole veel olemas.
- Infosüsteemide arendamisel kasutatud platvormide ajakohasus on postkvant-krüptograafiale ülemineku eeldus — st taakvara probleemi lahendamine on turbe seisukohalt hädavajalik.

3.1 Peamised tegevused ja ajakava

Liidu tegevuskava näeb ette, et **31.12.2035** on postkvant-krüptograafiale ülemineku keskmise riskiga kasutusmallides lõpuni viidud ja madala riskiga kasutusmallides on ülemineku samuti tehtud nii suures ulatuses, kui see on mõistlikult võimalik (joonis 1, ptk 2).

3.1.1 Esmased tegevused

Esmased tegevused (*First Steps*) peavad riigi poolt olema teostatud hiljemalt 31.12.2026, sh peab olema valminud esmane postkvant-krüptograafiale ülemineku riiklik tegevuskava ning algatatud peab olema ülemineku planeerimine ja pilootprojektid kõrge ja keskmise riskiga kasutusmallidele.

- **Esmased tegevused on** (vt täpsemalt liidu tegevuskava p 6.2):
 - tuvastada ja kaasata sidusrühmad (vt ptk 3.2.1)
 - toetada küpset krüptograafiliste varade haldust (vt ptk 5.5.2).
 - koostada sõltuvuskaardid (sisemised ja välised (vt ptk 5.4.1 ja 5.5.1.4) sõltuvused)
 - viia läbi kvanttehnoloogiaga seotud riskianalüüs (vt ptk 5.3 ja lisa D)
 - kaasata tarneahel (vt ptk 5.4.2 ja ja 5.5.1.4)
 - luua riiklik teadlikkuse ja kommunikatsiooni programm (vt ptk 3.4)
 - jagada teadmisi ja osaleda NIS CG PQC töövoos (vt ptk 3.5)
 - töötada välja ajakava ja rakendusplaan (vt ptk 2 ning 4.2.3 ja 5.5.3.1)
- **Peamised oodatavad tulemid**
 - Kõrge ja keskmise riskiga kasutusmallide jaoks on algatatud postkvant-krüptograafiale ülemineku planeerimine ja pilootprojektid.
 - Esmane riiklik postkvant-krüptograafiale ülemineku teekaart on valmis.

3.1.2 Teisesed tegevused

Teisesed tegevused (*Next Steps*) peavad riigi poolt olema teostatud hiljemalt 31.12.2030. Selleks ajaks on ette nähtud, et ülemineku postkvant-krüptograafiale on kõrge riskiga kasutusmallides lõpuni viidud ning keskmise riskiga kasutusmallides on see kavandatud ja pilootprojektid on lõpetatud. Kvantkindla tarkvara ja püsivara uuendused peaksid toimuma vaikimisi.

- **Teisesed tegevused on** (vt täpsemalt liidu tegevuskava p 6.3):
 - toetada krüptograafilist kohandatavust ja kvantturvalist teerada (dialoogid huvipoolte ja tootjate vahel jätkuvad; uued lahendused peavad olema krüptograafiliselt kohandatavad ja kasutama kvantkindlaid uuendussignatuure)
 - eraldada üleminekuks vajalikud ressursid (vt ptk 3.6)
 - kohandada sertifitseerimisskeeme (krüptograafiliste lahenduste sertifitseerimise teemaga Eestis tegeleb VÕIME projekt, vt nt [8])
 - arendada edasi postkvant-krüptograafiaga seotud nõudeid (vt peatükk 4)
 - leida võimalusi ökosüsteemi sees (huvipoolte ühendamine: tootjad-kasutajad; koolitused ja rahastus)
 - arvestada läbivate tegevustega kogu teekaardi loomise ja rakendamise vältel (nt postkvant-krüptograafiaga seotud tööühmades osalemine, asjaomase uurimistegevuse toetamine, doktorantuuri õppekavade arendamine)
 - rakendada pilootkasutusmalle ja panustada testimiskeskustesse
- **Peamised oodatavad tulemid**
 - Kõrge riskiga kasutusmallide üleminek postkvant-krüptograafiale on lõpule viidud.
 - Keskmise riskiga kasutusmallide postkvant-krüptograafiale ülemineku planeerimine ja pilootprojektid on lõpule viidud.
 - Kvantturvalised tarkvara- ja püsivara (*firmware*) uuendused on vaikimisi lubatud.

3.2 Ministeeriumide ja pädevate asutuste soovituslikud tegevused

3.2.1 Kiireloomulisemad tegevused

Riik peab otsustama, millised ministeeriumid ja organisatsioonid võtavad rolli postkvant-krüptograafiale ülemineku koordineerimisel ja nõuete täitmisega seotud järelevalves. Tagada tuleb, et organisatsioonidele (subjektidele), kes üleminekut praktikas teostavad (lähevad üle postkvant-krüptograafiale), oleks olemas neile vajalik informatsioon edukaks üleminekuks.

Üksusel, mis hakkab riiklikul tasemel koordineerima postkvant-krüptograafiale üleminekut, on suur roll. Ilma tugeva keskse koordinatsioonita ei pruugi õigeaegne üleminek soovitud viisil toimuda. Seetõttu on esmaseks kiireloomulisemaks tegevuseks keskse koordinatori määramine. Selleks võib olla konkreetne ministeerium (nt Justiits- ja Digiministeerium) või ministeeriumi valitsemisalas tegutsev valitsusasutus (nt Riigi Infosüsteemi Amet), aga ka koordinatsioonikogu (*postkvant-krüptograafia nõukogu*), kuhu määratakse liikmed erinevatest otseselt üleminekuga seotud organisatsioonidest.

Hästi oluline on saada kõik olulised rühmad ühise laua taha, eeskätt asjaomased ministeeriumid ja pädevad asutused, ning sõlmida kokkulepped, sh milline on kõige mõistlikum viis nõuete kehtestamiseks ning millised saavad olema pädevate asutuste ülemineku läbiviimise ja järelevalvega seotud õigused ja kohustused. Arvesse tuleb võtta, et täiendavate ülesannete panemine pädevatele asutustele võib eeldada ka asjaomaste ressursside eraldamist.

- **Postkvant-krüptograafia ümarlaud** – Justiits- ja Digiministeerium organiseerib hiljemalt II kvartalis 2026.
- tulemid:

- määratakse üleminekut koordineeriv organisatsioon ja osaliste ülesanded (sh kavandatakse peatükkides 3.6.1, 3.4, 3.4.1, 3.4.2 ja 3.5 esitatud tegevusi) ning iga organisatsiooni kontaktisik

Kokkulepitud plaan tuleks kommunikeerida esimesel võimalusel ka järelevalvesubjektidele, st organisatsioonidele, kes peavad hakkama nõudeid rakendama.

- **Postkvant-krüptograafia ümarlaud erialaliitudega** – Justiits- ja Digiministerium organiseerib hiljemalt III kvartalis 2026
- tulemid:
 - erialaliidud on informeeritud ja saavad kavandatavate muudatuste osas kaasa rääkida

Liikmesriikidel soovitatakse integreerida postkvant-krüptograafiaga seotud nõuded ka riiklikesse hankemenetlustesse ning suhelda praeguste IT-tarnijatega, et hinnata nende valmisolekut postkvant-krüptograafia valdkonnas ([3] p 6.3). Kui riiklikud hanked nõuavad mingil tasemel kindlust (näiteks sertifitseerimise kaudu), tuleb hinnata võimalikke vajadusi uute sertifikaatide väljastamiseks ning teha koostööd hindamisasutustega nende väljatöötamiseks ([3] p 6.3).

Postkvant-krüptograafia koolitus kesksetele hankijatele – hiljemalt III kvartalis 2026

- tulemid:
 - kesksed hankijad, hankespetsialistid ja juristid on teadlikud kvanttohtudest ning kavandavad hankeid, mis puudutavad krüptograafiliste lahenduste hankimist, lähtuvalt Eesti postkvant-krüptograafia ülemineku plaanist, sh soovituslike krüptograafiliste algoritmide valikust

Kavandatava eelnõu menetlemise ajakava võivad mõjutada 2027. a toimuvad Riigikogu valimised.

3.2.2 Kõrgete prioriteedikategooriatega organisatsioonide tuvastamine

Kuivõrd õiguslike nõuete kehtestamine postkvant-krüptograafia üleminekuks võib võtta aega ja soovituslike juhendite järgimine ei ole subjektide jaoks siduv, tuleks riigil teostada esmane hinnang, millised organisatsioonid kuuluvad „väga kõrgesse“ või „kõrgesse“ prioriteedikategooriasse võttes aluseks peatükis 5.3 esitatud klassifitseerimismeetodid. Täidesaatval institutsioonil tuleb nende klassifitseerimismeetoditega tutvuda ja seejärel leida meetod, mille alusel välja valida organisatsioonid, mida klassifitseerima asuda. Meetod peab tagama, et väljavalmimata organisatsioonid ei kuulu „väga kõrgesse“ ega „kõrgesse“ kategooriasse. Organisatsioonidele, mis tuvastatakse kuuluvat „väga kõrgesse“ või „kõrgesse“ kategooriasse, tuleb sellest teada anda. Organisatsioonide klassifitseerimine tuleks lõpetada 2026. aasta 3. kvartalis ja organisatsioonid peaksid olema teavitatud hiljemalt 2026. aasta lõpuks.

3.2.3 Organisatsioonide tegevuskavade võrdlemine

Organisatsioonide postkvant-krüptograafia ülemineku tegevuskavade omavahel kooskõlas hoidmine võiks toimuda kaheetapilisena:

1. *I etapp*: Esimeses etapis paluvad pädevad asutused näha subjektide sõltuvusanalüüse. Neist analüüsides selgub, kes on ühe või teise organisatsiooni tarnijad ja teenusepakkujad.
2. *II etapp*: Teises etapis, siis kui organisatsioonid on koostanud individuaalsed tegevuskavad, toimub organisatsioonide tegevuskavade võrdlemine ja kooskõlastamine:

- kui kaks organisatsiooni on tarnija-kliendi suhtes, siis võrreldakse nende organisatsioonide tegevuskavasid omavahel;
- kui kahel organisatsioonil on ühine tarnija, siis võrreldakse nende organisatsioonide individuaalseid tegevuskavasid omavahel selles osas, milliseid nõudeid üks ja teine tegevuskava tarnijale esitab (millal ja kuhu peab tarnija välja jõudma) ning antakse soovitusi, et nõuded oleksid ühesugused.

Mõlema etapi tähtaeg sõltub sellest, millal on organisatsiooni sõltuvusanalüüsi või individuaalse tegevuskava koostamise tähtaeg.

3.2.4 Tehtud otsuste dokumenteerimine

Kui organisatsioonid koostavad ja viivad ellu oma üleminekuplaane, teevad nad otsuseid, kuidas üleminekut läbi viia. Oleks hea, kui tehtud otsused ja otsusteni viinud mõttekäigud oleksid dokumenteeritud. See teave võib olla vajalik järelevalvele ja oluline ka auditite edukaks läbimiseks.

Ainult organisatsioonides olevast dokumentatsioonist tehtud otsuste ja nende põhjenduste kohta ei piisa. Taoline dokumentatsioon võiks tekkida ka riiklikult. Selliselt on võimalik madalama prioriteedikategooria organisatsioonidel ära kasutada kõrgema kategooria organisatsioonide kogemust. Lisaks otsustele ja põhjendustele võiks dokumenteerida ka elluviidud otsuste tulemusi.

3.3 Kontrollimine ja seire

Postkvant-krüptograafia üleminekul on oluline seirata organisatsioonide migratsiooniplaanide täitmise edenemist. Milline organisatsioon (või organisatsioonid) kõnealust rolli Eestis täitma hakkab, sõltub nii poliitilistest kui ka regulatiivsetest valikutest.

Pädeva asutuse keskseid ülesandeid postkvant-krüptograafia üleminekul on seirata organisatsioonide edenemist asjaomaste tegevuste tähtaegsel elluviimisel. Pädeval asutusel on õigus anda välja soovitusliku sisuga suuniseid, juhendeid, korraldada teabepäevi, et toetada organisatsioonide üleminekut ja krüptograafilise kohandatavuse saavutamist. Pädeva asutuse volitused organisatsioonide abistamisel on piiratud tema õiguste ja kohustustega, st abi andmine ei saa minna vastuollu järelevalve põhiolemusega.

Ka ministeeriumitel (ja/või nende allasutustel) on võimalik toetada postkvant-krüptograafia üleminekut, nt tõsta huvirühmade teadlikkust (vt ptk 3.4), pakkuda koolitusi (vt ptk 3.4.1), viia läbi kommunikatsioonitegevusi (vt ptk 3.4.2) ja osaleda rahvusvahelistes temaatilistes koordineerimise tegevustes (vt ptk 3.5) ning jagada ülemaailmseid parimaid praktikaid.

3.4 Teadlikkuse tõstmine

Teadlikkuse tõstmise eesmärgiks on teha sidusrühmad teadlikuks kvantarvutite võimalikust mõjust kasutatavale krüptograafia üleminekuks ning anda neile teadmised, mida kasutades oma süsteemid kvantarvutikindlaks muuta. „Teadlikkuse tõstmine“ koosneb seega kahest osast: kommunikatsioon ja õpetamine.

3.4.1 Koolitumisvõimaluste loomine

Riigi ülesanne on pakkuda organisatsioonide ülemineku eest vastutavatele töötajatele koolitamisvõimalusi, korraldades seda kas läbi ülikoolide, kutseõppeasutuste või muude sobivate teenu-

sepakkujate. Üks võimalik väljund võiks olla Digiriigi akadeemia. Lihtsaim viis koolituse korraldamiseks on iseseisvalt kasutatavate õppematerjalide tellimine, sest edasiantavad teadmised ja oskused võiksid olla hõlpsasti pakitavad õpiobjektidesse¹, mille läbimist ja õpieesmärkide kontrolli infotehnoloogilised lahendused toetavad. Asjaomased õppematerjalid võiksid valmida **2027. aasta esimeses kvartalis**. Loodud õppematerjalide hoidmiseks ja kasutamiseks on ülikoolidel olemas oma infosüsteemid, aga kaaluda võib ka Digiriigi Akadeemia platvormi kasutamist.

Koolitus peaks sisaldama nii õiguslikke kui ka tehnilisi postkvant-krüptograafiaga seotud aspekte ja andma osalejatele valmisoleku kas luua ja/või ellu viia organisatsioonisisest üleminekukava. Koolitus tuleks jagada mitmeks kursuseks, mõni neist suunatud tehnilistele töötajatele, mõni keskastmejuhtidele. Koolituse kõik kursused läbinud õppija võiks olla saavutanud järgmised õpieesmärgid:

- koolituse läbinu on tuttav terve teekaardi sisuga;
- koolituse läbinu on algtasemel tuttav postkvant-krüptograafia alustega ning teab, mis on enimsoovitatud postkvant-krüptograafia algoritmid;
- koolituse läbinu on teadlik riskidest, mis kaasnevad nii postkvant-krüptograafia ülemineku kui ka ülemineku hilinemisega;
- koolituse läbinu teab peamisi õigusakte ja õiguslikke nõudeid, mis seonduvad postkvant-krüptograafiaga või sellele ülemineku²;
- koolituse läbinu oskab hinnata organisatsiooni krüptograafilist küpsust;
- koolituse läbinu on teadlik erinevatest krüptoinventuuri meetoditest ja vahenditest ning oskab nende hulgast valida enda organisatsiooni vajadustele vastavad vahendid;
- koolituse läbinu oskab juhtida krüptoinventuuri läbiviimist;
- koolituse läbinu oskab koostada oma organisatsiooni olemusest lähtuva postkvant-krüptograafia ülemineku ajakava ja juhtida selle täitmist.

Osad neist eesmärkidest on seotud tehniliste teadmiste ja oskustega, teised aga protsesside juhtimisega. Eesmärkide täpne jagunemine eri kursuste vahel võiks selguda tellija ja koolitaja vahelises sünergias.

3.4.2 Kommunikatsioonitegevused

Riik peaks võimalikult varakult, aga kindlasti aastast 2026, alustama kommunikatsioonitegevustega, et ühtlustada teadmisi postkvant-krüptograafia olulisusest ning kavandatavatest plaanidest ja subjektide kohustustest.

Üht esimestest kommunikatsioonitegevustest kirjeldab peatükk 3.2.2: pädev asutus selgitab välja väga kõrge ja kõrge üleminekuprioriteediga organisatsioonid ja annab neile teada, et nad on vastavalt kategoriseeritud ning neil tuleb mingiks tähtjaks täita mingid kindlad nõuded.

Ministerium (või selle allasutus) peab algatama ja läbi viima riigiülese teavituskampaania vähemalt 2027. aasta lõpuks, et garanteerida madalamates prioriteedikategooriates olevate organisatsioonide teadlikkus postkvant-krüptograafia ülemineku vajadusest ning kavandatavatest õiguslikest nõuetest.

¹– Internetis: <https://sisu.ut.ee/opiobjekt/>

²Teema sisu sõltub ka asjaolust, millisesse etappi on jõudnud postkvant-krüptograafia üleminekuks vajalikud õiguskeskkonna muudatused (st millises faasis on asjaomase eelnõu menetlemine).

Kampaania peaks edastama sõnumi, et kvantarvutite probleem on olemas, aga sellest on võimalik üle saada, kui tehakse vajalikke tegevusi. Kampaania peaks mainima muu hulgas soovituslikke tähtaegu „keskmise“ ja „madala“ prioriteedikategooria organisatsioonide jaoks. Viiteid võib teha ka krüptograafiliste algoritmide elutsüklite aruannetele teema paremaks mõistmiseks (vt nt [9, 10]).

Liidu tegevuskava (p 6.3) kohaselt eeldab postkvant-krüptograafia laialdane kasutuselevõtt nii vastavate toodete kättesaadavust kui ka institutsioonide poolset eeskuju. Samuti soovitatakse tööstusega kokku leppida ajakava postkvant-krüptograafia-toodete turule jõudmiseks ([3] p 6.3).

3.5 Üle-Euroopaline ja ülemaailmne koordineerimine

Liidu tegevuskava esmaste tegevuste jaotis (p 6.2) näeb ette liitumist NIS CG postkvant-krüptograafia töövooga. Vastavalt liidu tegevuskavale võiks liitumine toimuda juba 2026. aasta jooksul.

Järgmisteks aastateks soovitab liidu tegevuskava [3, ptk 6.3] „valdkondadevahelisi tegevusi“: standardiseerimisprotsessis osalemist, postkvant-krüptograafia alase teadustegevuse toetamist, infovahetust ja muud koostööd teiste liikmesriikidega, sealhulgas ühiseid uurimis- ja koolitusprogramme.

Hea tavana võiks jälgida globaalsel tasandil toimuvaid tegevusi postkvant-krüptograafia üleminekul, neist õppida ja jagada asjakohaseid soovitusi.

3.6 Eelarveliste vahendite leidmine

Postkvant-krüptograafia üleminekuks eeldab mitmeaastast ja koordineeritud eelarve planeerimist riigi tasandil. Kuna tegevused puudutavad paljusid avaliku sektori infosüsteeme ning sõltuvad ka tarnijatest ja koostööpartneritest, on oluline selgelt määratleda võimalikud rahastamisallikad ning põhimõtted, mille alusel üleminekuks vajalikud vahendid leitakse ja jaotatakse. Peatükk annab ülevaate võimalikest lahendustest eelarvevahendite leidmiseks, sealhulgas rahastusvoorude korraldamisest ning avaliku ja erasektori rollist ülemineku rahastamisel.

3.6.1 Rahastusvoorude korraldamine

Rahastusvoorud on üks võimalik mehhanism postkvant-krüptograafia ülemineku toetamiseks riigi tasandil. Nende eesmärk on suunata vahendeid prioriteetsetesse tegevustesse ning toetada asutusi, kelle infosüsteemide kohandamine eeldab täiendavaid investeeringuid. Rahastuse eraldamisel on otstarbekas lähtuda süsteemide kriitilisusest, riskitasemest ning ülemineku ajalisest prioriteedist.

Rahastusvoorud võivad toimuda etapiviisiliselt, hõlmates näiteks krüptograafia inventuuri ja mõjuanalüüsi läbiviimist, pilootprojektide elluviimist ning infosüsteemide järkjärgulist kohandamist. See võimaldab paremini hallata ülemineku seotud riske ning jaotada kulusid mitme eelarveperioodi peale. Samuti aitab keskne koordineerimine tagada, et ülemineku toimub ühtsete põhimõtete alusel ning arvestab süsteemidevahelisi sõltuvusi.

Riik peab tagama, et eelarvetes ette nähtud vahendid ülemineku toetamiseks (ptk 3.6.2) jõuaksid ülemineku tegelevate organisatsioonideni. Toetuse eraldamise tingimused tuleb paika panna piisavalt vara, et toetust oleks võimalik saada õigeaegselt (tabel 1). Peab arvestama, et aastad 2026 ja 2027 kuuluvad eelmise eelarveperioodi alla ning uue perioodi rahastus aasta-

Üleminekutegevus	„Väga kõrge“ ja „kõrge“ kategooria	„Keskmine“ kategooria
Inventuuri tegemine	03.2028 – 01.2029	10.2029 – 05.2030
Täideviimine	02.2029 – 09.2030	06.2030 – 12.2035

Tabel 1. Täiendavat toetust vajavate üleminekutegevuste toimumisajad ja vajamineva toetuse olematav maht

teks 2028 ja 2029 on avanemas alles siis, kui juba ajakavaliselt peaks I ja II kategooria asutused olema läbi teinud ülemineku esmased tegevused. Paika tuleb panna, kuidas rahastustaotlus esitatakse, millised andmed esitatakse, kuidas taotluses olevat teavet kontrollitakse, kuidas toetuse kasutamist jälgitakse (vt ka ptk 3.3). Rahastustingimuste paikapanekeuga tuleks alustada võimalikult varakult, et toetusmeede jõuaks õigeaegselt abivajajateni.

Lisaks asutuspõhisele rahastamisele võib teatud tegevuste puhul olla otstarbekas kasutada tsentraalset rahastamist. Eelkõige puudutab see lahendusi ja arendusi, mille mõju ulatub mitme asutuse või kogu avaliku sektorini, näiteks kesksed digiteenused, ühised krüptograafilised komponendid või juhendmaterjalide ja meetodikate väljatöötamine. Tsentraalne rahastamine aitab vältida dubleerimist, tagada ühtse lähenemise ning vähendada üksikute asutuste koormust olukorras, kus vajalikud muudatused tulenevad riigiülestest nõuetest või kokkulepetest.

Samuti võib tsentraalne rahastus olla põhjendatud juhtudel, kus mitmed asutused kasutavad sama tarkvaralahendusi või sõltuvad samadest tarnijatest. Sellisel juhul võimaldab koordineeritud lähenemine planeerida muudatusi tervikuna ning saavutada kulude ja ajakava osas paremaid tulemusi.

3.6.2 Avalik sektor

Kuigi üleminek muudab infosüsteemides kasutatavatele krüptograafilistele algoritmidele esitavaid nõudeid, ei tohiks muutunud nõuded märkimisväärselt mõjutada süsteemide tegevuskulusid. Tegevused on samad, kuid tehnilised detailid võivad olla erinevad, sh ressursinõudlikumad.

Arendusteks erinevatel tehnoloogia valmidustasemetel (TVT) on olemas erinevad finantseerimisvahendid. Madala kuni keskmise TVTga arenduste toetamiseks sobivad ETAGi uurimistoetused, Euroopa Horisondi teadus- ja arendustegevuse toetused, rakendusuuringute toetused (RITA+, TemTA), Riigi Infosüsteemide Ameti küberinnovatsiooni toetus. Kõrgemal TVTI arendusi tuleb toetada riigieelarvest või Euroopa Liidu Konkurentsivõime Fondist³ (2028+).

Selles postkvant-krüptograafia ülemineku tegevuskavas ei kirjeldata ega soovitata madala või keskmise TVTga arendusi. See aga ei tähenda, et ükski riiklikest kasutusmallidest enam postkvant-krüptograafia üleminekuks keskmise TVTga arendusi ei vajaks. Need kasutusmallid on aga unikaalsed (näiteks e-hääletamine). Kasutusmallide ammendavat loetelu ei ole siinkohal võimalik anda. Kasutusmallide haldajad on teadlikud nii kasutusmallide unikaalsusest kui ka vajalikest keskmise TVTga arendustest. On lootus, et kasutusmallide haldajad oskavad kasutusmallide arenduste jaoks pakkuda ise välja sobivad ajakavad ja rahastusallikad, nii et peale keskmise TVTga arenduste tegemist on nad võimelised kõrge TVTga arendusi tegema enam-vähem kooskõlas käesoleva tegevuskavaga.

Infosüsteemide uuendamise detaile kirjeldab peatükk 5. Olulised üleminekutegevused, mis va-

³- Internetis: <https://www.mkm.ee/ministeerium-uudised-ja-kontakt/valisvahendite-kasutamine/euroopa-konkurentsivoime-fond-ecf>

jaksid täiendavat toetust, on olemasolevate krüptograafiliste algoritmide kasutusest arusaamine (ptk 5.5.2) ja algoritmide väljavahetamine (mis langeb kokku süsteemide üldise uuendamisega, ptk 5.5.3). Sellele lisaks on tavaliselt tüüpilisel asutusel vaja planeerida kulud:

- rakendusserverite uuendamiseks,
- PQC kasutuselevõtuks,
- vähemalt kaheks süsteemiuuenduseks,
- töötajate koolitusteks,
- projektijuhtimiseks,
- litsentside haldamiseks / uuendamiseks (võivad olla püsikulud).

Lisaks infosüsteemide tehnilistele muudatustele tuleb arvestada ka riigi tasandi tegevustega, mis on vajalikud postkvant-krüptograafia ülemineku koordineerimiseks. Riigil on oluline roll ülemineku üldise suuna määramisel, tegevuste koordineerimisel, edenemise seiramisel ning vajadusel õigusraamistiku ajakohastamisel. Samuti tuleb planeerida vahendeid avaliku sektori asutustele suunatud tehniliste koolituste ning teadliku tellija pädevuse arendamiseks, et tagada ülemineku sisuline ja jätkusuutlik elluviimine. Nende tegevuste elluviimine eeldab eraldi ressursse ning eelarve planeerimisel tuleks arvestada ka võimalike kulude muutustega ajas, sealhulgas inflatsiooni mõjuga. Samal ajal ei tasu unustada, et infosüsteeme tuleb niikuinii pidevalt uuendada ja arendada, seega postkvant-krüptograafia ülemineku eelarvet on võimalik planeerida ka olemasolevate infosüsteemide tavapärase uuenduste ja hoolduste osana, ilma et see tähendaks alati eraldi lisakulusid. Mõjuanalüüs kirjeldab põhjalikumalt eelarve kulude kujunemist.

Eeltoodu puhul on tegemist kõrgel TVTI toimuvate arenduste ja juurutamisega. Seega tuleks vastavad vahendid plaanida Euroopa Liidu konkurentsivõime fondi pikaajalisse eelarvesse (aastateks 2028–2034) või järgmiste aastate riigieelarvetesse. Euroopa Liidu eelarves võivad need vahendid endale koha leida kas Riigiplaanis või Konkurentsivõime Fondis.

Seadusandlikud ja täidesaatvad institutsioonid peavad üheskoos paika panema ka toetusmeetmed, sealhulgas viisid, kuidas toimub finantsvahendite taotlemine ja eraldamine. Toetusmeetmete kavandamisega ei tohi venitada; tuleb arvesse võtta, kui pikalt (aasta või enam) selliseid meetmeid tüüpiliselt luuakse ja kooskõlastatakse. On võimalik, et eeskuju saab võtta meetmetest küberturvalisuse tõstmiseks.

3.6.3 Erasektor

Tegevuskava peamine eesmärk on toetada avaliku sektori organisatsioonide üleminekut postkvant-krüptograafia. Kuigi tegevuskava on koostatud viisil, millest võivad kasu saada ka erasektori ettevõtted, ei ole selles eraldi ette nähtud eelarvevahendeid erasektori ülemineku rahastamiseks. Erandiks võivad olla olukorrad, kus erasektori ettevõtte tegutseb avaliku sektori organisatsiooni tarnijana. Sellisel juhul võib avaliku sektori organisatsioonil olla võimalik taotleda üleminekuga seotud kulude katmiseks toetust ka nende lahenduste osas, mida pakub tarnija rahastusallikatest, mis on kirjeldatud peatükis 3.6.2.

Samas võib huvitatud osapooltega edasise suhtluse käigus selguda vajadus kaaluda ka täiendavaid meetmeid erasektori toetamiseks, näiteks ettevõtete puhul, kes ei paku teenuseid otseselt avalikule sektorile, kuid kelle roll on oluline kriitilise taristu või oluliste teenuste toimimisel.

4 Nõuete kehtestamine

Põhipunktid:

- Postkvant-krüptograafia ülemineku edukus ja tempo sõltuvad sellest, kas õigusruumi tehakse vajalikud täiendused ja millal need tehakse.
- Krüptograafia peab kehtestama turvanõuded, mis on normatiivsed ja mille täitmist kontrollitakse.

4.1 Nõuete kehtestamise ajend

Komisjoni soovitus [3] ja liidu tegevuskava [2] peamine eesmärk on tugevdada Euroopa Liidu vastupanuvõimet kvantohutudele. Komisjoni soovitus sedastatakse, et andmete kaitsmine ja tundliku side turvalisuse tagamine on ühiskonna, majanduse, julgeoleku ja heaolu jaoks ülioluline, mistõttu nähakse vajadust minna võimalikult kiiresti üle postkvant-krüptograafia. See kõrvaldaks praeguse asümmeetrilise krüptograafia teadaolevad nõrkused ja suurendaks stabiilsust kvantarvutite kuritahtlikust kasutamisest põhjustatud ohtude tingimustes. Liidu tegevuskava kohaselt on üleminek postkvant-krüptograafia koordineeritud pingutus, mis nõuab erinevatelt pooltelt koheseid samme ja tegevuskavas pakutud ajakava järgimist.

Nõuded peaksid tagama eduka ja õigeaegse migratsiooni postkvant-krüptograafia, sh kvantkindlate lahenduste kasutuselevõtu, mis tugevdaks vastupanuvõimet kvantarvutitega seotud ohtude suhtes ja leevendaks asjaomaseid riske. Eelnev kätkeb endas mitmeid alameesmärke/tegevusi:

- **kaitsta parima teadmise kohaselt olemasolevaid lahendusi ja kavandada võimalikult turvalisi uusi lahendusi.** Seetõttu on oluline tagada Eesti praeguste ja tulevaste digiteenuste, andmekogude, infosüsteemide, kommunikatsioonikanalite ja muu kriitilise taristu kaitse kvantarvutite võimalike ebasoovitavate mõjude eest, eesmärgiga kindlustada püsiv ja tõrgeteta andmevahetus ning konfidentsiaalse teabe pikaajaline salajasus;
- **olla kohanemisvõimeline ja vähendada sõltuvust konkreetsetest lahendustest.** Oluline on krüptograafilise kohandatavuse (ingl *cryptographic agility*) saavutamine kõikides organisatsioonides, et tekiks võime asendada ohumaastiku muutumisel hõlpsasti üks krüptograafiline lahendus teisega. Krüptograafiline kohandatavus võimaldab kombineerida postkvant-krüptograafiat olemasolevate krüptograafiliste lahenduste või kvantvõtmejaotustega. Postkvant-krüptograafilistele lahendustele ülemineku käigus soovitatakse võimalikult suures ulatuses kasutada standardiseeritud ja testitud postkvant-krüptograafiat sisaldavaid hübriidlahendusi;
- **tagada, et oleks kvantkindlaid lahendusi, mida kasutusele võtta.** Nimetatud hõlmab planeerimist ja praktilisi samme, et toetada kvantkindlate tehnoloogiate arendamist ja kasutuselevõttu nii avalikus kui ka erasektoris.

Liidu tegevuskava (p 6.3) kohaselt võivad liikmesriikidel olla riiklikud ja valdkondlikud seadused või määrused (või riiklike organisatsioonide krüptograafilised soovitused), mis sisaldavad tehnilisi nõudeid. Esmaseks keerukaks ülesandeks on nende regulatsioonide ja krüptopoliitike tuvastamine ning seejärel nende süstemaatiline ajakohastamine, lähtudes postkvant-krüptograafia uusimatest soovitustest. Juhul kui selliseid regulatsioone või krüptopoliitika ei ole, peaksid

liikmesriigid kaaluma nende loomist.

Lisaks komisjoni soovitusel ja liidu tegevuskavale avaldas komisjon jaanuaris 2026 küberturvalisuse 2. määruse ettepaneku [5] ja sellega seonduvalt küberturvalisuse 2. direktiivi muudatusettepaneku [6]. Küberturvalisuse 2. direktiivi, mille nõuded on üle võetus Eesti õigusesse KütSiga, üks muudatusettepanekutest käsitleb riikliku küberturvalisuse strateegia täiendamist. Nimelt esitatakse küberturvalisuse 2. direktiivi muudatusettepaneku artikli 1 lõikes 5 ettepanek täendada küberturvalisuse 2. direktiivi artikli 7 lõiget 2 punktiga „k“, mille kohaselt võtavad liikmesriigid oma riikliku küberturvalisuse strateegia osana vastu poliitikameetmed, mis on vajalikud üleminekuks postkvant-krüptograafiale, võttes arvesse ülemineku ajakavasid ning kohaldatavates liidu õigusaktides ja poliitikates sätestatud asjakohaseid nõudeid.

Küberturvalisuse 2. direktiivi põhjenduspunktis 8 on selgitatud, et meetmete võtmine kvantohuga tegelemiseks on vajalik, kuna ühiskond ja majandus sõltuvad üha enam digitehnoloogiast. Ründed nagu *harvest-now-decrypt-later* („korja kohe, dekrüpteeri hiljem“, vt 5.5.2.3), võimalik signatuuride võltsimine ja kehtivate krüptograafiliste algoritmide kasutuselt kõrvaldamine, muudavad ülemineku postkvant-krüptograafiale kiireloomuliseks. Seetõttu peaksid liikmesriigid võtma oma riiklike küberturvalisuse strateegiate raames vastu postkvant-krüptograafiale ülemineku poliitikad. Need poliitikad peaksid toetama strateegilist planeerimist, krüptograafiliste varade riskihindamist, ülemineku kavandamist ja testimist ning nõuetele vastavate Euroopa postkvant-krüptograafia-lahenduste kasutuselevõttu. Need peaksid olema kooskõlas liidu õigusaktide, poliitikate ja liidu tegevuskavaga, tagades ülemineku postkvant-krüptograafiale 2030. aastaks kriitiliste kasutusjuhtude puhul ja 2035. aastaks muudel juhtudel.

Kuigi õiguskeskkond ei takista postkvant-krüptograafiale üleminekut, on selge vajadus konkreetsemate reeglite kehtestamise järgi. Postkvant-krüptograafiale üleminek peab toimuma riigis tervikuna. Riigi toimimise seisukohalt on keskse tähtsusega nii avalik kui ka erasektor, mis on omavahel tihedalt põimunud koostöö ja teenuste kaudu. Turvalisuse terviklikuks tagamiseks peab postkvant-krüptograafiale üleminek hõlmama mõlemat sektorit. Seetõttu lähtuvad selles peatükis esitatud soovitused eeldusest, et kohaldamisalasse kuuluvad nii avaliku kui ka erasektori osalised. Konkreetsete üleminekutegevuste ulatus ja sisu sõltuvad seejuures määratletud prioriteedikategoriatest. Rakendada tuleks riskipõhist lähenemist ja alustada kriitilisematest valdkondadest ja teenustest, kuid selle juures pidada alati silmas ka üldpilti.

4.2 Nõuded

4.2.1 Peamised nõuded subjektidele

Peamised nõuded subjektidele on esitatud peatükis 5.5 „Üleminekutegevused teiste prioriteedikategoriate jaoks“, mis kirjeldab üleminekutegevusi järgmiste prioriteedikategoriate jaoks:

- I – väga kõrge prioriteediga
- II – kõrge prioriteediga
- III – keskmise prioriteediga

Madala prioriteediga organisatsioonide üleminekutegevusi käsitleb peatükk 5.4 „Üleminekutegevused madala prioriteedikategooria jaoks“.

Organisatsiooni kategooria selgitatakse välja enesehindamise teel. Põhjalikud juhised selleks on esitatud peatükis 5.3 „Kategoriseerimine“. Enesehindamise esimene samm on määrata töödeldavate andmete kaitsetarve, sh andmekogu turbeaste, ning vastata enesehindamise küsimustikule (vt joonis 3).

Nõuded krüptograafilistele algoritmidele on võimalik kehtestada Vabariigi Valitsuse määruse nr 101 peatükis 3 „Turvameetmete nõuded“, aga ka Vabariigi Valitsuse 20. detsembri 2007. a määruses nr 262 „Riigisaladuse ja salastatud välisteabe kaitse kord“ ja selle lisas 14 „Nõuded salastatud teabe töötlussüsteemile“. Nõudeid krüptograafilistele algoritmidele on võimalik adresseerida ka Finantsinspektsiooni soovituslikes juhendites.

4.2.2 Aruandlus

Subjektide seire ja aruandlus peaksid olema vastavuses peatükis 5 toodud sammudega. Halduskoormuse tõusu vältimiseks tuleks postkvant-krüptograafiale üleminekuga seotud aruandlus integreerida võimaluse korral subjektide olemasolevatesse aruandluskohustustesse. Aruandluse samm peaks olema mõistlik (näiteks kord aastas või „väga kõrge“ prioriteedikategooria organisatsioonidel tihedamini). Sõltuvalt organisatsiooni kategooriast võiks aruandlus olla järgmine:

Väga kõrge prioriteediga:

- **sagedus:** 2–3 korda aastas;
- **käsitlemist vajavate teemade hulka peaksid kuuluma (kuid mitte ainult):**
 - postkvant-krüptograafiale ülemineku eest vastutava isiku nimi ja kontaktandmed;
 - millist abi on vaja tuvastatud tarnijatega kontakteerumise juures;
 - kas kinnitatud on inventuuriplaan ja üleminekuplaan ning vastavad eelarved;
 - kinnitatud üleminekuplaan;
 - vajadus uute krüptograafiat kasutavate lahenduste väljatöötamise järele.

Kõrge prioriteediga:

- **sagedus:** 1–2 korda aastas;
- **käsitlemist vajavate teemade hulka peaksid kuuluma (kuid mitte ainult):**
 - postkvant-krüptograafiale ülemineku eest vastutava isiku nimi ja kontaktandmed;
 - millist abi on vaja tuvastatud tarnijatega kontakteerumise juures;
 - kinnitatud üleminekuplaan.

