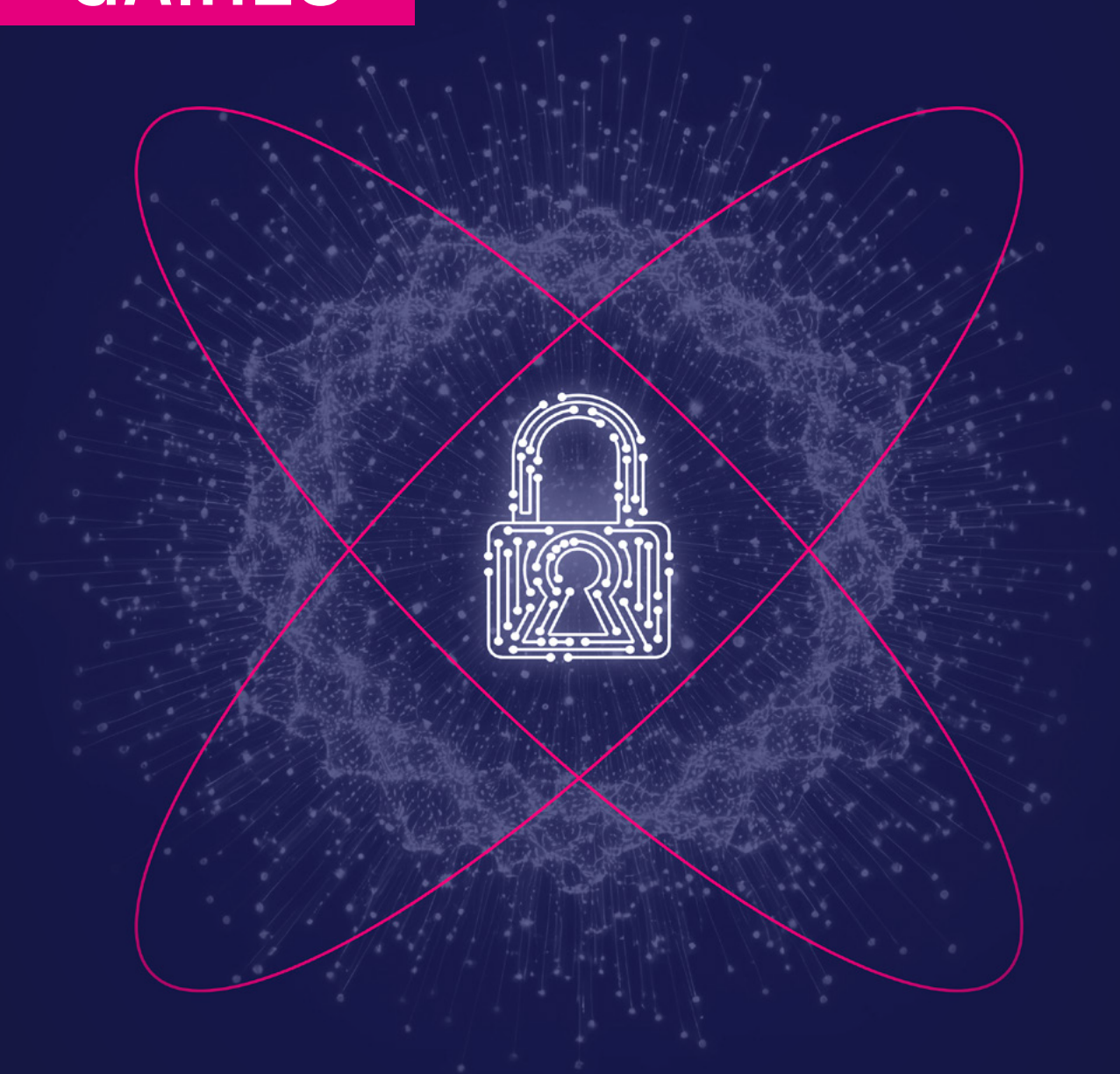
KRAŠTO APSAUGOS
MINISTERIJA

PERĖJIMO PRIE POSTKVANTINĖS KRIPTOGRAFIJOS <GAIRĖS>



Santrauka

Perėjimo prie postkvantinės kriptografijos (angl. post-quantum cryptography, trump. PQC) gairės skirtos padėti kibernetinio saugumo subjektams ir kitoms organizacijoms sistemingai planuoti bei pasirengti šiam perėjimui. Jų tikslas – užtikrinti, kad procesas vyktų sklandžiai, koordinuotai ir nuosekliai, stiprinant organizacijų technologinį bei kibernetinį atsparumą. Gairėse apžvelgiamos pagrindinės kvantinių technologijų keliamos rizikos, nustatomos prioritetinės veiklos sritys ir pateikiami praktiniai žingsniai, padedantys organizacijoms kryptingai pasirengti postkvantiniam laikotarpiui. Kadangi gairės yra rekomendacinio pobūdžio, jose pateiktos priemonės turėtų būti taikomos atsižvelgiant į organizacijos veiklos pobūdį, kibernetinio saugumo brandą, išteklius ir rizikų kontekstą. Ne visos priemonės vienodai tinka visoms organizacijoms – kiekviena jų turėtų pasirinkti tinkamiausius veiksmus pagal savo poreikius.

Gairėse paaiškinama, kaip kvantiniai kompiuteriai keičia tradicinės kriptografijos saugumo prielaidas ir daro esminį poveikį visai kriptografijai, ypač asimetrinei kriptografijai, ir ja pagrįstoms kriptografinėms schemoms, tokioms kaip RSA, Diffie–Hellman ir eliptinių kreivių kriptografija (ECC), bei nuo jų priklausančiam duomenų saugumui ir informacinių sistemų patikimumui.

Jos ragina organizacijas atlikti kriptografijos taikymo inventorizaciją, įvertinti, kurios sistemos yra labiausiai pažeidžiamos, ir nustatyti, kurių duomenų apsauga yra kritiška ilgalaikiam saugumui. Šios gairės pateikia bendrą metodinį pagrindą, o išsamesnės inventorizacijos gairės parengtos atskirai – tai leis organizacijoms giliau įvertinti savo kriptografinių sprendimų būklę ir pasirengimą perėjimui prie postkvantinės kriptografijos.

Remiantis atlikta analize, rekomenduojama nustatyti prioritetus, parengti veiksmų planą ir koordinuoti perėjimą organizacijos mastu, įtraukiant informacinių technologijų, kibernetinio saugumo ir valdymo grandis. Didelis dėmesys skiriamas testavimui ir bandymams – prieš pradedant plataus masto diegimą siūloma išbandyti postkvantinius algoritmus bei mišrius („*hybrid*“) sprendimus, siekiant įsitikinti jų suderinamumu, patikimumu ir veikimo stabilumu. Įgyvendinus sprendimus, rekomenduojama užtikrinti nuolatinę stebėseną ir priežiūrą, kad perėjimas vyktų nuosekliai, o sistemos liktų saugios ir tarpusavyje suderintos.

Šis dokumentas yra pirminis gairių leidimas, kuris bus toliau tobulinamas ir plečiamas, atsirandant naujai informacijai apie standartizaciją, technologinius sprendimus bei gerąją praktiką. Gairės yra nuolat peržiūrimos ir atnaujinamos, atsižvelgiant į mokslo bei technologijų pažangą, standartizacijos eigą ir naujausias tarptautinių institucijų, tokių kaip JAV Nacionalinis standartų ir technologijų institutas (NIST) ir Tarptautinė standartizacijos organizacija (ISO), rekomendacijas. Rekomenduojama taikyti tik tarptautiniu mastu standartizuotus arba oficialiai standartizavimo procesuose patvirtintus kriptografinius algoritmus, protokolus ir sprendimus, vengiant nuosavų („*custom*“) ar nepatikrintų kriptografinių įgyvendinimų, kurie gali kelti papildomą saugumo riziką.

Perėjimas prie postkvantinės kriptografijos yra strateginis procesas, reikalaujantis ankstyvo planavimo, institucinio koordinavimo ir nuoseklaus įgyvendinimo. Šios gairės suteikia organizacijoms aiškų metodinį pagrindą, kaip vertinti rizikas, planuoti ir įgyvendinti pokyčius, siekiant užtikrinti ilgalaikį duomenų ir paslaugų saugumą kvantinių technologijų eroje. Gairių 3 priede pateikiamos nuorodos į dokumentus, laikomus pagrindiniais metodiniais orientyrais, kuriais organizacijos turėtų vadovautis planuodamos ir įgyvendindamos perėjimą prie postkvantinės kriptografijos. Šie dokumentai padeda nustatyti perėjimo kryptį, įvertinti kriptografinių sprendimų būklę, suplanuoti migracijos etapus ir pasirinkti tinkamus techninius sprendimus.

Turinys

1. Kriptografijos reikšmė ir kvantinių grėsmių poveikis

Kriptografija yra esminis kibernetinio saugumo pagrindas skaitmeninėje valstybėje. Ji užtikrina valstybės ir visų piliečių duomenų apsaugą, pasitikėjimą valstybės teikiamomis skaitmeninėmis paslaugomis ir nacionalinio saugumo stabilumą.

Pagrindiniai kriptografijos tipai apima asimetrinę (viešojo rakto) kriptografiją, simetrinę kriptografiją ir maišos funkcijas bei sudaro pagrindą įvairiems saugumo mechanizmams, taikomiems duomenų konfidencialumui, autentiškumui ir vientisumui užtikrinti.

Duomenų autentiškumui ir vientisumui užtikrinti taip pat plačiai naudojami kriptografiniai pranešimų autentifikavimo mechanizmai (MAC), tokie kaip HMAC (Hash-based Message Authentication Code), grindžiami bendru slaptu raktu ir maišos funkcijomis. Šie mechanizmai taikomi saugaus ryšio protokoluose bei sistemų tarpusavio sąveikoje tais atvejais, kai nereikalingas nepaneigiamumas.

