



EUROOPA
KOMISJON

Brüssel, 11.4.2024
C(2024) 2393 final

KOMISJONI SOOVITUS,

11.4.2024,

postkvantkrüptograafiale ülemineku koordineeritud rakendamise tegevuskava kohta

KOMISJONI SOOVITUS,

11.4.2024,

postkvantkrüptograafia ülemineku koordineeritud rakendamise tegevuskava kohta

EUROOPA KOMISJON,

võttes arvesse Euroopa Liidu toimimise lepingut, eriti selle artiklit 292,

võttes arvesse Euroopa Parlamendi ja nõukogu 14. detsembri 2022. aasta direktiivi (EL) 2022/2555, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega muudetakse määrust (EL) nr 910/2014 ja direktiivi (EL) 2018/1972 ning tunnistatakse kehtetuks direktiiv (EL) 2016/1148 (küberturvalisuse 2. direktiiv)¹,

ning arvestades järgmist:

- (1) Andmete kaitsmine ja tundliku side turvalisuse tagamine on liidu ühiskonna, majanduse, julgeoleku ja heaolu jaoks ülioluline. Digiajastule vastava Euroopa² ülesehitamisel on küberturvalisus strateegilise tähtsusega ning ühtlasi on tegemist poliitikaprogrammi „Tee digikümnendisse“³ ühe peamise eesmärgiga.
- (2) Nii ELi julgeolekuliidu strateegias⁴ kui ka ELi küberturvalisuse strateegias⁵ on rõhutatud, et krüpteerimine on kerksuse ja tehnoloogilise suveräänsuse saavutamiseks ning küberrünnete ärahoidmiseks vajaliku tegevussuutlikkuse ülesehitamiseks oluline tehnoloogia. Krüpteerimine on digimaailmas eluliselt tähtis digitaalsete süsteemide ja tehingute turbe, mitmesuguste põhiõiguste kaitse ja kaitsevõime tagamise jaoks. Eri riikide ja eraõiguslike üksuste võidujooks kvantarvutusvõimekuse arendamisel ja uute potentsiaalselt kasulike võimaluste otsimisel seab ohtu praegused krüpteerimisstandardid. Neil standarditel on keskne roll andmete konfidentsiaalsuse ja tervikluse tagamisel, tundliku side kaitsmisel ja võrguturbe oluliste elementide toetamisel.
- (3) Võimalus, et tulevikus arendatakse välja kvantarvutid, mis suudavad praegused krüpteeringud lahti murda, tähendab, et Euroopas on vaja leida tugevamaid kaitsemeetmeid, mis tagaksid tundliku side kaitse ja konfidentsiaalse teabe pikaajalise tervikluse, st vaja on minna võimalikult kiiresti üle postkvantkrüptograafia. Selline uut liiki krüptograafia kõrvaldab praeguse asümmeetrilise krüptograafia teadaolevad nõrkused ja suurendab stabiilsust kvantarvutite kuritahtliku kasutamise põhjustatud ohtude tingimustes.
- (4) Olles tõdenud, et kvantarvutus võib seada ohtu praeguse avaliku võtmega krüptograafia, on komisjon üle kümne aasta rahastanud postkvantkrüptograafia alast teadus- ja arendustegevust.

¹ ELT L 333, 27.12.2022, lk 80.

² COM(2020) 67 final

³ Euroopa Parlamendi ja nõukogu 14. detsembri 2022. aasta otsus (EL) 2022/2481, millega luuakse digikümnendi poliitikaprogramm 2030 (ELT L 323, 19.12.2022, lk 4).

⁴ COM(2020) 605 final.

⁵ JOIN(2020) 18 final.