Keskmise prioriteediga:

- **sagedus:** üks kord aastas;
- **käsitlemist vajavate teemade hulka peaksid kuuluma (kuid mitte ainult):**
 - postkvant-krüptograafiale ülemineku eest vastutava isiku nimi ja kontaktandmed;
 - millist abi on vaja tuvastatud tarnijatega kontakteerumise juures.

Madala prioriteediga: aruandluskohustus laieneb ainult organisatsioonidele, mis käitlevad tundlike andmeid, mida töödeldakse süsteemides, mida organisatsioon ise ei halda.

- **sagedus:** üks kord aastas;
- **käsitlemist vajavate teemade hulka peaksid kuuluma (kuid mitte ainult):**
 - postkvant-krüptograafiale ülemineku eest vastutava isiku nimi ja kontaktandmed;
 - kas tarnijad on tuvastatud ja nendega ühendust võetud.

Kõigi prioriteedikategooriate organisatsioonide koostatavate aruannete põhisisuks peaks olema ülevaade edukalt ellu viidud tegevustest, täiendavat tuge nõudvatest tegevustest ning järgmise aruandlusperioodi eesmärkidest. Teised aruandes kajastamist nõudvad teemad sõltuvad organisatsiooni kategooriast ning on kokku võetud peatükis 5.

4.2.3 Ajakava

Soovituslik ajakava koos peamiste üleminekutegevustega postkvant-krüptograafia riskikategooriate lõikes on esitatud joonisel 2. Ajakava kujunemise kohta on antud selgitusi peatükkides 1.4.4 ja 2. Suure tõenäosusega on vajalik ajakava kohandamine vastavalt asjaoludele, mis selguvad või lepatakse kokku pärast selle projekti lõppu, mistõttu on ajakava mõistlik esitada subjektidele esmalt soovituslikuna.

Liidu tegevuskava ütleb (p 4.1) et, kui soovitatud tähtaegadeks ei ole võimalik üleminek postkvant-krüptograafia, tuleb konkreetseid riske põhjalikult hinnata ning vajadusel rakendada muid ajutisi meetmeid. Eeskätt on oluline saavutada krüptograafiline kohandatavus.

4.2.4 Nõuded krüptograafilistele algoritmidele

Krüptograafilistele algoritmidele esitatavad nõuded võivad uute ohtude esilekerkimise tõttu aja jooksul (kiiresti) muutuda. Krüptograafiliste algoritmide kohta on avaldatud erinevaid soovitusi. Heaks näiteks on Riigi Infosüsteemi Ameti tellitud perioodilised krüptograafiliste algoritmide elutsükli uuringud. Viimane neist koostati aastal 2023 [10], järgmine valmib suvel 2026. Uuringu eesmärgiks on anda ülevaade krüptograafilistest algoritmidest, mis pakuvad kaitset teadaolevatele turvalisusega seotud ohtudele. Hiljuti uuendas ka Saksamaa Infoturbe Liiduamet (BSI, *Bundesamt für Sicherheit in der Informationstechnik*) krüptograafiliste mehhanismide juhendit („Cryptographic Mechanisms: Recommendations and Key Lengths“) [11]. Need on siiski soovituslikud juhendid ja ei ole siduva iseloomuga, mistõttu tuleb kaaluda nõuete kehtestamist õigusaktiga.

Peamised nõuded sobivatele postkvant-krüptograafia algoritmidele, mis tuleks kehtestada õigusaktiga, on järgmised.

- Tuleb koostada ja kehtestada ühtne õigusterminoloogia, mis oleks kooskõlas varasemate õigusaktide¹ ja asjaomastes tehnilistes standardites kasutuselolevate terminitega. See on oluline õigusakti nõuete üheseks mõistmiseks. Näiteks võiks defineerida järgmised mõisted:
 - „**pärandalgoritm**“ (*legacy (cryptographic) algorithm*) on kasutusel, kuid aegunud krüptograafiline algoritm või mehhanism. Pärandalgoritmi kasutamine ei ole soovitatav uutes süsteemides selle ebapiisava või nõrgenenud turbetaseme tõttu, kuid seda ei saa täielikult keelata, kuna see on vajalik olemasolevate pärandsüsteemide või -rakenduste toimimiseks²;
 - „**krüptograafiline kohandatavus**“ (*cryptographic agility*) on süsteemi modulaarsusomadus, mille puhul süsteemis kasutatavaid krüptograafilisi algoritme on võimalik kiiresti asendada ja uuendada, näiteks nõrkuse avastamisel eelmises algoritmis või seoses kvantarvutite tulekuga.³ NIST on terminit sisustanud järgmiselt: see on infosüsteemi, protokoll, rakenduse, tarkvara, riistvara või taristu võime asendada, uuendada või kohendada kasutatavaid krüptograafilisi algoritme, võtmeparametreid ja krüptograafilisi mehhanisme ilma

¹Krüptograafiaalaseid termineid käsitlevate õigusaktide ülevaade on esitatud Eesti postkvant-krüptograafia ülemineku riikliku teekaardi lisa B „Krüptograafia-alased õigusaktid“ (vt Projekti 1. etapi aruanne, 23.12.2025, D-16-714)

²Vt nt IBM, Legacy algorithms. – Internetis: <https://www.ibm.com/docs/en/sdk-java-technology/8?topic=customization-legacy-algorithms> (26.02.2026)

³AKIT. – Internetis: <https://akit.cyber.ee/term/17175-cryptographic-agility> (26.02.2026)

teenuse toimimist katkestamata ning ilma süsteemi ümberorganiseerimiseta, tagades järjepidevuse ja vastupanuvõime muutuvatele krüptograafilistele ohtudele.⁴

- Postkvant-krüptograafiale ülemineku üheks alustalaks on hübriidrežiimide [12, ptk 2.7] kasutamiseks vajaliku krüptograafilise kohandatavuse saavutamine.
- Õigusaktiga tuleb siduvaks muuta soovituslike krüptoalgoritmide kasutus (vt ptk 5.5.3.3).
- Pärandalgoritmide kasutamine peab olema põhjendatud riskihinnangus.
- Välistada tuleks pärandalgoritmide kasutamine uutes süsteemides.
- Õigusaktis võib ette näha ka loetelu algoritmidest, mida on keelatud võtta kasutusele uute süsteemide arhitektuuris ning riist- või tarkvaras, sh algoritmide, mida asjaomane tehniline juhend nimetab mittesoovitavaks (*deprecated*) või taunitavaks (*discouraged*).
- Krüptograafilise skeemi parameetrid peavad tagama vähemalt 128-bitise klassikalise ja kvanturvalisuse taseme (nt aruandes [12, ptk 2.1] esitatud algoritmide või nendega võrdväärsed algoritmide).
- Kui kasutatava krüptosüsteemi tüüpi krüptoskeeme standardivad rahvusvahelised standardiorganisatsioonid (nt NIST, ISO, IETF), tuleb eelistada standarditud algoritme.

⁴Vt nt NIST, Crypto Agility. – Internetis: <https://csrc.nist.gov/projects/crypto-agility> (26.02.2026)

5 Organisatsioonide tegevused

See peatükk annab ülevaate organisatsioonide kvantkindlale krüptograafiale üleminekuks vajalikest tegevustest. Ehkki väliste koostööpartnerite ja konsultantide kasutamine selle elluviimiseks on lubatud ja koguni ootuspärane, soovime siinkohal rõhutada, et allpool kirjeldatavad tegevused on eelkõige mõeldud organisatsioonisisestena. Samas sõltub nende tegevuste täpsem planeerimine ja ajastus ka riigi tasandil kehtestatavatest nõuetest, sealhulgas võimalikest õigusaktidest, juhistest ja muudest suunistest, mis võivad mõjutada organisatsioonide sisemiste tegevuskavade koostamist ja ülemineku elluviimist.

Põhipunktid:

- Postkvant-krüptograafiale üleminekut saab keskselt koordineerida, kuid ülemineku eest vastutavad e-teenuseid käitavad organisatsioonid ise.
- Organisatsioon peab määrama postkvant-krüptograafiale ülemineku juhi, kes teostab tegevused vastavalt organisatsiooni prioriteedikategooriale.
- Krüptoinventuur on kõige tähtsam osa tööst – kui me ei tea, milline krüptograafia meil kasutusel on, ei saa me seda üle viia.

5.1 Allikad

Olemasolevate üleminekkavade põhjaliku analüüsi tulemusena jäid üleminekutegevuste kirjeldamisel põhiliste eeskujudena sõelale järgmised neli allikat.

Esiteks, üleminekutegevuste alusstruktuuri määratlemisel lähtutakse siin PQCC¹ avaldatud tegevuskavast „Post-Quantum Cryptography (PQC) Migration Roadmap“ [13]. Sama dokument on eeskujuks ka iga etapi jaoks selgete eesmärkide määratlemisel. PQCC tegevuskava puuduseks on praktilisemat laadi juhiste puudumine individuaalsete tegevuste jaoks.

Teiseks, kasutusmallide näited ja konkreetsete täpsustavad küsimused põhinevad ETSI tegevuskaval „A Repeatable Framework for Quantum-Safe Migrations [14]“. Need aitavad lugejal luua selge pildi täpsematest iga tegevusega seotud nõuetest.

Kolmandaks oli suureks abiks Nätheri jt kokkuvõtlik analüüs postkvant-krüptograafiale ülemineku käsitlevatest allikatest [15], eriti nende esitatud üleminekuga seotud rollide määratlused.

Neljandana tasub esile tõsta TNO postkvant-krüptograafiale ülemineku käsiraamatut [16]. Kuigi TNO käsiraamat ei ole otseselt kasutatav konkreetsete üleminekutegevuste allikana, on see kõigi postkvant-krüptograafiale üleminekuga tegelejate jaoks sisuliselt kohustuslik kirjandus, käsitledes kõiki sellega seotud möödapääsmatuid ja olulisi küsimusi. Seepärast mainitakse ja viidatakse TNO käsiraamatule mitmel pool postkvant-üleminekuga seotud tegevuste kirjeldustes.

5.2 Üleminekutegevuste jaotus

Siin esitatav organisatsioonide tegevuskava jaguneb kolmeks.

1. Esmalt määratleme tegevused, mis on vajalikud **enesehindamiseks**. Meie meetodika jaotab organisatsioonid prioriteetsuse alusel (st kui prioriteetne peaks üleminek postkvant-krüptograafiale).

¹Postkvant-krüptograafia koalitsioon (Post Quantum Cryptography Coalition), <https://pqcc.org>.

tograafiale nende jaoks olema) nelja kategooriasse. Seetõttu on tegevuskava esimeseks sammuks enesehindamine (kategoriseerimine), mida kirjeldab peatükk 5.3. Kategoriseerimise tulemused aitavad määratleda ülemineku ajakava ning visandada organisatsiooni järgmised tegevused.

2. Teiseks määratleme eraldi **kõige madalama prioriteedikategooria (IV kategooria) jaoks vajalikud tegevused**, kuivõrd sellesse kategooriasse kuuluvad organisatsioonid ei käita süsteeme ise ning sõltuvad suures osas välistest teenuseandjatest. Neid tegevusi kirjeldab peatükk 5.4.
3. Kolmandaks määratleme **kõigi teiste prioriteedikategooriate jaoks vajalikud tegevused**. Nende tegevuste kirjeldused on üksikasjalikumad ja tehnilisemad ning eeldavad üleminekut juhtiva ja selle eest vastutava isiku olemasolu. Teiste prioriteedikategooriate jaoks vajalike tegevuste kirjeldused leiab peatükist 5.5.

5.3 Kategoriseerimine

Enne postkvant-ülemineku otsest käivitamist peavad tegevuskava käsitlusalasse kuuluvad organisatsioonid välja selgitama, millisesse prioriteedikategooriasse nad kuuluvad. Prioriteedikategooria määrab ära, milliseid tegevusi nõuab üleminek postkvant-krüptograafiale ning kas organisatsioon võib mõne neist vahele jätta. Esmase kategooriatesse jaotuse viib läbi riik, määratledes ja teavitades organisatsioone, kes kuuluvad kõrgeimasse kategooriasse. Selle põhjal saavad ka teised organisatsioonid järeldada, et nad ei kuulu nimetatud kategooriasse.

Selles alapeatükis on toodud kõigi prioriteedikategooriate ülevaatlilikud kirjeldused, millele järgnevad kategoriseerimisega seotud tegevuste üksikasjalikumad selgitused.

• KATEGOORIA I: väga kõrge prioriteediga

- Organisatsioon käitleb **tundlikke andmeid**, mis oleksid **väga suure tõenäosusega** potentsiaalse ründaja sihtmärgiks või siis peavad organisatsiooni käideldavad andmed **püsimisega veel väga pikalt salajasena**. Neid andmeid töödeldakse organisatsiooni enda hallatavates süsteemides.
- Organisatsioon tarnib **kriitilise tähtsusega või pika eluaga taristut**.
- Kui organisatsiooni tabaks krüptograafiaga seotud rike, võib potentsiaalselt toimuda **laiaulatuslik andmeleke** või mõni **kriitilise tähtsusega teenus lõpetaks toimimise**.
- Organisatsioon **sõltub tugevalt riistvara tarnijatest**.
- Organisatsioon **koostab endale ise oma postkvant-krüptograafiale ülemineku tegevuskava ning vastutab ise selle teostamise eest**.
- **Näited:**
 - * *suured haiglad* käitlevad nii isikuandmeid kui ka terviseandmeid ning katkestus nende pakutavate teenuste toimimises võib lõppeda inimelude kaotusega;
 - * *kriitilise taristu tarnijate* puhul võib krüptograafiaga seotud rike esile kutsuda mõne kriitilise tähtsusega teenuse katkemise (nt elektri- või veevarustus);
 - * *ministeeriumid* käitlevad tundlikke andmeid sealhulgas isikuandmeid ja riigisaladusi;
 - * *riigi IT-majad* annavad krüptograafiaga seotud teenuseid teistele organisatsioonidele, sealhulgas ministeeriumitele. Lisaks on nendel organisatsioonidel potentsiaalselt rohkem postkvant-krüptograafiale üleminekuga seotud oskusteavet;
 - * *pangad* käitlevad nii isikuandmeid kui ka finantsandmeid ning krüptograafiaga seotud rike võib esile kutsuda laiaulatusliku andmeleke või katkestuse finantsteenustes.

• KATEGOORIA II: kõrge prioriteediga

- Organisatsioon käitleb **tundlikke andmeid**, mis oleksid **võrdlemisi suure tõenäosusega** potentsiaalse ründaja sihtmärgiks. Neid andmeid töödeldakse organisatsiooni enda hallatavates süsteemides.
- Kui organisatsiooni tabaks krüptograafiaga seotud rike, võib mõni **oluline põhiteenus katkeda**.
- Organisatsioon **vastutab väljastpoolt pärineva postkvant-krüptograafia ülemineku tegevuskava teostamise eest**.
- **Näited:**
 - * *tehnoloogiatarnijad* on organisatsioonid, mis tarnivad teistele organisatsioonidele erinevaid tehnoloogilisi teenuseid ja lahendusi. Need organisatsioonid vastutavad tõenäoliselt ise oma postkvant-krüptograafia ülemineku eest (sealhulgas ka võib-olla selle jaoks tegevuskava koostamise eest) ning neil võib seetõttu olla ka rohkem postkvant-krüptograafia üleminekuga seotud oskusteavet.
- **KATEGORIA III: keskmise prioriteediga**
 - Organisatsioon käitleb **tundlikke andmeid**, mis oleksid **väiksema tõenäosusega** potentsiaalse ründaja sihtmärgiks. Neid andmeid töödeldakse organisatsiooni enda hallatavates süsteemides.
 - Kui organisatsiooni tabaks krüptograafiaga seotud rike, võib mõni **vähemoluline teenus katkeda**.
 - Organisatsioon **tellib postkvant-krüptograafia ülemineku teenusena sisse**.
 - **Näited:**
 - * *ülikoolid* käitlevad isikuandmeid ning suure tõenäosusega ei tooks krüptograafiaga seotud rike kaasa põhiteenuste katkemist. Nad sõltuvad tugevalt teiste organisatsioonide tarnitavatest krüptograafilistest lahendustest;
 - * *kohalikud omavalitsused* käitlevad isikuandmeid ning suure tõenäosusega ei tooks krüptograafiaga seotud rike kaasa põhiteenuste katkemist. Nad sõltuvad tugevalt teiste organisatsioonide tarnitavatest krüptograafilistest lahendustest.
- **KATEGORIA IV: madala prioriteediga**
 - Kõik teised organisatsioonid. Need organisatsioonid võivad käidelda tundlikke andmeid ja andmeid mis peavad püsima veel väga pikalt salajasena, aga neid andmeid töödeldakse **teiste organisatsioonide hallatavates süsteemides**.
 - **Näited:**
 - * *koolid* käitlevad isikuandmeid, kuid vähesemal määral kui näiteks ülikoolid. Krüptograafiaga seotud rike ei tooks endaga kaasa teenuste katkemist.

5.3.1 SC.1: organisatsiooni kategooria määratlemine

Organisatsiooni kategooria määratlemine koosneb kahest alamtegevusest:

1. andmekogu turbeastme määratlemine²;
2. joonisel 3 esitatud küsimustiku täitmine.

Kuigi joonis lähtub avaliku teabe seadus (AvTS) mõistes määratletud andmekogudest, on esitatud küsimusi võimalik kohaldada ka muudele andmestikele ja andmekogumitele, mis ei kvalifitseeru AvTSi tähenduses andmekogudena. Sellisel juhul tuleb küsimusi tõlgendada sisuliselt,

²<https://www.riigiteataja.ee/akt/127092025002>

hinnates näiteks, kas vähemalt üks organisatsiooni hallatav andmestik või andmekogum eeldab kõrget (H) turbetaset või sellega võrreldavat kaitsevajadust.

Kategoriseerimisküsimustiku täitmisele peab eelnema organisatsiooni andmekogude turvalisuse hindamine. Selle aluseks on võrgu- ja infosüsteemide küberturvalisuse nõuetes³ määratletud kategooriad. Sarnaselt kategoriseerimisküsimustikule on selle eesmärgiks organisatsiooni kõige olulisemate (kõrge (H) turbeastmega) andmekogude kindlaksmääramine ja hindamine.

Joonisel 3 esitatud vooskeem aitab organisatsioonidel hinnata postkvant-krüptograafia ülemineku prioriteetsust. Organisatsioonil võib olla mitmeid erinevate turvanõuetega IT-süsteeme; enesehindamise eesmärk peaks seetõttu olema määratleda kõige olulisemate (st kõrgeima turbeastmega) süsteemide prioriteedikategooria. Juhul kui organisatsioon käitab vähemalt ühte (teiste süsteemide või andmekogudega võrreldes) kõrgema prioriteediga süsteemi või andmekogu, tuleks organisatsiooni lugeda sellesse kõrgemasse prioriteedikategooriasse kuuluvaks.

Kuigi joonis 3 lähtub avaliku teabe seadus(AvTS) mõistes määratletud andmekogudest, on esitatud küsimusi võimalik kohaldada ka muudele andmestikele ja andmekogumitele, mis ei kvalifitseeru AvTSi tähenduses andmekogudena. Sellisel juhul tuleb küsimusi tõlgendada sisuliselt, hinnates näiteks, kas vähemalt üks organisatsiooni hallatav andmestik või andmekogum eeldab kõrget (H) turbetaset või sellega võrreldavat kaitsevajadust.

5.3.2 SC.2: ülemineku edasilükkamisega seotud riskide analüüs

See toiming on IV kategooria organisatsioonide jaoks vabatahtlik.

Organisatsiooni postkvant-krüptograafia ülemineku prioriteedikategooria määratlemise järel tuleb analüüsida ülemineku edasilükkamisega seonduvaid ning üleminekuprotsessiga kaasnevaid riske. Lähemaid juhiseid selle kohta leiab lisast D.

See toiming võimaldab organisatsioonil luua pildi üleminekuprotsessi raskuskohtadest, mida tuleb arvesse võtta järgmiste tegevuste plaanimisel. Võimalike riskide teadvustamine aitab hinnata alamtegevuste ajakava, aga ka otsida ja määrata üleminekukava teostamiseks pädevaid töötajaid.

5.3.3 SC.3: tutvumine väljapakutud ülemineku ajakavaga

See toiming on kõigi kategooriate (I-IV) organisatsioonide jaoks kohustuslik

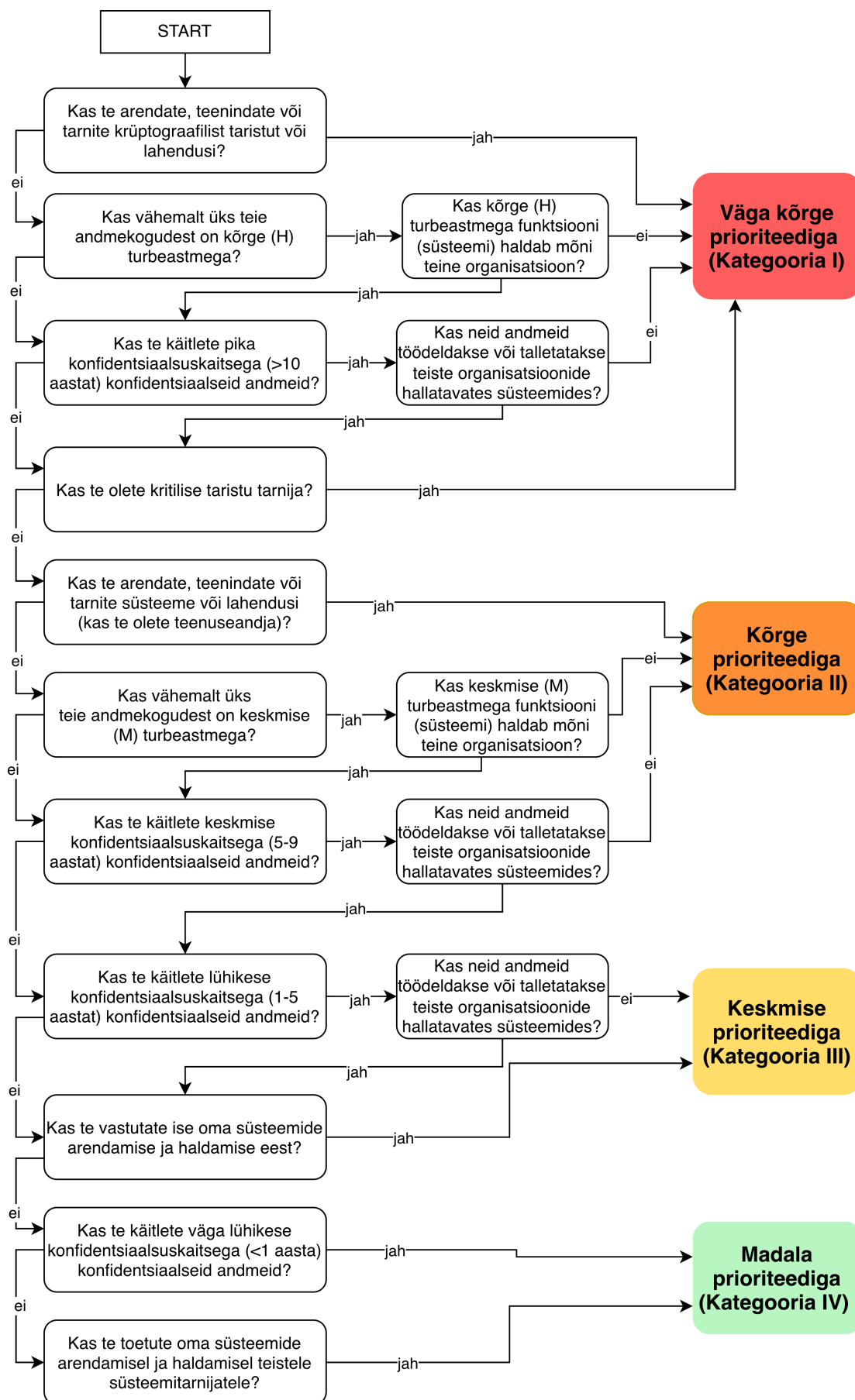
Organisatsioon peab saama ülevaate dokumendist ja selles sisalduvatest nõuetest. Eelkõige tähendab see tutvumist erinevatele riskikategooriatele määratud tegevuste tähtaegadega. Ajakava olulisemate punktidega saab tutvuda peatükis 2.

Ajakavaga tutvumise järel võiks läbi viia ka kiire analüüsi, mille järel saavutatakse arusaam tähtaegade täidetavusest ning selleks vajaminevatest ressurssidest.

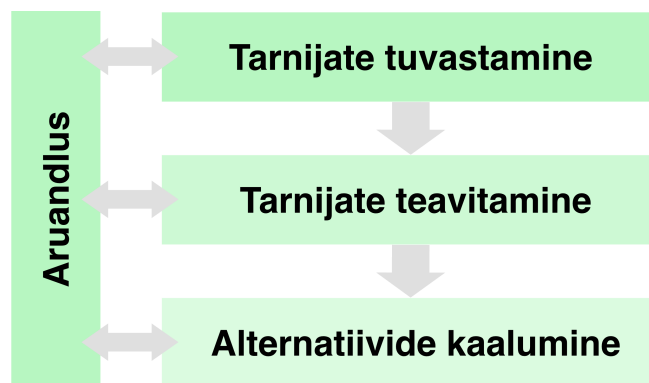
5.4 Üleminekutegevused madala prioriteedikategooria (IV kategooria) jaoks

Järgnevad toimingud on kohustuslikud madala prioriteedikategooria jaoks. Teiste kategooriate kohta vt ptk 5.5.

³<https://www.riigiteataja.ee/akt/127092025002>



Joonis 3. Kategoriseerimisküsimustik



Joonis 4. Üleminekutegevused madala prioriteedikategooria (IV kategooria) jaoks

See peatükk kirjeldab „madalasse“ prioriteedikategooriasse kuuluvate organisatsioonide jaoks kohustuslikke tegevusi (nummerdatud kujul „MP.number“). Joonis 4 esitab illustratiivse ülevaate peamistest tegevustest madala prioriteedikategooria jaoks. Kategoriseerimisküsimustik näitab, et madalasse prioriteedikategooriasse kuuluvad organisatsioonid sõltuvad nii riistvara kui ka tarkvaralahenduste puhul välistest tarnijatest ja edasimüüjatest ning neil puudub võimalus mõjutada mainitud toodete ja nende taristu turvasätteid.

Soovitame sellesse kategooriasse kuuluvatel organisatsioonidel tungivalt läbi viia vähemalt järgmised kolm tegevust.

5.4.1 LP.1: tarnijate tuvastamine

Organisatsioonid peavad kindlaks tegema oma IT-süsteemide tarnijad ning langetama teadliku otsuse, kas neid tarnijaid postkvant-krüptograafia üleminekust teavitada või mitte. Otsuse langetamisel tasub lähtuda järgmistest juhistest.

1. Loetlege kõik tarnijad, kellelt teie organisatsioon hangib mis tahes IT-teenuseid.
2. Tuvastage nende seast sellised, kes on seotud ainult teie organisatsiooniga, st:
 - ei hõlma üldkasutatavaid Eesti infosüsteeme (nagu X-tee, UXP, Smart-ID, CDOC jne);
 - ei hõlma rahvusvahelistele tehnoloogiaorganisatsioonidele (Microsoft, Google, Apple jne) kuuluvaid ja nende hallatavaid süsteeme.
 - näited: eKool, Stuudium, perearst24, e-perearstikeskus
3. Kaaluge, millise tõenäosusega kasutavad tuvastatud tarnijad sedasama postkvant-ülemineku tegevuskava.
4. Kaaluge, millise tõenäosusega võivad teie tarnijatest sellised, kes ei kasuta siinset tegevuskava, iseseisvalt püüelda üleminekut postkvant-krüptograafia.
5. Koostage loetelu tarnijatest, keda soovite üleminekust teavitada ja kellelt nõuda teavet, milliseid toiminguid nad on sooritanud teie andmete ja tegevuse kaitsmiseks kvantarvutuse ohtude eest.
 - Kaaluge seejuures oma andmete ja tegevuse tähtsust:
 - kas teie tegevusele või teie hallatavatele andmetele kohaldatakse turvalisuse alaseid õigusakte (nt andmekaitse ja küberturvalisuse valdkonna õigusaktid)?
 - kas teie andmete salastatus peab säilima rohkem kui 5–10 aastat?
 - kas IT-süsteemi asendamine oleks tehniliselt keeruline?
 - millised on teie plaanid seoses hübriidsüsteemidega (PQ/T)?

- kas süsteem on teie tegevuse jaoks kriitilise tähtsusega ning selle turvalisuse murdmisel oleksid tõsised tagajärjed?
- Loetelusse peavad automaatselt kuuluma kõik tarnijad, kelle puhul vastus ükskõik millisele neist küsimustest on „jah“.

5.4.2 LP.2: tarnijate teavitamine

Järgmise sammuna soovime läbi vaadata [tegevusena LP.1](#) koostatud tarnijate loetelu ning astuda nendega kontakti. Seejuures soovime käsitleda järgmisi teemasid:

- kas tarnija on kvantohust teadlik?
- kas tarnija plaanib toiminguid kvantohu leevendamiseks?
- kas tarnija järgib kvantohu leevendamiseks riiklikus tegevuskavas (st selles dokumendis) loetletud tegevusi?
- milline on tarnija ajakava kvantohu leevendamiseks?
- kas tarnija nõuab meilt (organisatsioonina) mingeid toiminguid kvantohu leevendamiseks?

5.4.3 LP.3: alternatiivide kaalumine

Enamik tarnijatest vastab tõenäoliselt, et mingeid erilisi toiminguid teie organisatsioonilt ei nõuta ning teie süsteemide uuendamine toimub mingiks tähtjaks automaatselt.

Siiski tuleb olla valmis olukordadeks, kus tarnija ei näita üles valmisolekut küsimustele vastata või nende ajakava ei klapi teie organisatsiooni ajakavaga kvantohu leevendamiseks. Sellistel juhtudel soovime kaaluda alternatiivseid tarnijaid ning astuda nendega kontakti.

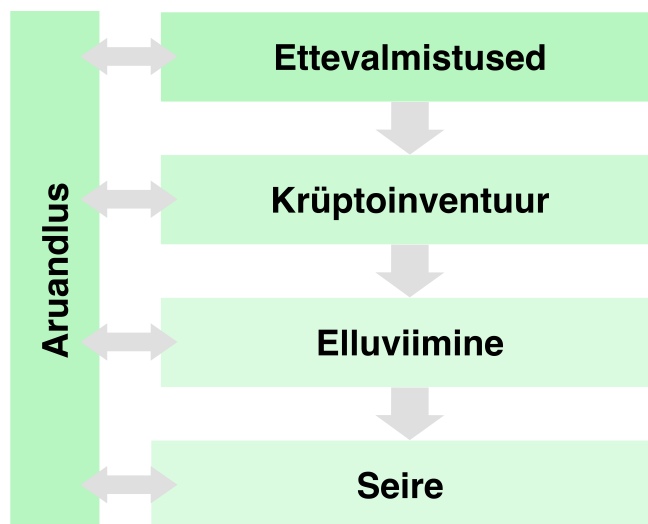
Märkigem, et isegi juhul kui tarnijad lubavad sobivaks tähtjaks üleminekut postkvant-krüptograafiale, ei pruugi kõik neist olla suutelised toetama organisatsiooni hübriidskeemide elluviimisel. Juhul kui teie organisatsiooni süsteemid peavad kasutama hübriidskeeme, kuid tarnija ei kinnita valmisolekut neid teostada, soovime otsida alternatiivseid tarnijaid.

5.5 Üleminekutegevused teiste prioriteedikategooriate jaoks (OP)

See peatükk kirjeldab üleminekutegevusi teiste prioriteedikategooriate jaoks, st:

- I – väga kõrge prioriteediga
- II – kõrge prioriteediga
- III – keskmise prioriteediga

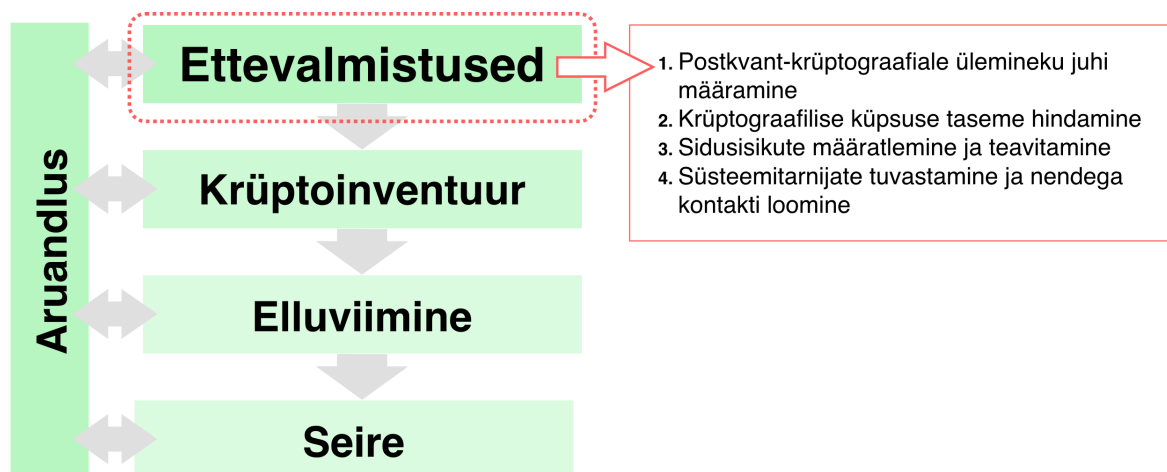
Kirjeldatavad tegevused jagunevad omakorda neljaks keskseks tegevuseks, mida kirjeldavad järgmised neli alapeatükki („Ettevalmistused“, „Inventeerimine“, „Elluviimine“, „Seire“). Joonis 5 esitab illustratiivse ülevaate peamistest tegevustest teiste prioriteedikategooriate jaoks. Märkigem, et igaüks neist tegevussammudest (mis on nummerdatud kujul „OP.number“) sisaldab märget selle kohta, milliste kategooriate jaoks on see kohustuslik ja milliste jaoks soovituslik. Mõned tegevused võivad ühtlasi sisaldada erinevate prioriteedikategooriate jaoks erinevaid juhiseid. Kõigi tegevuste all on ühtlasi välja toodud nende oodatavad tulemid. Viimased on mõeldud (1) esitama kokkuvõtte toimingust, (2) võimaldama tagasivaatavalt kinnitada toimingu täitmist ja (3) esitama tegevuse alamtegevused (nummerdatud kujul „OP.number.number“).



Joonis 5. Üleminekutegevused teiste prioriteedikategooriate jaoks

5.5.1 Ettevalmistused

Postkvant-krüptograafia ülemineku esimene oluline etapp on vajaliku teadmuse ning baasarusaamade omandamine sellest, kui valmis on organisatsioon üleminekuks. Joonis 6 esitab illustreeriva ülevaate esimese etapi tegevustest.



Joonis 6. Esimene ülemineku etapp (ettevalmistused)

5.5.1.1 OP.1: postkvant-krüptograafia ülemineku juhi määramine

See tegevus on kohustuslik I, II ja III kategooria organisatsioonidele.

Organisatsioon peaks määrama ühe või mitu töötajat „üleminekujuhtideks“, kes jälgiks, kehtestaks ja viiks edasi kõiki järgmisi postkvant-ülemineku etappe. Üleminekujuhi vastutusala ja töökoormus oleneb organisatsioonist ja selle prioriteedikategooriast. Ülemineku eest vastutava inimese (või inimeste) või inimeste olemasolu isegi „keskmise“ prioriteedikategooria organisatsioonides on kogu riigi eduka ülemineku jaoks postkvant-krüptograafia siiski ülimalt oluline.

Soovitame tungivalt üleminekujuhiks määratud inimesel viia ennast võimalikult põhjalikult kurssi postkvant-krüptograafia üleminekuks. Suurepärase sissejuhatuse neisse teemadesse pakub TNO avaldatud käsiraamat „The PQC Migration Handbook“ [16].

Üleminekujuhi roll ei tähenda tingimata organisatsiooni tippjuhti (nt ministeeriumi puhul kantslerit), vaid eelkõige projekti- või programmi eest vastutavat isikut, kellele on antud piisav mandaat üleminekuga seotud tegevuste koordineerimiseks. Olenevalt organisatsiooni suuruselt ja ülemineku mahust võib see olla nii eraldi ametikoht kui olla üks osa teise ametikoha tööülesannetest.

Üleminekujuht:

- peaks olema organisatsiooni töötaja;
- peaks tundma organisatsiooni tehnoloogilist taristut/arhitektuuri (või tal peaks olema sellele juurdepääs);
- peaks tundma krüptograafia põhimõisteid;
- peaks suutma suhelda nii juhtkonna kui ka tehnilise personaliga;
- peaks olema volitatud tegema järgnevates etappides toimuvate tegevuste raames siduvaid otsuseid vastavalt organisatsiooni kehtivale korrale ning vajadusel vastava taseme juhi poolt või tema volitusel;
- peaks olema volitatud algatama ja juhtima üleminekuga seotud hankeid vastavalt organisatsiooni kehtivale hankekorrale ning talle peaks olema tagatud vajalik mandaat, ressursid ja rahalised vahendid nende hangete elluviimiseks.

I ja II prioriteedikategooria organisatsioonidel soovitame ühtlasi moodustada ülemineku jaoks töörühma, mis hõlmaks vara- ja riskihaldurit, turvaeksperti ning arendajat või administraatorit ja määrata ka nendesse rollidesse konkreetseid töötajad.

Nätheri jt [15] soovitude järgi peaks vara- ja riskihaldur tundma organisatsiooni andmeid ja varasid ning suutma läbi viia riskianalüüsi. Turvaekspert peaks olema võimeline selle põhjal tuvastama krüptograafia kasutusjuhud organisatsiooni taristus. Arendaja või administraatori ülesandeks peaks olema muudatuste tegelik sisseviimine organisatsiooni koodivaramusse.

OP.1: oodatavad tulemid

- OP.1.1: organisatsioon on määranud üleminekujuhi, kes vastutab selle tegevuskava järgmistest etappidest elluviimise eest;
- OP.1.2: üleminekujuht on tutvunud postkvant-krüptograafiale ülemineku problemaatika ja tegevuskava teiste osadega.

5.5.1.2 OP.2: krüptograafilise küpsuse taseme hindamine

See tegevus on I kategooria organisatsioonidele kohustuslik, II kategooriale soovituslik ja III kategooria organisatsioonide jaoks vabatahtlik.