1.1. Kriptografijos tipai

1.1.1. Asimetrinė kriptografija

Asimetrinė kriptografija, dar vadinama viešojo rakto kriptografija, yra pagrįsta dviejų raktų pora – viešuoju ir privačiuoju raktu. Ši technologija leidžia saugiai perduoti informaciją, vykdyti raktų nustatymą bei, naudojant skaitmeninius parašus, užtikrinti duomenų autentiškumą, vientisumą ir nepaneigiamumą.

Pagrindinės asimetrinės kriptografijos funkcijos apima raktų nustatymą, kai dvi šalys sukuria bendrą slaptą raktą, naudojamą tolesniam simetriniam šifravimui, taip pat skaitmeninius parašus, kai duomenų autentiškumas ir vientisumas užtikrinamas pasirašant privačiuoju raktu, o patikrinimas atliekamas viešuoju raktu. Tarp dažniausiai naudojamų klasikinių asimetrinių kriptografinių schemų yra RSA (Rivest–Shamir–Adleman), Diffie–Hellman (DH), eliptinių

kreivių Diffie–Hellman (ECDH) ir eliptinių kreivių skaitmeninio parašo algoritmas (ECDSA). Šios schemos šiuo metu sudaro didžiąją dalį saugaus ryšio internetu, elektroninių paslaugų, elektroninio parašo ir sertifikatų infrastruktūros kriptografinio pagrindo.

1.1.2. Simetrinė kriptografija

Simetrinė kriptografija naudoja tą patį slaptą raktą tiek duomenims užšifruoti, tiek iššifruoti. Tai reiškia, kad abi komunikacijos šalys turi žinoti ir saugoti tą patį raktą, o jo konfidencialumas yra būtina saugumo sąlyga.

Simetrinė kriptografija paprastai naudojama duomenų konfidencialumui užtikrinti tiek perduodant duomenis, tiek juos saugant (pvz., diskuose, duomenų bazėse ar debesijos aplinkoje). Kadangi simetrinė kriptografija yra efektyvesnė už asimetrinę, ji taikoma didelės apimties duomenų šifravimui. Tuo tarpu saugus raktų nustatymas, reikalingas komunikacijos pradžioje, paprastai vykdomas naudojant asimetrinę kriptografiją (pvz., TLS protokoluose).

Plačiausiai naudojamas simetrinis šifras yra AES (Advanced Encryption Standard), tapęs tarptautiniu standartu (FIPS 197). AES veikia su 128 bitų duomenų blokais ir palaiko 128, 192 arba 256 bitų ilgio raktus. Praktikoje AES visada taikomas naudojant konkrečius veikimo režimus, kurie apibrėžia, kaip šifravimas taikomas duomenų srautams. Plačiai naudojami autentifikuoto šifravimo (AEAD) režimai, tokie kaip AES-GCM (Galois/Counter Mode) ir AES-CCM, kurie užtikrina tiek duomenų konfidencialumą, tiek jų autentiškumą ir vientisumą. Kai kuriose sistemose taip pat naudojami kiti simetrinio šifravimo algoritmai, pavyzdžiui, ChaCha20, kuris praktikoje dažniausiai taikomas kartu su Poly1305 kaip autentifikuoto šifravimo (AEAD) mechanizmas.

1.1.3. Maišos funkcijos

Maišos funkcijos (angl. *hash functions*) generuoja fiksuoto ilgio pseudoatsitiktinį rezultatą (maišą) iš bet kokio dydžio įvesties duomenų. Vieni iš pagrindinių jų bruožų yra vienpusis pobūdis, t. y. iš maišos rezultato praktiškai neįmanoma atkurti pradinės informacijos, bei kolizijų atsparumas, reiškiantis, kad labai mažai tikėtina rasti dvi skirtingas įvestis, duodančias tą pačią maišą.

Praktikoje maišos funkcijos plačiai naudojamos duomenų vientisumui užtikrinti ir yra esminė sudedamoji dalis įvairiuose kriptografiniuose mechanizmuose ir protokoluose, pavyzdžiui, skaitmeniniuose parašuose, raktų išvedimo funkcijose ar saugaus ryšio protokoluose.

Maišos funkcijos gali būti naudojamos be kriptografinio rakto arba kartu su slaptu raktu, pavyzdžiui, HMAC (angl. *Hash-based Message Authentication Code*) atveju, kai jos taikomos duomenų autentiškumui ir vientisumui užtikrinti.

1.1.4. Pranešimų autentifikavimo mechanizmai

Pranešimų autentifikavimo mechanizmai (angl. *Message Authentication Codes*, MAC) yra kriptografiniai mechanizmai, skirti užtikrinti perduodamų duomenų autentiškumą ir vientisumą, naudojant bendrą slaptą raktą. Skirtingai nuo skaitmeninių parašų, MAC mechanizmai neužtikrina nepaneigiamumo, nes tas pats slaptas raktas yra žinomas abiem komunikacijos šalims.

Vienas plačiausiai naudojamų MAC mechanizmų yra HMAC (angl. *Hash-based Message Authentication Code*), kuris grindžiamas saugiomis maišos funkcijomis ir bendru slaptu raktu. HMAC plačiai taikomas įvairiuose kriptografiniuose protokoluose ir sistemų tarpusavio sąveikoje, įskaitant saugaus ryšio protokolus, programų sąsajas (API) ir vidinius sistemų ryšius, kai nereikalingas nepaneigiamumas. MAC mechanizmai, tokie kaip HMAC, atlieka svarbų vaidmenį praktinėje kriptografijoje ir papildo simetrinio šifravimo bei maišos funkcijų taikymą, sudarydami pagrindą saugiems ir efektyviems duomenų mainams.

1.2. Kriptografijos taikymas

Kriptografijos sprendimai taikomi visais duomenų gyvavimo ciklo etapais. Perdavimo metu jie užtikrina komunikacijos ryšių kanalų saugumą ir apsaugą nuo duomenų perėmimo ar pakeitimo. Ramybės būsenoje duomenys saugomi informacinėse sistemose, valstybiniuose registruose, debesijos infrastruktūroje, organizacijų vidinėse duomenų bazėse, atsarginėse kopijose ir kitose saugojimo vietose, kad būtų apsisaugota nuo neteisėtos prieigos ar pakeitimo. Apdorojimo metu kriptografija padeda išlaikyti duomenų konfidencialumą ir vientisumą, ypač tais atvejais, kai tradiciniai apsaugos metodai duomenims „ramybės būsenoje“ ar „perdavimo metu“ yra nepakankami.

Kriptografija yra būtina ir tapatybės valdymui, prieigos kontrolei bei duomenų vientisumo užtikrinimui. Skaitmeniniai parašai, sertifikatai ir tapatybės valdymo sprendimai sudaro pagrindą skaitmeniniam pasitikėjimui. Tačiau kvantinės grėsmės kelia strategines pasekmes. Duomenys, saugomi klasikinėmis kriptografinėmis priemonėmis, tampa pažeidžiami ir gali būti pasiekiami turint pakankamai galingą kvantinį kompiuterį. Kriptografinė infrastruktūra praranda patikimumą, o pasitikėjimas skaitmeninėmis paslaugomis smarkiai mažėja.

1.3. Kriptografijos pažeidžiamumas kvantinėms grėsmėms

Iš šiandien naudojamų kriptografijos tipų strategiškai pažeidžiama laikoma asimetrinė (viešojo rakto) kriptografija. Jos saugumas remiasi matematinėmis problemomis, kurias klasikiniai kompiuteriai šiuo metu sprendžia labai lėtai. Kvantinių kompiuterių plėtra kelia esminę riziką šiuolaikiniams viešojo rakto kriptografiniams algoritmams, nes teoriškai leidžia efektyviai spręsti matematines problemas, kuriomis šie algoritmai grindžiami. Atsiradus pakankamai galingiems kvantiniams kompiuteriams, tai galėtų lemti šių algoritmų saugumo prielaidų nebegaliojimą ir paveikti saugų ryšį bei skaitmeninius parašus. Kitaip tariant, tokioje situacijoje būtų įmanoma efektyviai atkurti privačius raktus iš viešųjų, o tai reikštų, kad saugus ryšys ir skaitmeniniai parašai taptų pažeidžiami.

Tuo tarpu simetriniai algoritmai ir maišos funkcijos iš esmės laikomi atspariais kvantinėms grėsmėms, jei taikomi pakankami raktų ilgiai ir maišos išvesties dydžiai. Pavyzdžiui, siekiant sumažinti kvantinę riziką, AES turėtų būti naudojamas su ne trumpesniais kaip 192 arba 256 bitų raktais, o maišos funkcijų išvesties dydis – ne mažesnis kaip 256 bitai.

Atsižvelgiant į tai, organizacijos turi planuoti perėjimą prie postkvantinių sprendimų asimetrinės kriptografijos atvejais, o simetrinius šifrus ir maišos funkcijas galima bus saugiai naudoti, užtikrinant pakankamą raktų ilgį ir maišos išvesties dydį.

Tikslus vadinamosios „Q dienos“ laikas – momentas, kai kvantinis kompiuteris taps pakankamai galingas pažeisti šiandien plačiai naudojamą kriptografiją, negali būti patikimai prognozuojamas. Nors ekspertų vertinimai svyruoja nuo kelerių metų iki ilgesnio laikotarpio, spartus technologijų vystymasis ir galimi netikėti moksliniai proveržiai reiškia, kad ši rizika gali tapti reali greičiau, nei tikimasi. Esminė problema nėra konkretus metų skaičius, o tai, kad perėjimas prie postkvantinės kriptografijos yra ilgas ir sudėtingas procesas, todėl veikti būtina jau dabar.

Šiuo metu didžiausią grėsmę kelia du kvantiniai algoritmai: Shor’o algoritmas, galintis pažeisti viešojo rakto kriptografiją (RSA, ECDSA, ECDH, DSA, DH), ir Groverio algoritmas, kuris pagreitina atakas prieš simetrinius šifrus ir maišos funkcijas (AES, SHA-1, SHA-2, SHA-3).