- (5) Liikmesriigid peaksid kaaluma oma praeguste avaliku halduse digitaristute ja -teenuste ning muu elutähtsa taristu üleviimist postkvantkrüptograafiale niipea kui võimalik, kutsudes sellega esile krüptograafiliste algoritmide, protokollide ja süsteemide põhjaliku muutumise. Nagu rõhutati komisjoni hiljutises valges raamatus „Kuidas rahuldada Euroopa digitaristu vajadusi?“, on selleks vaja koordineeritud jõupingutusi, milles osalevad valitsusasutused, tööstuse sidusrühmad, teadlased ja küberturvalisuse spetsialistid.
- (6) Käesolevas komisjoni soovitusel julgustatakse liikmesriike töötama välja postkvantkrüptograafia kasutuselevõtu terviklik strateegia, et tagada eri liikmesriikide ja nende avaliku sektori asutuste koordineeritud ja sünkroniseeritud üleminek. Strateegias tuleks kindlaks määrata selged eesmärgid, vahe-eesmärgid ja ajakavad, mille tulemusena määratakse kindlaks ühine postkvantkrüptograafia rakendamise tegevuskava. See peaks tooma kogu liidus kaasa postkvantkrüptograafia tehnikate kasutuselevõtu olemasolevates avaliku halduse süsteemides ja elutähtsates taristutes, kasutades selleks hübriidkavasid, milles võib postkvantkrüptograafia ühendada seniste krüptograafiameetoditega või kvantvõtmete jagamisega.
- (7) Tulemusliku postkvantkrüptograafiale ülemineku huvides peaks postkvantkrüptograafia koordineeritud rakendamise tegevuskava sisaldama selliste meetmete loetelu, millega liikmesriigid peavad tegelema, muu hulgas postkvantkrüptograafia algoritmide kaalumise, koos eri etappide selge ajakava ja saavutatavate vahe-eesmärkidega, võttes arvesse nende vastastikust sõltuvust, aga ka kaasatavaid sidusrühmi.
- (8) Postkvantkrüptograafia ühtlustatud rakendamiseks kogu liidus on oluline töötada välja ühised Euroopa standardid ja raamistik, mis võimaldab kindlaks teha ja valida postkvantkrüptograafia algoritme, mis kõikjal liidus digivõrkudes ja -teenustes kasutusele võtta. ELi rahastatavate teadlaste aktiivse osalemise kaudu toetab liit juba praegu selliste postkvantkrüptograafia algoritmide väljatöötamist ja testimist, mida võiks kasutada postkvantkrüptograafia standardite rahvusvahelises valikuprotsessis kandidaatidena. Käesolevas komisjoni soovitusel julgustatakse liikmesriike tegema ELi tasandil tihedat koostööd liidu küberturvalisuse ekspertide, võrgu- ja infoturbe koostöörühma ja Euroopa Liidu Küberturvalisuse Ametiga (ENISA), et hinnata ja valida välja asjakohaseid postkvantkrüptograafia algoritme ning võtta need vastu ELi standarditena, et tagada nende ühtlustatud rakendamine kogu liidus.
- (9) Liikmesriigid ja liit peaksid jätkama postkvantkrüptograafia rahvusvaheliste standardite väljatöötamisel aktiivset koostööd strateegiliste rahvusvaheliste partneritega, et tagada ka edaspidi side koostalitlusvõime.
- (10) Kui liikmesriigid on postkvantkrüptograafia koordineeritud rakendamise tegevuskavas kokku leppinud, tuleks sellest eeskaju võttes määrata kindlaks riiklikud postkvantkrüptograafiale ülemineku kavad, või kui riiklik kava on juba olemas, viia see vastavusse postkvantkrüptograafia koordineeritud rakendamise ühise tegevuskavaga.
- (11) Tagamaks, et käesoleva soovitusel eesmärkide saavutamisel liigutakse edasi, kavatses komisjon tähelepanelikult jälgida soovitusel põhjal võetud meetmeid. Sellise jälgimise tagamiseks julgustatakse seega liikmesriike esitama komisjonile tema taotluse korral kogu asjassepuutuva teabe, mille esitamist neilt võib mõistlikult eeldada. Sel moel saadud teabe ja kogu muu kättesaadava teabe põhjal hindab komisjon käesoleva soovitusel mõju ja otsustab, kas on vaja võtta täiendavaid meetmeid, sealhulgas teha ettepanekuid siduvate liidu õigusaktide vastuvõtmiseks.

- (12) Käesolev postkvantkrüptograafiat käsitlev soovitus tugineb ELi küberturvalisuse strateegias sätestatud poliitikaeesmärkidele parandada haldusasutuste jaoks kasutatavate liidu digitaristute ja -teenuste ning muu elutähtsa taristu läbivat turvet ja kerksust; soovitus toetab digitaalse ühtse turu ja Euroopa majandusjulgeoleku strateegiat käsitleva ühisteatise 10919/23⁶ eesmarke ning selles võetakse arvesse nii riske, mis ohustavad elutähtsa taristu füüsilist ja küberturvalisust, kui ka riske, mis tehti kindlaks kvanttehnoloogia hiljutise riskihindamise käigus⁷. Soovitus austatakse põhiõigusi ja järgitakse eeskätt ELi põhiõiguste hartas (artiklites 7, 8 ja 11) ja Euroopa inimõiguste konventsioonis (artiklites 8 ja 10) tunnustatud põhimõtteid, millest tuleneb valitsuste positiivne kohustus viia ebaseadusliku juurdepääsu ja teabe kontrollimise risk miinimumi, ning see eeldab krüptotehnoloogiate kaitsmist ja edendamist,

ON VASTU VÕTNUD KÄESOLEVA SOOVITUSE:

1. KOHALDAMISALA JA EESMÄRGID

Käesoleva soovituse eesmärk on edendada üleminekut postkvantkrüptograafiale, et kaitsta haldusasutuste kasutatavaid digitaristuid ja -teenuseid ja muud elutähtsat taristut liidus ning anda liikmesriikidele võimalus:

- (1) määrata kindlaks postkvantkrüptograafia koordineeritud rakendamise tegevuskava, mille eesmärk on sünkroniseerida liikmesriikide töö riiklike üleminekukavade kujundamisel ja rakendamisel, tagades samal ajal piiriülese koostalitlusvõime;
- (2) toetada küberturvalisuse ekspertide abiga asjaomaste ELi postkvantkrüptograafia algoritmide hindamist ja väljavalimist ja seejärel selliste algoritmide vastuvõtmist liidu standarditena, mida tuleks kogu liidus postkvantkrüptograafia koordineeritud rakendamise tegevuskava raames rakendada;
- (3) võtta selle ülemineku ettevalmistamiseks asjakohaseid ja proportsionaalseid meetmeid.