Organisatsioon peaks esmalt hindama krüptograafilise küpsuse hetketaset. Organisatsiooni krüptograafiline küpsus tähendab, et kõik krüptograafilised toimingud viiakse läbi korrektselt ja efektiivselt.

TNO käsiraamatu [16] järgi võib organisatsiooni lugeda krüptograafiliselt küpseks, kui:

1. organisatsioonil on täielik ülevaade oma krüptovaradest;
2. organisatsioon mõistab oma krüptosüsteemidega seotud riske;
3. organisatsioonil on asjakohastele nõuetele ja normatiividele vastav krüptograafiapoliitika;

4. organisatsioon jälgib ja ajakohastab järjepidevalt eelmistes punktides loetletut.

Krüptograafilise küpsuse hetketaseme mõistmine (või isegi mis tahes sellesuunalised katsetused ja tegevused) võib osutada postkvant-krüptograafia ülemineku kontekstis vägagi kasulikuks, aidates säästa aega ja raha. Esiteks tagab see, et ühtegi toimingut ei dubleerita. Edasised üleminekutegevused võivad nõuda organisatsioonilt krüptoinventuuri läbiviimist, mis võib aga olla juba toimunud varem. Teiseks aitab olemasolevate krüptograafia-alaste teadmiste dokumenteerimine mõista ja tuvastada koolitus- ja hankevajadusi, mis samuti võib potentsiaalselt kokku hoida vahendeid ja tööaega.

Organisatsioon peaks selles punktis endale esitama mitmesuguseid küsimusi ning viima end kurssi mitmesuguste teemadega, mis panevad paika selle krüptograafilise küpsuse hetketaseme.

Näidisküsimused ja võimalikud vastused:

- Kui hästi on meie süsteem dokumenteeritud?
- Kas meil on olemas sisemine krüptograafia-alane oskusteave (nt erinevate krüptograafia valdkondade põhimõistete tundmine, nagu avaliku võtmega ja sümmeetriline krüptograafia, räsifunktsioonid jne)?
- Milline on organisatsioonisisene teadlikkus kvantohust ja selle leevendamisest (eelkõige postkvant-krüptograafiast)?
- Kas me oleme varem läbi viinud krüptoinventuure?
 - Kui oleme, siis kas nende tulemused on taaskasutatavad? On nad ajakohased? Kas süsteemis on inventuuri järel tehtud olulisi muudatusi?
- Kas me viime regulaarselt läbi või oleme aeg-ajalt läbi viinud infoturbe riskianalüüse?
- Kas meil on kehtestatud infoturbe-/krüptograafiapoliitika?
- Kas me teeme krüptograafiliste toimingute ja varade regulaarset seiret?
- Kas meie tarkvaraarendustegevus tähtsustab krüptograafilist kohandatavust?
- Kas meie arhitektuur/infrastruktuur on täpselt kirjeldatud (diagrammide, dokumentatsioonina)? Kui jah, siis kas selle kirjeldus hõlmab krüptograafia kasutust?
- Kas me järgime mingeid krüptograafia-alaseid standardeid/normatiivakte?

Soovitame läbi viia paar nende küsimuste teemalist ajurünnakut, milles osaleksid üleminekujuhi (OP.1.1) valitud ja kutsutud töötajad. Teise võimalusena võib üleminekujuht koguda vajalikku teavet ise (OP.1.2).

Vastused eeltoodud küsimustele on juba iseenesest kasulik ressurss, kuid varasemad krüptograafiaga seotud tegevused võivad ülemineku tegevuskava kontekstis tuua nähtavale nii otseteid kui ka kohti, kus tuleb takistuste kõrvaldamiseks peatuda. Näiteks organisatsiooni võrdlemisi madal krüptograafiline küpsus võib tingida vajaduse väliste nõustajate/seminaride järele. Juhul kui organisatsioonil puudub põhjalik arhitektuuri dokumentatsioon, võib see nõuda peatust selle koostamiseks. Seevastu võrdlemisi kõrge krüptograafilise küpsuse korral võivad mõned teist tegevustest olla juba läbi viidud või vähem asjakohased.

OP.2: oodatavad tulemid

- OP.2.1: üleminekujuht on saanud ja koondanud vastused eeltoodud küsimustele.

- OP.2.2: organisatsioon on tuvastanud potentsiaalsed puudused krüptograafilises küpsuses (ebapiisav ülevaade krüptograafilistest varadest, infoturvariskide puudulik hindamine, puuduv infoturvapoliitika, ebapiisav seire jne).

5.5.1.3 OP.3: sidusisikute määratlemine ja teavitamine

See tegevus on I kategooria organisatsioonidele kohustuslik, II kategooriale soovituslik ja III kategooria organisatsioonide jaoks vabatahtlik.

Organisatsiooni juhtivtöötajad peavad mõistma postkvant-krüptograafia ülemineku väärtust ja eesmärki. Niisuguste sidusisikute hulka võiksid kuuluda need, kelle tegevus sõltub, toetab või saab potentsiaalselt kasu organisatsiooni üleminekust postkvant-krüptograafia. Üleminekujuht peaks looma kommunikatsioonikanali, mille kaudu sidusisikuid teavitada ülemineku käigust. Sama kanalit võib ühtlasi kasutada täiendavate ressursside või allüksuste vahelise koostöö koordineerimiseks.

Sissejuhatav teade sidusisikutele võiks sisaldada vastuseid järgmistele küsimustele (mis peaksid olema kogutud tegevuse OP.1.2 käigus):

- Millist kasu saab meie organisatsioon üleminekust postkvant-krüptograafia?
- Kui kiiresti tuleb üleminek käivitada?
- Millised on postkvant-krüptograafia ülemineku seotud rahalised ja operatsioonilised vajadused?

Sidusisikute määratlemine ja teavitamine võiks ühtlasi hõlmata neile ülevaate andmist vajaka jäämistest organisatsiooni krüptograafilises küpsuses (OP.2.2) ning puuduste kõrvaldamist väliskonsultantide kaasamise või organisatsioonisisese oskusteabe levitamise teel (loengute/seminaride vormis).

OP.3: oodatavad tulemid

- OP.3.1: üleminekujuht on määratlenud organisatsiooni olulistest või juhtivtöötajatest sidusisikud;
- OP.3.2: olemas on kommunikatsioonikanal sidusisikute ja üleminekujuhi vahel;
- OP.3.3: sidusisikutele on antud ülevaade postkvant-krüptograafia ülemineku problemaatikast.

5.5.1.4 OP.4: süsteemitarnijate tuvastamine ja nendega kontakti loomine

See tegevus on kohustuslik kategooriatele I, II ja III.

Mõni osa organisatsiooni süsteemide krüptofunktsioonistikust võib olla hangitud väliselt edasimüüjalt või tarnijalt. Sel juhul tuleb võimalikult varakult luua kontakt tarnijatega, eesmärgiga selgitada välja, kas nende plaanid üleminekuks postkvant-krüptograafia ühilduvad organisatsiooni plaanide ja ajakavaga. Ülemineku käigus võib tekkida vajadus mõne tarnija kiireks välja vahetamiseks. Seda riski tasub arvesse võtta juba ettevalmistuste faasis.

Üleminekujuhi ülesanne on siin välja selgitada (tõenäoliselt sidusisikute abiga, kasutades OP.3.2 tulemusena loodud kanalit) ja läbi vaadata asjakohaste lepingutega seotud dokumentatsioon (reeglina ostuarved või tarnelepingud). Kas lepingud sisaldavad mingit teavet kasutatava krüptograafia kohta? Kas kusagil on otseselt mainitud postkvant-krüptograafiat?

Asjakohaste lepingute esemeks võivad olla:

- terviklikud IT-süsteemid (kliendi- või kasutajahaldus jne);
- riistvarakomponendid (füüsiline turvamoodul, kiipkaart, YubiKey jne);
- allsüsteemid (X-tee, Kubernetes, AWS jne);
- omand-krüptoteegid.

Märkigem, et tarnijate loetelu võib olla koostatud juba [tegevuse OP.2](#) osana. Seda võib aga igal hetkel täiendada.

Lepingute läbivaatuse järel tuleks kindlasti võtta ühendust tarnijatega ja paluda neilt teavet nende postkvant-krüptograafia ülemineku plaanide ja konkreetsemalt selle ajakava kohta. Täpsemaid suuniseid (nt pöördumise soovitatava sisu kohta) leiab [tegevuse LP.2](#) alt.

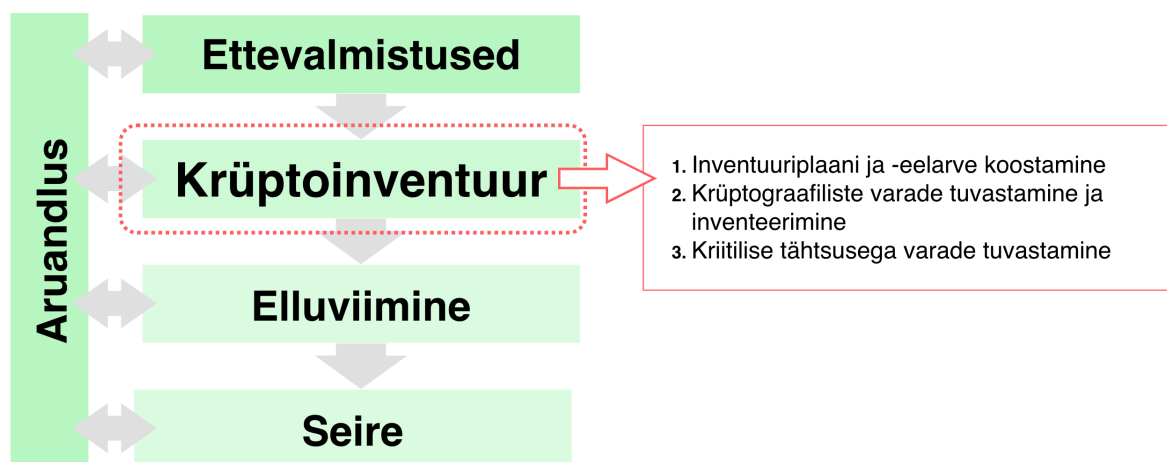
OP.4: oodatavad tulemid

- OP.4.1: organisatsioon on välja selgitanud ja läbi vaadanud kehtivad lepingud krüptosüsteemide tarnijatega.
- OP.4.2: organisatsioon on võtnud ühendust tuvastatud tarnijatega ning palunud neilt teavet postkvant-krüptograafia ülemineku seotud plaanide ja ajakavade kohta.

5.5.2 Krüptoinventuur

Postkvant-krüptograafia ülemineku teine oluline etapp on krüptovarade inventuuri läbiviimine. Kuivõrd krüptograafiat kasutatakse tänapäeva maailmas sisuliselt kõikjal, on väga oluline, et krüptovarade (krüptograafiaga seotud objektide, nagu krüptoalgoritmid, võtmed, toimingud jne) tuvastamine ja läbivaatus oleks dokumenteeritud ja põhjalik. Üheainsagi krüptograafia kasutuskoha kahe silma vahele jätmise võib potentsiaalselt luua süsteemis nõrga koha. Joonis 7 esitab illustratiivse ülevaate teise etapi tegevustest.

Paljud allikad peavad krüptoinventuuri postkvant-krüptograafia ülemineku kõige olulisemaks, ent ka kõige keerukamaks osaks. Soovime sarnaselt neile samuti siinkohal rõhutada inventuuri olulisust ning soovime varuda selle juures kannatust ja läheneda ülesandele võimalikult suure põhjalikkusega.



Joonis 7. Teine ülemineku etapp (krüptoinventuur)

5.5.2.1 OP.5: inventuuriplaani ja -eelarve koostamine

See tegevus on I kategooria organisatsioonidele kohustuslik, II kategooriale soovituslik ja III kategooria organisatsioonide jaoks vabatahtlik.

Organisatsioon peab selles etapis esmalt koostama krüptoinventuuri plaani, mis käsitleks muuhulgas järgmisi küsimusi:

- olemasolevad teadmised krüptoinventuuri protsessist ja meetoditest;
- täieliku/täiendava krüptoinventuuri ulatus;
- krüptovarade avastamismeetodite ja -vahendite tuvastamine (vt soovitusi järgmise tegevuse all);
- krüptovarade inventariloendi vormi määratlemine;
- hinnanguline inventuuri jaoks nõutav aeg;
- toimingute eest vastutavad töötajad;
- inventuuri läbiviimiseks vajalik välisabi (välised konsultandid, seminarid, loengud).

Märkigem, et loetletud asjaoludest osad võivad olla kindlaks määratud juba osana tegevusest OP.2.1.

Saadud teabe põhjal on organisatsioonil võimalik koostada inventuuri hinnanguline eelarve. Selle koostamise protsess on organisatsiooniti erinev, mistõttu me seda siin lähemalt ei käsitle.

Soovitame tutvuda lisa B esitatud krüptoinventuuri läbiviimist käsitleva kirjanduse ülevaatega. See sisaldab muuhulgas inventuuriprotsessi kondikava ja selle eri aspektide kirjeldusi. Samuti sisaldab lisa B kokkuvõtet olemasolevatest krüptoinventuuri tööriistudest.

OP.5: oodatavad tulemid

- OP.5.1: organisatsioon on koostanud krüptoinventuuri plaani.
- OP.5.2: organisatsioon on koostanud selle tegevuse hinnangulise eelarve.

5.5.2.2 OP.6: krüptograafiliste varade tuvastamine ja inventeerimine (krüptoinventuur)

See tegevus on kategooriate I, II ja III jaoks kohustuslik.

See tegevus hõlmab organisatsiooni taristus leiduvate krüptograafiliste varade tuvastamist (inventuuriplaani alusel; vt OP.5.1). Ühtset metoodikat kõigi prioriteedikategooriate organisatsioonide jaoks ei ole selle jaoks võimalik esitada, kuivõrd iga süsteem ja infrastruktuur on erineva ülesehitusega. Siiski oleme allpool püüdnud välja tuua inventuuriprotsessi põhietapid.

Krüptovarade tuvastamis- ja inventeerimisprotsessi esimese sammuna võiks üleminekujuhut enne tabelite jms koostamist alustada krüptovarade kandmisest diagrammile. Visuaalsed materjalid (kaardistused, diagrammid) peaksid usutavasti hõlbustama protsessi sisse elamist ning olema sellele inimsõbralikuks lähtepunktiks.

Märkigem, et tegevus OP.2 võib juba olla andnud ülevaate varasematest krüptovarade inventeerimiste tulemustest.

Soovituslikud üldtoimingud:

1. leidke või koostage süsteemi taristu kaardid/diagrammid. Võtke seejuures arvesse:
 - süsteemi arhitektuuri; ja
 - äri-/andmetöötlusprotsesse ja töövooge;
2. tooge diagrammidel välja kõik krüptovarad (vt määratlust allpool). Soovitame üles märkida ka:
 - objekti liigi (võti, sertifikaat, digitaalsignatuur, signeeritud fail, protokoll jne);
 - selle krüptograafilised parameetrid (algoritm, võtmepikkus, elliptikõver, šifrikomplekt jne);
 - selle eesmärk (logifaili signeerimiseks, jaossiladuse loomiseks jne); ja
 - selle säilituskoha üksikasjad (kus seda säilitatakse, kuidas säilituskohta kaitstakse jne);
3. koondage krüptovarad tabeli vormi (tabel, tööleht, CSV, SQL-andmebaas vms):
 - esmase andmestiku rolli võivad täita eelmise alamtegevuse käigus tuvastatud krüptovarad, kuid kaaluda tasub ka muid kogumisviise, nagu automaattööriistad või andmete käitsi sisestamine;
 - iga organisatsioon peaks valima selle organisatsiooni süsteemide keskkonda sobiva vormingu ning ideaaljuhul koostama inventariloendi nullist. Alternatiivina sellele soovitame PQCC krüptoinventuuri töölehte <https://pqcc.org/pqc-inventory-workbook/>, mis on spetsiaalselt krüptoinventuuri läbiviimiseks mõeldud tabelleid ja andmevälju sisaldav töövihiku mall;
4. koguge ja kategoriseerige täiendavaid metaandmeid, nagu:
 - krüptovara sisaldava süsteemi osa eest vastutav kontaktisik;
 - milline on objekti praegune kvantkindlus (kvantohu hinnang);
 - milline on selle vara elutsükkel;
 - sõltuvus välistarnijast; ja
 - täiendavad märkused.

Mis on krüptograafilised varad? Krüptovarade hulka loetakse krüptograafilisi komponente ja kõiki nendega seotud digitaalsete objekte. Nende põhiülesanne on tagada andmete konfidentsiaalsus, terviklus, autentsus, salgamatus või loetletud turvafunktsioonide mis tahes kombinatsioon. Krüptovaradeks võivad olla krüptograafilised algoritmid, protokollid, krüptovõtmed, sertifikaadid, teenused ja süsteemi loogilised osad.

Krüptograafilisi varasid võidakse rakendada tarkvaras (krüptoteegid, võtmed, identsustõendid, tookenid jne), operatsioonisüsteemides (VPNid, 2-faktoriline autentimine, hoideandmete krüpteerimine, turvaline buutimine jne) ja võrguliikluses (TLS, krüpteeritud elektronpostiside, veebi lehitsemine, pilvteenused jne).

Rohkem teavet krüptograafiliste varade kohta leiab krüptovarade inventeerimist käsitleva erialakirjanduse ülevaatest (lisa B). Peatükist B.2.2 leiab loetelu konkreetsetest näitlikest kohtadest, kust krüptovarasid otsida.

Krüptoprimitiivid. Põhjaliku ülevaate kõige levinumatest krüptoprimitiividest ja nende kvantkindlusest leiab TNO postkvant-krüptograafia ülemineku käsiraamatu [16] 6. peatükist („Background on Primitives“), aga ka sama käsiraamatu terminoloogia peatükist.

Kvantohu hindamine. Soovitame iga tuvastatud krüptovara kvantkindlust hinnata eraldi. Krüptograafilise küpsuse taseme tõstmiseks tasub seejuures tutvuda ETSI juhiseiga „Repeatable Fra-

mework for Quantum-Safe Migration“ [14] (ptk 6.4, tabel 2), mis sisaldab selgelt määratletud kriteeriume (mitte üksnes kvantohuga seotud) nõrkuste hindamiseks.

Iteratiivne protsess. Ülesande olulisusest ja keerukusest tulenevalt on ootuspärane, et kõigi organisatsiooni krüptovarade täielikku loetelu ei õnnestu juba esimesel katsel veel koostada. Seepärast tuleks selle tegevuse tulemeid käsitleda võrdlusalusena tulevaste krüptoinventuuride ja krüptovarade loetelu täiendamise jaoks.

Soovitame inventuuri käigus püüda tuvastada võimalikult suure hulga krüptovarasid kuid püsida seejuures mõistlikes ajalistes raamides, et mitte pidurdada sellega üleminekuprotsessi tervikuna. Teisisõnu, üleminekujuht peaks otsustama, millal on aeg liikuda edasi järgmiste tegevuste juurde. Seejuures peaks ta aga silmas pidama, et mitte kõik krüptovarad ei pruugi veel olla leitud ning inventuuriprotsessi on seetõttu vaja tulevikus korrata.

OP.6: oodatavad tulemid

- OP.6.1: Organisatsioon on tuvastanud enamiku oma krüptovaradest ning säilitab neid dokumenteeritud ja süstemaatilisel viisil.
- OP.6.2: Organisatsioonil on paigas plaanid inventuuriprotsessi täiendavate iteratsioonide jaoks.
- OP.6.3: Organisatsioon on välja selgitanud kõigi tuvastatud krüptovarade kvantkindluse taseme.

5.5.2.3 OP.7: kriitilise tähtsusega varade tuvastamine

See tegevus on I kategooria organisatsioonide jaoks kohustuslik ning II ja III kategooria jaoks soovituslik.

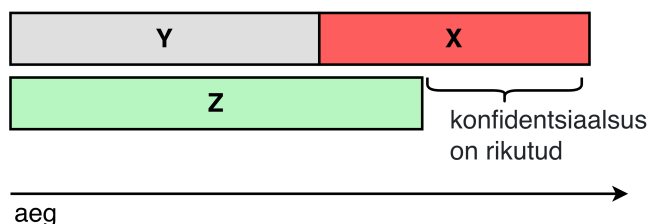
Krüptovarade inventuurile (OP.6) järgneb tuvastatud varade prioriseerimine ülemineku vaatenurgast. Üleminekujuht peab vaatama läbi krüptovarade loendi (OP.6.1) ja hindama sellesse koondatud andmeid ning tõstma nende seast esile krüptograafilised varad, millele organisatsioon ülemineku elluviimise etapis peaks esmajärjekorras keskenduma. Selle juures tuleks keskenduda kolmele aspektile.

Avatus harvest-now-decrypt-later rünnete. Postkvant-krüptograafia üleminekul tuleb prioriseerida krüptograafilisi varasid, mille ülesandeks on tagada kestvalt tundlike andmete (nagu riigialadused, tervise- ja finantsandmed) konfidentsiaalsus olukorras, kus nende andmete konfidentsiaalsusnõue kehtib kauem kui hinnanguliselt kulub praeguseid avaliku võtmega krüptosüsteeme murdva suutvate kvantarvutite väljatöötamiseks. Selle ohumudeli järgi, mis on inglise keeles tuntud *harvest-now-decrypt-later* ründena, võivad potentsiaalsed vastased juba praegu koguda krüpteeritud andmeid, et neid dekrüpteerida millalgi tulevikus, kui kvantarvutid „õpivad“ murdma klassikalisi krüptoalgoritme.

Üleminekuvajaduse pakilisuse hindamise aluseks võib võtta Mosca teoreemi⁴ [17], mis pakub selleks lihtsa praktilise kriteeriumi: kui andmed peavad säilitama konfidentsiaalsuse vähemalt X aastaks, neid kaitsva süsteemi üleviimine postkvant-krüptograafia võtab Y aastat ning Z aasta jooksul võivad tootmisesse jõuda kasutatavat krüpteeringut murda suutvad kvantarvutid, siis on kohene tegutsemine nõutav juhul kui $X + Y > Z$ (Joonis 8). Näiteks kui andmete konfidentsiaal-

⁴Märkigem, et Mosca teoreem ei ole ranges mõistes teoreem, vaid pigem heuristik üleminekuvajaduse hindamiseks.

sus peab säilitama vähemalt 25 aastat ning me eeldame, et sobiv kvantarvuti jõuab tootmisesse 30 aasta pärast ja postkvant-krüptograafia üleminek võtab 10 aasta, siis $25 + 10 > 30$ on tõene.



Joonis 8. Mosca teoreem

Pikad üleminekuperioodid. Keerukate süsteemide ja pika tööeaga seadmetega kaasneb ülemineku viibimise risk. Seetõttu tuleks prioriteediks seada ka sedalaadi süsteemides kasutatavad krüptovarad. Nende hulka kuuluvad näiteks avaliku võtme taristud, esemevõrgu seadmed, kiipkaardid jne. Arvesse tuleb võtta ka toimingus OP.4.1 tuvastatud tarnijaid ja nende üleminekupeioode.

Organisatsioonispetsiifilised kriitilise tähtsusega varad. Organisatsioon peaks lisaks viima riskikontrolli, mille objektiks oleks hüpoteetilised stsenaariumid, kus vastasel on juba olemas klassikalise krüptograafia murdmiseks võimeline kvantarvuti. Millised varad on organisatsiooni toimimise seisukohast kõige kriitilisemad? Võib-olla need varad juba tuvastati toimingus OP.2.1 ja nende üle peetakse arvet.

OP.7: oodatavad tulemid

- OP.7.1: organisatsioon on tuvastanud kriitilise tähtsusega krüptovarad, mis peavad olema tegeliku ülemineku protsessi esimene prioriteet.
- OP.7.2: Kriitilise tähtsusega krüptovarad on kantud krüptovarade loendisse.

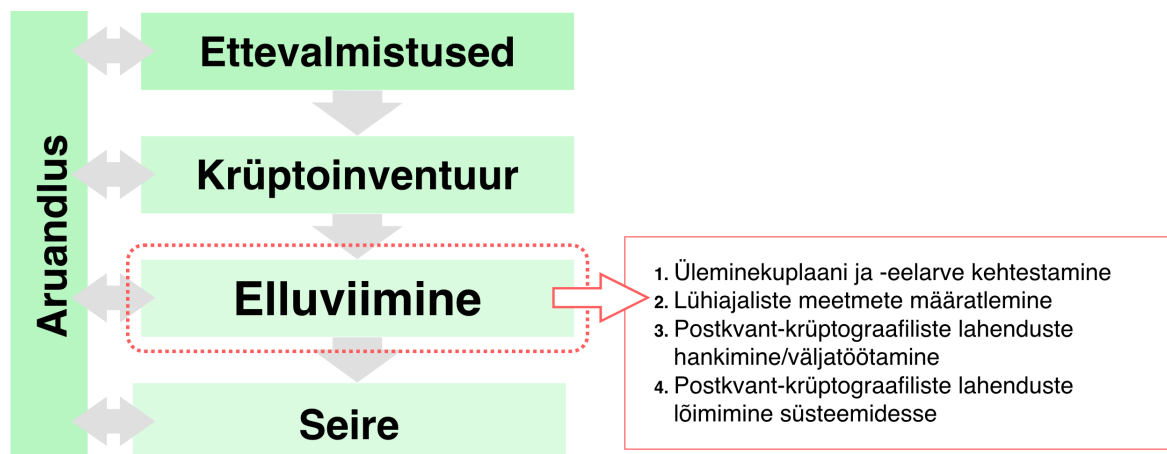
5.5.3 Elluviimine

Postkvant-krüptograafia ülemineku kolmas põhietapp tähistab tegelikku üleminekut klassikaliselt postkvant-krüptograafia. Kasutatavate krüptosüsteemide otsese ajakohastamise kõrval on selle käigus siiski veel vaja langetada mitmeid otsuseid ja sooritada mitmeid toiminguid. Joonis 9 esitab illustratiivse ülevaate kolmanda etapi tegevustest.

5.5.3.1 OP.8: ülemineku plaani ja -elarve kehtestamine

See tegevus on I kategooria organisatsioonidele kohustuslik, II kategooriale soovituslik ja III kategooria organisatsioonide jaoks vabatahtlik.

Organisatsioonil võib olla mitu erinevat teenust, mis kasutavad erinevaid krüptograafilisi varasid. Mõned organisatsiooni teenused või andmekogud on kõrgema prioriteetiga, sest andmed mis seal töödeldakse on kriitilisemad. Seega, organisatsioon peab enda teenuseid prioritseerida ülemineku protsessi jaoks. Võttes aluseks tegevuse OP.7 tulemusel koostatud (prioriteetsete) krüptovarade loendi, peavad organisatsioonid iga tuvastatud vara jaoks valima toimimisviisi – kas leevendada kvantriski postkvant-krüptograafia üleminekuuga või riski aktsepteerida. Lisaks peaks organisatsioon selles punktis võtma uuesti ühendust olemasolevate tarnijatega (OP.4.1)

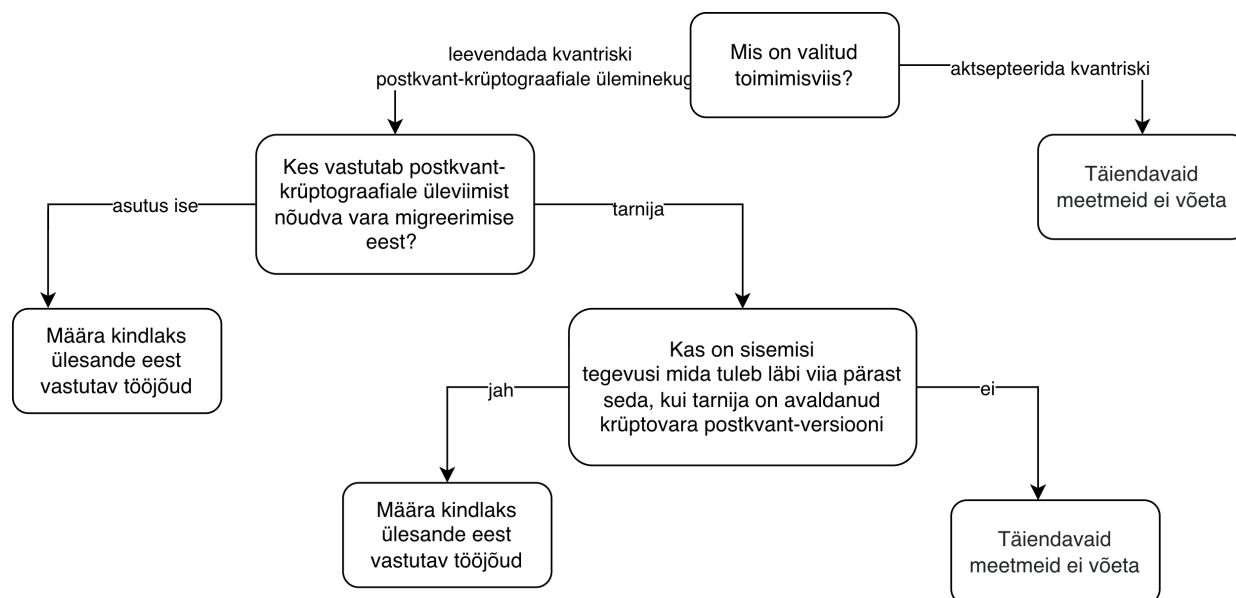


Joonis 9. Kolmas ülemineku etapp (elluviimine)

või tuvastatud potentsiaalsete uute tarnijatega (OP.4.2 tulemuste põhjal), et nõuda neilt teavet nende postkvant-krüptograafia ülemineku kulgemise kohta. Organisatsioon peab välja selgitama, kes vastutab iga postkvant-krüptograafia üleviimist nõudva vara migreerimise eest – kas tarnija või organisatsioon ise. Esimesel juhul peab organisatsioon ühtlasi hindama, milliseid sisemisi tegevusi tuleb läbi viia pärast seda, kui tarnija on avaldanud kõnealuse krüptovara postkvant-versiooni.

Lisaks peab üleminekujuht selle tegevuse osana välja selgitama kõik üleminekuuga seotud süsteemid ja allsüsteemid organisatsiooni taristus, milleks ta peab vaatama iteratiivselt läbi krüptovarade loendi (OP.6.1) ja tuvastama kõik süsteemi osad, milles konkreetset vara kasutatakse.

Organisatsioon peab ühtlasi tuvastama postkvant-krüptograafia üleminekuuga seotud tööjõuvajadused. See võib hõlmata määratletud ülesannete täitmiseks uute töötajate leidmist. Selle tegevuse võtab kokku joonis 10.



Joonis 10. OP.8: nõutavad toimingud

Postkvant-krüptograafia üleviimist vajavate varade hulka ning nende üleviimise eest vastutavat poolt puudutavate andmete põhjal peab organisatsioon koostama eelarve tuvastatud tegevustega seotud kulutuste katmiseks. Eelarve koostamise protsessi siin lähemalt ei käsitleta.

Hübriidrežiimid. „Hübriidrežiim“ tähendab selles kontekstis klassikalise ja postkvant-krüptograafia kombineerimist eesmärgiga kaitsta krüptograafilisi süsteeme nii kvantohu kui ka potentsiaalselt tuvastamata postkvant-krüptograafia vastu suunatud rünnete eest. Sarnaselt enamikult teiste maailma riikide tegevuskavadele soovime ka meie siin üldreeglina kasutada just nimelt hübriidrežiime.

Siiski peab üleminekujuht ise teadlikult otsustama, kas teostada postkvant-krüptograafiat hübriidrežiimis (millega kaasneb vajadus uue üleminekuprotsessi järele kunagi tulevikus ning teostuse suurem keerukus) või minna üle vahetult postkvant-krüptograafiale.

Märkigem, et ka mõned tarnijad võivad hübriidskeemide teostamise asemel minna kohe üle postkvant-krüptograafiale. Juhul kui organisatsioon vajab hübriidrežiimis töötavaid süsteeme, soovime sellisel juhul otsida sellistele tarnijatele teisi alternatiive.

OP.8: oodatavad tulemid

- OP.8.1: organisatsioon on koostanud üldise üleminekuplaani.
- OP.8.2: organisatsioon on vajaduse korral võtnud (taas) ühendust olemasolevate/tuvastatud tarnijatega ja nõudnud teavet nende postkvant-krüptograafiale ülemineku protsessi kulgemise kohta.
- OP.8.3: organisatsioon on koostanud ülemineku hinnangulise eelarve.
- OP.8.4: organisatsioon on langetanud otsuse hübriidrežiimide kasutamise vajalikkuse kohta (kõikjal või konkreetses süsteemides).

5.5.3.2 OP.9: lühiajaliste meetmete määratlemine

See tegevus on I kategooria organisatsioonidele kohustuslik, II kategooriale soovituslik ja III kategooria organisatsioonide jaoks vabatahtlik.

Üleminekujuht peab üleminekuprotsessi käigus jälgima, kas tundlike süsteemide ja teabe kaitseks on vaja rakendada täiendavaid meetmeid. Need ei ole loomult mitte lõplikud kvantohu eest kaitsvad meetmed, vaid pigem lühiajalised kaitsemeetmed, mis peavad parandama süsteemide ja teabe kaitset kuni postkvant-lahenduste juurutamiseni.

Neid meetmeid võib käsitleda ka pinnase ettevalmistamisena tulevastele postkvant-krüptosüsteemidele, mis aitab tagada praktilisest vaatepunktist sujuvama ülemineku.

Võimalike lühiajaliste meetmete hulka võivad kuuluda [13]:

- uute sertifikaatide kehtivusaja lühendamine;
- genereeritavate võtmete (nii sümmeetriliste kui asümmeetriliste) pikkuse suurendamine;
- plaanid pika kehtivusega sertifikaatide tühistamiseks;
- TLSi teostuste üleviimine versioonile 1.3;
- pika elueaga andmete füüsiliste turvaprotseduuride ja hoideandmete kaitsemeetmete läbi vaatamine;
- vajaduse korral andmete kaitseks täiendavate turvakihtide lisamine (nt VPN või võtmehoidlad).

Lühiajaliste meetmete määratlemine hõlmab ühtlasi väljavalitud meetmete rakendamise tähtaegade kehtestamist ning selle ülesande eest vastutavate töötajate kinnitamist.

OP.9: oodatavad tulemid

- OP.9.1: organisatsioon on määratlenud sobivad lühiajalised meetmed.

5.5.3.3 OP.10: postkvant-krüptograafiliste lahenduste hankimine/väljatöötamine

See tegevus on kohustuslik kategooriatele I, II ja III.

Organisatsioon peab tuvastama kvantkindlad alternatiivid postkvant-krüptograafiale üleviimist vajavatele varadele (OP.6.3). Juhul kui vara pärineb väliselt tarnijalt (OP.4.1), tuleb välja selgitada, kas seda saab tarnida postkvant-krüptograafia toega (potentsiaalselt OP.4.2 tulemusena). Ühtlasi tuleb seejuures kontrollida, kas tarnija täidab organisatsioonile kohalduvaid NISTi (või muid asjakohaseid) krüptoalgoritmidega seotud standardeid ja normatiive.

Organisatsiooni enese hallatavate varade (OP.8.1) jaoks on vaja tuvastada ja luua/välja töötada uued krüptograafilised komponendid ja meetmed. Äärmiselt soovitatav on, et üleminekujuht teeks selleks koostööd tehnilise personaliga.

Soovitame esmalt keskenduda ainult kriitilise tähtsusega varadele (OP.7.1, OP.7.2), sealhulgas nendega seotud täiendavatele kaitsemeetmetele. Ülejäänud varadele tasub keskenduda alles pärast kriitilise tähtsusega varade üleviimist postkvant-krüptograafiale.

Järgnevas tabelis on välja toodud soovituslikud põhifunktsioonide jaoks sobivad (avaliku võtme-ga) krüptoalgoritmid. „Võimalikud algoritmid“ on välja valitud tulevaste standardite jaoks, mis ei ole aga veel jõudnud kehtestamiseni. Mõnede funktsioonide juures oleme välja toonud ka võimalikud hübriidrežiimid.

Funktsioon	Soovituslikud algoritmid	Võimalikud algoritmid	Hübriidrežiim
Võtmekehtestus	ML-KEM [18]	HQC [19]	Algoritmid: (EC)DH + ML-KEM Võtmeühendusfunktsioonid: võtmeühendusfunktsioonid võtmetuletusmeetoditest või võtmeühendusmeetoditest [20, 21]
Digitaalsignatuur	ML-DSA [22], SLH-DSA [23]	FN-DSA [24]	Algoritmid: ECDSA + ML-DSA, RSA + ML-DSA Võtmeühendusfunktsioonid: sidurdus, identifikaatoritega sidurdus [21]
Digitaalsignatuur (olekufiltriga)	XMSS [25, 26], LMS [27, 26]		Võimalik kasutada iseseisvalt

OP.10: oodatavad tulemid

- OP.10.1: organisatsioon on koostanud postkvant-krüptograafiliste algoritmide juurutamiskava.
- OP.10.2: organisatsioon on välja selgitanud, kas tarnijate pakutavad lahendused vastavad standarditele/normatiividele.
- OP.10.3: organisatsioon on välja selgitanud krüptograafiliste lahenduste ise loomise vajaduse.

5.5.3.4 OP.11: postkvant-krüptograafiliste lahenduste lõimimine süsteemidesse

See tegevus on kohustuslik kategooriatele I, II ja III.

Üleminekujuht korraldab koostöös tehnilise personaliga (tegevuse OP.9) tulemusena määratletud lühiajaliste meetmete ja tegevuse OP.10 tulemusena hangitud või välja töötatud postkvant-krüptograafiliste lahenduste installimise/juurutamise. Ülimalt oluline on seejuures ühtlasi selgitada välja võimalike organisatsiooni tegevusega seotud halvangute ulatus ning koostada plaanid ettenägematute pikemate halvangute jaoks.

Enamikul juhtudest soovitame selleks tugineda kas põhjalikele organisatsioonisisestele uuringutele, otsida konsultante väljastpoolt või viia esmalt läbi eksperimentaalseid pilootprojekte. Praktiliste suuniste pakkumine kõigi võimalike kasutusmallide jaoks ei ole aga üheainsa dokumendi raamides mõeldav.

Installimise/juurutamise käigus tuleks kindlasti täiendada olemasolevat krüptovarade loetelu (OP.6.1), et selles kajastuksid kohe ka uued muudatused.