Kvantinės grėsmės nėra vien teorinės – jos turi praktinę reikšmę ilgalaikio duomenų saugumo požiūriu. Vienas iš jau šiandien taikomų metodų yra „kaupti dabar, iššifruoti vėliau“ (angl. *harvest now, decrypt later*), kai šifruota jautri informacija sąmoningai kaupiama dabar, numatant jos iššifravimą ateityje, atsiradus pakankamai galingiems kvantiniams kompiuteriams.

Neveikimas arba delsimas pereiti prie kvantiniam atsparumui skirtų kriptografinių priemonių kelia rimtą grėsmę nacionaliniam saugumui, valstybės institucijų patikimumui ir visos valstybės stabilumui. Pakankamai galingas kvantinis kompiuteris gali būti panaudotas pažeisti duomenų konfidencialumą, vientisumą, autentiškumą ir prieinamumą, sukelti duomenų nutekėjimą, veiklos sutrikimus, finansinius nuostolius bei teisinių ar atitikties rizikų (pvz., privatumo reikalavimų pažeidimus, intelektinės nuosavybės praradimą). Tokios grėsmės gali lemti ilgalaikį suinteresuotųjų šalių pasitikėjimo praradimą.

Nors „Q dienos“ laikas nėra tiksliai žinomas, pasirengimą ir planavimą pereiti prie kvantinėms grėsmėms atsparios kriptografijos reikia pradėti kuo anksčiau, kad būtų laiku sumažinta rizika ir užtikrintas organizacijų bei visos valstybės saugumas.

2. Postkvantinė kriptografija

Postkvantinė kriptografija sukurta kaip atsakas į spartų kvantinių kompiuterių vystymąsi ir jų keliamą grėsmę šiuolaikinėms asimetrinės kriptografijos sistemoms.

Postkvantinės kriptografijos tikslas – užtikrinti ilgalaikį kriptografinių sprendimų saugumą ir patikimumą kvantinių kompiuterių eroje, sudarant sąlygas saugiai tęsti skaitmeninių paslaugų, elektroninių ryšių ir informacinių sistemų veikimą. Šiam tikslui pasiekti siekiama palaipsniui pakeisti pažeidžiamą klasikinę viešojo rakto kriptografiją postkvantiniais sprendimais, išlaikant suderinamumą su esama skaitmenine infrastruktūra.

Postkvantinės kriptografijos algoritmai kuriami taip, kad būtų atsparūs tiek klasikiniams, tiek kvantiniams kriptografiniams iššūkiams, pavyzdžiui, Shor'o algoritmui, kuris kelia esminę grėsmę klasikiniams asimetriniams kriptografiniams metodams. Simetrinių algoritmų saugumo vertinime taip pat įvertinamas Groverio algoritmo poveikis, kuris mažina efektyvų saugumo lygį, todėl jų saugumui palaikyti taikomi didesni raktų ar kitų saugumo parametrų dydžiai.

Postkvantinė kriptografija pakeis pažeidžiamas viešojo rakto kriptografines schemas, tokias kaip RSA, ECDSA ir Diffie–Hellman, ir leis išlaikyti pagrindinius viešojo rakto kriptografijos taikymo scenarijus.

Postkvantiniai algoritmai gali būti:

- įgyvendinami tiek programinės, tiek techninės įrangos lygyje;
- integruojami į esamą infrastruktūrą ir kriptografines bibliotekas;
- pritaikomi įvairiose veiklos srityse, užtikrinant saugumą ir suderinamumą.

2.1. Postkvantinės kriptografijos standartizavimas

Tarptautiniai standartai ir rekomendacijos sudaro esminį pagrindą pereinant prie postkvantinės kriptografijos. Pagrindinės standartizacijos organizacijos – JAV Nacionalinis standartų ir technologijų institutas (NIST), Europos telekomunikacijų standartizacijos institutas (ETSI) ir Tarptautinė standartizacijos organizacija (ISO) – aktyviai kuria, testuoja ir diegia postkvantinės kriptografijos standartus, siekdamos užtikrinti naujos kartos kriptografinių technologijų

saugumą, suderinamumą ir patikimumą. NIST vadovauja tarptautiniam standartizavimo procesui, vykdydamas atvirą algoritmų vertinimo ir atrankos programą. Šios programos tikslas – atrinkti ir patvirtinti kvantiniams kompiuteriams atsparius algoritmus, kurie taptų tarptautiniu saugumo standartu. NIST rekomendacijos turi lemiamą įtaką tiek nacionalinėms kibernetinio saugumo politikoms, tiek praktiniam algoritmų diegimui įvairiose valstybėse ir sektoriuose.

ETSI plėtoja standartus, skirtus postkvantinės kriptografijos integracijai į telekomunikacijų, finansų ir kitus kritinės infrastruktūros sektorius, užtikrindama Europos saugumo reikalavimų laikymąsi ir skatindama tarpvalstybinį suderinamumą. ISO rengia technines gaires ir standartus, padedančius tiek viešojo, tiek privataus sektoriaus organizacijoms diegti patikimus postkvantinės kriptografijos sprendimus, skatindama vieningą metodinį požiūrį tarptautiniu mastu.

Vadovavimasis šių organizacijų standartais ir rekomendacijomis yra būtinas siekiant užtikrinti, kad perėjimas prie postkvantinės kriptografijos būtų koordinuotas, atitiktų aukščiausius saugumo standartus ir stiprintų atsparumą kvantinėms grėsmėms. Praktikoje tai reiškia, kad organizacijos turėtų diegti tik tarptautiniu mastu standartizuotus arba oficialiuose standartizavimo procesuose patvirtintus postkvantinės kriptografijos algoritmus ir protokolus, taip pat jų įgyvendinimus patikimose, plačiai naudojamose kriptografinėse bibliotekose. Rekomenduojama vengti nuosavų („custom“) ar nepakankamai įvertintų kriptografinių sprendimų, nes net ir teoriškai saugūs algoritmai gali tapti pažeidžiami dėl klaidų įgyvendinime, nesuderinamumo ar nepakankamo tarpusavio sąveikumo.

2024 m., po aštuonerius metus trukusios analizės ir tyrimų, NIST paskelbė pirmuosius tris postkvantinius standartus:

- FIPS 203[1]: ML-KEM, gardelių pagrindu veikiantis rakto kapsuliavimo mechanizmas, paremtas algoritmu *CRYSTALS-Kyber*;
- FIPS 204[2]: ML-DSA, gardelių pagrindu veikiantis skaitmeninio parašo algoritmas, paremtas algoritmu *CRYSTALS-Dilithium*;
- FIPS 205[3]: SLH-DSA, maišos pagrindu veikiantis skaitmeninio parašo standartas be būsenos, paremtas algoritmu *SPHINCS+*.

[1] NIST, *FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM)*, 2024. Nuoroda - Module-Lattice-Based Key-Encapsulation Mechanism Standard
[2] NIST, *FIPS 204: Module-Lattice-Based Digital Signature Algorithm (ML-DSA)*, 2024. Nuoroda - Module-Lattice-Based Digital Signature Standard
[3] *NIST, FIPS 205: Stateless Hash-Based Digital Signature Algorithm (SLH-DSA)*, 2024. Nuoroda - Stateless Hash-Based Digital Signature Standard

Be to, NIST atrinko dar du postkvantinius algoritmus, kurie šiuo metu nėra standartizuoti, tačiau yra numatyti būsimam standartizavimui:

- FALCON[4], gardelių pagrindu veikianti skaitmeninio parašo schema;
- Hamming Quasi-Cyclic[5] (HQC), kodų pagrindu veikiantis rakto kapsuliavimo mechanizmas, numatytas kaip atsarginė *ML-KEM* schema.

2.2. Hibridinis požiūris pereinant prie postkvantinės kriptografijos

Pereinant prie postkvantinės kriptografijos, hibridinis požiūris tampa kertiniu pereinamojo laikotarpio sprendimu, leidžiančiu užtikrinti saugumą, suderinamumą ir paslaugų tęstinumą. Kadangi visiškas perėjimas prie postkvantinės kriptografijos yra sudėtingas, reikalaujantis laiko ir reikšmingų infrastruktūrinių pakeitimų, hibridinis modelis suteikia galimybę valdyti riziką ir palaipsniui diegti naujus algoritmus kartu su esamais.

Hibridinis požiūris į kriptografiją reiškia šiuo metu naudojamų ir postkvantinių algoritmų naudojimą kartu vienoje sistemoje ar procese. Tokiu būdu sukuriamas daugiasluoksnės gynybos (angl. defence-in-depth) principu pagrįstas sprendimas, užtikrinantis, kad net ir paaiškėjus vienos kriptografinės schemos silpnumams, saugumas būtų palaikomas kitos schemos dėka. Pereinamuoju laikotarpiu hibridinis modelis laikytinas rekomenduojamu taikymo būdu, nes jis užtikrina dvisluoksnę apsaugą – tiek klasikinių, tiek postkvantinių algoritmų pagrindu.

Hibridiniai sprendimai taikomi įvairiose kriptografinėse operacijose, tačiau jų praktinis įgyvendinimas priklauso nuo konkretaus taikymo scenarijaus. Hibridinio raktų nustatymo (angl. Hybrid Key Establishment) atveju naudojami keli raktų nustatymo algoritmai, iš kurių išvedamas bendras sesijos raktas. Tokio sprendimo veikimas priklauso nuo saugaus ryšio protokolų palaikymo ir teisingai įgyvendintos sesijos rakto išvedimo logikos.

Hibridinių parašų (angl. Hybrid Signatures) atveju žinutė pasirašoma dviem algoritmais – klasikiniu (pvz., ECDSA) ir postkvantiniu (pvz., ML-DSA) – o gavėjas privalo patikrinti abu

[4] FALCON (Fast Fourier Lattice-based Compact Signatures over NTRU lattices) Nuoroda - CSRC Presentations | CSRC
[5] Hamming Quasi-Cyclic (HQC). Nuoroda - NIST Selects HQC as Fifth Algorithm for Post-Quantum Encryption | NIST

parašus. Šių sprendimų taikymas tiesiogiai priklauso nuo infrastruktūros ir programinės įrangos pasirengimo, įskaitant PKI sistemas, sertifikatų išdavėjus ir galinių įrenginių programinę įrangą, galinčią palaikyti dvigubų parašų tikrinimą.