2. KOORDINEERITUD RAKENDAMISE TEGEVUSKAVA, MIS KÄSITLEB ÜLEMINEKUT POSTKVANTKRÜPTOGRAAFIALE

- (4) Käesolevas soovitusel julgustatakse liikmesriike koordineerima oma tegevust liidu tasandil liikmesriikide sellekohase foorumi kaudu. Selleks soovib komisjon liikmesriikidel kasutada liidu tasandil küberturvalisuse valdkonnas olemasolevaid struktuure ning luua võrgu- ja infoturbe koostöörühma alarühm. Sellesse alarühma võiksid kuuluda riiklike julgeolekuasutuste esindajad ja küberturvalisuse eksperdid eeskätt riiklikest küberturvalisuse asutustest ja ENISAst. Alarühm võib kutsuda oma töös osalema asjaomaste sidusrühmade esindajaid, näiteks avalik-õiguslike organisatsioonide nõuandeorganite, tööstuse, teenuseosutajate ja operaatorite esindajaid, et koguda sisendit ja vahetada teavet haldusasutuste jaoks kasutatavate digitaristute ja -teenuste ja muude elutähtsate taristute postkvantkrüptograafiale ülemineku kohta eri sektorites, koordineerida oma tööd riigi tasandil ning töötada välja postkvantkrüptograafia koordineeritud rakendamise tegevuskava kooskõlas liidu konkurentsieeskirjade ja liidu andmekaitseõigusega.

⁶ <https://data.consilium.europa.eu/doc/document/ST-10919-2023-INIT/et/pdf>

⁷ JOIN(2023) 20 final.

- (5) Postkvantkrüptograafia alarühm peaks kaaluma asjakohaseid, mõjusaid ja proportsionaalseid meetmeid, et määrata kindlaks postkvantkrüptograafia koordineeritud rakendamise tegevuskava ja koordineerida selle väljatöötamist. Postkvantkrüptograafia alarühma julgustatakse pidama arutelusid muude asjaomaste organitega, näiteks Europol, NATO ja teistega, et hoiduda töö dubleerimisest ja tagada ühtne lähenemisviis esilekerkivate probleemide lahendamisele.
- (6) Seda silmas pidades esitatakse liikmesriikidele varsti pärast käesoleva soovitus avaldamist üleskutse luua selline postkvantkrüptograafia alarühm vastavalt komisjoni rakendusotsusele (EL) 2017/179 ja nimetada ekspertidest esindajad, kes peaksid tegema tihedat koostööd komisjoniga ja kellele tuleks teha ülesandeks määrata kindlaks ja töötada välja postkvantkrüptograafia koordineeritud rakendamise tegevuskava.
- (7) Postkvantkrüptograafia koordineeritud rakendamise tegevuskava peaks olema kättesaadav kahe aasta möödumisel käesoleva soovitus avaldamisest ning pärast seda töötatakse välja individuaalsete liikmesriikide postkvantkrüptograafia ülemineku kavad ja kohandatakse neid vastavalt postkvantkrüptograafia koordineeritud rakendamise tegevuskavas sätestatud põhimõtetele.

3. LIIDU TASANDI MEETMED

- (8) Komisjon jälgib ja hindab üldist tööd regulaarselt koostöös liikmesriikide ekspertidest esindajatega.
- (9) Sel eesmärgil võib komisjon paluda liikmesriikide esindajatel esitada kogu asjassepuutuva teabe, mille esitamist võib neilt mõistlikult eeldada, et tagada postkvantkrüptograafia koordineeritud rakendamise tegevuskava koostamisel tehtud edusammude ja meetmete tulemuslikkuse jälgimine.
- (10) Komisjon hindab kavandatud meetmeid ja liikmesriikide esindajate võrgustiku toimimist selle teabe ja kogu muu kättesaadava teabe põhjal ning otsustab, kas on vaja võtta täiendavaid meetmeid, sealhulgas teha ettepanekuid siduvate liidu õigusaktide vastuvõtmiseks.

4. LÄBIVAATAMINE

- (11) Liikmesriigid peaksid tegema komisjoniga koostööd, et hinnata käesoleva soovitusel mõju hiljemalt kolm aastat pärast soovitusel avaldamist ja otsustada, kuidas oleks otstarbekas edasi tegutseda. Hindamisel tuleks arvesse võtta riiklike ekspertide postkvantkrüptograafia alarühma töö tulemusi.

Brüssel, 11.4.2024

*Komisjoni nimel
komisjoni liige
Thierry BRETON*