Iteratiivne protsess. Täiesti ootuspärane on, et kõiki uusi lahendusi ühekorraga süsteemidesse lõimida ei õnnestu. Seda tegevust tuleks seetõttu käsitleda iteratiivse protsessina, mille tulemuseks on taristu järkjärguline ajakohastamine. Alustage (nende olemasolu korral) lühiajalistest meetmetest (OP.9.1) ja kriitilise tähtsusega varadest (OP.7.1) ning liikuge seejärel edasi muude loetelus välja toodud krüptovarade juurde.

OP.11: oodatavad tulemid

- OP.11.1: organisatsioon viib ellu tuvastatud lühiajalised meetmed.
- OP.11.2: organisatsioon juurutab järk-järgult kõik postkvant-lahendused.
- OP.11.3: tehtud muudatused kajastuvad organisatsiooni krüptovarade loetelus.

5.5.4 Seire

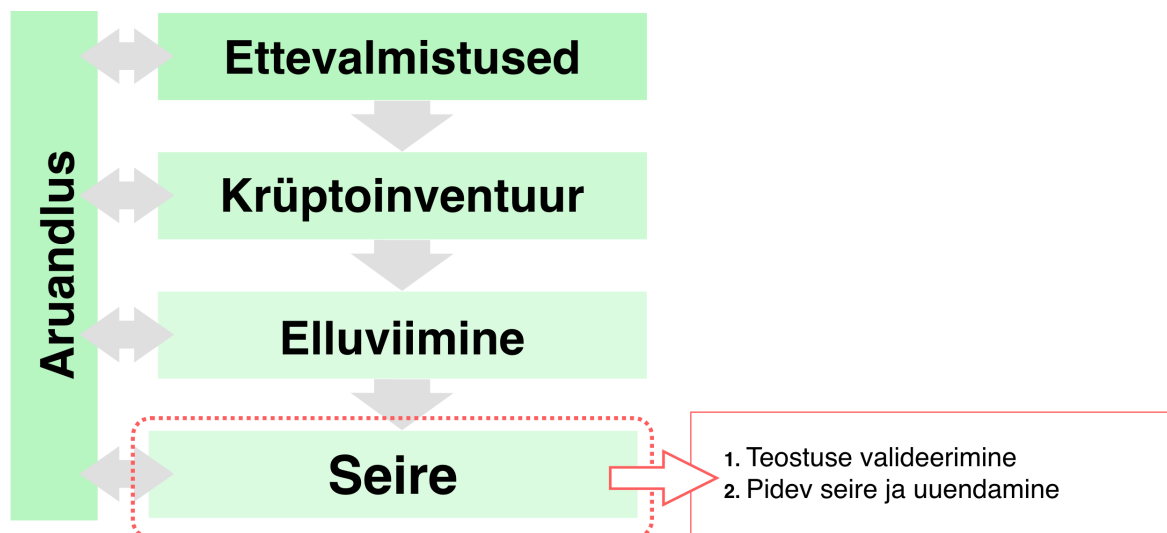
Neljandaks ja viimaseks keskseks tegevuseks on toimingute valideerimine, seire ja aruandlus, mille eesmärgiks on krüptograafilise küpsuse pidev arendamine ning kõigi kohalduvate nõuete järgimine organisatsiooni süsteemide kvantkindluse tagamise käigus. Joonis 11 esitab illustratiivse ülevaate neljanda etapi tegevustest.

5.5.4.1 OP.12: teostuse valideerimine

See tegevus on I kategooria organisatsioonidele kohustuslik, II kategooriale soovituslik ja III kategooria organisatsioonide jaoks vabatahtlik.

Üleminekujuhi järgmiseks ülesandeks on postkvant-krüptograafiliste lahenduste lõimimise/juurutamise (OP.11) tulemuste valideerimine. See hõlmab muuhulgas eelnevalt koostatud plaanide (OP.5.1, OP.8.1 ja OP.10.1) läbivaatamist, kõigi plaanitud tegevuste läbiviimise kontrollimist ning krüptoinventuuri (OP.6.1) tulemuste ülevaatamist.

Kuivõrd üleminek postkvant-krüptograafiale võib olla toimunud võrdlemisi pika aja vältel, võib krüptograafia valdkonnana ja sellega seotud standardid olla vahepeal edasi arenenud. Seetõttu on teostuse valideerimise osana kasulik hinnata ka tehnika hetketaset ning kontrollida, et orga-



Joonis 11. Neljas ülemineku etapp (seire)

nisatsiooni tegevus oleks kooskõlas uute standarditega.

Kokkuvõtlikult näeb see tegevus seega ette organisatsiooni kõigi eelnevate tegevuste eesmärgipärast auditeerimist.

OP.12: oodatavad tulemid

- OP.12.1: organisatsioon on hinnanud postkvant-krüptograafiliste lahenduste teostusi.
- OP.12.2: organisatsioon on läbi vaadanud eelnevalt koostatud plaanid.
- OP.12.3: organisatsiooni tegevus on viidud kooskõlla tehnika hetketasemega.
- OP.12.4: organisatsioon on analüüsinud üleminekuprotsessi senist kulgu.

5.5.4.2 OP.13: pidev seire ja uuendamine

See tegevus on I kategooria organisatsioonidele kohustuslik, II kategooriale soovituslik ja III kategooria organisatsioonide jaoks vabatahtlik.

Erinevalt eelmistest, piiratud kestvusega tegevustest hõlmab see tegevus krüptograafiliste varade, normatiivide, uue tarkvara (ning sellega seoses potentsiaalselt uute krüptograafia kasutusvormide) ja riskianalüüside pidevat seiret ja potentsiaalset ajakohastamist.

Üleminekujuht võiks ühtlasi koostada loetelu saadud õppetundidest ning juurutada organisatsioonis uusi protsesse, mis mõjutaks tulevikus krüptograafia käsitlemist ning turbe üldist paindlikkust.

OP.13: oodatavad tulemid

- OP.13.1: organisatsioon jätkab üleminekuprotsessi, sealhulgas krüptovarade loendi seiret ja ajakohastamist.
- OP.13.2: organisatsiooni arusaamad krüptograafia rollist muutuvad küpsemaks.
- OP.13.3: organisatsioon suurendab järjepidevalt valmisolekut krüptograafia ja turvalisusega seotud ülesannete täitmiseks.

5.5.4.3 OP.14: pidev aruandlus

See tegevus on kohustuslik neile, kellele paneb vastava kohustuse täidesaatev institutsioon

Aruandlus on iteratiivne protsess, mis peaks moodustama osa postkvant-krüptograafia ülemineku protsessist kui tervikust. Aruannete üksikasjalikkus ja sagedus sõltub organisatsiooni kategooriast.

OP.14: oodatavad tulemid

- organisatsioon on andnud järjepidevalt aru postkvant-krüptograafia ülemineku kulgemisest, sealhulgas teavitanud lõpetatud tegevustest ning probleemsetest tegevustest, mille juures võib olla vaja pädeva asutuse tuge.

5.6 Väljast tellimine

Postkvant-krüptograafia ning sellele ülemineku protsess võivad olla segased ja keerulised teemad; ometi ei vähenda see nende olulisust. Seepärast on otstarbekas otsida eeltoodud tegevuste läbiviimiseks abi väljastpoolt. See alapeatükk annab suuniseid, kuidas tellida postkvant-krüptograafia üleminekuga seotud teenuseid väliselt krüptograafia/küberturbe ekspordilt.

Kõigi välise teenuseandja pakutavate võimaluste ärakasutamine eeldab mitmete tegevuste puhul väliseksperdile juurdepääsu andmist organisatsiooni süsteemidele. Organisatsioon peab langetama kaalutletud otsuse, kas välise isiku lubamisest organisatsiooni süsteemidesse tulenevad riskid on vastuvõetavad.

Väljasttellimise üksikasjad ei kuulu selle dokumendi käsitlusalasse, kuid see võib hõlmata hankelepingu analüüsimist, kandidaadi taustakontrolli ning vajaduse korral konfidentsiaalsuslepete sõlmimist.

Enamik üleminekutegevusi on reeglina tellitavad väljastpoolt, eeldusel et teenuseandjal on piisav juurdepääs organisatsiooni ja selle taristut puudutavale teabele. Mõned tegevused tuleb siiski läbi viia organisatsioonisiseste vahenditega. Need tegevused on kokku võetud allpool.

- Kategoriseerimine (SC), ptk 5.3
 - SC.1, SC.2 ja SC.3: organisatsioon peaks ise läbi viima kõik kolm kategoriseerimise/enesehindamisega seotud tegevust, et saada ülevaade postkvant-krüptograafia ülemineku prioriteetidest, riskidest ja ajalistest raamidest.
 - Otsustusprotsessi käigus võib siiski konsulteerida ka organisatsiooniväliste ekspertidega; samuti võivad nad aidata tõlgendada enesehindamise tulemusi ning nende mõju organisatsioonile.
 - Välise eksperti teenuste kasutamine ainult nende kolme toimingu jaoks ei ole üldiselt ratsionaalne.
- Madal prioriteedikategooria (LP), ptk 5.4
 - Tegevused LP.1, LP.2 ja LP.3 on reeglina kõik väljast tellitavad. Samas võib eeldada, et enamiku madala prioriteedikategooria subjektide kasutatavaid süsteeme viivad postkvant-krüptograafia üle nende tarnijad.
 - Väliseksperdi teenuste kasutamine on seega vabatahtlik ning sõltub kasutada olevatest ressurssidest ja hoolsuskohustuse olemasolust.
- Teised prioriteedikategooriad (OP), ptk 5.5

- Alltoodud punktid käsitlevad ainult tegevusi, mida ei ole võimalik väljast tellida ja mis tuleb läbi viia organisatsioonisiseste vahenditega. Kõigil allpool loetlemata juhtudel on soovitatav kasutada välise eksperdi abi.
- Märkigem, et ka kõik väljast tellitavad nõuavad mingil määral organisatsiooni poolset panustamist. Ilma organisatsioonipoolse koostöö ning valmisolekuta jagada eksperdile teavet ja vastata tema küsimustele on eksperdi võimalused äärmiselt piiratud.
- OP.1: üleminekujahi roll on postkvant-krüptograafia üleminekul üks kesksemaid ning seda ei ole võimalik väljast tellida. Olenemata sellest, kes konkreetselt viib läbi üleminekuga seotud toiminguid, peab kokkuvõttes ikkagi nende eest vastutama ning nende läbiviimist kontrollima mõni organisatsiooni enda töötaja.
- OP.2: ehkki organisatsiooni krüptograafilise küpsuse hetketaseme hindamine nõuab kitsaid erialaseid teadmisi, võib siin eeldada, et organisatsioon teeb selles vallas tihedat koostööd välise eksperdiga.
- OP.4: selle tegevuse sisuks on olemasolevate lepingute läbivaatamine, milleks väline ekspert vajab juurdepääsu vastavatele lepingutele. Organisatsioon peab kas eksperdile andma vajaliku juurdepääsu või tuvastama süsteemitarnijad ise.
- OP.5 ja OP.8: kuigi inventuuri-/üleminekuplaani koostamisel on soovitatav tugineda välise eksperdi abile, kuulub eelarve ja vajaliku personali kinnitamine organisatsiooni vastutusalasse.
- OP.6: see tegevus nõuab kas väliseksperdile täieliku juurdepääsu andmist süsteemidele (sh lähtekoodile) või tihedat ja motiveeritud koostööd organisatsiooni ja eksperdi vahel.
- OP.7: erinevalt kõigist teistest varadest peab organisatsioonispetsiifilised kriitilised varad tuvastama organisatsioon ise.
- OP.13: seire ja ajakohastamine on pikaajalised ja katkematud tegevused. Väliseksperdi abi kasutamine ei pruugi nende puhul olla rahaliselt jätkusuutlik.

6 Tähelepanekud eduka ülemineku saavutamiseks

Põhipunktid:

- Hariduses, tervishoius ja finantssektoris kasutatavate infosüsteemide postkvant-krüptograafiale üleviimine peab toimuma koostöös teenuste arendajatega.
- Kui teenuse või süsteemi loomisel on oluline roll rahvusvahelistel tarnijatel, peab krüptograafiliste uuenduste nõuded esitama tarnijale.

„Eesti postkvant-krüptograafiale ülemineku riiklik teekaart“ toob välja olulisemad sammud Eesti avalikus sektoris kvanthaavatavate krüptoalgoritmide kasutamisest loobumiseks. See kirjeldab vajalikke tegevusi, nõuete kehtestamist, järelevalvet, tähtaegu, oletatavat kulu. Esitatud tegevuskava lisad kirjeldavad taustateadmisi, nii projektieelseid kui ka projekti ajal kogutuid, millele toetudes need sammud on välja valitud.

Postkvant-krüptograafiale üleminek on sisult tarkvara uuendamise projekt, millel ehk ei olegi põhimõttelisi erinevusi teistest tarkvarauuendusprojektidest. Erilisemaks teeb selle uuenduse küll asjaolu, et see peab toimuma väga paljudes infosüsteemides korraga, millega kaasneb vajadus eri organisatsioonide tegevusi omavahel kooskõlas hoida. Samuti on see uuendus erilisem selle tõttu, et selle tulemustele on kehtestatud konkreetsed nõuded, mida ja millal saavutada tuleb.

Teekaardis kirjeldatav tarkvarauuendus võiks olla ühekordne toiming – ühtede krüptoalgoritmide kasutuse ja toe eemaldamine, teiste toe lisamine. Tegevuskava valmimise ajal ei ole teada, et ettenähtavas tulevikus tuleks ette võtta järgmine krüptoalgoritmide vahetus. Ette pole näha sedagi, et algoritmide võtmepikkusi peaks tulevikus muutma hakkama (seda enam, et postkvant-krüptograafia algoritmide standardid ei annagi enam võimalust võtmepikkust enam-vähem piiramatult varieerida). Samas ei ole ka võimalik välistada, et mõni valitud algoritmide, mida praegu (kvant)turvaliseks peame, osutub nõrgemaks kui praegu arvame. Sellest tuleneb ka siin esitatud soovitus hübriidrežiimide kasutamiseks.

6.1 Piirangud

6.1.1 Heterogeensus

Alapeatükk 5.5.3 annab soovitusi, kuidas postkvant-krüptograafiat kasutavaid lahendusi hankida ja juurutada. Kuna organisatsioonid on väga erinevad, siis tegevuskavas antud soovitus ei saa olla kõigile organisatsioonidele ühtemoodi kasulikud.

Seetõttu on oluline, et organisatsioonid koostaksid detailse üleminekuplaani. Pädevad asutused saavad selle plaani koostamisel kaasa aidata, levitada paremaid meetodeid ning võrrelda eri organisatsioonide koostatud plaanide kooskõllalisust.

6.1.2 Keerulisemate infosüsteemidega organisatsioonid

Teekaardis esitatud soovitus on mõeldud olema rakendatavad kõigile avaliku sektori organisatsioonidele. Samas tuleb alati silmas pidada, et ühtede organisatsioonide infosüsteemid on

unikaalsemad kui teistel; sageli on need unikaalsed infosüsteemid avalikkuse teravdatud tähelepanu all. Sellisteks infosüsteemideks on näiteks isikutuvastussüsteemid, mille osad (ID-kaardid, passid) on kõigi elanike käes. Infosüsteemide unikaalsus võib tähendada, et ilmseid viise nad postkvant-krüptograafia üle viia on vähe. Organisatsioonidel, mis neid infosüsteeme haldavad, tuleb erilist rõhku panna oma tarnijatega suhtlemisele, nõudes tarnijatelt välja nende postkvant-krüptograafia ülemineku kavad.

6.1.3 Erasektor

Teekaart ei püüa reguleerida, kuidas erasektoris postkvant-krüptograafia kasutusele võetakse. Esile võib tõsta mõningaid tegevusvaldkondi, kus erasektoril on oluline roll eduka ülemineku saavutamisel.

6.1.3.1 Haridus

Eestis on mõned ettevõtted, mis loovad ja haldavad infosüsteeme, mida kasutavad koolid ja lasteaiad. Koolidele ja teistele õppeasutustele rakenduvate nõuete kaudu tekivad nõuded ka neile infosüsteemidele. Need ettevõtted peaksid ise leidma need vahendid, mille abil oma infosüsteemid kvantkindlaks muuta.

6.1.3.2 Meditsiin

Meditsiini vallas on nii väikseid kui ka suuri ettevõtjaid, üksikutest perearstidest suurte haiglateni. Perearstid kasutavad ilmselt enamasti standardseid IT-vahendeid, mille allikaks on enamasti riik: X-tee, Digidoc, riigiportaalid ja -teenused. Kui need teenused hakkavad postkvant-krüptograafiat kasutama, siis hakkab seda kasutama ka perearst.

Perearstidel ja ka suurematel ettevõtetel võib olla meditsiiniseadmeid, kus kasutatavad infotehnoloogilised lahendused on erilisemad; sageli on nende lahenduste üheks eesmärgiks kaughoolduse võimaldamine. Sel juhul peab kas perearst või tema infotehnoloogiline tugi otsustama, mis sellest seadmest saab. Üldisi soovitusi nende kõigi jaoks ei ole võimalik siin anda.

Perearstide infosüsteemide küberturbe olukord ei ole Eestis hea kontrolli all ja meetmete kehtestamine on keeruline. See võib mõjutada kiirust, millega perearstid postkvant-krüptograafia kasutusele võtavad. Siin esitatav tegevuskava seda olukorda parandada ei saa.

Suurtele meditsiiniettevõtetele rakenduvad KÜTSi nõuded. Nende kontroll ja kehtestamine on aga jällegi keeruline probleem.

Meditsiiniettevõtete infosüsteemide tarnijad on osaliselt riigiasutused (näiteks TEHIK), aga väga palju on ka teisi (IT-)ettevõtteid. Nende ettevõtete vahelisi suhteid on riigil keeruline hallata. IT-ettevõtete pakutavad teenused üldiselt ei ole KÜTSi subjektid, aga mingi osa neist peaksid olema.

6.1.3.3 Andme- ja muu side

Eestis on kolm suurt andme- ja mobiilsidevõrguoperaatorit, mis regulaarselt täiendavad ja uuendavad oma võrgutaristut. Postkvant-krüptograafia üleminek võib tekitada neil vajaduse oma võrguseadmeid uuendada kiiremini, kui see neil muidu plaanis oleks olnud.

Operaatorid on huvitatud, et nende investeeringud oleksid tasuvad. Nii mõnigi neist investeerin-gutest (võrgulitsentsid) kujutab endast maksmist selle eest, et nad avaliku ressursi (sagedusala) privatiseerivad. Mida rohkem nad selle eest maksnud on, seda kauem on neil soov seda kasu-

tada. Kui kalliks investeringuks on võrgulitsents, siis ei pruugi nad niipea soovida üle minna uuema põlvkonna võrkudele, mille opereerimiseks vajalik taristu oleks samuti uuem ja seetõttu loodetavasti lihtsamini üle viidav postkvant-krüptograafiat kasutama.

6.1.3.4 Elektrooniline andmevahetus (EDI)

EDI on teenus, mida kasutavad paljud kauplejad. EDI-sõnumid võivad olla signeeritud ja/või krüpteeritud [28]. Postkvant-krüptograafia kasutuselevõttu neis sõnumites peaksid vedama EDI-teenuste tarnijad.

6.1.3.5 Ettevõtte ressursiplaneerimine (ERP)

ERP-tarkvara kasutavad väga paljud ettevõtted. Tarkvara loojad on enamasti suured ettevõtted, mis asuvad väljaspool Eestit. Kui ERP-tarkvarale lisandub postkvant-krüptograafia tugi, siis aitab see kaasa ka Eesti ettevõtete üleminekule. Meil ei ole siiski mõistlikke hoobasid ERP-tarkvara tootjate tegevuskavades tähtaegade seadmiseks.

Bibliograafia

- [1] *Tehniline kirjeldus*. Riigihange „Postkvant-krüptograafia riiklik teekaart (Justiits- ja Digiministeerium)“ viitenumber 292945. 2025.
- [2] Euroopa Komisjon. *Komisjoni soovitus (EL) 2024/1101, 11. aprill 2024, postkvant-krüptograafia ülemineku koordineeritud rakendamise tegevuskava kohta*. Euroopa Liidu Teataja, apr 2024. URL: <http://data.europa.eu/eli/reco/2024/1101/oj>.
- [3] NIS Cooperation group. *A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography. Part 1, Version: 1.1, EU PQC Workstream*. Accessed: 2025-01-05. Juuni 2025. URL: <https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography>.
- [4] Majandus- ja Kommunikatsiooniministeerium. *Küberturvalisuse strateegia 2024–2030 “Läbivalt IT-vaatlikum Eesti”*. Avaldatud 2024. 2024. URL: https://www.mkm.ee/sites/default/files/documents/2024-07/Kyberturvalisuse%5C%20strateegia%5C%202024-2030_labivalt_IT_vaatlik_Eesti.pdf.
- [5] European Commission. *Proposal for a Regulation for the EU Cybersecurity Act*. Shaping Europe’s Digital Future, published 20 January 2026. Jaan 2026. URL: <https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-eu-cybersecurity-act>.
- [6] European Commission. *Proposal for a Directive as regards simplification measures and alignment with the Cybersecurity Act*. Shaping Europe’s Digital Future, published 20 January 2026. Jaan 2026. URL: <https://digital-strategy.ec.europa.eu/en/library/proposal-directive-regards-simplification-measures-and-alignment-cybersecurity-act>.
- [7] Justiitsministeerium ja Riigikantselei. *Mõjude hindamise metoodika*. <https://riigikantselei.ee/valitsuse-too-planeerimine-ja-korraldamine/politikakujundamise-tooriistad/mojude-hindamine>. 2021.
- [8] Cybernetica AS. *Krüptograafiliste turbelahenduste hindamisvõime loomise projekt – I etapp: Eelanalüüsi aruanne (Versioon 1.0)*. Sept 2024. URL: https://cyber.ee/uploads/Krueptograafiliste_turbelahenduste_hindamisvoime_loomise_projekti_I_etapi_aruande_avalik_versioon_c46de79c28.pdf.
- [9] *Krüptoalgoritmid ning nende tugi teekides ja infosüsteemides (Cryptographic algorithms and their support in libraries and information systems)*. <https://www.ria.ee/sites/default/files/content-editors/publikatsioonid/cryptoreport2021.pdf>. Cybernetica report no. T-184-7, v1.0 (in Estonian). 2021.
- [10] *Krüptoalgoritmid ning nende tugi teekides ja infosüsteemides (Cryptographic algorithms and their support in libraries and information systems)*. <https://www.ria.ee/sites/default/files/documents/2023-06/Cryptoreport%202023%20final.pdf>. Cybernetica report no. T-184-7, v2.0 (in Estonian). 2023.
- [11] Federal Office for Information Security (BSI). *BSI TR-02102-1: Cryptographic Mechanisms – Recommendations and Key Lengths*. Technical Guideline. Versioon 2026-01. Available in PDF and HTML formats. Last updated: 23 January 2026. Version 2026-01. Jaan 2026. URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf?__blob=publicationFile&v=13.

- [12] *Krüptoalgoritmid ning nende tugi teekides ja infosüsteemides (Cryptographic algorithms and their support in libraries and information systems)*. Riigi Infosüsteemi Ameti tellimus Cybernetica AS-le. Ilmub 2026. aasta suvel. 2026.
- [13] Post-Quantum Cryptography Coalition. *Post-Quantum Cryptography (PQC) Migration Roadmap*. Tehniline aruanne. Approved for public release. Distribution unlimited 24-03931-7. Accessed: 2025-10-02. Post-Quantum Cryptography Coalition, mai 2025.
- [14] ETSI. *CYBER; Quantum-Safe Cryptography (QSC); A Repeatable Framework for Quantum-Safe Migrations*. Technical Report ETSI TR 104 016 V1.1.1. Reference: DTR/CYBER-QSC-0024. Accessed: 2025-10-02. European Telecommunications Standards Institute, okt 2024.
- [15] Christian Näther *et al.* "Migrating Software Systems Toward Post-Quantum Cryptography—A Systematic Literature Review". *IEEE Access* 12 (2024). Accessed: 2025-10-02, lk-d 132107–132126. DOI: [10.1109/ACCESS.2024.3450306](https://doi.org/10.1109/ACCESS.2024.3450306).
- [16] Alessandro Amadori *et al.* *The PQC Migration Handbook: Guidelines for Migrating to Post-Quantum Cryptography*. Technical Handbook. Accessed: 2025-10-03. AIVD, CWI ja TNO, dets 2024.
- [17] Michele Mosca. "Cybersecurity in an Era with Quantum Computers: Will We Be Ready?" *IEEE Secur. Priv.* 16.5 (2018), lk-d 38–41. DOI: [10.1109/MSP.2018.3761723](https://doi.org/10.1109/MSP.2018.3761723). URL: <https://doi.org/10.1109/MSP.2018.3761723>.
- [18] 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](https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.pdf). URL: <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.pdf> (vaadatud 29.09.2025).
- [19] HQC Key Establishment Mechanism Project. *HQC (Hamming Quasi-Cyclic): code-based Key Encapsulation Mechanism (KEM)*. One of the selected algorithms from the NIST's Post-Quantum Cryptography Standardization Project. Accessed: 2026-02-20. URL: <https://pqc-hqc.org/index.html>.
- [20] Gorjan Alagic *et al.* *Recommendations for Key-Encapsulation Mechanisms*. Tehniline aruanne NIST SP 800-227. National Institute of Standards ja Technology, 2025, NIST SP 800-227. DOI: [10.6028/NIST.SP.800-227](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-227.pdf). URL: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-227.pdf> (vaadatud 29.09.2025).
- [21] European Telecommunications Standards Institute (ETSI). *ETSI TR 103 966 V1.1.1 (2024-10): Deployment Considerations for Hybrid Schemes*. Technical Report TR 103 966 V1.1.1. Sophia Antipolis, France: ETSI, okt 2024. URL: https://www.etsi.org/deliver/etsi_tr/103900_103999/103966/01.01.01_60/tr_103966v010101p.pdf.
- [22] 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](https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.204.pdf). URL: <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.204.pdf> (vaadatud 29.09.2025).
- [23] 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](https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.205.pdf). URL: <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.205.pdf> (vaadatud 29.09.2025).

- [24] Falcon Cryptographic Signature Algorithm Project. *Falcon: A Fast-Fourier Lattice-based Compact Signature Scheme*. Submitted to NIST Post-Quantum Cryptography Project on November 30, 2017. Accessed: 2026-02-16. 2017. URL: <https://falcon-sign.info>.
- [25] Andreas Huelsing *et al.* *XMSS: eXtended Merkle Signature Scheme*. RFC 8391. Mai 2018. DOI: [10.17487/RFC8391](https://doi.org/10.17487/RFC8391). URL: <https://www.rfc-editor.org/info/rfc8391>.
- [26] National Institute of Standards ja Technology. *Recommendation for Stateful Hash-Based Signature Schemes*. NIST Special Publication 800-208. Accessed: 2026-02-20. National Institute of Standards ja Technology, 2020. URL: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-208.pdf>.
- [27] David McGrew, Michael Curcio ja Scott Fluhrer. *Leighton-Micali Hash-Based Signatures*. RFC 8554. Apr 2019. DOI: [10.17487/RFC8554](https://doi.org/10.17487/RFC8554). URL: <https://www.rfc-editor.org/info/rfc8554>.
- [28] Dr. Dale W. Moberg ja Rik Drummond. *MIME-Based Secure Peer-to-Peer Business Data Interchange Using HTTP, Applicability Statement 2 (AS2)*. RFC 4130. Juuli 2005. DOI: [10.17487/RFC4130](https://doi.org/10.17487/RFC4130). URL: <https://www.rfc-editor.org/info/rfc4130>.
- [29] Peter W. Shor. "Algorithms for quantum computation: discrete logarithms and factoring". Teoses: *Proceedings 35th Annual Symposium on Foundations of Computer Science*. 1994, lk-d 124–134. DOI: [10.1109/SFCS.1994.365700](https://doi.org/10.1109/SFCS.1994.365700).
- [30] Lov. K Grover. "A fast quantum mechanical algorithm for database search". Teoses: *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*. STOC '96. Philadelphia, Pennsylvania, USA: Association for Computing Machinery, 1996, lk-d 212–219. ISBN: 0897917855. DOI: [10.1145/237814.237866](https://doi.org/10.1145/237814.237866). URL: <https://doi.org/10.1145/237814.237866>.
- [31] Gilles Brassard, Peter Høyer ja Alain Tapp. "Quantum cryptanalysis of hash and claw-free functions". Teoses: *LATIN'98: Theoretical Informatics*. Toim. Cláudio L. Lucchesi ja Arnaldo V. Moura. Berlin, Heidelberg: Springer Berlin Heidelberg, 1998, lk-d 163–169. ISBN: 978-3-540-69715-2.
- [32] Michele Mosca ja Marco Piani. *Quantum Threat Timeline Report 2024*. 2024. URL: <https://globalriskinstitute.org/publication/2024-quantum-threat-timeline-report/>.
- [33] Erdem Alkim *et al.* *FrodoKEM: Learning With Errors Key Encapsulation. Preliminary Standardization Proposal*. 2024. URL: https://frodokem.org/files/FrodoKEM_standard_proposal_20241205.pdf.
- [34] *BSI – Technical Guideline. Cryptographic Mechanisms: Recommendations and Key Lengths*. Tehniline aruanne. Federal Office for Information Security (BSI), 2025. URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf?__blob=publicationFile&v=7 (vaadatud 29.09.2025).
- [35] Pierre-Alain Fouque *et al.* *Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU. Specification v1.2*. 2020. URL: <https://falcon-sign.info/falcon.pdf>.
- [36] Daniel J. Bernstein *et al.* *Classic McEliece: conservative code-based cryptography: cryptosystem specification*. 2022. URL: <https://classic.mceliece.org/mceliece-spec-20221023.pdf>.
- [37] Philippe Gaborit *et al.* *HQC specifications*. 2025. URL: https://pqc-hqc.org/doc/hqc_specifications_2025_08_22.pdf.

- [38] Johannes Buchmann, Erik Dahmen ja Andreas Hülsing. "XMSS - A Practical Forward Secure Signature Scheme Based on Minimal Security Assumptions". Teoses: *Post-Quantum Cryptography*. Toim. Bo-Yin Yang. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, lk-d 117–129. ISBN: 978-3-642-25405-5.
- [39] Frank T. Leighton ja Silvio Micali. *Large provably fast and secure digital signature schemes based on secure hash functions*. 1995. URL: <https://patents.google.com/patent/US5432852A/en>.
- [40] Ward Beullens. "Breaking Rainbow Takes a Weekend on a Laptop". Teoses: *Advances in Cryptology – CRYPTO 2022*. Toim. Yevgeniy Dodis ja Thomas Shrimpton. Cham: Springer Nature Switzerland, 2022, lk-d 464–479. ISBN: 978-3-031-15979-4.
- [41] Jintai Ding ja Dieter Schmidt. "Rainbow, a New Multivariable Polynomial Signature Scheme". Teoses: *Applied Cryptography and Network Security*. Toim. John Ioannidis, Angelos Keromytis ja Moti Yung. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, lk-d 164–175. ISBN: 978-3-540-31542-1.
- [42] Wouter Castryck ja Thomas Decru. "An Efficient Key Recovery Attack on SIDH". Teoses: *Advances in Cryptology – EUROCRYPT 2023*. Toim. Carmit Hazay ja Martijn Stam. Cham: Springer Nature Switzerland, 2023, lk-d 423–447. ISBN: 978-3-031-30589-4.
- [43] Reza Azarderakhsh *et al.* *SIKE specification*. 2022. URL: <https://sike.org/files/SIDH-spec.pdf>.
- [44] Wouter Castryck *et al.* "CSIDH: An Efficient Post-Quantum Commutative Group Action". Teoses: *Advances in Cryptology – ASIACRYPT 2018: 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2–6, 2018, Proceedings, Part III*. Brisbane, QLD, Australia: Springer-Verlag, 2018, lk-d 395–427. ISBN: 978-3-030-03331-6. DOI: [10.1007/978-3-030-03332-3_15](https://doi.org/10.1007/978-3-030-03332-3_15). URL: https://doi.org/10.1007/978-3-030-03332-3_15.
- [45] Ward Beullens, Thorsten Kleinjung ja Frederik Vercauteren. "CSI-FiSh: Efficient Isogeny Based Signatures Through Class Group Computations". Teoses: *Advances in Cryptology – ASIACRYPT 2019*. Toim. Steven D. Galbraith ja Shiho Moriai. Cham: Springer International Publishing, 2019, lk-d 227–247. ISBN: 978-3-030-34578-5.
- [46] Marius A. Aardal *et al.* *SQIsign specification*. 2025. URL: <https://sqisign.org/spec/sqisign-20250707.pdf>.
- [47] Manuel Barbosa *et al.* "X-Wing - The Hybrid KEM You've Been Looking For". *IACR Communications in Cryptology* 1.1 (9. apr 2024). ISSN: 3006-5496. DOI: [10.62056/a3qj89n4e](https://doi.org/10.62056/a3qj89n4e).
- [48] Nina Bindel *et al.* *Transitioning to a Quantum-Resistant Public Key Infrastructure*. Cryptology ePrint Archive, Paper 2017/460. <https://eprint.iacr.org/2017/460>. 2017. URL: <https://eprint.iacr.org/2017/460>.
- [49] *Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process*. Tehniline aruanne. National Institute of Standards ja Technology, 2016. URL: <https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf> (vaadatud 29.09.2025).
- [50] Seongkwang Kim *et al.* *The AIMer Signature Scheme. Submission to the KpqC Competition*. 2024. URL: https://kqpc.or.kr/images/pdf/AIMer_Document.pdf.
- [51] Jung Hee Cheon *et al.* *HAETAE: Shorter Lattice-Based Fiat-Shamir Signatures*. 2024. URL: <https://aimer-signature.org>.

- [52] Jonghyun Kim ja Jong Hwan Park. *NTRU+. Algorithm Specifications And Supporting Documentation*. 2024. URL: https://kpmc.or.kr/images/pdf/NTRU+_Document.pdf.
- [53] Jung Hee Cheon *et al.* *SMAUG-T: the Key Exchange Algorithm based on Module-LWE and Module-LWR*. 2024. URL: https://kpmc.or.kr/images/pdf/SMAUG-T_Document.pdf.
- [54] *ANSSI views on the Post-Quantum Cryptography transition (2023 follow up)*. Tehniline aruanne. French Cybersecurity Agency (ANSSI), 2023. URL: https://cyber.gouv.fr/sites/default/files/document/follow_up_position_paper_on_post_quantum_cryptography.pdf (vaadatud 29.09.2025).
- [55] *NSM Cryptographic Recommendations*. Tehniline aruanne. Norwegian National Security Authority (NSM), 2025. URL: <https://nsm.no/getfile.php/1314334-1742808614/NSM/Filer/Dokumenter/Veiledere/NSM%5C%20Cryptographic%5C%20Recommendations%5C%202025.pdf> (vaadatud 29.09.2025).
- [56] *Next steps in preparing for post-quantum cryptography*. Tehniline aruanne. National Cyber Security Center, 2024. URL: <https://www.ncsc.gov.uk/whitepaper/next-steps-preparing-for-post-quantum-cryptography> (vaadatud 29.09.2025).
- [57] *Recommendations for a safe post-quantum transition*. Tehniline aruanne. Centro Criptológico Nacional, 2022. URL: <https://www.ccn.cni.es/gl/docman/documentos-publicos/boletines-pytec/499-ccn-tec-009-recomendaciones-transicion-postcuantica-segura-english/file> (vaadatud 29.09.2025).
- [58] Eric Rescorla ja Tim Dierks. *The Transport Layer Security (TLS) Protocol Version 1.2*. RFC 5246. Aug 2008. DOI: [10.17487/RFC5246](https://doi.org/10.17487/RFC5246). URL: <https://www.rfc-editor.org/info/rfc5246>.
- [59] Eric Rescorla. *The Transport Layer Security (TLS) Protocol Version 1.3*. RFC 8446. Aug 2018. URL: <https://rfc-editor.org/rfc/rfc8446.txt>.
- [60] Douglas Stebila, Scott Fluhrer ja Shay Gueron. *Hybrid key exchange in TLS 1.3*. Internet-Draft draft-ietf-tls-hybrid-design-16. Work in Progress. Internet Engineering Task Force, sept 2025. 23 lk-d. URL: <https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/16/>.
- [61] Tirumaleswar Reddy.K *et al.* *Use of Composite ML-DSA in TLS 1.3*. Internet-Draft draft-reddy-tls-composite-mldsa-05. Work in Progress. Internet Engineering Task Force, juuli 2025. 11 lk-d. URL: <https://datatracker.ietf.org/doc/draft-reddy-tls-composite-mldsa/05/>.
- [62] Thom Wiggers *et al.* *KEM-based Authentication for TLS 1.3*. Internet-Draft draft-celi-wiggers-tls-authkem-06. Work in Progress. Internet Engineering Task Force, nov 2025. 26 lk-d. URL: <https://datatracker.ietf.org/doc/draft-celi-wiggers-tls-authkem/06/>.
- [63] Ahto Buldas *et al.* "Server-Supported RSA Signatures for Mobile Devices". Teoses: *Computer Security - ESORICS 2017 - 22nd European Symposium on Research in Computer Security, Oslo, Norway, September 11-15, 2017, Proceedings, Part I*. Toim. Simon N. Foley, Dieter Gollmann ja Einar Snekkenes. Kd 10492. Lecture Notes in Computer Science. Springer, 2017, lk-d 315–333. DOI: [10.1007/978-3-319-66402-6_19](https://doi.org/10.1007/978-3-319-66402-6_19). URL: https://doi.org/10.1007/978-3-319-66402-6_19.
- [64] *IVXV protokollide kirjeldus*. <https://www.valimised.ee/et/e-haaletamine/dokumendid>. Vabariigi Valimiskomisjon IVXV-PR-1.10.0 (in Estonian). 2025.