Hibridiniuose sertifikatuose (angl. Hybrid Certificates) gali būti naudojami keli viešieji raktai ir dvigubi parašai, leidžiantys taikyti tiek klasikinius, tiek postkvantinius autentifikavimo metodus. Tačiau praktinis šių sprendimų taikymas šiuo metu priklauso nuo ekosistemos brandos ir dažnai ribojamas dėl ne visur atnaujintos PKI infrastruktūros, sertifikatų formatų ir protokolų palaikymo.

Šiuo metu aiškiai išskiriami tipiniai ir plačiausiai vertinami hibridiniai deriniai, tokie kaip ECDHE + ML-KEM raktų nustatymui ir ECDSA + ML-DSA skaitmeniniams parašams. Tokie deriniai atitinka NIST rekomendacijas dėl hibridinių diegimų ir laikomi praktiškais bei saugiais pereinamojo laikotarpio sprendimais[6].

Nors hibridinis požiūris leidžia išlaikyti suderinamumą su esamomis sistemomis, jo praktinis įgyvendinimas priklauso nuo technologinės ekosistemos pasirengimo – kriptografinių bibliotekų, protokolų ir infrastruktūros (pvz., PKI, sertifikatų išdavėjų, galinių įrenginių programinės įrangos) atnaujinimo lygio. Dėl to organizacijoms gali tekti atlikti papildomus techninius ir organizacinius pritaikymus, siekiant užtikrinti, kad hibridinės schemos veiktų sklandžiai ir patikimai.

2.3. Klasikinių algoritmų nuoseklus atsisakymas

Pagal NIST IR 8547 parengtą dokumento projektą „Perėjimas prie postkvantinės kriptografijos standartų“[7], šiuo metu pateiktą viešosioms konsultacijoms numatomas nuoseklus perėjimas nuo klasikinių viešojo rakto kriptografinių schemų prie postkvantinių sprendimų, atsižvelgiant į kvantinių kompiuterių keliamą riziką.

Pagal šiame dokumente pateiktas gaires, nuo 2030 metų „*deprecated*“ statusas būtų taikomas toms klasikinėms viešojo rakto kriptografinėms schemoms, kurių saugumo lygis atitinka maždaug 112 bitų klasikinį saugumą, pavyzdžiui, RSA su 2048 bitų raktu. Tai reiškia, kad tokių algoritmų naudojimas dar galėtų būti leidžiamas esamose sistemose, tačiau nebebūtų reko-

[6] Nuoroda - *NIST IR 8547 initial public draft, Transition to Post-Quantum Cryptography Standards*
[7] Nuoroda - *NIST IR 8547 initial public draft, Transition to Post-Quantum Cryptography Standards*

menduojama jų diegti naujose sistemose ar infrastruktūroje. Šiuo laikotarpiu organizacijos turėtų aktyviai planuoti perėjimą prie postkvantinių alternatyvų, o pereinamuoju laikotarpiu gali būti taikomi hibridiniai sprendimai, derinantys klasikinius ir postkvantinius algoritmus, siekiant išlaikyti reikiamą saugumo lygį.

Nuo 2035 metų NIST gairėse numatoma, kad visos kvantiniams kompiuteriams pažeidžiamos viešojo rakto kriptografinės schemos būtų laikomos „*disallowed*“, nepriklausomai nuo raktų dydžio. Tai apimtų tokius algoritmus kaip RSA, ECDSA / EdDSA, Diffie–Hellman ir ECDH, kuriuos reikėtų visiškai pašalinti iš naudojimo ir pakeisti postkvantiniais sprendimais. Šiame etape hibridiniai sprendimai nebebūtų laikomi tinkamais, nes galutinis tikslas yra visiškas perėjimas prie postkvantinių algoritmų, užtikrinančių atsparumą kvantinėms atakoms.

Nuoseklaus atsisakymo politika reiškia, kad praktikos, kurios anksčiau buvo laikomos pakankamai saugiomis, ilgainiui taps nebepriimtinos. Organizacijos turi iš anksto planuoti kriptografinių sprendimų atnaujinimą ir pasirengti laipsniškam perėjimui prie postkvantinės kriptografijos.

2.4. Kriptografijos lankstumas

Pereinant prie postkvantinės kriptografijos, kritiškai svarbu užtikrinti organizacijos gebėjimą greitai reaguoti į kylančias kriptografines grėsmes ir standartų pokyčius. Šiam tikslui būtinas kriptografinis lankstumas (angl. crypto agility) – gebėjimas operatyviai keisti kriptografinius algoritmus, jų parametrus ir protokolus be esminių sistemos pertvarkymų ar paslaugų sutrikdymo.

Kriptografinis lankstumas reiškia, kad kriptografiniai sprendimai gali būti valdomi konfigūracijos lygmeniu. Tai leidžia organizacijoms laipsniškai pereiti prie postkvantinių algoritmų, taikyti hibridinius sprendimus pereinamuoju laikotarpiu ir greitai reaguoti į naujai identifikuotas grėsmes.

Minimalus kriptografinio lankstumo rinkinys turėtų apimti šiuos esminius elementus:

- algoritmų ir protokolų keitimą per konfigūraciją, be reikšmingų programinės įrangos pakeitimų;
- kriptografinių identifikatorių (OID) valdymą, užtikrinant teisingą algoritmų ir sertifikatų atpažinimą keičiantis standartams;

- raktų ilgių ir kitų saugumo parametrų keitimą, leidžiant palaipsniui didinti saugumo lygį;
- HSM ir (ar) TPM palaikymą, užtikrinant saugų raktų generavimą, saugojimą ir atnaujinimą;
- dvigubų (hibridinių) parašų palaikymą, reikalingą pereinamuoju laikotarpiu, kai kartu naudojami klasikiniai ir postkvantiniai algoritmai.

Organizacijos turėtų aiškiai įtvirtinti kriptografinio lankstumo reikalavimus tiekėjų sutartyse ir techninėse specifikacijose. Tiekėjai turi pateikti informaciją apie savo sprendimų pasirengimą keisti algoritmus, palaikyti hibridinius sprendimus, valdyti raktus ir OID, taip pat apie technologinius apribojimus, terminus ir procedūras, reikalingas tokiems pokyčiams įgyvendinti. Tokiu būdu kriptografinis lankstumas tampa esminiu veiksniu, užtikrinančiu, kad organizacijos infrastruktūra išliktų saugi, prisitaikanti ir ilgaamžė net sparčiai keičiantis kriptografiniams standartams ir grėsmių aplinkai.

3. Organizacijų perėjimas prie postkvantinės kriptografijos

3.1. Organizacijų veiksmų plano rengimo prielaidos

Organizacijų veiksmų planas (toliau – Veiksmų planas) turi būti grindžiamas rizikos vertinimu ir skirtas užtikrinti atsparumą tiek esamoms, tiek prognozuojamoms grėsmėms, kylančioms dėl spartaus kvantinių technologijų vystymosi. Ypač svarbu įvertinti „kaupti dabar, iššifruoti vėliau“ scenarijų bei pereinamojo laikotarpio iššūkius, kylančius dėl sudėtingų informacinių sistemų, tokių kaip viešojo rakto infrastruktūra (angl. Public Key Infrastructure, PKI), bei įrenginių, turinčių ilgą gyvavimo ciklą. Tokiose aplinkose postkvantinės kriptografijos diegimas reikalauja kruopštaus planavimo, išsamios rizikos analizės ir gerai koordinuotų veiksmų. Perėjimas prie postkvantinės kriptografijos turi būti įgyvendinamas nuosekliai, sistemiškai, užtikrinant tiek technologinį, tiek organizacinį pasirengimą, taip pat suderinamumą su taikomu reglamentavimu bei tarptautiniais standartais.

Siekiant sklandaus perėjimo, rekomenduojama Veiksmų planą grįsti šiais pagrindiniais etapais:

3.2. Parengiamasis etapas

Parengiamasis etapas sudaro pagrindą koordinuotam ir efektyviam perėjimui prie postkvantinės kriptografijos. Šio etapo tikslas – įvertinti organizacijoje naudojamus kriptografinius sprendimus, priklausomybes nuo trečiųjų šalių bei kvantinių grėsmių rizikas. Tokiu būdu sudaromos prielaidos detaliam postkvantinės kriptografijos diegimo planui parengti ir įgyvendinti.

3.2.1. Projekto komandos sudarymas

Perėjimas prie postkvantinės kriptografijos yra kompleksinis procesas, todėl jis turi būti valdomas kaip projektas. Projekto valdymas užtikrina veiklų koordinaciją, atsakomybės paskirstymą, išteklių planavimą ir rizikų kontrolę, taip pat sudaro prielaidas efektyviam perėjimo plano parengimui ir įgyvendinimui. Parengiamajame etape paskiriamas projekto vadovas, atsakingas už perėjimo prie postkvantinės kriptografijos veiklų organizavimą ir koordinavimą organizacijoje. Projekto komanda turi apimti pagrindines kompetencijų sritis: IT ir kibernetinio saugumo, rizikų valdymą, teisės ir atitikties, IT infrastruktūros administravimą bei tiekėjų valdymą.

3.2.2. Kriptografijos taikymo inventorizacija

Šio veiksmo metu atliekamas išsamus organizacijoje naudojamų kriptografinių sprendimų identifikavimas. Tai apima:

- Kriptografinius algoritmus, kartu su naudojamais kriptografiniais raktais ir jų ilgiais;
- Kriptografinius protokolus;
- Fizines kriptografines priemones;
- Kriptografinių raktų valdymo priemones;
- Skaitmeninius sertifikatus ir skaitmeninius parašus;
- Programines bibliotekas ir kitus komponentus, susijusius su duomenų šifravimu, pasirašymu ar apsauga.