- [65] Kiarash Sedghighadikolaei ja Attila Altay Yavuz. "A Survey of Threshold Signatures: NIST Standards, Post-Quantum Cryptography, Exotic Techniques, and Real-World Applications". *ACM Comput. Surv.* 58.6 (dets 2025). ISSN: 0360-0300. DOI: [10.1145/3772274](https://doi-org.ezproxy.utlib.ut.ee/10.1145/3772274). URL: <https://doi-org.ezproxy.utlib.ut.ee/10.1145/3772274>.
- [66] Antonín Dufka *et al.* *Trilithium: Efficient and Universally Composable Distributed ML-DSA Signing*. Cryptology ePrint Archive, Paper 2025/675. 2025. URL: <https://eprint.iacr.org/2025/675>.
- [67] Alexander Bienstock *et al.* *Efficient, Scalable Threshold ML-DSA Signatures: An MPC Approach*. Cryptology ePrint Archive, Paper 2025/1163. 2025. URL: <https://eprint.iacr.org/2025/1163>.
- [68] Giacomo Borin *et al.* *Threshold Signatures Reloaded: ML-DSA and Enhanced Raccoon with Identifiable Aborts*. Cryptology ePrint Archive, Paper 2025/1166. 2025. URL: <https://eprint.iacr.org/2025/1166>.
- [69] Sofía Celi, Daniel Escudero ja Guilhem Niot. "Share the MAYO: Thresholdizing MAYO". Teoses: *Post-Quantum Cryptography - 16th International Workshop, PQCrypto 2025, Taipei, Taiwan, April 8-10, 2025, Proceedings, Part I*. Toim. Ruben Niederhagen ja Markku-Juhani O. Saarinen. Kd 15577. Lecture Notes in Computer Science. Springer, 2025, lk-d 165–198. DOI: [10.1007/978-3-031-86599-2_6](https://doi.org/10.1007/978-3-031-86599-2_6). URL: https://doi.org/10.1007/978-3-031-86599-2_6.
- [70] Standards for Efficient Cryptography Group. *Standards for Efficient Cryptography 1 (SEC 1): Elliptic Curve Cryptography*. version 2.0. 2009.
- [71] Canadian Centre for Cyber Security. *Roadmap for the migration to post-quantum cryptography for the Government of Canada (ITSM.40.001)*. Accessed: 2025-10-02. 2025. URL: <https://www.cyber.gc.ca/en/guidance/roadmap-migration-post-quantum-cryptography-government-canada-itsm40001>.
- [72] Amare Geremew ja Atif Mohammad. "Preparing Critical Infrastructure for Post-Quantum Cryptography: Strategies for Transitioning Ahead of Cryptanalytically Relevant Quantum Computing". *International Journal on Engineering, Science, and Technology* 6.4 (2024). Accessed: 2025-10-02, lk-d 338–365. DOI: [10.46328/ijonest.240](https://doi.org/10.46328/ijonest.240).
- [73] ETSI. *CYBER; Migration strategies and recommendations to Quantum Safe schemes*. Technical Report ETSI TR 103 619 V1.1.1. Reference: DTR/CYBER-QSC-0013. Accessed: 2025-10-02. European Telecommunications Standards Institute, juuli 2020.
- [74] Khondokar Fida Hasan *et al.* "A Framework for Migrating to Post-Quantum Cryptography: Security Dependency Analysis and Case Studies". *IEEE Access* 12 (2024). Accessed: 2025-10-02, lk-d 23427–23450. DOI: [10.1109/ACCESS.2024.3360412](https://doi.org/10.1109/ACCESS.2024.3360412).
- [75] National Cyber Security Centre. *Timelines for migration to post-quantum cryptography*. Accessed: 2025-10-02. Märts 2025. URL: <https://www.ncsc.gov.uk/guidance/pqc-migration-timelines>.
- [76] OWASP Foundation. *OWASP CycloneDX: Authoritative Guide to CBOM*. Technical Guide. Accessed: 2025-10-15. OWASP Foundation, 2024. URL: https://cyclonedx.org/guides/OWASP_CycloneDX-Authoritative-Guide-to-CBOM-en.pdf.

- [77] Thom Sijpesteijn, Maaike van Leuken ja Frederik Kerling. *Cryptographic Asset Discovery and Inventory: A market landscape and fit-gap analysis (in Dutch)*. Tehniline aruanne TNO 2025 P11921. Gefinancierd door CIO Rijk, Nationaal Cyber Security Centrum, en Ministerie van Economische Zaken. TLP:CLEAR. Accessed: 2025-10-15. TNO, märts 2025. URL: <https://www.ncsc.nl/documenten/publicaties/2025/september/25/tno-cryptographic-asset-discovery-and-inventory>.
- [78] HSBC, InfoSec Global ja Thales. *Cryptographic Inventory: Deriving Value Today, Preparing for Tomorrow*. White Paper. Accessed: 2025-10-15. HSBC, InfoSec Global (a Keyfactor Company), ja Thales, 2025. URL: <https://408597.fs1.hubspotusercontent-na1.net/hubfs/408597/2025-content/Cryptographic%5C%20Inventory%5C%20-%5C%20Deriving%5C%20Value%5C%20Today%5C%20-%5C%20Preparing%5C%20for%5C%20Tomorrow.pdf>.
- [79] National Institute of Standards, Technology ja National Cybersecurity Center of Excellence. *Migration to Post-Quantum Cryptography: Quantum Readiness*. NIST Special Publication 1800-38B, Preliminary Draft. Accessed: 2025-10-02. National Institute of Standards ja Technology, 2023. URL: <https://www.nccoe.nist.gov/sites/default/files/2023-12/pqc-migration-nist-sp-1800-38b-preliminary-draft.pdf>.
- [80] F. Muller ja M. P. P. van Heesch. *Migration to Quantum-Safe Cryptography: About Making Decisions on When, What and How to Migrate to a Quantum-Safe Situation*. Position Paper. Accessed: 2025-10-17. TNO, 2020. URL: <https://publications.tno.nl/publication/34637213/SDdGJI/TNO-2020-migration.pdf>.
- [81] Australian Signals Directorate. *Planning for Post-Quantum Cryptography*. Last updated: August 2023. Accessed: 2025-10-02. 2023. URL: <https://www.cyber.gov.au/business-government/secure-design/planning-for-post-quantum-cryptography>.
- [82] CISA, NSA ja NIST. *Quantum-Readiness: Migration to Post-Quantum Cryptography*. Cybersecurity Information Sheet. Accessed: 2025-10-02. Cybersecurity ja Infrastructure Security Agency, aug 2023. URL: https://www.cisa.gov/sites/default/files/2023-08/Quantum%5C%20Readiness%5C_Final%5C_CLEAR%5C_508c%5C%20%5C%283%5C%29.pdf.
- [83] Nasjonal sikkerhetsmyndighet. *NSM Cryptographic Recommendations 2025*. Guidance document U-25-41. Accessed: 2025-10-02. Nasjonal sikkerhetsmyndighet, 2025. URL: <https://nsm.no/getfile.php/1314334-1742808614/NSM/Filer/Dokumenter/Veiledere/NSM%5C%20Cryptographic%5C%20Recommendations%5C%202025.pdf>.
- [84] State Secretariat for International Finance. *Action Plan to a Quantum-Safe Financial Future*. Tehniline aruanne. Accessed: 2025-10-02. Switzerland: State Secretariat for International Finance (SIF), märts 2025. URL: <https://www.sif.admin.ch/dam/de/sd-web/5jN0vjz3EBDi/Action%5C%20Plan%5C%20to%5C%20a%5C%20Quantum-Safe%5C%20Financial%5C%20Future.pdf>.
- [85] National Cyber Security Centre. *Post-Quantum Cryptography: What comes next?* Accessed: 2025-10-02. Märts 2025. URL: <https://www.ncsc.gov.uk/blog-post/post-quantum-cryptography-what-comes-next>.
- [86] William Barker ja Murugiah Souppaya. *Migration to Post-Quantum Cryptography*. Draft Technical Report. Draft, Dakota Consulting and NIST. Accessed: 2025-10-17. National Cybersecurity Center of Excellence, National Institute of Standards ja Technology, juuni 2021.
- [87] EU Cybersecurity Agencies Joint Statement. *Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography*. Joint Statement from Partners from 18 EU Member States.¹ Accessed: 2025-10-17. Nov 2024.

¹Partners include: Secure Information Technology Center Austria, Centre for Cybersecurity Belgium, National Cyber

- [88] Dan Bogdanov *et al.* *Krüptograafiliste turbelahenduste hindamisvõime loomise projekt - I etapp*. Eelanalüüsi aruanne D-31-1. Cybernetica AS, sept 2024.
- [89] Michele Mosca ja John Mulholland. *An Updated Methodology for Quantum Risk Assessment*. Tehniline aruanne. EvolutionQ, 2025. URL: <https://globalriskinstitute.org/publication/an-updated-methodology-for-quantum-risk-assessment/>.
- [90] *Guide for conducting risk assessments*. 2012. DOI: [10.6028/nist.sp.800-30r1](https://doi.org/10.6028/nist.sp.800-30r1). URL: <http://dx.doi.org/10.6028/NIST.SP.800-30r1>.

and Information Security Agency Czech Republic, Centre for Cyber Security Denmark, Information System Authority Estonia, Finnish Transport and Communication Agency, ANSSI France, BSI Germany, National Cyber Security Authority Hellenic Republic, NCSC Ireland, National Cybersecurity Agency Italy, Ministry of Defense Latvia, NCSC Lithuania, Luxembourg, NLNCSA Netherlands, NCSC Netherlands, Research and Academic Research Center Poland, Government Information Security Office Slovenia, National Cryptologic Center Spain.

Lisa A Ülevaade

postkvant-krüptograafia hetkeseisust

Kvantarvutus on kiiresti arenev arvutiteaduse haru. Kvantarvutite potentsiaalsete rakendustena nähakse eelkõige modelleerimisülesandeid ravimitööstuses, materjaliteaduses ning finantsvaldkonnas, kuid kvantarvutuse areng ohustab ka praegu kasutuses olevaid krüptograafilisi algoritme. Igapäevastes toimingutes digimaailmas kasutame kahte tüüpi algoritme – sümmeetrilisi (kiireks andmevahetuseks) ning avaliku võtmega algoritme (et kehtestada poolte vahel võtmeid sümmeetriliste algoritmide jaoks või digisignatuuride väljastamiseks). Avaliku võtmega krüptograafia turvalisus põhineb mitmesugustel rasketel arvutusülesannetel. Nendest olulisemad on diskreetse logaritmi ülesanne ja täisarvude tegurdamise keerukus. Aastal 1994 pakkus Peter Shor välja kvantalgoritmi, mis suudab efektiivselt lahendada mõlemaid ülesandeid ja seetõttu murda enamiku kasutuses olevatest avaliku võtmega krüptoskeemidest. Seetõttu on selle sajandi alguskümnel hakatud tähelepanu pöörama alternatiivsetele, kvantturvalistele avaliku võtmega süsteemidele. Selle uurimis- ja arendustöö tulemuseks peaksid saama standardiseeritud krüptoalgoritmid, mis on kaitstud nii klassikaliste kui ka kvantrünnete eest ning mis peaksid täielikult asendama praegu kasutuses olevad süsteemid. USA Riiklik Standardi- ja Tehnikainstituut (NIST) on juba mõned algoritmid standardiseerinud ning valinud välja järgmised algoritmid, mida asutakse standardiseerima.

Selle peatüki eesmärk on anda ülevaade postkvant-krüptograafia hetkeseisust ning teha sobivate krüptoalgoritmide vahel valimine hõlpsamaks ning läbimõeldumaks.

A.1 Kvantarvutus

Superpositisioon. Tavalises arvutis saab bitt olla kahes olekus, kas 0 või 1. Kvantbitt saab olla kahe baasoleku – 0 ja 1 – superpositisioonis ehk kujul $|\Psi\rangle = c_1|0\rangle + c_2|1\rangle$, kus $|0\rangle$ ja $|1\rangle$ tähistavad kahte baasolekut ning c_1 ja c_2 on kompleksarvud, mille moodulite ruutude summa on 1 ehk $|c_1|^2 + |c_2|^2 = 1$. Kõiki võimalikke olekuid võib seetõttu ette kujutada ühikera (kera, mille raadius on 1) pinnana, mille põhjapoolus on 0 ning lõunapoolus on 1. Esitust $|\Psi\rangle$ kutsume kvantbiti *kvantolekuks*.

Kui superpositisioonis kvantbitti vaadelda (üldjuhul kasutatakse mõistet *mõõtma*), siis superpositisioon laguneb ning kvantbitt läheb seisundisse 0 (tõenäosusega $|c_1|^2$) või seisundisse 1 (tõenäosusega $|c_2|^2$).

A.1.1 Kvantalgoritmid

Kvantalgoritmid on juhised, mida kvantarvuti kasutab kvantbittide manipuleerimiseks. Üldjuhul hõlmavad need algoritmid kvantbittide superpositiooni viimist, tehete tegemist ning lõpuks mingite kvantbittide mõõtmist.

Shori algoritm. Klassikaline näide kvantalgoritmist on Shori algoritm, mille avaldas 1994. aastal Peter Shor [29]. Shori algoritm lahendab funktsiooni perioodi leidmise ülesande ning selle abil lahendab see ka täisarvude tegurdamise ja diskreetse logaritmi ülesande. See tähendab, et Shori algoritmi abil on võimalik murda kõik nendel ülesannetel põhinevad krüptosüsteemid – ühel või teisel moel puudutab see enamikku tänapäevaseid krüptosüsteeme.

Groveri algoritm. Krüptograafilisi algoritme mõjutab ka Groveri algoritm [30], mis leiab suure tõenäosusega n -liikmelisest järjendist \sqrt{n} sammu jooksul soovitud omadustega elemendi. Klassikaline algoritm, mis seda ülesannet lahendab, jõuab lahenduseni keskmiselt $n/2$ sammu jooksul. Kui järjendis on vähemalt n/k elementi, mis on soovitud omadustega, siis leiab Groveri algoritm suure tõenäosusega neist ühe üles umbes $\sqrt{n/k}$ sammuga (klassikaline algoritm vajab keskmiselt n/k sammu).

Kuna Groveri algoritm lahendab üsna üldist ülesannet, siis saab teda rakendada paljudes olukordades. Näiteks saab Groveri algoritmi kasutada sümmeetriliste primitiivide võtmeruumi läbiotsimiseks. Kui üldjuhul kasutatakse selleks otstarbeks 128-bitiseid võtmeid ja võtmeruum on suurusega 2^{128} , siis Groveri algoritm leiab sealt õige võtme üles 2^{64} sammuga. Samuti saab seda kasutada n -bitise väljundiga räsifunktsioonide kollisioonide leidmiseks umbes $\sqrt[3]{n}$ sammuga [31], mis tähendab, et 128-bitise kollisioonikindluse saavutamiseks peaks räsifunktsiooni väljund olema vähemalt 384 bitti.

A.1.2 Kvantarvutuse arengusuunad

Esimese krüptograafiliselt märkimisväärse kvantarvuti (ingl *cryptographically significant quantum computer*, CSQC) valmimist ja arengut mõjutavad mitmesugused tegurid. Lisaks sellele, et on keeruline omavahel põimida suurt hulka kvantbitte ning neid hallata, on takistuseks veel järgnevad probleemid:

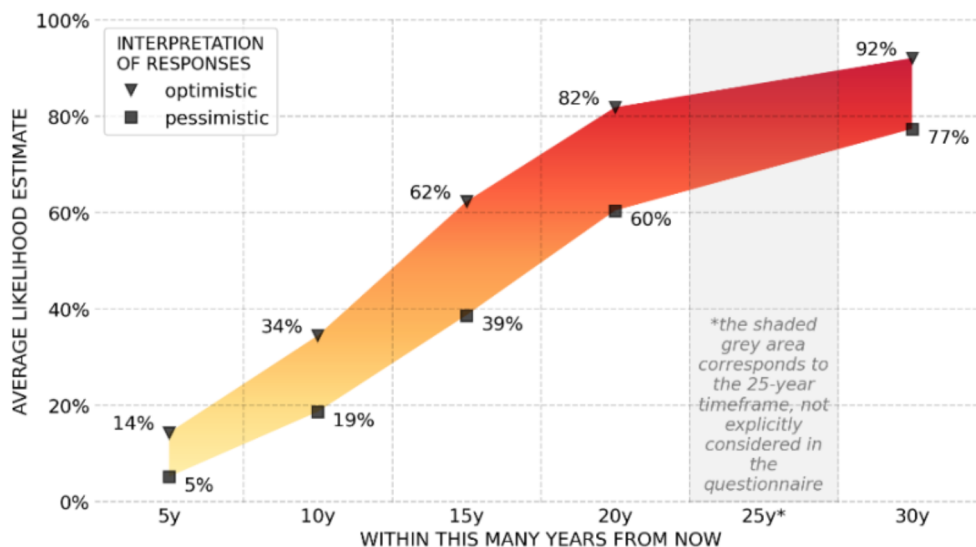
- veaparandus – füüsilised kvantbitid on väga tundlikud müra suhtes ning tekkivate vigade parandamine on seetõttu üks olulisemaid lahendamist nõudvaid ülesandeid. Kvantsüsteemides on veaparandus keeruline ülesanne kloonimise keelamise teoreemi ning suurema võimalike vigade arvu tõttu;
- kvantalgoritmide optimeerimine – see tähendab vajaminevate kvantbittide arvu vähendamist või spetsiifiliste loogikaelementide kasutamist;
- kvantbittide tüübi valimine – füüsilisi kvantbitte on võimalik realiseerida mitmetel viisidel (näiteks ioonlõksud, footonid või ülijuhtivad kvantbitid). Igaühega neist kaasnevad erinevad nõuded kiibi koostamisel kasutatavale arhitektuurile.

Kuivõrd kvantarvuti arengut mõjutavad edusammud kõigis ülaltoodud valdkondades, siis on muutujate rohkuse tõttu keeruline hinnata, millal võib kvantvastane muutuda tõsiseltvõetavaks ohuks. Joonisel 12 on kujutatud kokkuvõtvalt erinevate kvantarvutusega tegelevate ekspertide hinnangud sellele, millal võiks esimene krüptograafiliselt märkimisväärne kvantarvuti valmida (Mosca jt. raportist [32]). Ekspertid arvavad, et RSA-2048 on tõenäoliselt murtav juba 20–30 aasta pärast.

A.1.2.1 Kvantarvuti mõju krüptoskeemidele

Tabel 2 koondab andmeid enim kasutatavate krüptoskeemide kvantkindluse kohta. Nagu märgitud, on kvantohule kõige avatumad avaliku võtmega süsteemid. Sümmeetriliste primitiivide nagu sümmeetrilise krüpteerimise ja räsifunktsioonide funktsionaalse turvalisuse tagamiseks piisab vastavalt võtme pikkuse ning väljundi pikkuse suurendamisest.

2024 OPINION-BASED ESTIMATES OF THE LIKELIHOOD OF A DIGITAL QUANTUM COMPUTER ABLE TO BREAK RSA-2048 IN 24 HOURS, AS FUNCTION OF TIME
Range between average of an optimistic (top value) or pessimistic (bottom value) interpretation of the likelihood intervals indicated by the respondents



Joonis 12. Hinnangud esimese krüptograafiliselt märkimisväärse kvantarvuti valmimisajale [32]

Tabel 2. Krüptoprimitiivid Eesti digitaristus ja nende postkvant-turvalisus

Krüptoskeem	Otstarve	Postkvant-turvalisus	Kasutusnäited
RSA	krüpteerimine, signatuurid	murtud	Smart-ID, ID-kaart, X-tee
ElGamal	krüpteerimine	murtud	e-hääletamine
ECDSA	signatuurid	murtud	ID-kaart, Mobiil-ID
ECDH	võtmekehtestus	murtud	TLS, ID-kaart (CDOC)
ChaCha20	krüpteerimine	peab suurendama võtme pikkust	TLS, ID-kaart (CDOC)
AES	krüpteerimine	peab suurendama võtme pikkust	TLS
SHA2, SHA3	räsifunktsioon	peab suurendama väljundi pikkust	kõik ülaltoodud tehnoloogiad

A.2 Postkvant-krüptograafia

A.2.1 Kaasaegne krüptograafia

Laias laastus saab krüpteerimisalgoritmide jaotada sümmeetrilisteks ning avaliku võtmega skeemideks. Sümmeetriliste algoritmide puhul peavad mõlemad pooled kasutama üht ja sama salajast võtit. Sümmeetrilised skeemid on arvutuslikult efektiivsed, mistõttu on neid hea kasutada krüpteeritud andmevahetuseks ning andmete hoiustamiseks. Aga nagu öeldud, peavad mõlemad pooled kasutama üht ja sama salajast võtit. Selle jaoks kasutatakse võtmekehtestus- või võtme-

vahetusmehhanisme, mis rakendavad avaliku võtmega krüptograafiat.

Avaliku võtmega krüptograafias genereerib üks pool kaks võtit – salajase ja avaliku võtme. Avaliku võtit jagab genereerija teiste pooltega ning salajase võtme jätab ta ainult enda teada. Avaliku võtmega krüptoskeemide hulka kuuluvad võtmekehtestusprotokollid, avaliku võtmega krüpteerimisalgoritmid ja signatuuriskeemid.

Kui avaliku võtmega skeemide puhul on tarvis võtta kasutusele uued meetodid, siis sümmeetrilisi skeeme mõjutab kvantarvuti tulek vähesemal määral. Nende puhul tuleb Groveri algoritmi [30] tõttu suurendada vaid võtmepikkuseid ning räsifunktsioonide väljundite pikkust. Praeguse seisuga pole leitud teisi meetodeid, mille abil saaks kvantarvuti sümmeetriliste skeemide turvalisust oluliselt mõjutada.

Avaliku võtmega krüpteerimisalgoritmid. Avaliku võtmega krüptosüsteem koosneb järgmistest algoritmidest:

- võtmete genereerimine – algoritm, mille sisendväärtused on vastavad turvaparameetrid ning väljundväärtuseks võtmepaar, mis koosneb avalikust võtmest ja salajasest võtmest;
- krüpteerimine – algoritm, mille sisendväärtused on krüpteeritav teade ja avalik võti ning väljundväärtuseks krüptogramm;
- dekrüpteerimine – algoritm, mille sisendväärtused on krüptogramm ja salajane võti ning väljundväärtuseks algne teade.

Avaliku võtmega krüptosüsteemide hulka kuuluvad näiteks RSA, ElGamal ja Paillier. Kvantarvuti ohustab nende kõigi turvalisust.

Võtmekehtestus. Võtmekehtestusprotokolli abil saavad kaks poolt leppida kokku ühises salajas võtmes, kasutades selleks kanalit, mis ei taga üle selle edastatavate sõnumite konfidentsiaalsust ja terviklust. Ühist võtit saab edaspidi kasutada sümmeetriliseks krüpteerimiseks või andmete autentimiseks. Põhiliselt kasutatakse selleks kahte tüüpi meetodeid – võtmekapseldusmehhanisme ja interaktsioonita võtmevahetust.

Võtmekapseldusmehhanism koosneb järgnevatest algoritmidest:

- võtmete genereerimine – algoritm, mille sisendväärtused on vastavad turvaparameetrid ning väljundväärtusteks salajane lahtikapseldusvõti ja sellele vastav avalik kapseldusvõti;
- kapseldus – algoritm, mille sisendväärtus on kapseldusvõti ning väljundväärtuseks ühine võti k ja sellele vastav krüptogramm (kapsel). Võtme jätab kapseldaja endale ning krüptogrammi saadab ta teisele poolele;
- lahtikapseldus – algoritm, mille sisendväärtused on ühist salajast võtit sisaldav krüptogramm ja lahtikapseldusvõti ning väljundväärtuseks krüptogrammis sisaldav ühine võti.

Üks pooltest genereerib võtmed, jätab lahtikapseldusvõtme endale ja saadab kapseldusvõtme teisele poolele. Teine pool kasutab kapseldusalgoritmi talle saadetud kapseldusvõtmega ja saab selle väljundist ühise võtme ning sellele vastava krüptogrammi. Seejärel saadab ta krüptogrammi võtmed genereerinud poolele, kes kapseldab selle lahtikapseldusvõtme abil lahti.

Interaktsioonita võtmevahetusmehhanism koosneb järgnevatest algoritmidest:

- võtmete genereerimine – algoritm, mille sisendväärtused on vastavad turvaparameetrid ning väljundväärtusteks salajane võti ning sellele vastav avalik võti;
- võtmevahetus – algoritm, mille sisendväärtused on ühe poole salajane võti ja teise poole

avalik võti ning väljundväärtuseks ühine salajane võti.

Interaktsioonita võtmevahetus võimaldab kahel poolel, kes teavad teineteise avalikke võtmeid, kokku leppida ühises salajases võtmes teineteisega suhtlemata. Kui võtmekapseldusmehhanismi puhul genereerib ühise võtme ainult üks pool, siis interaktsioonita võtmevahetusmehhanismi kasutades osalevad mõlemad pooled ühise võtme genereerimises. Interaktsioonita võtmevahetusmehhanismid on näiteks Diffie-Hellmani (DH) võtmevahetus ja selle elliptiköveraid kasutav analoog (ECDH).

Digitaalsignatuurid. Signatuuriskeem koosneb järgnevatest algoritmidest:

- võtmete genereerimine – algoritm, mille sisendväärtused on vastavad turvaparameetrid ning väljundväärtusteks salajane võti ning sellele vastav avalik võti;
- signeerimine – algoritm, mille sisendväärtused on sõnum ja salajane võti ning väljundväärtuseks digitaalsignatuur;
- verifitseerimine – algoritm, mille sisendväärtused on avalik võti, sõnum ja sellele vastav digitaalsignatuur ning väljundväärtuseks tõeväärtus, mis tähistab signatuuri korrektsust.

Tänapäeval kasutatakse näiteks RSA, ECDSA, EdDSA ja Schnorri signatuuriskeeme. Mitte ükski neist ei ole vastupidav kvantrünnete.

A.2.2 Postkvant-krüptograafia

Postkvant-krüptograafia uurimisobjekt on krüptoskeemid, mis võiksid olla vastupidavad nii klassikalistele kui ka kvantrünnete. Need skeemid põhinevad mitmesugustel arvutusülesannetel, mida ei suuda lahendada ei tavaline ega ka kvantarvuti. Enim tähelepanu on saanud järgmised algoritmide pered:

- võrepõhised
- veaparanduskoodidepõhised
- räsifunktsioonide põhised
- mitme muutuja polünoomide põhised
- isogeensete teisenduste põhised

Esimesest kolmest perest on juba mõned algoritmid standardiseeritud ja järgmisel NISTi välja kuulutatud signatuuriskeemide konkursil on algoritme ka ülejäänud peredest.

Võrepõhine krüptograafia. Võre koosneb n -mõõtmelises ruumis mingi mustri alusel paiknevatest punktidest (või vektoritest). Neid punkte saab omavahel liita ja lahutada nagu tavalises vektorruumis ning tehete tulemuseks on uuesti mõni võres asuv punkt. Analoogiliselt vektorruumidega leidub ka võrel mitmeid baase ning iga võrepunkti saab väljendada baasivektorite lineaarkombinatsioonina. Ilmneb aga, et mõnede võre baasidega on kergem arvutada kui teistega. Kui võre on esitatud n -õ halva baasi abil, siis on raske:

- leida võres asuvat lühimat vektorit (lühima vektori ülesanne);
- leida n -mõõtmelises ruumis valitud punktile lähimal asuv võrepunkt eeldusel, et valitud punkt pole juba ise võrepunkt (lähima vektori ülesanne).

Nende ülesannete keerukusel tugineb valdav osa võrepõhisest krüptograafiast.

Kui me ütleme, et punktide koordinaadid kuuluvad hulka \mathbb{Z}_q , mis on kõigi jääkide hulk, mis teivad täisarvude jagamisel algarvuga q , siis saame tulemuseks aritmeetilised versioonid algsest võreülesannetest (lühima ja lähima vektori ülesanded on olemuselt geomeetrilised), nimelt vigadega õppimise ülesande (LWE – *learning with errors*) ja lühikese täisarvlahendi ülesande (SIS – *short integer solution*). Vigadega õppimise ülesande puhul peame lahendama lineaarvõrrandisüsteemi kordajatega hulgast \mathbb{Z}_q , mille vabaliikmete veerule on juurde liidetud lühike veavektor (lühike tähendab seda, et vektori norm ehk pikkus on väike), mille täpseid koordinaate lahendaja ei tea, mistõttu ei anna kasutada Gaussi elimineerimismeetodit. Lühikese täisarvlahendi ülesande puhul on vaja leida lühike lahend homogeenisele lineaarvõrrandisüsteemile. Mõnedel juhtudel on see ülesanne kerge (näiteks, kui võrrandisüsteemi muutujate arv on võrdne võrrandite arvuga), kuid kui muutujaid on palju rohkem kui võrrandeid, on süsteem alamääratud ning Gaussi elimineerimismeetodist abi pole, sest see ei garanteeri alati lühikest lahendit. Võttes aluseks need kaks ülesannet, on võimalik luua efektiivseid krüptograafilisi primitiive, kuid nende ülesanded on võimalik taandada mõningatele variantidele lühima ja lähima vektori ülesannetest.

Vigadega õppimise ning lühikese täisarvlahendi ülesanded moodustavad võrepõhise krüptograafia praktilise vundamendi, kuid üldjuhul kasutatakse krüptoskeemide väljatöötamisel nende ülesannete mõningaid erijuhte. Võresid saab defineerida mitmete algebraliste struktuuride abil ning need allolevad struktuurid määravad selle, millise erijuhuga on tegu. Näiteks FrodoKEM [33] on üles ehitatud tavalisele vigadega õppimise ülesandele tugineb seetõttu üsna üldistel turvaeel-dustel [34]. Falconi [35] signatuuriskeem (tulevane FN-DSA-nimeline NISTi standard) põhineb lühikese täisarvlahendi versioonil, mis on defineeritud läbi kindlat tüüpi NTRU-võrede. NISTi standardiseeritud ML-KEM [18] (Module-Lattice-Based Key Encapsulation Mechanism) ja ML-DSA [22] (Module-Lattice-Based Digital Signature Algorithm) algoritmid on defineeritud moodulvõrede kaudu, mis koosnevad vektoritest, mille elemendid on mingit tüüpi polünoomid. Kuna ML-KEMi ülesehituses on kasutatud struktureeritumaid võresid kui FrodoKEMi puhul, on ML-KEMi võtmed ning krüptotekstid väiksemad kui FrodoKEMil. Täpse alusülesande valimine on krüptosüsteemi kavandaja otsus, kuid enamikku neist ülesannetest on mõningase lõtkuga võimalik teineteisele taandada. See tähendab, et kui kasvõi üks neist ülesannetest lahendatakse, võib kogu võrepõhine krüptograafia nõrgaks osutada.

Veaparanduskoodidel põhinev krüptograafia. Veaparanduskoodi kasutatakse sõnumi saatmiseks üle mürrarikka kanali. Saadetav sõnum kodeeritakse nii, et isegi kui osa informatsioonist müra tõttu moondub, on võimalik algne sõnum taastada. Selleks on tarvis defineerida kodeerimisalgoritm ning sellele vastav dekodeerimisalgoritm, kus kodeerimisel lisatakse sõnumile mingil kindlal viisil informatsiooni ning dekodeerimisel eemaldatakse sõnumist see lisainfo koos potentsiaalsete edastusel tekkinud vigadega. Dekodeerimisel saab parandada või tuvastada ainult mingil kindlal hulgal vigu ning parandatavate vigade hulk on otseses sõltuvuses kodeerimisel lisatud informatsiooni hulgast.

Veaparanduskoodide kasutus krüptograafias põhineb juhuslikult genereeritud koodide dekodeerimise raskusel. See tähendab, et kui üks pool näeb koodsõna, millele on lisatud eelnevalt kokku lepitud arv vigu, on tal ilma dekodeerimisalgoritmi teadmata väga raske algset sõnumit taastada. Seda ülesannet kasutades on võimalik võrdlemisi loomulikult viisil konstrueerida krüpteerimisskeeme. Selleks peab üks pool genereerima algset koodi, mille sisemine struktuur võimaldab ainult seda struktuuri teades sõnumeid dekodeerida. See tähendab, et kodeerimisalgoritm ei tohi olla võimalik tuletada dekodeerimisalgoritmi ning avalikuks võtmeks on kodeerimisalgoritm ja salajaseks võtmeks dekodeerimisalgoritm. Sõnumi krüpteerimiseks kodeerib saatja oma sõnumi ning lisab sellele eelnevalt kokkulepitud määralt vigu. Vigadega koodsõna

saadab ta üle avaliku kanali ning dekodeerimisalgoritmi abil saab salajase võtme omanik sõnumi dekrüpteerida.

Erinevate koodipõhiste algoritmide kavandamisel on kasutatud erinevaid lähenemisi, millest olulisim erinevus on baaskoodide pere valik. Koodipere valikust sõltub vastava krüptosüsteemi turvalisus, sest koodipere fikseerimine täpsustab kasutatavaid turvaeeldusi, kuid võimaldab samaaegselt efektiivsete süsteemide projekteerimist. Näiteks Classic McEliece [36] kasutab binaarseid Goppa koode ning peagi NISTi poolt standardiseerimisele minev HQC [37] kasutab Reed-Solomoni ja Reed-Mulleri koode. McEliece'i algoritmi on uuritud juba aastakümneid, mistõttu peetakse seda võrdlemisi konservatiivseks valikuks. HQC-d saab kasutada ML-KEMi asemel, kui soovitakse, et krüptoskeem põhineks võrede asemel veaparanduskoodidel.

Räsifunktsioonidel põhinev krüptograafia. Krüptograafilisi räsifunktsioone kasutatakse selleks, et panna suvalise pikkusega sisendväärtusele vastama juhuslikuna näiv kindla pikkusega väljundväärtus. Väljundväärtused peaksid olema ühtlaselt jaotunud ning täidetud peaksid olema järgnevad turvaeeldused:

- iga väljundväärtuse korral peaks olema raske leida sisendväärtust, mis genereerib selle väljundväärtuse (ühesuunalisus, pööramatus)
- iga sisendväärtuse-väljundväärtuse paari korral peab olema raske leida teist sisendväärtust, mis genereeriks sama väljundväärtuse (lisaoriginaalilikindlus);
- raske on leida kahte sisendväärtust, mille väljundväärtused oleksid võrdsed (kollisioonikindlus)

Kuigi räsifunktsioonid käituvad näiliselt juhuslikult, peavad nad tegelikult olema deterministlikud ning andma sama sisendväärtuse puhul iga kord sama väljundväärtuse. Välja on küll töötatud mitmeid räsifunktsioone, kuid paljud neist on juba murtud, mis tähendab, et funktsioon ei vasta mõnele ülaltoodud eeldusele.

Räsifunktsioonide abil on võimalik ehitada ühekordseid signatuuriskeeme. Ühekordse signatuuriskeemi korral tohib võtmepaari kasutada vaid ühe korra ühe signatuuri andmiseks. Ühekordsete signatuuriskeemide abil on võimalik konstrueerida mõnekordseid signatuuriskeeme. Lisaks sellele on võimalik sama seemne abil genereerida mitu erinevat ühekordset võtmepaari, mis võimaldab ühe salajase võtme (seemne) abil anda mitu signatuuri. Räsifunktsioonidel põhinevad signatuuriskeemid võib jaotada kahte klassi – olekuta ja olekuga skeemid. Olekuga skeemide puhul peab signeerija lisaks salajasele võtmele hoidma meeles ka skeemi olekut. Olek sisaldab endas infot selle kohta, milliseid ühekordseid võtmeid on juba signeerimiseks kasutatud. Seetõttu saab skeemi abil anda iga võtmepaari kohta ka piiratud arvu signatuure. Olekuga skeeme soovitatakse kasutada ainult olukordades, kus on võimalik tagada turvaline ning veakindel olekuhaldus. Olekuga skeemide hulka kuuluvad näiteks laiendatud Merkle'i signatuuriskeem (XMSS) [38] ning Leighton-Micali signatuuriskeem (LMS) [39].

Olekuta räsifunktsioonidel põhineva signatuuriskeemi puhul võetakse olekuhalduse vajadusest vabanemiseks kasutusele paar lisaomadust. Selleks kasutatakse näiteks mõnekordseid signatuuriskeeme. Olekuta signatuuriskeemide hulka kuulub näiteks SLH-DSA (Stateless Hash-based Digital Signature Algorithm) [23], mis tugineb XMSSi versioonil, kus räsipuud kasutatakse koos Winternitzi ühekordsete signatuuridega.

Nii olekuga kui olekuta süsteemide turvalisus tuleneb süsteemi aluseks oleva räsifunktsiooni turvalisusest. Kui osutub, et valitud räsifunktsioon pole turvaline, võib selle lihtsalt mõne teise vastu välja vahetada.

Mitme muutuja polünoomidel põhinev krüptograafia. Mitme muutuja ruutpolünoome sisaldava võrrandisüsteemi lahendamine üle lõplike korpuste on NP-raske ülesanne. Selle ülesande raskust kasutades saab konstrueerida erinevaid krüptosüsteeme, kuid enim on selle eelduse abil loodud signatuuriskeeme. Sarnaselt veaparanduskoodidel põhinevale krüptograafiale on süsteemi avalik võti mingi raskesti lahendatav võrrandisüsteem ning salajane võti sisaldab lisainformatsiooni selle kohta, kuidas avalik võti konstrueeriti. Seda infot kasutades on salajase võtme omanikul võimalik anda verifitseeritavaid signatuure.

Enim kasutatud meetod signatuuriskeemide koostamiseks on „õli ja äädika“ meetod (*Oil and Vinegar*), kus mõned muutujatest (on eraldi „õli“ ja „äädika“ muutujad) väärtustatakse signeerimise hetkel ning alles jääb lineaarvõrrandisüsteem, mida on seejärel võimalik lahendada ülejäänud muutujate väärtuste teada saamiseks. Võrrandisüsteemi lahendit kasutataksegi digisignatuurina ning verifitseerimiseks peab lihtsalt tegema kindlaks, et saadud lahend rahuldab avalikus võtmes sisalduvat võrrandisüsteemi.

NISTI standardiseerimise kolmandas voorus murti [40] mitme muutuja polünoomidel tuginev Rainbow [41] süsteem, mis vähendas oluliselt pere kõikide algoritmide standardiseerimislootuseid, kuid selle aluseks olevat rasket ülesannet skeemi murdmise käigus ei lahendatud, mistõttu polünoomidel põhinevate krüptoskeemide uurimine jätkub.

Isogeensetel teisendustel põhinev krüptograafia. Isogeensed teisendused on funktsioonid, mille abil saab liikuda erinevate elliptikõverate vahel. Praktikas saab nende abil muuta ühe elliptikõvera teiseks elliptikõveraks. Kui on antud kaks elliptikõverat, mille vahel leidub isogeenne teisendus, siis on raske leida seda teisendust ilmutatud kujul. Selle ülesande raskusele toetudes on võimalik konstrueerida Diffie-Hellmani võtmevahetusega sarnaseid skeeme. Jällegi, aastal 2022 murti [42] üks sellesse peresse kuuluv NISTI kandidaat, SIKE [43] (Supersingular Isogeny Key Exchange), mis kahandas isogeensetel teisendustel põhinevate skeemide standardiseerimise tõenäosust, kuid mitmed skeemid (CSIDH [44], CSI-FiSh [45], SQISign [46]) on veel murdmata ning mõni neist võib saada tulevikus standardiseeritud.

A.2.3 Hübriidskeemid

Selles peatükis käsitleme erinevaid viise, kuidas klassikalist ning postkvant-krüptograafiat ühendades ehitada signatuuriskeeme ja võtmekehtestusprotokolle. Mitmed asutused soovivad postkvant-krüptograafiale üleminekuks kasutada just selliseid hübriidmeetodeid. Hübriidskeemide mõte on kaitsta kasutajat üleminekuperioodil kvantvastase eest, tagades samas, et baasprotokollide väljavahetamine ei ohustaks süsteemide turvalisust.

Hübriidne võtmekehtestus. Hübriidseid võtmekehtestusmehhanisme saab konstrueerida klassikaliste ning kvantturvaliste võtmekehtestusmehhanismide ühendamise teel. Üldiselt tehakse seda nii:

- pooled kasutavad klassikalist võtmekehtestusprotokolli (nt. ECDH), et saada ühine salajane võti s_1 ;
- pooled kasutavad kvantturvalist võtmekehtestusprotokolli (nt. ML-KEM), et saada ühine salajane võti s_2 ;
- mõlemad pooled kasutavad eraldiseisvalt võtmeühendusfunktsiooni, et saada ühine salajane võti $k \leftarrow \text{Ühenda}(s_1, s_2, \text{aux})$, kus aux tähistab funktsioonispetsiifilist lisaparametrit.

Kaks põhilist turvaeeldust, millele võtmekehtestusprotokollid võivad vastata, on krüptogrammi-

de eristamatus valitud avatekstiga ründe korral (ingl *indistinguishability under chosen-plaintext attack*, IND-CPA) ja krüptogrammide eristamatus valitud krüptogrammiga ründe korral (ingl *indistinguishability under chosen-ciphertext attack*, IND-CCA). Hübridvõtmekehtestusmehhanismide turvalisus oleneb võtmeühendusfunktsiooni ülesehitusest. Lihtlabane võtmeühendusfunktsioon, mille sisendväärtuseks on ainult mõlematest protokollidest saadud ühised võtmed ($k \leftarrow \text{Ühenda}(s_1, s_2)$) ei ole turvaline [47]. Näite IND-CCA-turvalisust pakkuvast võtmeühendusfunktsioonist võib leida allikast [20]. NISTI nõuande järgi peaks, kui see on võimalik, alati kasutama IND-CCA-turvalist võtmekehtestusmehhanismi. Sealjuures märgib NIST siiski, et mõningate rakenduste puhul, nagu ühekordselt kasutatavate võtmete genereerimine, piisab ka IND-CPA-turvalisusest.

Hübriidsed digisignatuurid. Nagu võtmekehtestusmehhanismide puhul, on ka hübriidsete signatuuriskeemide eesmärk ühendada omavahel klassikaline ning kvantturvaline signatuuriskeem. Soovitatav turvaeeldus on signatuuri võltsimatus ründaja valitud sõnumi korral (EUF-CMA). Selle eelduse defineerimisel antakse ründajale algselt ligipääs oraaklile, mis väljastab signatuure vabalt valitud sõnumitele, ning pärast algset suhtlust oraakliga peab ründaja suutma iseseisvalt väljastada korrektse signatuuri tema enda valitud, kuid eelnevalt signeerimata sõnumile. Hübriidskeemid peaks suutma sellisele ründele vastu pidada.

Kõige loomulikum lähenemisviis kahe signatuuri ühendamiseks nii, et säiliks võltsimatus, on valida üheks liidetavaks skeemiks võltsimatu skeem [48] ning neid teineteise järel rakendada. Ilmneb aga, et leidub ka selliseid konstruktsioone, mille puhul on kombineeritud skeemil veel lisaks mõned head lisaomadused [48]: näiteks saab garanteerida, et ründajal pole võimalik hübriid-signatuurist eemaldada kumbagi osa-signatuuri nii, et seda eemaldamist poleks võimalik hiljem tuvastada.

Nii signatuuriskeemide kui ka võtmekehtestusmehhanismide puhul tuleb tähele panna, et hübriidskeemid on lisatud struktuuri tõttu märksa keerukamad kui nende tavalised versioonid, mis teeb nende teostamise keerulisemaks. Kuna hübriidskeemid koosnevad nii klassikalistest kui kvantturvalisest osadest, võib nende kasutamine avada võimaluse madaldusrünneteks.

A.2.4 Standardiseerimine

Aastal 2016 algatas USA Riiklik Standardi- ja Tehnikainstituut (NIST) postkvant-krüptograafia standardiseerimisprotsessi [49]. Protsessi käigus asuti otsima kvantturvalisi signatuuriskeeme ja võtmekapseldusmehhanisme. Mitu voozu kestnud analüüsi tulemusena standardiseeriti üks võtmekapseldusmehhanism (ML-KEM [18]) ning kaks signatuuriskeemi (ML-DSA [22] ja SLH-DSA [23]). Lisaks sellele töötatakse praegu välja standardit veel ühele signatuuriskeemile (FN-DSA, mis põhineb Falconil [35]) ning peagi standardiseeritakse ka veel üks võtmekapseldusmehhanism (HQC [37])¹. Et enamik kehtestatud standarditest põhineb võredel, siis otsustas NIST välja kuulutada uue konkursi signatuuriskeemide leidmiseks, et standardite valikut mitmekesistada.

Iseseisvat standardiseerimist viivad läbi ka ISO ja ETSI. ISO standardiseerimisprotsess on NISTiga võrreldes vähem avalik. Küll aga on teada, et projekti raames kaalutakse rahvusvahelise standardi kavandit (DIS), mis sisaldab endas ML-KEMi, FrodoKEMi ja Classic McEliece'i, mis lisatakse olemasolevale standardile ISO/IEC 18033-2².

ETSI on töötanud välja standardi „Varjatud juurdepääsureeglitega kvantturvalised hübriidvõt-

¹<https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms>

²<https://www.iso.org/standard/86890.html>

mevahetusmehhanismid³, mis sisaldab ML-KEMi ja kvantturvalist hübriidvõtmekehtestusmehhanismi⁴, mis ühendab omavahel ML-KEMi ja ECDH.

Kvantturvaliste krüptoskeemide standardiseerimisega tegelevad iseseisvalt veel ka Hiina⁵ ja Lõuna-Korea⁶. Kui Hiina on jõudnud oma protsessi ainult algatada, siis Lõuna-Korea on mõned standardiseeritavad skeemid juba välja valinud – signatuuriskeemid AlMer [50] ja HAETAE [51] ning avaliku võtmega krüptosüsteemid NTRU+ [52] ja SMAUG-T [53].

Soovitused. See jaotis annab ülevaate erinevatest kvantturvalistest algoritmidest, mida soovitavad kasutada erinevad institutsioonid. Nende soovitused on kokku võetud tabelis 3. Enamjaolt soovitavad erinevad riigid järgida NISTi standardeid, kuid mõned esitavad valikutena ka konservatiivsemaid võtmekapseldusmehhanisme. Märkime ära, et ANSSI soovib kasutada võtmekapseldusmehhanisme eelkõige ühekordsete võtmete genereerimiseks [54].

FrodoKEMi ja Classic McEliece'i peetakse teistest valikutest konservatiivsemaks ning neid tuleks kasutada olukordades, kus suurem turvalisus kaalub üle vähesema jõudluse (eriti andmevahetuse puhul) [54, 34].

Tabelis 4 on esitatud kasutussoovitused erinevate algoritmide kaupa.

A.3 Postkvant-krüptograafia teostused

Siin jaotises kirjeldame postkvant-krüptograafia eri liiki realisatsioonide hetkeseisu.

A.3.1 Krüptoteegid

Esimesed postkvant-krüptograafia teostused ilmusid umbes 2019. aastal, kaks aastat pärast NISTi standardiseerimisprotsessi algust, eksperimentaalsetes krüptoteekides, mis sisaldasid ainult postkvant-turvaliste algoritmide teostusi. Selle protsessi algatajateks olid teegi PQClean⁷ haldajad, kes kogusid teeki kokku kõigi NISTi protsessis osalevate algoritmide teostused. Neile järgnes OpenQuantumSafe'i projekt, mis töötas välja täisfunktsionaalse krüptoteegi, andes ühtse liidese PQCleani teostustele, liidesed erinevatesse programmeerimiskeeltesse ning kõrgema taseme protokollide ja krüptograafiatarnijate (*cryptographic provider*) eksperimentaalsed teostused. Teiste programmeerimiskeelte ja protsessoriarhitektuuride jaoks loodi veel teisigi eksperimentaalseid krüptoteeke.

2025. aasta lõpu seisuga on standardiseeritud postkvant-krüptograafia algoritmide (ML-DSA, ML-KEM ja SLH-DSA) teostused olemas populaarsetes krüptoteekides, nagu OpenSSL, WolfSSL, BouncyCastle, TinkCrypto ja teised. Nende teostuste turvalisuse eest vastutavad enamasti teekide haldajad ise, kuid mõned neist on juba ka FIPS 140-3 sertifitseerimise järjekorras.

Tänu neile teekidele hakkasid omakorda tekkima erinevate krüptoprotokollide postkvant-krüptograafilised teostused, nagu näiteks TLS (vt jaotist A.3.2).

Jõudsalt on arenemas ka kõrgkindlate krüptograafiliste teostuste valdkond (sealhulgas post-

³https://www.etsi.org/deliver/etsi_ts/104000_104099/104015/01.01.01_60/ts_104015v010101p.pdf

⁴https://www.etsi.org/deliver/etsi_ts/103700_103799/103744/01.02.01_60/ts_103744v010201p.pdf

⁵<https://www.niccs.org.cn/en/>

⁶https://kpqc.or.kr/competition_02.html

⁷<https://github.com/PQClean/PQClean>

Tabel 3. Erinevate riikide soovitud kvantturvaliste skeemide osas

Asutus	Võtmekapseldusmehhanismid	Signatuuriskeemid	Märkused
ANSSI (Prantsusmaa) [54]	ML-KEM, Frodo-KEM	ML-DSA, FN-DSA, XMSS/LMS, SLH-DSA	+ soovitavad hübriidmeetoodeid
BSI (Saksamaa) [34]	FrodoKEM, Classic McEliece, ML-KEM	SLH-DSA, ML-DSA, XMSS/XMSS ^{MT} , LMS/HSS	+ soovitavad hübriidmeetoodeid võtmekapselduseks ja signeerimiseks (väljaarvatud räsifunktsioonidel põhinevad skeemid) + tuleks eelistada tavalist ML-DSA-d ja SLH-DSA-d
NSM (Norra) [55]	ML-KEM	SLH-DSA, ML-DSA, XMSS, LMS	+ soovitavad hübriidmeetoodeid (väljaarvatud räsifunktsioonidel põhinevad skeemid) + võtmeühendusfunktsioonina tuleks kasutada CatKDFi + hübriidsignatuuride puhul tuleks kasutada kahe signatuuri ühendamist
NCSC (Ühendkuningriik) [56]	ML-KEM	ML-DSA, SLH-DSA, LMS, XMSS	+ ML-KEM ja ML-DSA sobivad üldiseks kasutamiseks + kui kasutada hübriidmeetoodeid, siis ainult ajutiselt ning hiljem tuleks minna üle ainult kvantturvalisele lahendusele
CCN (Hispaania) [57]	ML-KEM, Frodo-KEM	ML-DSA, FN-DSA, SLH-DSA, XMSS	+ püsivarauuenduste puhul tuleks kohe hakata kasutama XMSSi

Tabel 4. Postkvant-turvaliste algoritmide kasutussoovitused

Krüptoskeem	Kasutussoovitused
ML-KEM	üldkasutus
FrodoKEM	kõrgem turvalisus
Classic McEliece	kõrgem turvalisus
ML-DSA	üldkasutus
FN-DSA	väiksemad signatuurid
SLH-DSA	kõrgem turvalisus, olekuta
XMSS/LMS	püsivara- ning tarkvarauuendused

kvant-krüptograafia), kus uued teigid kasutavad verifitseeritavalt turvaliste teostuste pakku-

miseks formaalseid verifitseerimismeetodeid. Selle näitena võib tuua Libjade'i⁸, Libcruxi⁹, ja HAC-Li¹⁰(HACL ei paku veel postkvant-krüptograafia teostusi).

Rohkem infot postkvant-krüptograafia teostuste kohta krüptoteekides on võimalik leida aruandest „Krüptoalgoritmid ning nende tugi teekides ja infosüsteemides 2026“.

A.3.2 Krüptograafilised protokollid

Nagu eelnevalt mainitud, põhineb krüptograafiliste protokollide tugi üldjuhul protokollide teostamiseks kasutatud teekidel. Paljudel juhtudel peab aga postkvant-krüptograafia tugi selle jaoks olema protokollide spetsifikatsioonis või standardis otseselt lubatud. Järgnev jaotis annab põgusa ülevaate nende spetsifikatsioonide hetkeseisust postkvant-krüptograafia üleminekul.

A.3.2.1 TLS

TLSi (transpordikihi turve) kätluse jooksul kasutatakse mitmeid krüptograafilisi komponente. Mitmed neist põhinevad sümmeetrilisel krüptograafial ja nende kvantturvaliseks muutmiseks piisab vaid võtmepikkuse suurendamisest, kuid mõned asümmeetrilised primitiivid vajavad kätluses väljavahetamist.

Kätluse jooksul peavad server ja kasutaja leppima omavahel kokku ühises võtmes, mille jaoks peavad nad kasutama mõnda võtmevahetus- või võtmekapseldusmehhanismi ning klient peab ennast kätluse käigus serverile autentima, mille jaoks signeerib ta oma salajase võtmega kätluse senise protokolliga [58, 59].

Levinuim kvantturvalise võtmevahetuse meetod on kasutada hübriidselt ML-KEMi ja mõnda elliptilise võtmevahetusskeemi (nagu X25519) [60]. Seda lähenemist kasutavad näiteks AWS¹¹, CloudFlare¹², Meta¹³ ja Chrome¹⁴. Teostusi leiab OpenSSLi¹⁵, WolfSSLi¹⁶ ja go/crypto teegist¹⁷.

Autentimisprotsessi kvantturvaliseks tegemine on saanud vähem tähelepanu, sest selle puhul pole ohtu *harvest-now-decrypt-later* rünneteks: isegi kui kvant-ühendustega hiljem salajane võti leida, siis saab selle abil võltsida vaid uusi signatuure, kuid vanade signatuuride puhul enam võltsimisest kasu pole.

Sellegipoolest leidub lahendusi, kus ML-DSA kombineeritakse hübriidselt mõne klassikalise signatuuriskeemiga [61] või kus autentimine seotakse ühise võtme kokku leppimisel kasutatava võtmekehtestusprotsessiga [62].

⁸<https://github.com/formosa-crypto/libjade>

⁹<https://github.com/cryspen/libcruX>

¹⁰<https://github.com/hACL-star/hACL-star>

¹¹<https://aws.amazon.com/about-aws/whats-new/2025/11/network-load-balancers-post-quantum-key-exchange-tls/>

¹²<https://pq.cloudflare.com/>

¹³<https://engineering.fb.com/2024/05/22/security/post-quantum-readiness-tls-pqr-meta/>

¹⁴<https://security.googleblog.com/2024/09/a-new-path-for-kyber-on-web.html>

¹⁵<https://openssl-foundation.org/post/2025-04-22-pqc/>

¹⁶<https://www.wolfssl.com/products/wolfcrypt-post-quantum/>

¹⁷<https://pkg.go.dev/crypto/tls>

A.3.2.2 X.509 sertifikaadid ja avaliku võtme infrastruktuur (PKI)

X.509 sertifikaatide (ja üldisemalt PKI) üleminek postkvant-krüptograafiale on esialgu kulgenud aeglaselt. Siiski on praeguseks märgata mõningast edasiliikumist RFC-mustandite ja üksikute teadustööde näol.

Esiteks seostatakse sertifikaate enim signatuuridega, mis täidavad küll väga olulist rolli turvalisuse tagamisel, kuid mille puhul pole ohtu *harvest-now-decrypt-later* rünneteks. Teiseks peab avaliku võtme taristu arendamisel arvestama mitmete postkvant-krüptograafia tehniliste piirangutega – pikemate võtmete ja suuremate signatuuride puhul peab arvestama pikema töötlemisaja ning suurema mäluvajadusega, mis võib muuta suuremad PKId kasutuskõlbmatuks.

Enamik asjakohasest teadustööst keskendub hetkel sertifikaatide üksikute kasutusmallide uurimisele laiemas avaliku võtme taristus ning tegeleb krüptograafia-alaste soovitude andmisega (nt millised sertifikaadid peaksid esmajärjekorras postkvant-krüptograafiale üle minema ning kas tuleks kasutada hübriidseid meetodeid või mitte). Leidub ka soovitusi korraldada ümber avaliku võtme krüptograafia tervikuna, nii et see võiks (ahelsertifitseerimise kõrval) kasutada ka muid sertifikaadi struktuure, nt räsipuid. Nende ettepanekute eesmärk on vähendada PKIga seotud elementide mahtu.

Postkvant-krüptograafiliste sertifikaatide ja PKI teostusi on väga vähe ning enamik neist on loodud prototüüpimise ja uurimistöö eesmärgil.

A.3.3 Postkvant-krüptograafia riistvaralistes komponentides

Jaotises [A.3.1](#) rääkisime peamiselt postkvant-krüptograafia tarkvaralistest teostustest, kuid enamik valmis tarkvarast kasutab vajamineva krüptograafia teostamiseks riistvaralisi komponente.

Riistvarakomponentide tarnijad ei kiirusta postkvant-krüptograafiale üle minema, sest kvantturvaliste algoritmide suurem keerukus teeb komponentide arendamise raskemaks.

See-eest on tekkinud mitmeid erinevad idufirmasid, mille ainsaks eesmärgiks on arendada postkvant-krüptograafiat toetavaid tarkvaramooduleid. 2024. aasta lõpus ja 2025. aasta alguses hakasid võrdlemisi märkamatult ilmuma esimesed Ühiskriteeriumide (Common Criteria) jms sertifitseeringud postkvant-võimekatele moodulitele, kuid mitmed neist ei nimeta postkvant-suuteid oma turvasihis (*security target*), st formaalselt ei ole need suuted olnud hindamisobjektiks (TOE).

A.3.3.1 PKCS#11

PKCS#11 on krüptograafiliste moodulite liidest kirjeldav spetsifikatsioon. Kuigi seda on võimalik kasutada ka tarkvarapakujatel kindlate krüptograafiaga seotud eesmärkide täitmiseks, töötab see algselt välja riistvaramoodulite jaoks (nagu kiipkaardid ja krüptograafilised isikutõendid). Peagi valmiv versioon v3.2 lisab spetsifikatsiooni vahendid (algoritmide identifikaatorid) ML-DSA, ML-KEMi ja SLH-DSA jaoks koos vajaminevate funktsioonidega, nagu kapseldus- ja lahtikapseldusmeetodid.

A.4 Lüngad tehnoloogia arengus ning edasine uurimistöö

Selles jaotises kirjeldame mõningaid lünki postkvant-krüptograafia tehnoloogises arengus ning toome välja mõned valdkonnad, kus valmisolek postkvant-krüptograafiale üleminekuks nõuab edasisi uuringuid.

Lävikrüptograafia

Lävikrüptosüsteem on krüptosüsteem, kus süsteemi toimimiseks olulised saladused on jagatud mitme poole vahel, nii et tundliku operatsiooni (näiteks dekrüpteerimise või signeerimise) jaoks peab vähemalt mingi kindel arv neist pooltest omavahel koostööd tegema. Eesti kontekstis on olulisim lävikrüptograafiat kasutav süsteem Smart-ID [63], kus kahe poole koostöös luuakse standardseid RSA-signatuure. Lävikrüptograafia on kasutusel ka Eesti internetihääletamise süsteemis [64], kus anonümiseeritud häälte dekrüpteerimiseks vajalik võti on mitme poole vahel jagatud.

Leidub nii lävisignatuuri- kui ka krüpteerimisalgoritme, mille turvalisus põhineb mingite arvutusprobleemide eeldataval keerukusel ka sellise ründaja jaoks, kel on kasutada kvantarvuti [65]. Standardiseeritud signatuuriskeemidest on ML-DSA nii võtme genereerimise kui ka signeerimise jaoks olemas lävikrüptograafia protokollid [66, 67, 68]. Hetkel pole ükski neist protokollidest veel nii heade omadustega kui Smart-ID-s kasutatav SplitKey protokoll: vaja on rohkem pooli, või on signatuuri (mis küll vastab ML-DSA standardile) loomine nii erinev standardist, et seda võiks juba uueks signatuuriskeemiks pidada. ML-DSAst lihtsam on läviprotokolle välja töötada hetkel NISTi täiendavate signatuuriskeemide standardimisprotsessis püsiva MAYO skeemi jaoks [69]. Läviprotokolle FN-DSA ja SLH-DSA jaoks meie teada hetkel ei ole. Uute postkvant-turvaliste lävisignatuuride väljatöötamine (või olemasolevate postkvant-turvaliste signatuuriskeemide jaoks lävisigneerimisprotokollide väljatöötamine) jätkub.

Standardsete krüpteerimissüsteemide dekrüpteerimisalgoritmide jaoks reeglina mõistlikke läviprotokolle ei leidu, sest need süsteemid kasutavad samme, mida on ühel poolel lihtne läbi viia, kuid mitme poolega väga raske käitada nii, et saladused ei lekiks. Tõepoolest, sageli saavutavad need süsteemid turvalisuse valitud krüptotekstiga rünnete vastu niimoodi, et valitud avatekstiga rünnete vastu turvalise süsteemiga krüpteeritakse teade, millele on lisatud sõnumiautentimiskood. Sõnumiautentimiskood põhineb tavaliselt mingil räsifunktsioonil. Dekrüpteerimisel peab kontrollima ka seda sõnumiautentimiskoodi; kui kood ei ole korrektne, siis ei tohi avateksti edasi kasutada [70]. Läviprotokoll peaks läbi viima sõnumiautentimiskoodi kontrolli ilma avateksti lekitamata: see tähendaks räsifunktsiooni privaatselt arvutamist, mis on aga väga ressursinõudlik.

Lisa B Ülevaade krüptoinventuuri võimalikest meetoditest

See peatükk annab ülevaate krüptovarade avastamise ja inventuuri (*CADI — Cryptographic Asset Discovery and Inventory*) meetoditest ja neid toetavatest IT-vahenditest. Ülevaade põhineb suuresti olemasoleva kirjanduse analüüsil. Me ei ole püüdnud leida parimat allikat, et selle põhjal metoodikat välja pakkuda, vaid oleme kindlaks teinud, mis on need ühised väited, mida kõik (või enamused) allikaid CADI kohta teevad, ja kus mõned allikad midagi muud välja pakuvad. Saadud ühine vaade ning IT-vahendite otsingu ja analüüsi tulemused on aluseks meie soovitatavale metoodikale selle peatüki lõpus.

Terminoloogiajaotises (ptk B.1) me uurime, milliseid termineid ja nende kogumikke on CADI jaoks kasutatud. Me püüame neid terminikogumikke ühtlustada ning anname ise mõnede terminite definitsioonid, mida edaspidi selles peatükis kasutame. Järgnevalt, jaotises B.2, anname me omadefineeritud termineid kasutades ülevaate senistest CADI-teemalistest publikatsioonidest. Me kirjeldame mitmes allikas väljatoodud mõtteid, fakte, soovitatud tegevusi, jne. Jaotises B.3 anname ülevaatliku loetelu IT-vahenditest, mis neid tegevusi toetavad. Peatüki lõpus (B.4) loeme veel kord üles need allikad, millele käesolev ülevaade toetub.

B.1 Terminoloogia

Meie kirjanduse ülevaatest (ptk B.2) selgus, et eri allikad kasutavad samade mõistete jaoks üksteisest pisut erinevaid termineid, tekitades sellega segadust ja komplitseerides CADI-t kasutavate tegevuste kirjeldamist. Samale järeldusele jõuti ka ühes varasemas süstemaatilises ülevaates postkvant-krüptograafia üleminiku kirjandusest [15].

Olemasoleva kirjanduse analüüsis on meile silma jäänud vähemalt 38 enam või vähem erinevat fraasi, millega on tähistatud CADI-t või mingeid olulisi osi sellest. Paljudes fraasides esineb sõna *discovery* või *inventory*, aga nende täiendid varieeruvad. Ei ole selge, millised neist on samatähenduslikud ja millised tähendavad mingeid erinevaid tegevusi. Variatsioone esineb eri allikate vahel, aga ka sama allika piires. Osades allikates defineeritakse mõisted ja kasutatakse neid läbivalt kogu dokumendis, teistes aga nii järjepidev ei olda. Mõnes allikas kutsutakse CADI protsessi mingit sorti „diagnoosiks“, mis on veel laialivalguvam termin.

B.1.1 Eri tüüpi varad

Varasid avastades ja inventeerides tuleb meil arvestada nende erisustega. Mõned allikad annavad ammendava loetelu varade tüüpidest, ühes rohkem või vähem põhjalike näidetega, millele tähelepanu pöörata. Varatüüpide lõikes võib käsitluse vajalik detailsusaste ja rangus erinev olla.

Postkvant-krüptograafia üleminiku kontekstis kohtame mingeid varatüüpe sagedamini kui teisi. Kirjanduses kasutatakse nende jaoks jälle mitmeid eri termineid. Järgnevalt kirjeldame neid tüüpe.

Krüptograafilised varad Seda tüüpi varad, mida kirjanduses teistest palju rohkem mainitakse, sisaldavad kõikvõimalikke krüptograafiarealisatsioone ja nendega seotud objekte. Realisatsioonid võivad olla nii riist- kui ka tarkvaralised.

Krüptograafiliste varade peamine ülesanne on tagada süsteemi turvaomadusi, näiteks konfidentsiaalsust, terviklust, autentsust, salgamatust ja nende kombinatsioone. Nende koostisosa-deks on protokollid, algoritmid, krüptograafilised võtmed, sertifikaadid, teenused jms. Nad leiavad kasutust tarkvaraarenduses (kui krüptograafilised teegid, võtmed, mandaadid, tookenid, operatsioonisüsteemides (virtuaalsed privaativõrgud, kaksikautentimine, jõudeolekus andmete krüpteerimine, turvaline algladimine) ja võrguliikluses (kaitstes seal avaliku võtme taristut, meililiiklust, veebilehitsust).

Mõned, kuid mitte kõik kirjandusallikad eristavad „krüptograafilisi varasid“ ja „krüptograafiliselt kaitstud varasid“. Siin esimene on vara, mis teeb mingeid krüptograafilisi operatsioone. Teine aga on vara, millele on mingeid krüptograafilisi operatsioone rakendatud.

Infotehnoloogilised varad Seda tüüpi varad on taristu osa. Nende hulka kuuluvad võrguteenused, operatsioonisüsteemid, rakendused, tarkvaraarenduse konveierid, füüsilised IT-varad (seadmekapid, lauarvutid, mobiiltelefonid, võrguseadmed, printerid, VoIP-seadmed, riistvaralised turvamoodulid, kiipkaardid ja pääsmikud). Osad allikad soovivad kõigi infotehnoloogiliste vahendite inventeerimist, sõltumata sellest kas nad kasutavad krüptograafiat või ei.

Andmevarad Sellesse varatüüpi kuuluvad kõikvõimalikud andmed, mida organisatsioon töötleb, ühes oma metaandmetega: mis liiki andmetega on tegemist, kus need asuvad, mis on nende väärtus organisatsiooni jaoks, millised on nendega seotud reeglid ja riskid. Osad allikad soovivad kõigi andmevarade inventeerimist, sõltumata sellest kas nendega seotult on krüptograafiat kasutatud või ei.

Tarnitud varad, millest sõltutakse Sellesse tüüpi kuuluvad varad, mida haldavad organisatsioonist väljaspool asuvad tarnijad või teenusepakkujad. Selliste kolmandatele pooltele kuuluvate varade kohta võib olla raske leida detailset informatsiooni. Seetõttu loeme nad eraldi tüüpi kuuluvaks.

B.1.2 Krüptograafiliste varade avastamise ja inventuuri protsessid

Defineerime järgnevalt mõlemad protsessid. Leiame, et mõistlik on definitsioonid ise välja pakuda, sest eri allikates olevate arvukate mõistete ühtlustamine meil ilmselt ei õnnestuks. Meie definitsioonid püüavad võimalikult täpselt katta sõnade *discovery* ja *inventory* tähendust. Mär-gime, et need protsessid on suunatud ainult krüptograafilistele varadele (ptk B.1.1), kuid tänu terminoloogilisele mitmetähenduslikkusele teistes postkvant-krüptograafia ülemineku juhendes ja teekaartides võivad sobida ka muud tüüpi varadele.

Krüptograafiliste varade avastamine Me defineerime selle protsessi kui kõigi krüptograafiliste varade identifitseerimise ja nende oluliste atribuutide väljaselgitamise. Protsessi sisendiks on leitavate varade tüüp. Väljundiks on leitud varad. Protsessi läbiviimise piirkonnaks võib olla organisatsioon, taristu, süsteem, rakendus, teek, võrgukonfiguratsioon jms. Postkvant-krüptograafia üleminekul tuleb seda protsessi läbi viia korduvalt, eesmärgiga lõpuks absoluutselt kõik krüptograafilised varad üles leida, sest ainult nii saame lõpuni kindlad olla süsteemi kvant-turvalisuses.

Krüptograafiliste varade inventuur Selle protsessi defineerime me kui varade haldamise tegevuse. Siia alla kuulub varade kategoriseerimine, kirjeldamine ning täiendava informatsiooni kogumine nende kohta. Krüptograafiliste varade inventuuri sisendiks on varade avastamise väljund; väljundiks on krüptograafiliste varade andmebaas, mis sisaldab nende kategorisatsiooni, atribuutide nimekirja ja väärtusi, kvantohtudega seotud riskide hinnangut jne.

B.1.3 CADI

CADI (*Cryptographic Asset Discovery and Inventory*) kombineerib avastamise ja inventuuri protsesse. Selle mõistega tähistame tegevusi alates kõigi krüptograafia kasutamisega seotud olevate varade identifitseerimisest kuni nende selges ja organiseeritud vormis kirjeldamiseni.

CADI automatiseerimine Ilmsetel põhjustel (ükslused ja korduvad tegevused, üleviidavate süsteemide suur arv, inimressursi puudus) püütakse CADI protsesse (kas ühte või teist, aga enamasti mõlemat) automatiseerida. Loodavad tööriistad võivad näiteks automaatselt läbi vaadata mõne IT-süsteemi lähtekoodi ning väljastada nimekirja kasutatavatest krüptograafilistest operatsioonidest ühes kõigi asjassepuutuvate detailidega, seda nii masin- kui ka inimloetavas vormis. Täpsemalt käsitleb neid tööriistu peatükk [B.3](#).

B.2 Olemasolevate allikate ülevaade

Käesolev jaotis on põhjalikum sissejuhatus CADI teemasse. Poolpaksu kirjaga toome esile meie arvates olulisimad jutupunktid.

Me oleme analüüsinud kokku 24 postkvant-krüptograafia ülemineku juhtnööri või teekaarti ning akadeemilist tööd, kus on mingil viisil mainitud CADI-t või selle üle arutletud. Peatükis [B.4](#) on toodud nende allikate kategoriseeritud nimekiri.

B.2.1 Läbivad jutupunktid

Nagu juba mainisime, erinevad need 24 allikat üksteisest suurel määral. Erinevus on mitte ainult terminites, vaid ka üldistes CADI-alastes soovitusetes. Tavaliselt ei anna nad juhiseid, kuidas CADI-ga seotud tegevusi praktikas läbi viia. Siin jaotises püüame edasi anda neid jutupunkte, mis on enamusele allikatele ühised.

B.2.1.1 Sissejuhatus

Enam-vähem kõik allikad on ühel nõul selles, et identifitseerimine, kus ja kuidas krüptograafiat kasutatakse (s.t. CADI) on **kõige olulisem ja kriitilisem osa postkvant-krüptograafia üleminekust**. Samuti on tegemist **väga keerulise ülesandega**, sest tänapäevased infosüsteemid kasutavad krüptograafiat kõikjal. Seega on oluline **alustada nii vara, kui võimalik**.

Teine ühine jutupunkt on, et **identifitseerimisprotsessi läbiviimine on põhjendatud samm, mille tegemist ei ole põhjust edasi lükata**, sest sõltumata sellest, kas organisatsioon osutub või ei osutu tulevikus kvantarvutit kasutava ründe sihtmärgiks, on talle ikkagi kasulik teada, kus ja kuidas ta krüptograafiat kasutab. Krüptovarade identifitseerimisse tuleks suhtuda kui osasse organisatsiooni küberturvalisuse riskihalduse strateegiast.

CADI otsast lõpuni läbiviimine võib tunduda hoomamatu. Seetõttu tuleks **protsesside algatamisega ning paika panna iteratiivsed tegevused, mis lubaksid inventuuriga ajapikku valmis**

saada.

B.2.1.2 CADI eesmärgid

CADI peamine eesmärk on **anda arusaamine organisatsiooni krüptograafilisest kondikavast**. Tänu temale mõistame asjassepuutuvaid krüptograafilisi sõltuvusi, saame aru kvantarvutitega seotud riskidest ja prioritseerime krüptograafiliste algoritmide väljavahetamise vajadusi. Ta aitab ka organisatsioonidel rahuldada regulatiivseid nõudeid, kehtestada ja uuendada turvapolitiikaid ning **ilmutatult ja dokumenteeritult postkvant-krüptograafia üle minna ja/või seda kasutusele võtta**.

Krüptograafiliste algoritmide väljavahetamise praktiliste aspektide kontekstis, CADI

- **annab selge ülevaate hetkel kasutatavast krüptograafiast** (identifitseerib süsteemid ja komponendid, kus tuleb algoritme välja vahetada),
- **võimaldab kiireid muudatusi** (sel ebatõenäolisel juhul, kus praegused postkvant-krüptograafia algoritmid ise muutuvad ebatavaliseks tänu krüptanalüütilistele edusammudele),
- **identifitseerib mitte ainult kasutusel olevad kvanthaavatavad krüptograafilised algoritmid, vaid ka aegunud ja pärandalgoritmid** (näiteks MD5 ja SHA-1 räsifunktsioonid),
- **parendab üleüldist krüptograafiliste algoritmide haldust organisatsioonis**.

B.2.1.3 Krüptograafilise inventuuri jaoks andmete kogumine

Eri allikad annavad pisut erinevaid soovitusi selles osas, **milliseid andmeid koguda kasutusel oleva krüptograafia kohta**. Üldiselt soovitatakse üles märkida, millist krüptograafilist algoritmi kasutatakse, kus täpselt seda kasutatakse, miks kasutatakse, kes on kasutamise eest vastutav ning milline on selle konkreetse kasutusjuhu üleviimise prioriteet.

Mõnikord võib olla nii, et **krüptograafiliste algoritmide kasutust haldab väline teenusepakkuja**. Sel juhul on oluline järke pidada, milline pakkuja tarnis millised lahendused ja millised on kokkulepped selle lahenduse haldamise ja uuendamise osas. Osad allikad soovivad, et sellisel juhul tuleks tarnijatega otse ühendust võtta ja neilt küsida infot, mille struktuur on sarnane eelmises lõigus kirjeldatuga.

Osad allikad lähevad andmete kogumise soovitustes kaugemale, leides, et tuleb kirjeldada ka süsteeme ja teenuseid endid, organisatsioonis kasutatavaid tarkvararakendusi, võrgu- ja kommunikatsiooniriistvara, mobiilseadmeid, servereid ja tööjaamu, värgvõrguseadmeid jne.

B.2.1.4 Krüptoinventuuri vorming

Kirjandusallikad pakuvad tavaliselt välja mitu eri viisi krüptoinventuuri loomiseks ja haldamiseks. **Iga organisatsioon võib valida oma viisi**, soovitavalt sellise, mis sobitub tema olemasoleva dokumenteerimistaristu, poliitikate ja parimate praktikatega. Inventuur võib olla **tekstidokumendi, arvutustabeli, andmebaasi vormis**. Võib kasutada ka hiljuti väljapakutud **krüptograafiliste varade loendi (Cryptographic Bill of Materials)** vormingut (vt ptk B.3.1).

B.2.1.5 CADI tüüpilised väljakutsed

Väljakutseid saab kategoriseerida järgnevalt.

Süsteemi keerukus

Infosüsteemid on keerulised süsteemid, koosnedes paljudest erinevatest komponentidest, mis kasutavad erinevaid krüptograafilisi varasid. Nende varade identifitseerimine võib olla aeganõudev. Kui seda teha suures organisatsioonis lihtsa struktuuriga arvutustabeli abil, siis võib olla seda tegevust võimatu hallata.

Piiratud nähtavus heterogeenses keskkonnas

Organisatsiooni protsessid võivad toetuda erinevatele pärand-, ajakohastele ja sisseostetud teenustele. Üks teenus ei pruugi teise detaile näha, olles seega võimetu tuvastama kõiki krüptograafilisi varasid.

Krüptograafilised sõltuvused

Kõigi krüptograafiliste varade vaheliste sõltuvuste kaardistamine võib vajada süvateadmisi organisatsiooni süsteemidest, nende realisatsioonist ja nendevahelistest andmevoogudest.

Ligipääs

Varade avastamine ja inventeerimine vajab ligipääsu (lähte- ja objekti-)koodile, testkeskkondadele, virtuaalmasinatele pilves, võrgu otspunktidele ja muudele taolistele punktidele. See omakorda nõuab osakondade ja sidusrühmade üleseid ligipääsuõigusi.

Inimlikud vead või automaatsete protseduuride täielikkus

Ühest küljest on käsitsi varade avastamine ja inventeerimine üksluine ja veaohklik. Teisest küljest on peaaegu võimatu luua automatiseeritud töövahendit, mis kõik avastatava ja inventeeritava ära avastaks ja inventeeriks. Varade avastamine saab efektiivne olla ainult inimese ja arvuti koostöös.

Krüptograafia areng

Krüptograafia kui teadusharu ei ole staatiline. Uute algoritmide, protokollide, standardite jne. väljapakumine jätkub. Seetõttu võib olla vaja krüptograafiliste varade loendit, sealhulgas arvepidamise aluseks olevate atribuutide kogumit pidevalt uuendada.

Ressursipiirangud ja prioriteedid

Kvantarvutitest lähtuvate ohtude olemuse tõttu (mis veel ei ole kohal, kuid mingil hetk tulevikus realiseeruvad) võib olla raske põhjendada, miks on CADI vajalik ja miks peaks selle läbiviimisele pühendama märkimisväärset hulgal ressursse.