Papildomai turi būti nurodyta kiekvienos priemonės taikymo paskirtis, pavyzdžiui: duomenų perdavimui šifruoti, duomenų saugojimo apsaugai, skaitmeniniam pasirašymui, autentifikavimui ar duomenų apsaugai apdorojimo metu (pvz., naudojant homomorfinį šifravimą ar kitus pažangius metodus).

Taip pat būtina pažymėti kiekvienos priemonės taikymo infrastruktūrinę ir technologinę aplinką, pavyzdžiui:

- Organizacijos vidiniai tinklai;
- Debesijos infrastruktūra (viešoji, privati ar hibridinė);
- Mobiliosios ar žiniatinklio aplikacijos;
- Nuotolinės darbo vietos;
- Integruoti įrenginiai (IoT, daiktų internetas);
- Aplikacijų programavimo sąsajos (API).

Inventorizacijos metu tikslinga iš karto nustatyti, kuriuos komponentus organizacija valdo tiesiogiai, o kurie yra įgyvendinami per trečiųjų šalių įrangą, paslaugas ar programinę įrangą.

Inventorizacija yra procesas, svarbus net tik pereinant prie postkvantinės kriptografijos, tačiau ir priemonė užtikrinti efektyvesnį organizacijos saugumo valdymo procesą, ir padedanti:

- Laiku identifikuoti pažeidžiamumus;
- Valdyti rizikas;
- Užtikrinti atsparumą tiek esamoms, tiek kylančioms grėsmėms, įskaitant kvantines.

3.2.3. Priklausomybės nuo tiekėjų nustatymas

Šis vertinimas yra ypač svarbus tais atvejais, kai organizacija neturi galimybės savarankiškai atnaujinti ar pakeisti kriptografinių sprendimų.

Inventorizacijos duomenys papildomi šia informacija:

- Organizacijos priklausomybės nuo tiekėjų, kai naudojami kriptografiniai sprendimai yra pažeidžiami kvantinėms grėsmėms arba negali būti atnaujinti organizacijos iniciatyva;
- Tiekėjų pasirengimas palaikyti postkvantinės kriptografijos reikalavimus (pvz., paskelbti planai, atnaujinimų grafikai, suderinamumo įsipareigojimai);
- Kiekvieno sprendimo valdymo pobūdis – tiesiogiai organizacijos ar per tiekėjus.

Šiame etape ypač svarbi aktyvi komunikacija su tiekėjais, siekiant:

- Gauti tiksliausią informaciją apie jų planus pereiti prie postkvantinės kriptografijos;
- Suderinti atnaujinimų grafikus ir suderinamumo įsipareigojimus, užtikrinant sklandų perėjimą prie naujų standartų;
- Įvertinti tiekėjų galimybes užtikrinti kriptografinį lankstumą (Crypto-agility), t. y. gebėjimą operatyviai keisti algoritmus ir protokolus pagal kylančias grėsmes ir naujus standartus;
- Aptarti pereinamąjį hibridinį laikotarpį, kai tiek klasikiniai, tiek postkvantiniai algoritmai gali būti naudojami kartu, ir numatyti planus klasikinės kriptografijos palaipsniui pašalinimui.

3.2.4. Rizikų vertinimas ir prioritetų nustatymas

Remiantis inventorizacijos rezultatais, atliekamas kriptografinių sprendimų pažeidžiamumo kvantinių kompiuterių grėsmėms vertinimas ir nustatomi prioritetiniai objektai, kuriems būtina pirmiausia užtikrinti apsaugą nuo kvantinių grėsmių, siekiant, kad ištekliai būtų paskirti ten, kur kvantinių grėsmių poveikis būtų didžiausias.

Vertinant su postkvantine kriptografija susijusią riziką, atsižvelgiama į šiuos kriterijus:

1. Sistemos kritiškumą ir galimą neigiamą poveikį organizacijos veiklai, įskaitant esminių ar kritinių funkcijų vykdymą ir veiklos tęstinumą;
2. Naudojamų kriptografijos sprendimų pažeidžiamumą kvantinių grėsmių atžvilgiu, atsižvelgiant į taikomus kriptografinius algoritmus;
3. Pereinamojo laikotarpio trukmę, t. y. laikotarpį, per kurį organizacija planuoja įdiegti postkvantinės kriptografijos sprendimus; ilgesnis pereinamasis laikotarpis laikomas riziką didinančiu veiksniu ir lemia poreikį ankstesniam planavimui.

Remiantis šiais rizikos vertinimo kriterijais, aukštos kvantinės rizikos sistemomis laikomos ir prioritetinėmis pereiti prie postkvantinės kriptografijos pripažįstamos sistemos, atitinkančios bent vieną iš šių sąlygų:

- sistemos, kurių veiklos sutrikimas ar duomenų praradimas sutrikdytų kibernetinio saugumo subjekto esminių funkcijų vykdymą taip, kad kibernetinio saugumo subjekto veiklos tęstinumas taptų neįmanomas;
- sistemos, kurių veiklos sutrikimas, neteisėta prieiga, duomenų atskleidimas, pakeitimas ar praradimas turėtų neigiamą poveikį Lietuvos Respublikos nacionaliniam saugumui, viešajam saugumui arba valstybės institucijų ir įstaigų funkcijų vykdymui;

- sistemos, kurių veiklos sutrikimas ar jose tvarkomų duomenų saugumo pažeidimas sukeltų arba galėtų sukelti kibernetinio saugumo subjektui teisinę atsakomybę, įskaitant atsakomybę už asmens duomenų apsaugos, finansinių ar sutartinių įsipareigojimų vykdymo ar intelektinės nuosavybės teisių pažeidimus;
- sistemos, kuriose tvarkomų ar saugomų duomenų konfidencialumas teisės aktų nustatyta tvarka turi būti užtikrintas ne trumpesnį kaip 10 metų laikotarpį;
- sistemos, kuriose postkvantinės kriptografijos algoritmų diegimas dėl tinklų ir informacinių sistemų techninių, architektūrinių ar suderinamumo apribojimų truktų ilgiau kaip 8 metus.

Klausimynas, padedantis įsivertinti sistemas pagal šiuos kriterijus, yra pateiktas Gairių 1 priede.

3.2.5. Diegimo plano parengimas

Diegimo planas rengiamas remiantis kriptografinių priemonių inventorizacijos duomenimis, rizikų vertinimo rezultatais, nustatytais prioritetais bei organizacijos strateginiais tikslais. Plane turi būti aiškiai apibrėžti konkretūs veiksmai, atsakomybės, įgyvendinimo etapai, terminai ir reikalingi ištekliai, užtikrinant sklandų ir valdomą perėjimą prie postkvantinės kriptografijos. Planavimas turi būti grindžiamas kriptografinio lankstumo (angl. crypto-agility) principu, užtikrinančiu, kad diegiami sprendimai būtų pritaikomi prie naujų algoritmų, standartų ir kylančių grėsmių be reikšmingų technologinių pakeitimų ar papildomų sąnaudų.

Organizacijos plane turi būti nurodyta:

- kokie kriptografiniai sprendimai, sistemų komponentai ar paslaugos turi būti atnaujinti ar pakeisti;
- įgyvendinimo etapai ir terminai, įskaitant tarpinius etapus (pvz., testavimo, pilotavimo, hibridinių sprendimų taikymo bei visiško perėjimo prie postkvantinės kriptografijos fazes);
- atsakingi asmenys ar padaliniai už kiekvieno veiksmo įgyvendinimą;
- reikalingi techniniai, finansiniai ir žmogiškieji ištekliai;
- suinteresuotųjų šalių įtraukimo būdai (vidaus ir, jei taikytina, išorės);
- plano peržiūros ir atnaujinimo sąlygos, įskaitant reguliarių peržiūrų dažnumą bei kriterijus, kurių pagrindu planas turi būti koreguojamas;
- hibridinių sprendimų taikymo laikotarpis ir taikymo sritis, siekiant užtikrinti apsaugą iki visiško perėjimo prie postkvantinės kriptografijos.

3.2.6. Įrangos ir programinės įrangos gyvavimo ciklo valdymas bei pirkimų reikalavimai

Pereinant prie postkvantinės kriptografijos, būtina atsižvelgti į tai, kad daugumos informacinių technologijų, tinklo ir saugumo įrangos gyvavimo ciklas sudaro nuo 5 iki 15 metų. Tai reiškia, kad šiandien priimami pirkimų sprendimai tiesiogiai lemia organizacijos galimybes įgyvendinti postkvantinius kriptografinius sprendimus ateityje. Neatsižvelgus į šį aspektą, kyla rizika, kad naujai įsigyta infrastruktūra taps kliūtimi perėjimui prie postkvantinės kriptografijos arba pareikalaus neproporcingų papildomų investicijų.
Todėl organizacijos turėtų užtikrinti, kad nuo šių gairių įsigaliojimo visi nauji IT, tinklo ir kibernetinio saugumo sprendimų pirkimai būtų planuojami ir vykdomi vadovaujantis „PQC-ready“ (postkvantinei kriptografijai pasirengusių sprendimų) principu.

„PQC-ready“ principas reiškia, kad įsigyjama įranga, programinė įranga ar paslaugos:

- leidžia įdiegti ir naudoti postkvantinius kriptografinius algoritmus, kai jie tampa taikytini pagal tarptautinius standartus;
- užtikrina kriptografinį lankstumą (crypto-agility), t. y. galimybę keisti algoritmus, jų parametrus ir kriptografinius profilius konfigūracijos lygmeniu, be esminių infrastruktūros pakeitimų;
- palaiko pereinamuosius (hibridinius) sprendimus, leidžiančius kartu naudoti klasikinius ir postkvantinius algoritmus iki visiško perėjimo.

Minimalūs reikalavimai pirkimams, kuriuos organziacijos, turėtų nusimatyti:

- Kriptografinių modulių palaikymas: galimybė naudoti HSM, TPM ar kitus saugius kriptografinius modulius, galinčius palaikyti postkvantinius algoritmus (pvz., ML-KEM, ML-DSA) arba jų integraciją ateityje.
- Konfigūracinis atnaujinimas: galimybė atnaujinti kriptografinius identifikatorius (OID), raktų ilgius, algoritmų rinkinius ir saugumo parametrus konfigūracijos lygmeniu, nekeičiant aparatinės įrangos.
- Tiekėjų įsipareigojimai: aiškiai apibrėžtas tiekėjo įsipareigojimas dėl postkvantinės kriptografijos palaikymo, įskaitant numatomą įgyvendinimo grafiką, technologinius apribojimus ir suderinamumo užtikrinimą.
- Įrodymų pateikimas: mechanizmai, leidžiantys pagrįsti tiekėjo teiginius (pvz., techninės specifikacijos, produktų vystymo gairės, testavimo ar sertifikavimo rezultatai).

Pirkimų ir gyvavimo ciklo planavimo integravimas. Pirkimų reikalavimai turėtų būti tiesiogiai susieti su organizacijos kriptografinių priemonių inventorizacija, rizikų vertinimu ir diegimo planu. Tai leidžia:

- sumažinti riziką ateityje patirti reikšmingas papildomas sąnaudas dėl neplanuoto kriptografinių sprendimų keitimo;
- užtikrinti, kad naujai įsigyjami sprendimai neprieštarautų ilgalaikei perėjimo prie postkvantinės kriptografijos strategijai;
- sudaryti prielaidas nuosekliam ir ekonomiškai pagrįstam perėjimui viso sprendimų gyvavimo ciklo metu.

Detalesni „PQC-ready“ pirkimų reikalavimai, rekomenduojamos formuluotės pirkimų dokumentams ir įrodymų pateikimo pavyzdžiai pateikiami atskirame gairių 2 priede.

Gairių 2 priede pateikiami rekomenduojami klausimai, skirti organizacijoms, planuojančioms įsigyti arba vertinančioms jau naudojamus IT, tinklo ar kibernetinio saugumo sprendimus, siekiant įvertinti jų pasirengimą perėjimui prie postkvantinės kriptografijos.

Priedas skirtas padėti įgyvendinti „PQC-ready“ principą, įvertinti tiekėjų techninį ir organizacinį pasirengimą bei sumažinti riziką įsigyti sprendimus, kurie taps kliūtimi pereinant prie postkvantinės kriptografijos. Organizacijos gali taikyti visą šiame priede pateiktą klausimų rinkinį arba jo dalį, atsižvelgdamos į sprendimo kritiškumą, duomenų ilgaamžiškumo reikalavimus ir planuojamą sprendimo eksploatavimo laikotarpį.

Rekomenduojama dokumentuoti tiekėjų atsakymus ir naudoti juos kaip pagrindą sprendimų palyginimui, rizikų vertinimui ir sutarčių sąlygų formavimui.

3.3. Testavimai ir bandymai

Testavimo ir bandymų etapas yra esminė organizacijos perėjimo prie postkvantinės kriptografijos proceso dalis ir turėtų būti pradėtas kuo anksčiau. Ankstyvas testavimas leidžia laiku identifikuoti rizikas, techninius apribojimus ir sumažinti netikėtumų tikimybę diegimo metu. Šio etapo tikslas – praktiškai įvertinti pasirinktų technologinių sprendimų (tiek postkvantinių, tiek hibridinių) tinkamumą, saugumą, veikimo efektyvumą ir suderinamumą su organizacijos IT infrastruktūra.

Nepriklausomai nuo kriptografinių sprendimų valdymo modelio, organizacija turėtų:

- įgyvendinti pilotinius projektus, leidžiančius praktiškai įvertinti sprendimų tinkamumą ribotoje veiklos srityje;
- dokumentuoti testavimo rezultatus, identifikuoti rizikas ir parengti rekomendacijas tolesniam diegimui organizacijos mastu;
- atnaujinti kriptografinių priemonių valdymo dokumentus ir diegimo planą, atsižvelgiant į testavimo rezultatus ir išmoktas pamokas.

3.3.1. Atvejai, kai kriptografinės priemonės valdomos pačios organizacijos viduje

Kai organizacija pati tiesiogiai diegia, konfigūruoja ar palaiko kriptografines bibliotekas, protokolus ir sistemas, testavimo etapas apima:

- postkvantinių algoritmų integravimo testavimą, siekiant įvertinti jų veikimą kartu su esamomis sistemomis, programine įranga ir duomenų srautais;
- hibridinių sprendimų testavimą, vertinant jų efektyvumą pereinamuoju laikotarpiu ir poveikį našumui bei suderinamumui;
- našumo ir stabilumo testus, įvertinant poveikį sistemų apkrovai, vartotojo patirčiai ir reakcijos laikui;
- saugumo įvertinimą, identifikuojant galimus naujus pažeidžiamumus ar nesuderinamumus su saugumo politika;
- dokumentacijos ir konfigūravimo analizę, užtikrinant aiškų algoritmų diegimo, konfigūravimo ir atnaujinimo procesų valdymą.

3.3.2. Atvejai, kai kriptografinės priemonės įgyvendinamos per trečiąsias šalis

Kai organizacija naudojasi tiekėjų teikiamomis paslaugomis, įranga ar programine įranga, kurioje kriptografinės funkcijos yra integruotos, testavimas apima:

- sąveikos su organizacijos IT sistemomis testavimą, įskaitant integraciją į esamus procesus, užtikrinant, kad tiekėjo sprendimai sklandžiai veiktų ir nesukeltų sutrikimų;
- paslaugų kokybės ir veikimo vertinimą, įskaitant patikimumą, greitaveiką ir saugumą;
- teisinės ir reguliacinės atitikties peržiūrą, ypač susijusią su skaitmeniniu pasirašymu, autentifikavimu ar raktų valdymu;
- sutarčių ir tiekimo grandinės analizę, įvertinant tiekėjų atsakomybes, įsipareigojimus dėl postkvantinės kriptografijos palaikymo ir technologinių atnaujinimų užtikrinimo;
- hibridinių sprendimų veikimo per pereinamąjį laikotarpį patikrinimą, kad pereinamasis laikotarpis būtų saugus ir suderintas su organizacijos IT aplinka.

Testavimo metu taip pat gali būti įvertinti kriptografinio lankstumo (crypto-agility) mechanizmai, siekiant patikrinti gebėjimą operatyviai keisti algoritmus ar protokolus pagal kylančias grėsmes ar naujus standartus.

3.4. Laipsniškas diegimas

Pasirengus postkvantinės kriptografijos diegimo planą ir atlikus technologinių sprendimų testavimą organizacijoje, pereinama prie laipsniško diegimo etapo. Šio etapo tikslas – nuosekliai ir koordinuotai diegti postkvantinės kriptografijos sprendimus realioje veikloje, užtikrinant paslaugų tęstinumą ir saugumą. Diegimo metu gali būti taikomi tiek postkvantiniai sprendimai, tiek pereinamuoju laikotarpiu hibridiniai sprendimai, kai kartu naudojami klasikiniai ir postkvantiniai algoritmai. Pereinamojo hibridinio laikotarpio metu organizacija turi numatyti mechanizmus, kurie užtikrintų saugumą, operatyvumą ir suderinamumą su esamomis sistemomis, kol bus visiškai pereita prie postkvantinių sprendimų.

Diegimo metu turi būti užtikrintas veiklos tęstinumas, todėl svarbu:

- sustiprinti informacinių sistemų stebėseną;
- numatyti incidentų valdymo scenarijus;
- užtikrinti, kad informacinių sistemų administratoriai ir pagalbos komandos galėtų operatyviai reaguoti į trikdžius;
- informuoti paslaugų naudotojus apie galimus pokyčius, ypač jei jie gali paveikti paslaugų teikimą.

Diegimas pradedamas tose srityse, kuriose technologiniai sprendimai jau išbandyti ir pasirengimas užbaigtas. Įgyvendinimas vykdomas pagal nustatytus prioritetus. Jei organizacija naudoja trečiųjų šalių sprendimus – programinę įrangą, infrastruktūrą ar paslaugas – būtina koordinuoti diegimą su tiekėjais.

Kiekvienas diegimo etapas turi būti dokumentuojamas, apibendrinant pasiektus rezultatus, nustatytus iššūkius ir priimtas valdymo priemones. Tai leidžia kaupti žinias, kurios tampa pagrindu tolesniam diegimui visos organizacijos mastu.

Pereinant prie postkvantinės kriptografijos, svarbu nepamiršti suplanuoti ir įgyvendinti laipsnišką klasikinių algoritmų atsisakymą, užtikrinant, kad po perėjimo būtų naudojamos tik standartizuotos ir ištestuotos postkvantinės priemonės, o visos sistemos ir paslaugos nebenaudotų pažeidžiamų algoritmų.

Postkvantinės kriptografijos diegimas laikomas įgyvendintu, kai prioritetiniuose sistemos komponentuose taikomi nauji kriptografiniai sprendimai – pereinamuoju laikotarpiu tai gali būti hibridiniai sprendimai (vienu metu klasikiniai ir postkvantiniai algoritmai), o galutinai – tik postkvantiniai algoritmai – ir tuo pat metu išlaikomi visi saugumo, veiklos tęstinumo ir paslaugų kokybės kriterijai:

- sistemos ir procesai veikia be reikšmingų trikdžių, pagrindinės paslaugos teikiamos įprasta apimtimi ir kokybe;
- saugumo lygis išlieka aukštas arba pagerėja, nėra naujų pažeidžiamumų;
- kriptografinės priemonės tinkamai integruotos į gamybinę aplinką ir suderintos su vidinėmis bei išorinėmis sistemomis;
- organizacijos personalas pasirengęs valdyti ir palaikyti naujus sprendimus;
- dokumentacija ir valdymo procedūros atnaujintos;
- įgyvendinti sprendimai atitinka reguliacinius ir teisės reikalavimus.