Pidevad uuendused

Krüptograafiliste varade avastamist tuleks teha perioodiliselt ning loendit tuleks järjekindlalt uuendada. See vajab pidevat seiret, hindamist ja taas kord ressursinõudlikke uuendamistevõusi.

B.2.2 Täiendavad tähelepanekud ja märkused

Selles jaotises loeme üles mõned tähelepanekud eri allikatest, mida me tähelepanuväärseks pidasime. Siintoodud informatsioon võiks lugeja jaoks olla kui näited, kuidas ülalpool toodud üldiseid ideid konkreetsetel juhtudel ellu viia.

Allikas [71] on siiani üks sisukamaid saadaolevaid teekaarte. Selle teekaardi teeb märkimisväärseks **detailne nimekiri sellest, millist informatsiooni iga süsteemi (näiteks võrguteenus, rakendus, kiipkaart jne.) kohta krüptograafiliste varade avastamisel koguda tuleks:**

1. Millised süsteemikomponendid kasutavad krüptograafiat?
2. Kes tarnis komponendi? Mis on komponendi versiooninumber?
3. Milline turvafunktsionaalsus sõltub avastatud krüptograafilistest varadest?

4. Millistes võrgusegmentides (sise- või välisvõrk jms.) neid süsteeme kasutatakse?
5. Milliseid krüptokonfiguratsioone kasutatakse?
6. Millistel platvormidel kirjeldatavad süsteemid jooksevad?
7. Millistest teistest süsteemidest või komponentidest need süsteemid sõltuvad?
8. Millised on asjassepuutuvad hoolduslepingud ning neis lepingutes olevad tähtajad?
9. Mis aastal on plaanis süsteemi või tema komponente uuendada?
10. Kes on selle süsteemi jaoks organisatsioonisisene kontaktisik?
11. Kas süsteemi üleviimine postkvant-krüptograafiale on organisatsiooni jaoks kõrge prioriteediga?

Allikas [14] kirjeldab raamistikku, mille abil kogu suur organisatsioon või ettevõtte ajapikku viia üle kvant-turvalise krüptograafia kasutamisele. Selle raamistiku **kohustuslik osa on organisatsiooni jagamine (loogilisteks) osakondadeks**. Peake sellist jagamist teeb iga osakond iseseisvalt CADI. Teisisõnu, organisatsioonis saab olema mitu väiksemat PQCle ülemineku meeskonda.

Sealsamas soovitatakse ka, et krüptoinventuuri jaoks tuleb üles otsida **iga krüptograafiline vara ja iga muu vara, millele rakendatakse krüptograafilisi operatsioone**. Soovitatakse, sisse viia **märgendamissüsteem**, andmaks märgendid igale varale vastavalt nende tundlikuse tasemele ja süsteemile, kuhu nad kuuluvad. Samuti soovitatakse, et iga vara **sõltuvused (mõlemas suunas)** tuleks inventeerida. Sarnaseid soovitusi annab allikas [3], mis samuti rõhutab **krüptograafiliste varade ja varade, millele krüptograafilisi operatsioone rakendatakse** tähtsust ja **sõltuvusgraafide** loomist.

Allikas [72] annab põhjaliku nimekirja **krüptograafiliste varade avastamise ja inventuuri vahenditest ja meetoditest**:

Võrguliikluse analüüs

Võrguliikluse seire ja analüüsimine, et leida sealt krüpteeritud liiklust ja krüpteeritud andmete vahetamist.

Protokollianalüüs

Kasutusel olevate krüptograafiliste protokollide (nagu näiteks TLS) identifitseerimine ja ülevaatamine.

Otspunkti turvalahendused

Selliste otspunkti turvalahenduste kasutamine, mis suudavad krüptograafilisi protsesse tuvastada ja raporteerida.

Tulemüüri logid

Tulemüüri logidest krüpteeritud liikluse (ja muu krüptograafiakasutuse) märkide otsimine.

Sissetungituvastuse süsteemid (IDS)

IDSi kasutamine märkamaks võrguliiklust, mis sisaldab krüpteeritud andmeid võid muud krüptograafiakasutust.

Võrgu skaneerijad

Võrgu skaneerijate kasutamine, et leida seadmeid ja teenuseid, mis kasutavad krüptograafiat.

Konfiguratsiooni auditeerimine

Krüptograafiliste seadete leidmine võrguseadmete konfiguratsioonist.

Läbistustestimine

Krüptograafiliste nõrkuste ja väärkonfiguratsioonide leidmine läbistustestimise abil.

Tarkvara inventeerimise vahendid

Nende vahendite kasutusele võtmine selleks, et krüptoteekide ja muu krüptograafilise tarkvara kasutamist leida.

Pakettide süvakontroll

Võrgupakettidest krüpteeritud liikluse ja krüpteerimisliikide leidmine.

Digitaalkriminalistika (*digital forensics*)

Digitaalkriminalistika töövahendite kasutamine analüüsimaks andmeosiseid, mis viitavad krüptograafiliste operatsioonide kasutusele.

Vastavuse skaneerimine (*compliance scanning*)

Skaneerimise abil tuvastamine, et vastatakse asjakohastele krüptograafiastandarditele.

Sisseostetud infoturbeteenused

Küberkaitsettevõtelt spetsialiseeritud krüptograafiliste tegevuste skaneerimise ja seireteenuste hankimine.

Masinõppemudelid

Traditsiooniliste meetodite jaoks tuvastamatute krüptograafiakasutusmustrite ja -anomaaliate leidmine tehisintellekti abil.

Nõrkuseotsing (*vulnerability scanning*)

Võrgus selliste nõrkuste otsimine, mis võivad mõjuda krüptograafilistele funktsionaalsustele.

SIEM analüüs

SIEM süsteemide abil krüptograafiaga seotud turvaintsidentide analüüs ja haldus.

Sama allikas annab ka **Krüptoinventuuri asukohtade loetelu**, kust võiks alustada krüptograafiliste varade avastamist:

- **Koodipõhised varad**
 - Rakenduste lähtekood: krüptoteegid, ise loodud realisatsioonid krüptograafilistele algoritmidele.
 - Krüpteeritud andmebaasid: salvestatud andmete krüpteerimine, võtmehaldus.
 - Rakendusprogrammiliidesed: krüptograafiline funktsionaalsus lähtekoodis, dokumentatsioon.
- **Võrgupõhised varad**
 - TLSi kasutused: veebis, meiliserverites, jne.
 - Võrguseadmed: tulemüürid, koormusejaoturid, sissetungi avastamise süsteemid.
 - Virtuaalsete privaattvõrkude konfiguratsioonid: krüpteerimise ja autentimise meetodid.
 - Traadite võrgud: krüpteerimismeetodid Wi-Fi protokollides
- **Riistvara**
 - Riistvaralised turvamoodulid (HSM): krüptovõtmete haldus ja salvestus.
 - Sardsüsteemid ja värkvõrguseadmed: krüptograafia realisatsioonid.
 - Andmesalvestusseadmed: krüpteeritud kettad, krüpteerimismeetodid.
- **Sisseostetud ja pilveteenused**
 - Pilveteenusepakkujad: andmete krüpteerimine edastamise ja salvestamise ajal.
 - Tarkvara teenusena: krüpteerimismeetodid andmekaitseks.
 - Välised tarnijad: krüptograafilised standardid ja vastavus neile.
- **Avaliku võtme taristu (PKI)**

- Sertifitseerimiskeskused: sertifikaatide loetelu.
- SSL/TLS sertifikaadid: krüpteerimis- ja räsimalgoritmid.
- Võtmehaldussüsteemid: krüptovõtmete haldus.
- **Administratiiv- ja haldusliidesed**
 - Konfigureerimis- ja haldustööriistad: krüptograafilised seaded.
 - Pääsukontrollisüsteemid: krüpteerimine ja räsimine autentimisel.
- **Arendus- ja testkeskkonnad**
 - Arendusvahendid: krüptograafia kasutus tarkvaraarenduses.
 - Testimiskriptid ja -vahendid: krüptograafia kasutus testkeskkondades.
- **Varundamissüsteemid**
 - Varundamislahendused: krüpteerimine varundustarkvaras ja -riistvaras.
 - Õnnetusest taastumise plaanid: krüptograafilised meetmed ja uuendused.
- **Mobiilsed ja kaugkeskkonnad**
 - Mobiilirakendused: krüpteerimise kasutus rakendustes, mis pääsevad ligi organisatsiooni andmetele.
 - Töölaua kaugligipääsuprotokollid: krüptograafia kasutus kaugligipääsuks.
- **Pärandsüsteemid**
 - Vanem riist- ja tarkvara: krüptograafiastandardite ülevaatamine.
 - Ajaloolised andmed: krüpteeritud arhiveeritud andmete turvalisus.
- **Dokumentatsiooni ja konfiguratsiooni haldus**
 - Turvapoliitikad: vastavus värskete krüptograafiastandarditega.
 - Konfiguratsioonifailid: krüptograafiliste seadete haldamine failides ja mallides.
- **Tarnehela sõltuvused**
 - Sisseehitatud krüptograafia: väliste tarnijate tooted, millel on krüptograafilist funktsionaalsust.
 - Teenusepakkujad: taristu ja hallatud teenuste pakkujate krüptograafiapraktikad.
- **Erilised kasutusjuhud**
 - Plokiahela tehnoloogiad: kasutatavad krüptoalgoritmid.
 - Tööstusharu-spetsiifilised seadmed: krüptograafia kasutamine neis seadmetes.
 - Teadus ja arendus: projektid, mis uurivad uusi krüptograafilisi tehnoloogiaid.
- **Auditeerimise ja vastavustestimise tööriistad**
 - Auditilogid ja seirevahendid: krüptograafia, mida turvaseirevahendid kasutavad.

Allikal [73] on lisa A.1, milles on **küsimustik inventuuriks valmistumiseks ja läbiviimiseks**. Ta annab nimekirja kogutavatest andmeelementidest ja samuti toob välja küsimused, mida esitada nende andmete otsimise ajal. Näiteks:

1. Tüüp: millistesse kategooriatesse kuuluvaid andmeid tuleb krüpteerida (isikuandmed, ärisaladus, kohtusaladus, riigisaladus, jne)?
2. Tugevus: kui tugev on iga krüptograafiline võti klassikaliste ja kvant-rünnete suhtes?
3. Säilitus: kas krüpteeritud andmeid kustutatakse regulaarselt?
4. Veel palju küsimusi.

Allikas [74] toodud PQCle ülemineku raamistik **jagab CADI protsessi järgmiseks osadeks:**

1. manuaalne avastamine / kokkukorje,
2. automatiseeritud avastamine / kokkukorje,
3. avaliku võtme taristu (võtmed sertifikaatides),
4. võrguskaneerimine,
5. pilvepõhine inventuur.

PQCle ülemineku käsiraamat [16] soovib **alustada organisatsiooni krüptopoliitike identifitseerimisest** ja viia CADI läbi alles peale seda. Nendest poliitikatest saab siis olla abi järgmiste tegevuste juures:

- Võtmete genereerimise, jagamise, salvestamise, roteerimise ja hävitamise protsesside paikapanek.
- Krüptograafiliste võtmete elutsükli defineerimine.
- Andmete krüpteerimise ja tervikluse tagamise algoritmide ja nende parameetrite paikapanek.
- Autentimis- ja autoriseerimismehhanismide valik.
- Andmete volitamata muutmise vältimise meetodite valik.
- Konkreetsete protokollide ja protokolliversioonide lubamine ja keelustamine.
- Krüptograafiliste üleminekute teekaartide ja tähtaegade fikseerimine.
- Muud seotud teemad.

Sama allikas teeb ka tähelepaneku, et **erinevatele tööstusharudele ja regioonidele rakenduvad andmekaitseregulatsioonid ja -standardid** võivad **olla erinevad**. Mõned poliitikad on kohustuslikud, näiteks PCI DSS finantsinstitutsioonidele, GDPR, NIS2, jms. **Nende poliitike identifitseerimine lubab krüptoinventuurile strateegiliselt läheneda**, aidates varasid prioritseerida ja samuti andes vihjeid, kus need varad olla võiks.

PQCle ülemineku käsiraamat annab ka soovitusi krüptograafiliste varade leidmiseks. Nad soovivad järgmist:

1. **Peaesmärgi defineerimine:** Tee kindlaks, miks krüptograafiliste varade leidmist tehakse. Selle hulgas võivad olla sellised eesmärgid nagu vastavuse tagamine, hoolduse läbiviimine, krüptograafiliste meetmete uuendamine.
2. **Skoobi defineerimine:** Tee kindlaks, mis tüüpi varad tuleb leida ja mida tuleb prioritseerida. Siinhulgas võivad olla võtmed, krüptoalgoritmide sertifitseerimise metaandmed, sõltuvalt nende kriitilisusest ja organisatsiooni vajadustest.
3. **Leidmismetoodika defineerimine:** Tuvasta töövahendid ja võtted, mida avastamise juures kasutada. Sisaldab sobivate vahendite valimist, uuritavate süsteemide kindlakstegemist ja meeskonnaliikmete vahel ülesannete jagamist.
4. **Andmeanalüüsi defineerimine:** Tee kindlaks, mis liiki informatsiooni iga vara jaoks vaja on ja kui detailne see peab olema. See võib sisaldada mõõdikuid iga krüptograafilise varaga seotud kasulikkuse, vastavuse ja riskide hindamiseks.
5. **Aruandlus:** Pane paika, kuidas kogutud andmed tuleks inventeerida ja kuidas neid tuleks analüüsida. Defineeri aruannete vorming ja struktuur, tagades, et informatsioon on esitatud selgelt ja kasutatavalt.
6. **Ülevaatamine:** Määra, kui tihti ja kuidas tuleb varade loetelu üle vaadata ja uuendada.

Käsiraamat nimetab kolm peamist stsenaariumit, milles krüptograafilisi varasid kasutatakse ja millele avastamisprotsess seega tähelepanu peab pöörama:

1. **Tarkvaraarendus:** krüptoteegid.
2. **Operatsioonisüsteemid ja rakendused:** virtuaalsed privaatvõrgud, kaksikautentimise lahendused, krüpteeritud andmete salvestamine, turvaline alglaadimine, süsteemiuuendused jne.
3. **Võrguliiklus:** ISO-OSI pinu iga kihti (v.a. kõige alumine — füüsiline) kaitseb mingi protokoll.

B.3 Infotehnoloogilised vahendid CADI jaoks

Käesolevas jaotises kirjeldame olemasolevaid tehnilisi vahendeid CADI jaoks. Sellised vahendid võiksid suuta automaatselt tuvastada ja raporteerida krüptograafiliste algoritmide kasutust erinevates süsteemiosades, nagu näiteks riist- ja tarkvaramoodulites, teekides, lõimitud koodis, aga ka krüptograafiliste võtmete haldussüsteemides ja protsessides mis kaitsevad salvestatud, edastatavaid või kasutuses andmeid.

Järgnevalt võtame kokku olemasolevates allikates leiduva asjakohase informatsiooni.

Olemasolevate kirjandusallikate laialivalgusus. Suur osa olemasolevatest PCIe ülemineku teekaartidest ja juhenditest, mida me analüüsisime, ei nimeta konkreetseid tehnilisi töövahendeid CADI läbiviimiseks. Tavaliselt nad ütlevad ainult, et sellised vahendid on olemas, või ütlevad ilmutatult, et see teema on skoobist väljas (näiteks [14, 75]). IT-süsteemide suure mitmekesisuse tõttu on selline lähenemine vägagi arusaadav: kõigi üleminekustsenaariumite jaoks sobilikku vahendite loetelu on liiga keeruline kokku panna. Seega on käesoleva jaotise eesmärk kirjeldada olemasolevate vahendite hetkeseisu.

CADI-vahendite kujud. Infotehnoloogiline CADI-vahend ei pea tingimata olema ainult kvant-haavatavate algoritmide leidmiseks loodud. Ka lihtne logifail võib olla CADI jaoks kasulik töövahend, kui see sisaldab kindlat laadi informatsiooni ja seda kasutatakse õigesti. Mõned vahendid võivad juba olemasolevaid küberturvalisuse teenuseid kasutada (turvateabe ja -sündmuste haldus (SIEM), võrgu seire ja uurimine, otspunkti ohuavastus ja reageerimine (EDR)). Teised vahendid võivad olla loodud identifitseerima krüptograafia kasutust lähtekoodis ja muudes kohtades. CADI-vahendite kategoriseerimist ja eri tüüpi vahendite loetelu vaata jaotisest [B.3.2](#).

Piirangud. Mõningatel juhtudel (näiteks lõimitud krüptograafiline funktsionaalsus mingite toodete, näiteks riistvaraliste turvamoodulite sees) ei pruugi infotehnoloogilised töövahendid olla suutelised süsteemi seesmist arhitektuuri uurima. Sel juhul ei pruugi neist vahenditest kasu olla.

Kus neid töövahendeid kasutatakse? Üldiselt uuritakse nende vahenditega võrguprotokolle, lõppkasutajasüsteemide ja serverite varasid, krüptograafilist koodi ja selle sõltuvusi. Konkreetsemaid kasutusjuhte kirjeldame jaotises [B.2.2](#).

CADI-vahendid ei ole täislahendus PCIe üleminekuks. Infotehnoloogiliste vahendite töötulemuste mõistlikust tuleb kontrollida, sest nad tüüpiliselt ei anna vihjeid kõigi kasutusel olevate turvameetmete kohta. Näiteks võib mingi krüptograafiline võti olla mingil ajal tugev, kuid tegelikult võib olla juba vananenud ja vajada väljavahetamist. Üldiselt tuleb IT-vahendeid kombi-

neerida tulemuste käsitsi interpreteerimise ja kontekstist arusaamisega, et otsustada, mis on järgmised sammud.

B.3.1 Krüptograafiliste varade loend (CBOM)

CBOM on populaarsust koguv laiendus CycloneDXi¹ tarkvaraliste materjalide loetelu standardile, mille abil kirjeldada krüptograafiakasutust süsteemi osades. Ta lihtsustab IT-vahendite tulemuste interpreteerimist, edasist modelleerimist ja krüptograafiliste varade esitamist mõnes struktureeritud objektide notatsioonis. Lisaks varadele nagu algoritmid, sertifikaadid, protokollid, võtmed, krüptogrammid jms. saab CBOMi abil kirjeldada ka krüptograafilisi sõltuvusi ning varade krüptograafilisi omadusi. Samuti on võimalik kirjeldada võtmehalduse aspekte, nagu näiteks võtmete elutsükleid.

CBOM on põhimõtteliselt struktureeritud nagu JSONi list. IBM on avalikuks teinud koodihoidla², milles on CBOMi kirjeldus ja skeema. CBOMi struktuuridiagrammide (ja muu täiendava informatsiooni) jaoks viitame allikale *OWASP CycloneDX: Authoritative Guide to CBOM* [76].

Toome näitena ühe (mittetäieliku) CBOMi nimetatud koodihoidlast:

```
"components": [
  {
    "type": "crypto-asset",
    "bom-ref": "oid:2.16.840.1.101.3.4.1.6",
    "name": "AES",
    "cryptoProperties": {
      "assetType": "algorithm",
      "algorithmProperties": {
        "variant": "AES-128-GCM",
        "primitive": "ae",
        "mode": "gcm",
        "implementationLevel": "softwarePlainRam",
        "implementationPlatform": "x86_64",
        "certificationLevel": "none",
        "cryptoFunctions": ["keygen", "encrypt", "decrypt", "tag"]
      },
      "classicalSecurityLevel": 128,
      "nistQuantumSecurityLevel": 1
    }
  },
  {
    "type": "crypto-asset",
    "bom-ref": "ref:10:e6:fc:62:b7:41:8a:d5:00:5e:45:b6",
    "name": "cert-wikipedia-10:e6:fc:62:b7:41:8a:d5:00:5e:45:b6",
    "cryptoProperties": {
      "assetType": "certificate",
      "certificateProperties": {
        "subjectName": "C=US, ST=California, L=San Francisco, O=Wikimedia Foundation,
          ↪ Inc., CN=*.wikipedia.org",
        "issuerName": "C=BE, O=GlobalSign nv-sa, CN=GlobalSign Organization
          ↪ Validation CA - SHA256 - G2",
        "notValidBefore": "2016-11-21T08:00:00Z",
        "notValidAfter": "2017-11-22T07:59:59Z",
        "certificateAlgorithm": "prime256v1",

```

¹<https://cyclonedx.org>

²<https://github.com/IBM/CBOM>

```
    "certificateSignatureAlgorithm": "sha256WithRSAEncryption",  
    "certificateFormat": "X.509"  
  }  
}  
}  
{  
  ...  
  {  
    "type": "library",  
    "bom-ref": "cpe:2.3:a:openssl:openssl:1.1.1q:*:*:*:*:*:*:*",  
    "name": "openssl",  
    "version": "1.1.1q"  
  }  
  ...  
}
```

B.3.2 CADI-t toetavate IT-vahendite kategooriad

Infotehnoloogilisi CADI-töövahendeid on mitut sorti. Järgnevalt püüame nende erinevusi ja sobivaid kasutusjuhte kirjeldada, lähtudes allikast *A Dutch market survey and fit-gap analysis* [77].

Aktiivne või passiivne. Uurides võrguturbeprotokolle, **aktiivne** skaneerija sondeerib, seirab ja suhtleb süsteemidega, et saada teada, milliseid krüptograafilisi algoritme kasutatakse. Siia alla käivad võrguskaneerijad ja sissetungituvastuse süsteemid, mis on konfigureeritud olema aktiivsed.

Passiivsed tööriistad on konfigureeritud süsteemi käitumist (s.t. võrguliiklust) ilma vahelesegamata järgima. Nad koguvad vaikselt andmeid, mida sageli kasutatakse seireks ja auditeerimiseks. Siia alla käivad paketi- ja logianalüsaatorid, logianalüsaatorid ja võrguseirevahendid, mis on konfigureeritud töötama passiivsel viisil.

Staatiline või dünaamiline. Krüptograafiat kasutava programmikoodi analüüsil uurivad **staatiliselt** töövahendid programmi lähtekoodi, konfiguratsioonifaile ja üleüldist taristu ülesehitust, käivitamata seejuures objektikoodi. Nad loevad programmiteksti ja püüavad sealt leida krüptograafiate kutseid.

Dünaamilised analüsaatorid käivitavad uuritavat koodi ja püüavad haavatavaid algoritme tuvastada koodi töö ajal, pannes tähele, milliseid funktsioone ta välja kutsub, milliseid konfiguratsioonifaile laadib jne.

Sidus- või vallasrežiimis. See võimalik erinevus lähtub sellest, kas uuritav / skaneeritav süsteem uurimise ajal töötab või ei. Lähtekoodi staatilist analüüsi saab läbi viia vallasrežiimis, süsteemi toimimist kuidagi mõjutamata. Dünaamiline koodianalüüs on võimalik nii vallasrežiimis (testkeskkonnas) kui ka sidusrežiimis (tootmiskeskkonnas). Vallasrežiimis aktiivne võrguanalüüs ei ole võimalik.

Agentprogrammide kasutus. Agent on tarkvaratükk, mis jookseb sihtsüsteemil. Tema ülesanne on süsteemis olla ja koguda andmeid selle kohta, milliseid krüptograafilisi varasid süsteem kasutab. CADI tehnilised vahendid ei eristu üksteisest väga selles osas, et kas nad agente kasutavad või mitte, vaid pigem selles, et millisel kujul ja kui palju nad oma ülesannete täitmiseks agentprogramme rakendavad. Seega on agentprogrammide kasutus mitte binaarne, vaid pidev atribuut.

Näited. Konkreetsemad näitekategooriad, neisse kuuluvad töövahendid ja meetodid on toodud nimekirjas, mille esitab allikas [72]. Tõime selle välja jaotises B.2.2.

B.3.3 CADI töövahendite funktsionaalsused

Allikas [77] annab loetelu CADI-vahendite potentsiaalsetest funktsionaalsustasemetest; toome selle siinkohal välja. Nimekiri on funktsionaalsuse kasvamise järjekorras; ühes funktsionaalsusega kasvavad üldiselt ka kasutamise kulud, aga samuti paraneb täpsus ja täielikkus.

1. **Taaskasuta** informatsiooni, mis on pärit juba kasutusel olevatest infoturbevahenditest.
2. Küsi **tarnijate CBOM-e**.
3. Lisa oma võrku **passiivselt skaneerivaid** sõlmi.
4. Lisa oma võrku **aktiivselt skaneerivaid** sõlmi.
5. Kasuta oma olemasolevaid otspunkti ohuavastuse ja reageerimise (EDR) vahendeid, et **agente jooksutada**.
6. Vii läbi oma tarkvara objektikoodi staatiline skaneerimine.
7. Vii läbi oma rakenduste ja teekide staatiline skaneerimine.
8. Vii läbi oma rakenduste ja teekide dünaamiline skaneerimine.
9. Vii läbi püsivara staatiline analüüs.

B.3.4 Olemasolevad töövahendid CADI jaoks

B.3.4.1 Omanditarkvara

Allikas [77] annab ülevaate CADI-töövahendite turust. Ta toob välja tähelepaneku, et **CADI-töövahendite valdkond on veel üpris ebaküps ja arenemises**. Üldiselt näib nende töövahendite hinnastamine sõltuvat hangitud funktsionaalsusest ja edaspidise pakkujapoolse toe mahust. Mõnede lahenduste ärimudel on „tarkvara teenusena“ (*software as a service*).

Viidatud allikas otsib vastuseid järgmistele uurimisküsimustele:

1. Mis on ühe CADI-töövahendi minimaalne töötav toode (*MVP*) ja milline võiks olla ideaalne, lõpetatud toode? Milliseid nõudeid nad peaksid rahuldama?
2. Millises seisus on praegu CADI-töövahendite turg? Millised on pakutavad tooted võrdluses MVP-ga ja ideaalse tootega?
3. Kuidas jõuda MVP-st ideaalse tooteni?

Peale turuanalüüsi tegemist tõdevad autorid, et **enamus pakutavaid lahendusi tuleb idufirmadelt ja informatsioon nende toodete kohta on sageli väga piiratud**. Keeruline on aru saada, mida pakutakse. Autorid hindavad seejärel kolme „parimat“ toodet, aga allika [77] avalik versioon ei sisalda nende toodete nimesid.

Allika [77] kokkuvõtted on järgmised:

- CADI-töövahendid teevad kompromissi täpsuse ja jõupingutuse vahel; eri tooted teevad eri valikud. **Mida rohkem panustada töövahendi ülesseadmisel, seda täpsemad saavad olla tulemused.**
- Olemasolevad **täislahendust pakkuvad omanditooted on kallid** (hinnad võivad ulatuda sadadesse tuhandettesse või isegi miljonitesse eurodesse).

- CADI-töövahendite turg on **orienteeritud vastavuse näitamisele** (põhiliselt PQC kasutust nõudvate regulatsioonidega).
- **Käidutehnoloogia (*operational technology, OT*) jääb infotehnoloogiast maha** nii turvalisuse kui ka CADI-töövahendite olemasolu osas. OT on märksa väiksem turg kui IT, seetõttu on ka äristiimulid väiksemad. Samuti on paljud väljakutsed siiani vastamata.
- **Varahalduse juures üldisemalt on vastamata väljakutseid.** Näiteks, kui organisatsioonid alustavad CADI-töövahendite juurutamisega, siis nad tihti ei tea, kust tegelikult alustama peaks. Neil ei pruugi olla isegi elementaarset arusaamist oma kõige olulisematest varadest.

B.3.4.2 Üldised infoturbevahendid

Nagu ülalpool arutasime, saab üldiste infoturbevahendite abil luua ka hea CADI-võimekuse. Al-lik [77] andmetel plaanivad paljud nende vahendite tarnijad neid vahendeid täiendada krüptograafiliste varade avastamise ja inventeerimise jaoks kasuliku funktsionaalsusega. Sõltuvalt infoturbevahendi liigist võivad need täiendused olla järgmised:

Otspunkti ohutuvastus ja reageerimine (EDR/XDR). EDR/XDR vahendid annavad detailse ülevaate otspunktides toimuvast, sealhulgas protsesside käivitamisest, failipöördustest ja võrguliik- lusest. Kui täiendada nende vahendite käitumisanalüüsi ja telemeetriakogumise funktsionaal- sust krüptograafiliste operatsioonide toimumise (sh. võtmegenereerimine, sertifikaatide kasu- tus, TLSi võtmevahetused) tuvastamisega, on võimalik krüptograafilisi varasid reaajas avastada ja inventeerida.

IT-varade haldus (ITAM). ITAM-süsteemid haldavad tark- ja riistavaraliste varade katalooge. Nen- de kataloogide täiendamine krüptograafiliste varade metaandmetega (näiteks krüptograafiliste algoritmide kasutus, võtmete paiknemine nende elutsükli, sertifikaatide kehtetuks muutumise kuupäevad), annab organisatsioonidele vundamendi CADI jaoks. Kui ITAM-süsteem integreerida varasid avastavate agentide või konfiguratsioonihaldusvahenditega, siis on võimalik krüptograa- filisi varasid jälgida füüsilistes, virtuaalsetes ja pilvekeskkondades.

Sertifikaatide elutsükli haldus (CLM). CLM-vahendid haldavad digitaalseid sertifikaate. Kui kor- releerida sertifikaate nendega seotud privaatvõtmete ja teenustega, siis on võimalik CLM-vahendi abil koostada detailne ja täpne loetelu krüptograafilistest vahenditest.

Konfiguratsioonihalduse andmebaas (CMDB). See andmebaas hoiab IT-taristu ja -teenuste konfiguratsiooniandmeid. Lisades CMDB kirjetele krüptograafiliste varade atribuutide väärtused (nagu näiteks võtme tüüp, algoritmi tugevus, kasutamise kontekst, näiteks TLS või koodisigneer- imine), on võimalik luua infoallikas, millest on leitavad kõik krüptograafilised sõltuvused.

Nõrkuseotsingu tööriistad. Need tööriistad suudavad muuhulgas märgata krüptograafilisi nõr- kusi nagu nõrgad algoritmid, aegunud protokolliversioonid, valesti konfigureeritud sertifikaadid. Lisades neile tööriistadele krüptograafiliste varade aktiivse skaneerimise ja kataloogimise, seda eriti pärandüsteemide jaoks, on organisatsioonidel võimalik luua põhjalik loetelu krüptograafi- listest varadest.

Infotehnoloogiliste teenuste haldus (ITSM). ITSMi raamistikud (näiteks ITIL) korraldavad teenusepäringuid, muudatuste läbiviimist ja intsidentide haldust. Lisades ITSMi protessidele CADI töövood (näiteks nõudes, et enne süsteemidesse muudatuste sisseviimist oleks krüptograafiliste varade loetelu uuendatud) on võimalik hoolitseda selle eest, et krüptograafiliste varade üle peetaks arvet kogu nende elutsükli jooksul.

B.3.4.3 PQC inventuuri tööleht

*PQC Inventory Workbook*³, mille on välja andnud *PQC Coalition*, ei ole iseenesest infotehnoloogiline töövahend CADI jaoks, kuid meie arvates väärib mainimist kui krüptograafiliste varade käsitsi avastamist toetav töövahend, andes ette tabelarvutuse tabeli vormingu, mille alusel inventuuriga alustada. Selle töölehe abil on võimalik

1. identifitseerida, milliseid süsteeme ja varasid tähele panna,
2. varasid prioriteetide järgi kategooriatesse jagada,
3. inventuuri lehte leitud informatsiooniga täita ja
4. uute andmete ja süsteemide identifitseerimisel inventuuriga kogutud informatsiooni uuendada.

Tööleht seletab, mis on nõutud väljade tähendus. Temaga on kaasas inventuuri tulemuse ja visualiseerimise näited, sõnastik ja muudetav konfiguratsioon, mille abil saab määrata rippmenüüde elemente ja andmete visualiseerimise kujundust.

B.3.4.4 IBMi CBOM-tööriistakast

Ülalmainitud IBMi CBOM-koodihoidla⁴ nimetab avatud lähtekoodiga töövahendite komplekti CBOM-kit, mis on arendatud IBM Researchis. See komplekt sisaldab allpoolkirjeldatud vahendeid, mille abil on võimalik läbi viia CBOM vastavuskontrolle ning luua CBOMi andmebaas olemasolevate CBOMide halduseks.

CBOMkit-hyperion. CBOMkit-hyperion⁵ on SonarQube'i⁶ pistikprogramm, mis tuvastab krüptograafiliste varade asukohti analüüsitud lähtekoodis ja genereerib selle põhjal CBOM-e. Programmeerimiskeeltest on toetatud Java ja Python, teekide tugi on kahel Java ja ühel Pythoni krüptoteegil.

CBOMkit-coeus. CBOMkit-coeus⁷ on veebipõhine tarkvara olemasolevate CBOMide visualiseerimiseks ja mitme CBOMi põhjal statistiliste kokkuvõtete genereerimiseks.

CBOMkit-theia. CBOMkit-theia⁸ leiab krüptograafilisi varasid konteinerpakettidest ja kataloogidest ning genereerib nende põhjal CBOM-e.

³<https://pqcc.org/pqcinventory-workbook/>

⁴<https://github.com/IBM/CBOM>

⁵<https://github.com/IBM/sonar-cryptography>

⁶SonarQube on populaarne avatud lähtekoodiga platvorm koodikvaliteedi automaatseks matemaatiliseks analüüsiks.

⁷<https://www.zurich.ibm.com/cbom/>

⁸<https://github.com/IBM/cbomkit-theia>

CBOMkit-action. CBOMkit-action⁹ on GitHubi toiming (*action*), mis etteantud GitHubi koodihoidlat automaatselt CBOMkit-hyperioniga skaneerib.

B.3.4.5 Cryptobom Forge Tool

*Cryptobom Forge Tool*¹⁰ on avatud lähtekoodiga töövahendite kogum, mille abil lugeda CodeQLi¹¹ jooksude loodud Multi-Repository Variant Analysis tegevuste väljundit ja selle põhjal luua CBOM-faile. See tähendab, et igas GitHubi koodihoidlas, kus on lubatud CodeQL funktsionaalsuse kasutamine, saab Cryptobom Forge Tooli abil luua sellele vastava CBOMi.

B.3.4.6 Crypto Bill of Materials tegevus

Crypto Bill of Materials tegevuse¹² hoidla kasutab samuti ära CodeQLi väljundit. Ta instrueerib kasutajat looma GitHubi töövoogu,¹³ mis loob CBOMi.

B.3.4.7 CryptoMon

*CryptoMon*¹⁴ on võrgus kasutatav krüptograafia seiraja. Töövahendit ei loeta veel piisavalt küpsiks, et teda tootmiskeskkonnas kasutada. CryptoMon näitab, kuidas võiks toimuda TLSi analüüs tema võrguliikluse alusel. Ta teeb seda, analüüsides TLSi *hello*-teateid, kogudes sealt krüptograafiliste varade kirjeldusi ja salvestades neid MongoDB andmebaasi.

B.3.4.8 OCS Inventory NG

*OCS Inventory NG*¹⁵ on avatud lähtekoodiga riistvara ja tarkvara haldamise töövahend. Tegemist on ITAM-tööriistaga, mis ilmutatud kujul CADI-t ei toeta. Me nimetame teda siin kui üht näitevahendit, mida on võimalik kohandada nii, et see aitaks ka krüptograafiliste varade inventuuri luua.

B.4 Olemasolev (teadus)kirjandus / Kuidas edasi?

Loetleme siin jaotises kõik allikad, mida oleme käesolevas peatükis toodud analüüsi jaoks kasutama. Järjestame need allikad „kasulikkuse“ järjekorras, nimetades kõigepealt need, mis meile rohkem informatsiooni andsid. Seega on esimesed allikad järgnevas loetelus ka meie peamised soovitusel, mida järgmisena lugeda.

B.4.1 CADiIle fokuseeruvad allikad

Siinses loetelus olevad allikad kirjeldavad ainult krüptograafiliste varade avastamist ja inventuuri, mitte tervet PQCle ülemineku protsessi. Seega on neis avastamise ja inventuuri kohta rohkem detaile.

- *Cryptographic Inventory: Deriving Value Today, Preparing for Tomorrow* [78] on otsustajatele

⁹<https://github.com/PQCA/cbomkit-action>

¹⁰<https://github.com/Santandersecurityresearch/cryptobom-forge>

¹¹CodeQL on GitHubi arendatud koodianalüüsimisvahend, millega saab turvakontrolle automaatselt läbi viia.

¹²<https://github.com/advanced-security/cbom-action>

¹³*Workflow*; konfigureeritav automaatne protsess, mis jooksub hoidlal ühte või enamat tööülesannet.

¹⁴<https://github.com/Santandersecurityresearch/CryptoMon>

¹⁵<https://ocsinventory-ng.org>

(CIO, CTO, CISO) suunatud seletusartikkel. Ta annab ülevaate CADI protsessidest ja seotud mõistetest ärile suunatud vormis.

- *Cryptographic Asset Discovery and Inventory: A market landscape and fit-gap analysis [77]* (hollandi keeles) analüüsib olemasolevat CADI-vahendite turgu ja kirjeldab ka olemasolevate küberkaitsevahendite kasutatavust CADI juures.
- *NIST SP 1800-38B: Migration to Post-Quantum Cryptography: Quantum Readiness [79]* ei kirjelda CADI-t üldiselt, vaid konkreetseid kasutusjuhte, mida NIST koos partnerorganisatsioonidega läbi viinud on. Samuti dokumenteerib see allikas mõtteviise neid konkreetseteid CADI-eksperimente tehes.

B.4.2 Üldised PQCle ülemineku tegevuskavad ja juhised

PQCle ülemineku tegevuskavade ja juhiste seast on siin välja valitud need, mis mainivad CADIt. Järgnev loetelu on allikatest, mille sisu on aruande autorite arvates kasulik ja mida tasub esimesena lugeda:

- *Roadmap for the migration to post-quantum cryptography for the Government of Canada [71]* – täielik teekaart PQCle üleminekuks, mille on välja andnud ühe riigi valitsus.
- *The PQC Migration Handbook [16]* – üldiselt parim allikas kõige PQCle üleminekusse puutuva kohta.
- *Preparing Critical Infrastructure for Post-Quantum Cryptography: Strategies for Transitioning Ahead of Cryptanalytically Relevant Quantum Computing [72]* – suur osa informatsioonist käesolevas peatükis pärineb sellest allikast.
- *Post-Quantum Cryptography (PQC) Migration Roadmap [13]* ja *CYBER; Quantum-Safe Cryptography (QSC); A Repeatable Framework for Quantum-Safe Migrations [14]* – mõlemad allikad annavad hästistruktureeritud üleminekuplaani kirjelduse ühes mõõdetavate sammudega.
- *Migrating Software Systems Toward Post-Quantum Cryptography—A Systematic Literature Review [15]* – selles seletusartiklis on toodud süstemaatiline kirjandusülevaade, s.t. see artikkel on väga sarnane käesoleva peatükiga.