3.5. Stebėjimas ir vertinimas

Įdiegus postkvantinės kriptografijos priemones, būtina užtikrinti nuolatinį ir sistemingą jų stebėjimą bei vertinimą. Tai leidžia laiku identifikuoti galimus veiklos trikdžius, saugumo pažeidžiamumus ar technologinius neatitikimus ir garantuoti, kad įdiegta technologija veiktų efektyviai, atitiktų organizacijos saugumo reikalavimus bei užtikrintų paslaugų tęstinumą. Stebėjimo ir vertinimo procesai turi būti nuoseklūs, aiškiai dokumentuoti ir apimti tiek techninius, tiek organizacinius aspektus. Surinkti duomenys ir analitiniai vertinimai yra pagrindas pagrįstiems sprendimams priimti bei esamiems sprendimams laiku koreguoti.

Organizacija turėtų:

- nuolat rinkti techninius veikimo rodiklius, registruoti ir analizuoti incidentus, trikdžius bei jų priežastis;
- greitai reaguoti į saugumo incidentus ir identifikuotus pažeidžiamumus, inicijuoti technologinių priemonių atnaujinimus ir organizacinius koregavimus;
- vertinti diegimo poveikį organizacijos saugumo lygiui ir paslaugų kokybei, atsižvelgiant į vidinius ir išorinius veiksnius;
- reguliariai teikti ataskaitas vadovybei ir suinteresuotosioms šalims;
- nuosekliai dokumentuoti stebėjimo, vertinimo ir adaptacijos veiksmus, sudarant prielaidas gerosios praktikos kaupimui ir diegimui;
- palaikyti aktyvų dialogą su tiekėjais, partneriais ir reguliavimo institucijomis, užtikrinant sprendimų suderinamumą ir dalijantis aktualia informacija;
- užtikrinti nuolatinį darbuotojų mokymą ir kompetencijų tobulinimą valdyti bei palaikyti postkvantinės kriptografijos sprendimus.

Sprendimų adaptavimas yra dinamiškas procesas, leidžiantis organizacijai prisitaikyti prie besikeičiančios technologinės ir saugumo aplinkos. Remiantis surinktais duomenimis ir vertinimų išvadomis, organizacija turi laiku koreguoti technologines priemones, procedūras bei politiką, atsižvelgdama į naujas grėsmes, technologines galimybes ir teisės aktų reikalavimus. Šis procesas užtikrina ilgalaikį postkvantinės kriptografijos sprendimų efektyvumą, prisideda prie organizacijos kibernetinio atsparumo stiprinimo ir mažina saugumo incidentų riziką.

4. Gairių strateginis suderinamumas

Gairės grindžiamos Europos Sąjungos (toliau – ES), nacionaliniais teisės aktais ir strateginiais dokumentais, kurie nustato reikalavimus kibernetiniam saugumui, duomenų apsaugai, skaitmeninių paslaugų patikimumui ir technologijų pažangai. Šie dokumentai tiesiogiai ar netiesiogiai įpareigoja valstybės institucijas, kritinės infrastruktūros valdytojus bei kitus svarbius ūkio subjektus užtikrinti atsparumą kvantinių kompiuterių keliamiems iššūkiams, įskaitant kriptografinių sistemų saugumą.

Gairių rengimo pagrindai:

Europos Komisijos rekomendacija dėl Koordinuoto perėjimo prie postkvantinės kriptografijos[8]. 2024 m. balandžio 11 d. Komisijos rekomendacija (ES) 2024/1101 nustato aiškias gaires valstybėms narėms, kaip koordinuotai ir laiku pasirengti kvantinių kompiuterių keliamiems iššūkiams. Dokumente pabrėžiama būtinybė sistemingai identifikuoti pažeidžiamiausius informacinių technologijų sprendimus bei kuo skubiau pradėti diegti postkvantinius kriptografinius algoritmus. Taip siekiama užtikrinti ilgalaikį valstybės institucijų ir skaitmeninių paslaugų saugumą bei atsparumą.

Europos Komisijos koordinuoto perėjimo prie postkvantinės kriptografijos gairės[9]. 2025 m. birželio 11 d. paskelbtose veiksmų gairėse nustatyti konkretūs žingsniai ir etapai, kuriuos turi įgyvendinti visos ES valstybės narės. Taip pat numatyti pasiekimo rodikliai, padedantys vertinti perėjimo pažangą bei užtikrinti nuoseklų įgyvendinimą visoje ES.

Gairės taip pat prisidės prie kitų svarbių ES ir nacionalinių teisės aktų bei strategijų įgyvendinimo. Šie dokumentai nustato reikalavimus kibernetiniam atsparumui, asmens duomenų apsaugai, skaitmeninių paslaugų saugumui bei technologiniam atsinaujinimui, kuriuos įgyvendinti padės sistemingas postkvantinės kriptografijos diegimas:

Bendrasis duomenų apsaugos reglamentas (BDAR)[10]. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB, įpareigoja užtikrinti fizinių asmenų duomenų konfidencialumą, vientisumą ir prieinamumą. Kriptografija yra esminė šių tikslų įgyvendinimo priemonė.

[8] L_202401101LT.000101.fmx.xml
[9] A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography | Shaping Europe's digital future
[10] L_2016119LT.01000101.xml

Tinklų ir informacinių sistemų direktyva (TIS2)[11]. 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos direktyva (ES) 2022/2555 (TIS2) nustato aukštus kibernetinio saugumo reikalavimus svarbiausiems sektoriams, įpareigodama valstybes nares užtikrinti nuoseklų atsparumo didinimą ir technologinį atnaujinimą, atsižvelgiant į grėsmių pobūdį ir rizikų vertinimą.

Kibernetinio atsparumo aktas[12]. 2024 m. spalio 23 d. Europos Parlamento ir Tarybos reglamentas (ES) 2024/2847 dėl horizontaliųjų kibernetinio saugumo reikalavimų, keliamų produktams su skaitmeniniais elementais, kuriuo iš dalies keičiami reglamentai (ES) Nr. 168/2013 bei (ES) 2019/1020 ir Direktyva (ES) 2020/1828, nustato privalomus kibernetinio saugumo reikalavimus į rinką tiekiamiems produktams su skaitmeniniais elementais. Reglamentuojamas saugumo užtikrinimas viso produkto gyvavimo ciklo metu, įskaitant atsparumą kriptografinių priemonių silpnėjimui ir šifravimo sprendimų patikimumą. Tai sudaro prielaidas ankstyvai postkvantinių sprendimų integracijai į skaitmeninius produktus.

Skaitmeninės tapatybės reglamentas[13] **(eIDAS2)**. 2024 m. balandžio 11 d. Europos Parlamento ir Tarybos reglamentas (ES) 2024/1183, kuriuo iš dalies keičiamas Reglamentas (ES) Nr. 910/2014, kiek tai susiję su Europos skaitmeninės tapatybės sistemos nustatymu, nustato teisinį pagrindą Europos skaitmeninės tapatybės dėklei ir išplečia reglamentavimą paslaugų, būtinų saugiam elektroniniam tapatybės patvirtinimui, elektroniniams parašams, elektroninių dokumentų pristatymui bei kitoms susijusioms funkcijoms. Reglamente pabrėžiama pažangių technologijų, kriptografijos svarba užtikrinant ilgalaikį duomenų apsaugos, autentiškumo ir patikimumo lygį.

Skaitmeninės veiklos atsparumo finansų sektoriuje reglamentas (DORA)[14]. 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos reglamentas (ES) 2022/2554 įpareigoja finansų sektoriaus subjektus užtikrinti veiksmingą informacinių ir ryšių technologijų rizikų valdymą, ypatingą dėmesį skiriant kriptografinių algoritmų atsparumui ir jų pažeidžiamumo mažinimui, siekiant užtikrinti sklandų ir saugų finansinių paslaugų teikimą.

[11] L_2022333LT.01008001.xml
[12] L_202402847LT.000101.fmx.xml
[13] L_202401183LT.000101.fmx.xml
[14] L_2022333LT.01000101.xml

Europos vidaus saugumo strategija (ProtectEU)[15]. 2025 m. balandžio 1 d. Europos Komisijos pristatytoje strategijoje pabrėžiama būtinybė modernizuoti skaitmeninės tapatybės, duomenų perdavimo ir apsaugos technologijas, atsižvelgiant į kvantinės kompiuterijos raidą. Postkvantinės kriptografijos diegimas įvardijamas kaip viena iš esminių priemonių siekiant užtikrinti ES gyventojų skaitmeninių interesų apsaugą ir sustiprinti bendrą atsparumą būsimiems technologiniams iššūkiams.

Lietuvos Respublikos kibernetinio saugumo įstatymas[16]. Įstatymas įpareigoja kibernetinio saugumo subjektus taikyti rizikų valdymu grindžiamas organizacines ir technines saugumo priemones. Patikimos ir technologiškai pažangios kriptografinės priemonės yra viena iš šių reikalavimų dalis, užtikrinanti ilgalaikį atsparumą besikeičiančioms grėsmėms, įskaitant ir kvantinės kompiuterijos keliamus iššūkius.

[15] https://data.consilium.europa.eu/doc/document/ST-7750-2025-INIT/lt/pdf
[16] XII-1428 Lietuvos Respublikos kibernetinio saugumo įstatymas

Perėjimo prie postkvantinės kriptografijos gairių
1 priedas

AUKŠTOS KVANTINĖS RIZIKOS SISTEMŲ ĮSIVERTINIMO KLAUSIMYNAS

55.4.1. sistemų veiklos sutrikimas ar duomenų praradimas sutrikdytų kibernetinio saugumo subjekto esminių funkcijų vykdymą taip, kad kibernetinio saugumo subjekto veiklos tęstinumas taptų neįmanomas

Kontrolinis klausimas

Ar bent vienos organizacijos esminių funkcijų *(t.y. funkcija, dėl kurios įstaiga buvo įsteigta ir kurios nevykdymas reikštų, kad įstaiga nebegali faktiškai vykdyti savo veiklos)* **vykdymas tiesiogiai priklauso nuo informacinių sistemų veikimo ar jose tvarkomų duomenų prieinamumo?** *(Pavyzdžiui, jeigu paslaugas teikianti įstaiga dėl informacinių sistemų sutrikimo negali teikti pagrindinių paslaugų, dėl kurių ji buvo įsteigta)*

☐ Taip ☐ Ne ☐ Iš dalies

Jeigu į šį klausimą atsakoma „Taip“ arba „Iš dalies“, laikoma, kad kriterijus yra tenkinamas.