Lisaks neile dokumentidele, mida me oleme käesoleva peatüki allikatena kasutanud, nimetame ka järgmisi, neid pikemalt kommenteerimata:

- *A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography [3]*
- *CYBER; Migration strategies and recommendations to Quantum Safe schemes [73]*
- *A Framework for Migrating to Post-Quantum Cryptography: Security Dependency Analysis and Case Studies [74]*
- *Migration to Quantum-Safe Cryptography: About Making Decisions on When, What and How to Migrate to a Quantum-Safe Situation [80]*
- *Planning for Post-Quantum Cryptography [81]*
- *Quantum-Readiness: Migration to Post-Quantum Cryptography [82]*
- *NSM Cryptographic Recommendations 2025 [83]*
- *Action Plan to a Quantum-Safe Financial Future [84]*
- *Timelines for migration to post-quantum cryptography [75]*
- *Post-Quantum Cryptography: What comes next? [85]*

- *Project Description: Migration to Post-Quantum Cryptography* [86]
- *Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography* [87]

Lisa C Üleminekut toetav inimressurss Eestis

Postkvant-krüptograafia üleminekuks vajab inimesi, kes infosüsteeme tegelikult uuendavad – kes lisavad süsteemidele postkvant-turvaliste algoritmide toe ja kes need süsteemid neid algoritme kasutama konfigureerivad. Infosüsteeme, mida uuendada, on palju ning aeg uuendamiseks on piiratud. Seega on edukaks üleminekuks vaja piisavalt palju sobivate teadmiste ja oskustega inimesi, kes need tööd suudaks etteantud aja jooksul ära teha.

Oma projektiplaanis me nägime ette, et inimressurss on üks olulisi sisendeid üleminekuprotsessidele. Seega tuleb uurida, kui palju meil seda ressursi on ja milliseid on nende inimeste oskused. Oluline on ka teada, milline on Eesti võimekus seda ressursi juurde tekitada.

C.1 Metoodika

Projektiplaanis me püstitasime uurimisküsimuse:

U-4: Milline on postkvant-krüptograafia üleminekut toetada suutev inimeressurss Eestis praegu ja lähematel aastatel?

Meie plaan oli sellele küsimusele leida vastus kahe allika abil. Neist esimene on Krüptograafiliste turbelahenduste hindamisvõime loomise projekti (VÕIME-projekt) esimese etapi aruanne [88]. Selles projekti eesmärk on [88, ptk 1.2.1]

...tekitada arusaamine, kuidas ja millisel moel oleks Eestis võimalik arendada välja teaduslikel alustel baseeruv krüptograafiliste turbelahenduste hindamise võime.

Projekti esimeses etapis kaardistati muuhulgas Eesti krüptograafia valdkonna inimressurss. See kaardistus toimus küll turbelahenduste hindamise ja sertifitseerimise kontekstis, mitte infosüsteemides kasutatavate krüptograafiliste algoritmide uuendamise kontekstis. Mõlema tegevuse jaoks vajalikel oskustel on ilmselt suur ühisosa, mis puudutab eelkõige tähelepanu süsteemi detailidele. Seega võiks tehtud kaardistusest käesolevas projektis kasu olla.

Teine allikas, mida plaanisime kasutada, on vastused meie küsimustele, mille organisatsioonidele laiali saatsime. Küsimustikus puudutasid seda teemat küsimused 15–18. Näeme, et ka need küsimused on vägagi üldised ning ka sõna “krüptograafia” on seal võimalik mõista natuke erinevalt (matemaatiliselt või tehniliselt). Usume aga, et üldisuse tase on õigesti valitud; küsimused süsteemides krüptograafiliste algoritmide vahetamise kogemuse kohta oleks andnud vastused, mida olnuks raske tulevikule üle kanda.

Inimressursi tulemusel tekib tehis:

A-21: Ülevaade Eesti inimressursist, kes on kvantarvutikindlate krüptoalgoritmide kasutuselevõtul spetsialistidena rakendatavad.

Seda tehist kasutame ühe alusena / põhjendusena postkvant-krüptograafia ülemineku teekaardis väljapakutavate tegevustele.

C.2 Tulemused

C.2.1 Olemasolev inimressurss

VÕIME-projektis on leitud, et Eesti ülikoolides ja ettevõtetes töötas 2024. aasta sügisel 26 “krüptograafi”. Siin “krüptograaf” on defineeritud kui [88, ptk 5.2]

inime[ne], kes on olnud vähemalt ühe krüptograafia-alase teadusartikli põhiautor või on tööalaselt tegelenud krüptograafia-alase teadus- ja arendustegevusega.

Neist krüptograafidest viis on välismaalased. Samuti töötab välismaal neli eestlasest krüptograafi [88, ptk 5.1].

Enamus neist 26 (või 21, või 25) inimesest ei ole küll need, kes hakkavad krüptograafilisi algoritme välja vahetama. Küll aga võivad nad juhendada insenere, kes seda teevad. Kahjuks jäi inseneride krüptograafia-alane profileerimine aruande [88] käsitlusalast välja. Samas ei pruukinuks sellest ka meie hinnangutele palju kasu olla — krüptograafiliselt asjatundliku juhendamise olemasolul on insenerilt oodatavad oskused eelkõige süsteemide konfigureerimine ja/või tarkvara refakteerimine.

Usume, et praegusel hetkel olemasolev inimressurss on hea algus postkvant-krüptograafiale üleminekuga alustamiseks. Inimressursi täpsem kaardistus ja kasvatamine (kas koolitamise või sisseostmise teel) peaks aga olema osa teekaardiga ettenähtavatest tegevustest. Teekaardil ja tegevuskavas, mille välja pakume, näeme selliseid tegevusi ette.

C.2.2 Inimressursi kasvatamise võimalused

Kui postkvant-krüptograafiale üleminekuks vajalik inimressurss on suurem kui saadaolev, siis tuleb seda juurde luua. Täiendava inimressursi loomise oluline viis on inimeste harimine. VÕIME-projektis on püütud anda ülevaade krüptograafia-alasest hariduslikest tegevustest Eestis [88, ptk 6.1–6.2]. Siinkohal on oluline eelkõige ülikoolides pakutavate kursuste valik ning ülikoolide (aga miks mitte ka rakenduskõrgkoolide või kutseõppeasutuste) võimekus vajaliku sisuga kursuseid luua ja läbi viia.

Tuvastatakse, et Tartu Ülikooli arvutiteaduse instituudis loetakse ligi kahtkümmet õppeainet, millel on mingi seos krüptograafiaga [88, Lisa A.1]. Krüptograafia-fookus on neist üheksal õppeainel [88, ptk 6.2.2]. Paljud neist kursustest on väikese arvu registreerunud tudengitega [88, Tabel 1], kuid leidub ka masskursusi. Postkvant-krüptograafiale üleminekuga seondub eriti kursuse MTAT.07.017 „Rakenduslik krüptograafia“ teemastik; sellel kursusel on igal aastal olnud u. 30 registreerunut, mis näitab, et kursuse läbiviimiseks sellise arvu tudengitega on meetodid olemas. Asjassepuutuv on ka aruandes [88] kajastamata kursus MTAT.07.015 „Turvalise programmeerimise meetodid“, mille on igal aastal läbinud u. 20 üliõpilast¹.

Ka Tallinna Tehnikaülikoolis loetakse krüptograafiat käsitlevaid õppeaineid [88, Lisa A.2]. Arvuliselt on neid küll vähem kui Tartu Ülikooli õppeaineid, kuid krüptograafia „esimese“ kursuse kuulajaid on pigem rohkem kui Tartus [88, Tabelid 1 ja 2].

Me leiame, et Eesti ülikoolides on piisav võimekus toetada postkvant-krüptograafiale üleminekuks vajaliku inimressursi kasvatamist, töötades välja ja viies läbi sobivate õpieesmärkidega kursuseid. Meie optimismi vähendab küll järgmine tähelepanek [88, ptk 6.1]:

¹Allikas: suhtlus kursust läbi viivate õppejõududega

Mitmed intervjueeritavad mainisid, et ülikoolihariduse käigus ei saa tudengid krüptograafia-alaseks inseneritööks vajalikke kogemusi, [...] Mitmete intervjueeritavate sõnul võiks ülikoolides olla rohkem rakenduslikku krüptograafiat käsitlevaid õppeaineid.

Siiski, me usume et rakenduslikumate krüptograafia-kursuste puudumine on tingitud pigem õppekavade koostajate arusaamast, kuidas kursustest moodustub terviklik õppekava, mitte vastavate kogemustega õppejõudude puudusest. Samuti piirab enamate krüptograafia-alaste kursuste pakkumist praegu neid kursusi võtvate üliõpilaste väike arv [88, ptk 6.2.2]. Seega leiame, et pigem on ülikoolidel vabu ressursse, mida õppetöös rakendada.

Lisa D Riskianalüüs

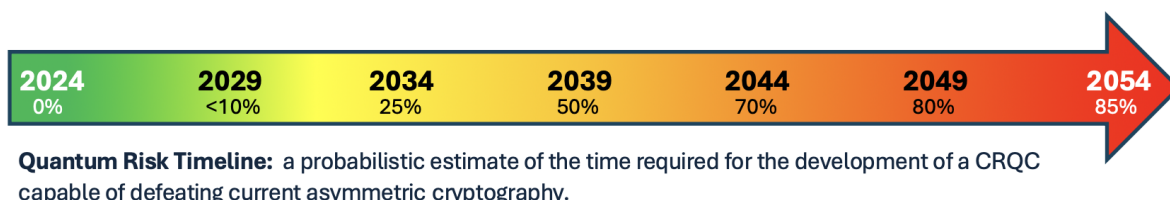
See lisa esitab postkvant-krüptograafia ülelemineku riskianalüüsi. Lisaks esitame ka erinevad riskid, mis kaasnevad üleminekuprotsessi endaga. Riskianalüüs kirjeldab riske nii organisatsioonile enesele kui ka välistele huvirühmadele, k.a laiemale ühiskonnale. Riskianalüüsis on võetud arvesse tehnilisi kahjusid, mis võivad tekkida siis, kui krüptograafiliselt märkimisväärne kvantarvuti on olemas enne seda, kui organisatsiooni infosüsteemid on selle jaoks valmis. Samuti on arvesse võetud koostalitlusvõime langust või mainekahjusid postkvant-krüptograafia ignoreerimisel. Riskianalüüs on koostatud põhiliselt riiklike strateegiate ning organisatsioonide käsitlemise alusel.

Selleks, et määratleda riski tõenäosust ja raskusastet, analüüsime iga organisatsioonide kategooriat eraldi. Nende hinnangute tegemiseks kasutame küsimustiku vastuseid. Lisaks kasutame „tähtaja“ mõõdet, mis näitab riski tõenäosuse ja tagajärje muutumist aja jooksul. Selle mõõtmega jaoks valitud kuupäevad on pärit ELi koordineeritud rakendamise tegevuskavast, mis käsitleb üleminekut postkvant-krüptograafia:

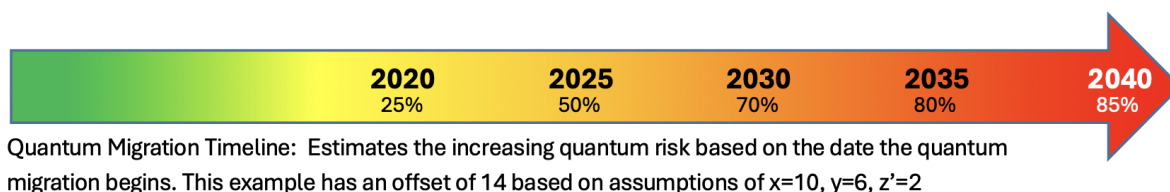
- kõrge riskiga süsteemid tuleks üle viia postkvant-krüptograafia võimalikult kiiresti, kuid mitte hiljem kui 2030. aasta lõpuks;
- 2035. aastaks tuleks üleminek lõpule viia nii paljude süsteemide puhul kui praktiliselt võimalik.

Lisaks kasutame 2028. aastat vahetähtajana enne 2030. aastat. Kuna krüptograafiliselt märkimisväärse kvantarvuti kättesaadavuse tõenäosus kasvab ajas, on selle mõõtmega lisamine riskianalüüsi jaoks oluline.

Kvantriski hindamisel tugineme GRI aruandes [89] esitatud andmetele, mida illustreerivad joonised 13 ja 14.



Joonis 13. Kvantriski ajatelg [89]



Joonis 14. Postkvant-krüptograafia ülelemineku riski ajatelg [89]

Tabel 5 aitab hinnata riski realiseerumise tõenäosust konkreetse infosüsteemi jaoks, võttes aluseks kvantriski (krüptograafiliselt märkimisväärse kvantarvuti) olemasolu tõenäosuse ja ründe sihtmärgiks olemise tõenäosuse. Hinnates tõenäosust, et organisatsioon sattub krüptograafiliselt märkimisväärse kvantarvutiga seotud ründe sihtmärgiks, tuleb arvesse võtta ründe tege-

vuskulusid. On hinnatud, et ühe RSA-2048 võtmepaari ründamise elektritarbimise kulud on suurusjärgus 50 000–100 000 USA dollarit¹. See omakorda tähendab, et kvantrüünded on suurema tõenäosusega suunatud kõige tundlikuma teabega organisatsioonide vastu.

	Kvantriski tõenäosus				
Ründe tõenäosus	Väga väike	Väike	Keskmine	Suur	Väga suur
Väga väike	väga väike	väga väike	väga väike	väga väike	väike
Väike	väga väike	väike	väike	väike	keskmine
Keskmine	väga väike	väike	keskmine	keskmine	suur
Suur	väga väike	väike	keskmine	suur	väga suur
Väga suur	väga väike	väike	keskmine	suur	väga suur

Tabel 5. Tõenäosuste kombinatsioonid

Riskiastmete hindamiseks kasutame tabelit G-5: Hindamisskaala – üldine tõenäosus, kirjeldatud [90].

	Tagajärg				
Tõenäosus	Väga väike	Väike	Keskmine	Suur	Väga suur
Väga väike	väga madal	väga madal	väga madal	madal	madal
Väike	väga madal	madal	madal	madal	keskmine
Keskmine	väga madal	madal	keskmine	keskmine	kõrge
Suur	väga madal	madal	keskmine	kõrge	väga kõrge
Väga suur	väga madal	madal	keskmine	kõrge	väga kõrge

Tabel 6. Riskiastmed

D.1 Uuendatud organisatsioonide kategooriad

Riskituvastusprotsessi käigus avastasime järgnevad põhitunnused, mis mõjutavad organisatsiooni riskitaset.

- Salvestatavate/tööeldavate andmete tundlikkus, mis on positiivses korrelatsioonis tõenäosusega, et organisatsiooni tabab andmeleke. Siinkohal peame silmas nii andmete konfidentsaalsust kui ka manipuleerimiskindlust.
- Organisatsiooni tarnitavate teenuste tähtsus neid ümbritsevale taristule. Siinkohal peame silmas nii seda, kui suur on teenuse kadumise mõju teda ümbritsevale süsteemile kui ka seda, kui suure tähtsusega on vastav süsteem, mis teenusele tugineb.
- Kui palju sõltub organisatsioon teiste organisatsioonide üleminekust postkvant-krüptograafia ehk kui suured on organisatsiooni riskid seoses üleminekuprotsessiga.

Arvestades ülaltoodud tunnuseid, jõudsime järeldusele, et algselt valitud kategooriad, mis on esitatud tehises A-17, ei ole piisavalt head, et nende alusel tegevuskava koostamisega jätkata.

¹<https://postquantum.com/post-quantum/energy-cost-rsa-2048-quantum/>

Algsed kategooriad arvestasid vaid vaadeldavate organisatsioonide antavate teenustega, kuid mitte nende organisatsioonide tähtsusega taristule ning nende organisatsioonide hallatavate andmete tundlikkusega. Järgnevalt pakume välja uued kategooriad, kuhu asetame algselt valitud organisatsioonide tüübid ümber, võttes arvesse nende organisatsioonide vastuseid küsimustikule ning neid organisatsioone ka iseseisvalt analüüsid. Selline kategooriate kohendamine oli ette nähtud ka projektiplaanis.

- **KATEGOORIA I: väga kõrge prioriteediga**

- Organisatsioon käsitleb **tundlikke andmeid**, mis oleksid **väga suure tõenäosusega** potentsiaalse ründaja sihtmärgiks või siis peavad organisatsiooni käsitletavad andmed **püüsimisega veel väga pikalt salajasena**.
- Organisatsioon tarnib **kriitilise tähtsusega või pika elueaga taristut**.
- Kui organisatsiooni tabaks krüptograafiaga seotud rike, võib potentsiaalselt toimuda **laiaulatuslik andmeleke** või mõni **kriitilise tähtsusega teenus lõpetaks toimimise**.
- Organisatsioon **sõltub tugevalt riistvara tarnijatest**.
- Organisatsioon **koostab endale ise oma postkvant-krüptograafia ülemineku teekaardi ning vastutab ise selle teostamise eest**.

- **KATEGOORIA II: kõrge prioriteediga**

- Organisatsioon käsitleb **tundlikke andmeid**, mis oleksid **võrdlemisi suure tõenäosusega** potentsiaalse ründaja sihtmärgiks.
- Kui organisatsiooni tabaks krüptograafiaga seotud rike, võib mõni **oluline põhiteenus lõpetada toimimise**.
- Organisatsioon **vastutab mõne mitte nende poolt koostatud postkvant-krüptograafia ülemineku teekaardi läbiviimise eest**.

- **KATEGOORIA III: keskmise prioriteediga**

- Organisatsioon käsitleb **tundlikke andmeid**, mis oleksid **väiksema tõenäosusega** potentsiaalse ründaja sihtmärgiks.
- Kui organisatsiooni tabaks krüptograafiaga seotud rike, võib mõni **väiksema olulisusega teenus lõpetada toimimise**.
- Organisatsioon **tellib postkvant-krüptograafia üleminekut teenusena sisse**.

- **KATEGOORIA IV: madala prioriteediga**

- Kõik teised organisatsioonid

D.2 Riskid

See peatükk kirjeldab riske, mis kaasnevad hilise üleminekul postkvant-krüptograafia ülemineku ja riskide, mis tulenevad üleminekuprotsessist endast. Peatükk käsitleb allpool määratletud riskide allikaid, võimalikke tagajärgi ning meetmeid, mida riski leevendamiseks rakendada. Riski raskusaste ja esinemise tõenäosus olenevad organisatsiooni kategooriast ja iga riski kirjeldusele järgneb tabel, kus on toodud riski raskusaste ja esinemise tõenäosus kategooriate kaupa. Tuleb märkida, et „Tähtaeg“ toodud aastaarvud aitavad võrrelda riskitasemeid olukorras, kus organisatsioon pole nimetatud tähtajaks jõudnud postkvant-krüptograafia ülemineku üle minna.

Riskide määratlemisel olid aluseks nii olemasolevates allikates [89] käsitletud riskid ja postkvant-krüptograafia teemalistes konverentsiettekannetes² mainitud üleminekuprotsessiga seotud prob-

²<https://publications.tno.nl/publication/34644707/tU5ixGDV/vries-2025-vendors.pdf>

leemid kui ka riskid, mis põhinevad teekaardi koostajate teadmistel ja kogemusel ülemineku teemal. Riskide tuvastamise käigus on arvesse võetud kõiki mõistlikuks peetavaid rünnete allikaid ja ohte.

Risk 1

- **Riskiallikas:** vastane, kellel on ligipääs krüptograafiliselt märkimisväärsele kvantarvutile.
- **Ohud:** vastane on mõnda aega kogunud krüpteeritud andmeid ning kasutab kvantarvutit eelnevalt kogutud andmete dekrüpteerimiseks.
- **Võimalikud tagajärjed:** vastane saab enda valdusesse tundlikku teavet (isikuandmed, äri-saladused jne).
- **Meetmed riski leevendamiseks:** tuleb üle minna postkvant-krüptograafiale enne krüptograafiliselt olilise kvantarvuti ehitamist, et takistada vastasel uute andmete dekrüpteerimist. Et hoida ära *harvest-now-decrypt-later* ründeid, tuleb postkvant-krüptograafiale üle minna võimalikult vara.

Tabel 7. Riski 1 tõenäosus ja raskusaste erinevate organisatsioonide kategooriate puhul

Kategooria	Tähtaeg	Tõenäosus	Raskusaste	Riskihinnang
Kategooria I	2028	väga väike	suur	madal
	2030	väike	väga suur	keskmine
	2035	keskmine	väga suur	kõrge
Kategooria II	2028	väga väike	suur	madal
	2030	väike	suur	madal
	2035	keskmine	väga suur	kõrge
Kategooria III	2028	väga väike	suur	madal
	2030	väike	suur	madal
	2035	keskmine	väga suur	kõrge
Kategooria IV	2028	väga väike	keskmine	väga madal
	2030	väga väike	keskmine	väga madal
	2035	väike	suur	madal

Tabel 7 kirjeldab riski esinemise tõenäosust ning selle raskusastet organisatsioonide kategooriate kaupa. Riski realiseerumise tõenäosus oleneb siin nii krüptograafiliselt märkimisväärse kvantarvuti ehitamise tõenäosusest toodud tähtajaks (2028 – väga väike, 2030 – väike, 2035 – keskmine) kui ka ründe sihtmärgiks olemise tõenäosusest (vt tabel 5). Raskusastme hinnang sõltub organisatsioonide töödeldavate ning salvestatavate andmete iseloomust. Lisaks sellest sõltub raskusastme hinnang sellest, kui kaua organisatsioon postkvant-krüptograafiale üleminekuga viibib ning kui palju krüpteeritud andmeid vastane endale dekrüpteerimiseks on jõudnud kokku koguda.

Risk 2

- **Riskiallikas:** vastane, kellel on ligipääs krüptograafiliselt märkimisväärsele kvantarvutile.
- **Ohud:** vastane muudab olemasolevaid andmeid (näiteks võltsib dokumentidele antud signatuure).
- **Võimalikud tagajärjed:** vastane muudab organisatsiooni andmeid, võltsib tehinguid, lepinguid, dokumente jne. Tagajärjena võivad organisatsiooni pakutavad teenused tõrkuda või katkeda.
- **Meetmed riski leevendamiseks:** tuleb üle minna postkvant-krüptograafiale enne krüptograafiliselt märkimisväärse kvantarvuti ehitamist, et takistada vastasel uute andmete muutmist. Et hoida ära *harvest-now-forge-later* ründeid, tuleb postkvant-krüptograafiale üle minna võimalikult vara.

Sarnaselt eelmise riskiga sõltub selle riski realiseerumise tõenäosus krüptograafiliselt märkimisväärse kvantarvuti ehitamise tõenäosusest konkreetseks tähtajaks (2028 – väga väike, 2030 – väike, 2035 – keskmine) vaid siis, kui risk mõjutab vastavat organisatsioonide kategooriat (vt tabel 5). Raskusaste sõltub organisatsiooni töödeldavate või salvestatavate andmete iseloomust. Riskitasemete kokkuvõte on esitatud tabelis 8.

Tabel 8. Riski 2 tõenäosus ja raskusaste erinevate organisatsioonide kategooriate puhul

Kategooria	Tähtaeg	Tõenäosus	Raskusaste	Riskihinnang
Kategooria I	2028	väga väike	suur	madal
	2030	väike	väga suur	keskmine
	2035	keskmine	väga suur	kõrge
Kategooria II	2028	väga väike	suur	madal
	2030	väike	suur	madal
	2035	keskmine	väga suur	kõrge
Kategooria III	2028	väga väike	suur	madal
	2030	väike	suur	madal
	2035	keskmine	väga suur	kõrge
Kategooria IV	2028	väga väike	keskmine	väga madal
	2030	väga väike	keskmine	väga madal
	2035	väike	suur	madal

Risk 3

- **Riskiallikas:** vastane, kellel on ligipääs krüptograafiliselt märkimisväärsele kvantarvutile.
- **Ohud:** vastane manipuleerib autentimisteavega, et pääseda ligi süsteemi komponentidele ja/või takistada volitatud isikute juurdepääsu süsteemile.
- **Võimalikud tagajärjed:** vastane sooritab organisatsiooni süsteemide või nendes salvestatud andmetega volitamata tegevusi. Volitamata tegevused võivad endaga kaasa tuua andmete paljastamise. Vastane segab organisatsiooni teenuste tööd, keelates ligipääsu süsteemidele, andmetele ja mitmesugustele funktsioonidele.

- **Meetmed riski leevendamiseks:** tuleb üle minna postkvant-krüptograafiaie enne krüptograafiliselt märkimisväärse kvantarvuti ehitamist.

Selle riski puhul ei ole oluline, kas vastane on kogunud enne rünnet krüpteeritud andmeid. See tõttu püsib riski raskusaste sama iga tähtaja puhul. Riski esinemise tõenäosus seevastu suureneb aja möödudes nagu eelnevate riskidegi puhul.

Tabel 9. Riski 3 tõenäosus ja raskusaste erinevate organisatsioonide kategooriate puhul

Kategooria	Tähtaeg	Tõenäosus	Raskusaste	Riskihinnang
Kategooria I	2028	väga väike	väga suur	madal
	2030	väike	väga suur	keskmine
	2035	keskmine	väga suur	kõrge
Kategooria II	2028	väga väike	suur	madal
	2030	väike	suur	madal
	2035	keskmine	suur	keskmine
Kategooria III	2028	väga väike	suur	madal
	2030	väike	suur	madal
	2035	keskmine	suur	keskmine
Kategooria IV	2028	väga väike	keskmine	väga madal
	2030	väga väike	keskmine	madal
	2035	väike	keskmine	madal

Risk 4

- **Riskiallikas:** isik, kes vastutab organisatsiooni postkvant-krüptograafiaie ülemineku planeerimise eest.
- **Ohud:** üleminekukava on koostatud valesti (sisaldab valesid tähtaegu, halbu soovitusi algoritmide valimiseks või ebasobivaid hübriidiseerimismeetodeid); krüptograafiliste varade tuvastamine ja inventeerimine on olnud puudulik.
- **Võimalikud tagajärjed:** organisatsiooni üleminek ei ole kooskõlas olemasolevate normatiivide ja standarditega, mistõttu organisatsioon ei täida neid pärast üleminekut postkvant-krüptograafiaie. Selle tagajärjel võib esineda nii mainekahju kui ka rahalist kahju. Samuti on üks võimalik tagajärg, et organisatsioon ei lähe postkvant-krüptograafiaie õigeks ajaks üle, mistõttu satub see kvantrünnete ohvriks. Krüptograafiliste varade puuduliku tuvastamise ja inventeerimise korral võib juhtuda, et mõni krüptograafiline komponent jääb kahe silma vahele ning muutub seega võimalikuks kvantründe sihtmärgiks.
- **Meetmed riski leevendamiseks:** üleminekukava koostamisel tuleb arvestada olemasolevate normatiivide ja standarditega ning järgida üldist head tava. Tuleb vältida ülemineku protsessiga kiirustamist.

Riski esinemise tõenäosus sõltub üleminekukava eest vastutavate inimeste teadmistest ja pädevustasemetest. Juhul kui üleminekukava töötatakse välja organisatsiooni sees, võib riski realiseerumise tõenäosus kasvada pädevuse puudumise või protsessi suletuse tõttu. Juhul kui üle-

minekukava töötatakse välja organisatsioonist väljaspool, oleneb riski realiseerumise tõenäosus vastavast organisatsioonist. Kui üleminekukava töötab välja organisatsioon, millel on palju postkvant-krüptograafiaga seotud teadmisi ja oskusteavet, on riski esinemise tõenäosus väiksem. Kui organisatsiooni oskusteave on piiratum, on tõenäosus suurem. Samas on organisatsioonist väljaspool välja töötatud üleminekukava puhul organisatsioonil alati vähem võimalust kava valmimisprotsessi mõjutada, mistõttu võivad mõned organisatsioonispetsiifilised detailid jääda märkamata või arvesse võtmata. Seetõttu on riski 4 esinemise tõenäosust siin loetud suuremaks organisatsioonidel, kes sõltuvad oma üleminekukava väljatöötamisel teistest. Riski esinemise tõenäosus siiski väheneb aegamööda, sest ilmneb rohkem asjakohaseid detaile ja probleeme. Riski raskusaste sõltub organisatsiooni töödeldavate ja salvestatavate andmete hulgast ja iseloomust ning krüptograafilise rikke võimalikest tagajärgedest. Riski raskusaste suureneb ajas.

Tabel 10. Riski 4 tõenäosus ja raskusaste erinevate organisatsioonide kategooriate puhul

Kategooria	Tähtaeg	Tõenäosus	Raskusaste	Riskihinnang
Kategooria I	2028	keskmine	suur	keskmine
	2030	väike	väga suur	keskmine
	2035	väike	väga suur	keskmine
Kategooria II	2028	keskmine	suur	keskmine
	2030	väike	suur	madal
	2035	väike	väga suur	keskmine
Kategooria III	2028	keskmine	suur	keskmine
	2030	keskmine	suur	keskmine
	2035	keskmine	väga suur	kõrge
Kategooria IV	2028	keskmine	keskmine	keskmine
	2030	keskmine	keskmine	keskmine
	2035	väike	suur	madal

Risk 5

- **Riskiallikas:** isik, kes vastutab organisatsiooni postkvant-krüptograafia ülemineku läbiviimise eest.
- **Ohud:** postkvant-krüptograafiat on teostatud valesti või seda pole integreeritud õigesti olemasolevate süsteemidega.
- **Võimalikud tagajärjed:** organisatsiooni töö on häiritud, sest süsteemid lõpetavad töö või toimivad valesti. Süsteemid ei tööta kooskõllaliselt teiste postkvant-krüptograafia üle läinud süsteemidega. Teostusvead suurendavad välise vastase ründepinda.
- **Meetmed riski leevendamiseks:** tõsta teadlikkust seoses erinevate murekohtadega, mis postkvant-krüptograafia teostamisel tekkida võivad. Testida uuendatud süsteeme enne nende juurutamist piisaval tasemel. Vältida kiirustamist üleminekuga.

Riski esinemise tõenäosuse hindamisel on siin lähtutud sellest, kui palju sõltub organisatsioon väliste teenuseandjate süsteemidest või süsteemikomponentidest. Juhul kui organisatsioon sõl-

tub välistest teenuseandjatest, on selle riski esinemise tõenäosus suurem, sest organisatsioonil on vähem mõju väliste komponentide integreerimisprotsessi üle.

Tabel 11. Riski 5 tõenäosus ja raskusaste erinevate organisatsioonide kategooriate puhul

Kategooria	Tähtaeg	Tõenäosus	Raskusaste	Riskihinnang
Kategooria I	2028	keskmine	väga suur	kõrge
	2030	keskmine	väga suur	kõrge
	2035	väike	väga suur	keskmine
Kategooria II	2028	keskmine	suur	keskmine
	2030	keskmine	suur	keskmine
	2035	väike	suur	madal
Kategooria III	2028	keskmine	suur	keskmine
	2030	keskmine	suur	keskmine
	2035	keskmine	suur	keskmine
Kategooria IV	2028	keskmine	keskmine	keskmine
	2030	keskmine	keskmine	keskmine
	2035	keskmine	keskmine	keskmine

Risk 6

- **Riski allikas:** krüptograafiat sisaldavate komponentide tarnijad (riistvara ja tarkvara)
- **Ohud:** tarnijate pakutavatel komponentidel puuduvad vajalikud funktsioonid (nt füüsilised turvamoodulid ei toeta standardiseeritud kvantturvalisi algoritme)
- **Võimalikud tagajärjed:** üleminekuprotsess viibib, sest on tarvis leida uusi tarnijaid. Kui komponent on süsteemi integreeritud, kuid ei paku vajalikke funktsioone, kaob koostalitlusvõime.
- **Meetmed riski leevendamiseks:** tuleb saada korralik ülevaade kõigist võimalikest tarnijatest ja defineerida väga selged nõudmised vajalikele komponentidele.

Kuna postkvant-krüptograafia on veel aktiivselt arenev ala, võivad tarnijatel olla erinevad arusaamad klientide vajadustest. Kuna enne NISTi standardite valmimist leidis juba mitmeid versioone ja teostusi standarditud algoritmide, on võimalik, et tarnijate tooted toetavad mõnda varasemat versiooni kliendile vajalikust algoritmist. Näiteks Amazon Web Services alustas Crystals-Kyberi toetamist nende turvakriitilistes teenustes enne, kui avaldati ML-KEMi kirjeldav standard. Seetõttu pidid nad eemaldama Crystals-Kyberi toetuse kõigis teenuse lõppseadmetes ning vahetama selle välja ML-KEMi vastu ³.

Kuna kõik organisatsioonide kategooriad kasutavad ühel või teisel viisil krüptograafilisi lahendusi, siis paratamatult sõltuvad nad ka nende lahenduste tarnijatest. Mõnel juhul võib see tähendada lihtsalt mõne krüptoteegi kasutamist; teisel juhul võidakse sõltuda mõnest teenusest, mis rakendab krüptograafiat ulatuslikumalt. Seetõttu võib eeldada, et riski esinemise tõenäosus

³<https://aws.amazon.com/blogs/security/ml-kem-post-quantum-tls-now-supported-in-aws-kms-acm-and-secrets-manager/>

on sarnane kõikides kategooriates ning väheneb ajapikku. Ainuke erand on väga kõrge prioriteediga organisatsioonid, mis eeldatavasti sõltuvad tarkvaratarnijatest teistest kategooriatest rohkem. Riski raskusaste see-eest erineb kategooriate lõikes olenevalt nii nende organisatsioonide salvestatavate/töödeldavate andmete tundlikkusest kui ka organisatsiooni pakutavate teenuste tähtsusest.

Tabel 12. Riski 6 tõenäosus ja raskusaste erinevate organisatsioonide kategooriate puhul

Kategooria	Tähtaeg	Tõenäosus	Raskusaste	Riskihinnang
Kategooria I	2028	suur	suur	kõrge
	2030	keskmine	suur	keskmine
	2035	keskmine	suur	keskmine
Kategooria II	2028	keskmine	suur	keskmine
	2030	keskmine	suur	keskmine
	2035	väike	suur	madal
Kategooria III	2028	keskmine	keskmine	keskmine
	2030	keskmine	keskmine	keskmine
	2035	väike	keskmine	madal
Kategooria IV	2028	keskmine	keskmine	keskmine
	2030	keskmine	keskmine	keskmine
	2035	väike	suur	madal

Risk 7

- **Riskiallikas:** väline vastane
- **Ohud:** vastane püüab kasutada kõrvalkanali- või muid ründeid postkvant-krüptograafia vastu, proovides omandada salajasi võtmeid.
- **Võimalikud tagajärjed:** selle tagajärjel võib tekkida andmeleke, mille käigus lekivad salajased võtmed ja ründaja kasutab neid, et andmeid dekrüptida ning signatuure võltsida.
- **Meetmed riski leevendamiseks:** postkvant-krüptograafiat tuleks teostada hübriidselt klassikaliste algoritmidega.

Kuna krüptoalgoritmide keerukus on aja jooksul kasvanud, siis on kasvanud ka ründepind kõrvalkanalirünneteks. On võimalik, et valitud krüptoalgoritmi teostus ei ole kaitstud kõrvalkanalirünnete eest või et avastatakse uusi ründeid. See tähendab, et kui kvantturvaline algoritm teostatakse eraldiseisvana, võib vastane leida sellega uuendatud süsteemi vastu ründeid, mis ei kasuta krüptograafiliselt märkimisväärset kvantarvutit.

Tabel 13. Riski 7 tõenäosus ja raskusaste erinevate organisatsioonide kategooriate puhul

Kategooria	Tähtaeg	Tõenäosus	Raskusaste	Riskihinnang
Kategooria I	2028	väga väike	suur	madal
	2030	väike	väga suur	keskmine
	2035	keskmine	väga suur	kõrge
Kategooria II	2028	väga väike	suur	madal
	2030	väike	suur	madal
	2035	keskmine	väga suur	kõrge
Kategooria III	2028	väga väike	suur	madal
	2030	väike	suur	madal
	2035	keskmine	väga suur	kõrge
Kategooria IV	2028	väga väike	keskmine	väga madal
	2030	väga väike	keskmine	väga madal
	2035	väike	suur	madal

Risk 8

- **Riskiallikas:** reguleerivad asutused
- **Ohud:** reguleerivad asutused avaldavad üksteisega vastuolus olevaid normatiive ning organisatsioon peab suutma täita neid kõiki (nt pangandus)
- **Võimalikud tagajärjed:** üleminekuprotsess võib aeglustuda ning viia mõne normatiivi täitmata jäämiseni.
- **Meetmed riski leevendamiseks:** erinevate normatiivide rühmitamine ja prioriteetide määramine. Lisaks võib luua jälgimissüsteemi, mis jälgib reguleerivate asutuste väljastatud uusi normatiive ja juhiseid.

Selle riski esinemise tõenäosus kasvab nende organisatsioonide puhul, kes tegutsevad mitmes riigis või peavad täitma mitmeid erinevaid (krüptograafiat hõlmavaid) normatiive. Erinevad reguleerivad asutused võivad seada erinevaid tähtaegu või siis võivad nende nõuded krüptograafiale olla üksteisega vastuolus. Võib eeldada, et mida tundlikumad on süsteemid või andmed, mida organisatsioon haldab, seda rohkem on erinevad norme, mida organisatsioon peab järgime. Kuna selle põhiline tagajärg on üleminekuprotsessi aeglustumine, siis selle riski raskusaste sõltub organisatsiooni töödeldavate või talletatavate andmete tundlikkusest.

Tabel 14. Riski 8 tõenäosus ja raskusaste erinevate organisatsioonide kategooriate puhul

Kategooria	Tähtaeg	Tõenäosus	Raskusaste	Riskihinnang
Kategooria I	2028	keskmine	suur	keskmine
	2030	keskmine	suur	keskmine
	2035	väike	suur	madal
Kategooria II	2028	keskmine	suur	keskmine
	2030	väike	suur	madal
	2035	väike	suur	madal
Kategooria III	2028	väike	keskmine	madal
	2030	väike	keskmine	madal
	2035	väga väike	keskmine	väga madal
Kategooria IV	2028	väike	keskmine	madal
	2030	väga väike	keskmine	väga madal
	2035	väga väike	keskmine	väga madal