55.4.2. sistemų veiklos sutrikimas, neteisėta prieiga, duomenų atskleidimas, pakeitimas ar praradimas turėtų neigiamą poveikį Lietuvos Respublikos nacionaliniam saugumui, viešajam saugumui arba valstybės institucijų ir įstaigų funkcijų vykdymui

Kontroliniai klausimai

1. **Ar informacinių sistemų veiklos sutrikimas, neteisėta prieiga prie sistemų ar duomenų, jų atskleidimas, pakeitimas ar praradimas galėtų pakenkti Lietuvos Respublikos nacionalinio saugumo interesams?** *(Pavyzdžiui, tvarkomi duomenys, susiję su gynyba, krizių valdymu, sistemos integruotos su nacionalinio saugumo ar gynybos institucijų sistemomis)*

   ☐ Taip ☐ Ne ☐ Iš dalies

2. **Ar sistemų veiklos sutrikimas ar duomenų praradimas galėtų neigiamai paveikti gyventojų saugumą, sveikatą ar viešąją tvarką?** *(Pavyzdžiui, sutriktų ekstremalių situacijų valdymas; nebūtų laiku suteiktos būtinos viešosios paslaugos)*

3. **Ar informacinių sistemų arba duomenų nepasiekiamumas ar pažeidimas galėtų sutrikdyti valstybės institucijų ar įstaigų funkcijų vykdymą?** *(Pavyzdžiui, sutriktų sprendimų priėmimas ar viešojo administravimo procesai; būtų nepasiekiami bendri registrai)*

   ☐ Taip ☐ Ne ☐ Iš dalies

4. **Ar informacinių sistemų arba duomenų nepasiekiamumas ar pažeidimas galėtų sutrikdyti valstybės institucijų ar įstaigų funkcijų vykdymą?** *(Pavyzdžiui, sutriktų sprendimų priėmimas ar viešojo administravimo procesai; būtų nepasiekiami bendri registrai)*

   ☐ Taip ☐ Ne ☐ Iš dalies

Jeigu bent į vieną iš aukščiau pateiktų klausimų atsakoma „Taip“ arba „Iš dalies“, laikoma, kad kriterijus yra tenkinamas.

55.4.3. sistemų veiklos sutrikimas ar jose tvarkomų duomenų saugumo pažeidimas sukeltų arba galėtų sukelti kibernetinio saugumo subjektui teisinę atsakomybę, įskaitant atsakomybę už asmens duomenų apsaugos, finansinių ar sutartinių įsipareigojimų vykdymo ar intelektinės nuosavybės teisių pažeidimus

Kontroliniai klausimai

1. **Ar organizacijos informacinių sistemų veiklos sutrikimas ar duomenų saugumo pažeidimas galėtų sukelti teisinę atsakomybę pagal teisės aktus, įskaitant asmens duomenų apsaugos ar kitų privalomų reikalavimų pažeidimą?** *(Pavyzdžiui, neteisėtas asmens duomenų atskleidimas; pareiga pranešti priežiūros institucijai; administracinės ar kitos sankcijos)*

   ☐ Taip ☐ Ne ☐ Iš dalies

2. **Ar incidentas galėtų lemti finansinių ar sutartinių įsipareigojimų nevykdymą ar netinkamą vykdymą, įskaitant galimą civilinę atsakomybę?** *(Pavyzdžiui, paslaugų teikimo sutrikimas; delspinigiai, baudos ar žalos atlyginimas; finansinių įsipareigojimų nevykdymas)*

   ☐ Taip ☐ Ne ☐ Iš dalies

Jeigu bent į vieną iš aukščiau pateiktų klausimų atsakoma „Taip“ arba „Iš dalies“, laikoma, kad kriterijus yra tenkinamas.

55.4.4. sistemose jose tvarkomų ar saugomų duomenų konfidencialumas teisės aktų nustatyta tvarka turi būti užtikrintas ne trumpesnį kaip 10 metų laikotarpį

Kontroliniai klausimai

1. **Ar organizacijos informacinėse sistemose tvarkomi ar saugomi duomenys, kurių konfidencialumą pagal teisės aktus privaloma užtikrinti ne trumpesnį kaip 10 metų laikotarpį?** *(Pavyzdžiui, teisės aktų nustatyti ilgalaikiai saugojimo terminai; archyviniai duomenys; registrų ar apskaitos duomenys, kuriems taikomi ilgalaikiai konfidencialumo reikalavimai.)*

   ☐ Taip ☐ Ne ☐ Iš dalies

Jeigu į šį klausimą atsakoma „Taip“ arba „Iš dalies“, laikoma, kad kriterijus yra tenkinamas.

55.4.5. sistemose postkvantinės kriptografijos algoritmų diegimas jose dėl tinklų ir informacinių sistemų techninių, architektūrinių ar suderinamumo apribojimų truktų ilgiau kaip 8 metus

Kontroliniai klausimai

1. **Ar dėl objektyvių techninių, architektūrinių ar suderinamumo apribojimų** *(ne dėl planavimo stokos ar finansinių priežasčių)* **postkvantinės kriptografijos algoritmų diegimas organizacijos tinkluose ir informacinėse sistemose galėtų užtrukti ilgiau kaip 8 metus?** *(Pavyzdžiui: naudojamos ilgalaikės sistemos; priklausomybė nuo trečiųjų šalių sprendimų ir jų atnaujinimo ciklų; ribotos galimybės keisti kriptografinius modulius; sudėtingi sertifikavimo ar akreditavimo procesai.)*

   ☐ Taip ☐ Ne ☐ Iš dalies

Jeigu į šį klausimą atsakoma „Taip“ arba „Iš dalies“, laikoma, kad kriterijus yra tenkinamas.

Perėjimo prie postkvantinės kriptografijos gairių 2 priedas

TIEKĖJŲ PASIRENGIMO POSTKVANTINEI KRIPTOGRAFIJAI VERTINIMO KLAUSIMAI

Pradinis klausimas tiekėjui - **Ar Jūsų siūlomas [produktas / paslauga] šiuo metu palaiko postkvantinius kriptografinius sprendimus arba yra numatytas jų palaikymas per produkto gyvavimo ciklą?** *(Atsižvelgiant į atsakymą, taikoma viena iš toliau pateiktų klausimų grupių)*

A. Atvejis, kai sprendimas jau palaiko postkvantinę kriptografiją

1. Kokie PQC algoritmai yra palaikomi? Kokias konkrečias FIPS versijas palaikote šiandien (203/204/205)? Kokius papildomus algoritmus (pvz., HQC) planuojate palaikyti ateityje ir kokiu grafiku?
2. Ar palaikomas hibridinis režimas (klasikinė kriptografija + PQC) pereinamuoju laikotarpiu?
3. Ar produktas sukurtas laikantis kriptografinio lankstumo (crypto-agility) principo – t. y. ar kriptografinius algoritmus bus galima pakeisti atsiradus poreikiui?
4. Ar PQC funkcijos įeina į standartinį palaikymą? Ar reikalingi mokami moduliai? Ar būtina naujesnė aparatinė įranga?

Papildomi klausimai specialistams, diegiantiems ir užtikrinantiems suderinamumą organizacijoje:

5. Kuriuose protokoluose (TLS 1.3, QUIC, IKEv2, SSH) šiuo metu palaikomi postkvantiniai ar hibridiniai raktų nustatymo mechanizmai (pvz., ML-KEM)? Ar hibridinis režimas (klasikinė + PQC) įgyvendintas pagal draft-ietf-tls-hybrid-design ar kitą dokumentą? Kaip planuojate sekti standartizaciją ir užtikrinti, kad produktas atitiktų galutinius RFC (Request for Comments)?
6. Ar Jūsų CA/sertifikatų grandinės palaiko ML-DSA/SLH-DSA algoritmus? Ar galima naudoti hibridinius/dual key sertifikatus pagal IETF LAMPS, kad pereinamuoju laikotarpiu būtų užtikrintas suderinamumas? Prašome nurodyti naudojamus kriptografinius identifikatorius (OID).
7. Kokiu algoritmu pasirašote programinę įrangą ir atnaujinimus (pvz., LMS/XMSS pagal NIST SP 800-208 arba ML-DSA/SLH-DSA)? Ar šie parašai generuojami ir saugomi Jūsų HSM (FIPS 140-3)? Kaip užtikrinamas jų saugus valdymas ir auditavimas?
8. Ar turite atliktų bandymų rezultatus (pvz., rankos paspaudimo vėlinimą (handshake latency), sertifikatų dydžius, CPU/RAM naudojimą)? Ar žurnalai fiksuoja, kurie algoritmai buvo panaudoti kiekvienam seansui?

B. Atvejis, kai sprendimas jau palaiko postkvantinę kriptografiją

1. Ar turite oficialų planą (roadmap), kada bus įdiegtas PQC palaikymas šiame produkte?
2. Kokie algoritmai bus palaikomi pirmiausiai?
3. Ar planuojate palaikyti hibridinį režimą (klasikinė + PQC) pereinamuoju laikotarpiu?
4. Ar bus laikomasi kriptografinio lankstumo (crypto-agility) principo – t. y. ar kriptografinius algoritmus bus galima pakeisti atsiradus poreikiui?
5. Ar PQC palaikymas bus pasiekiamas per programinį atnaujinimą, ar tik kartu su nauja produkto versija?
6. Ar atnaujinimas bus įtrauktas į standartinį palaikymą, ar reikės papildomai mokėti?
7. Ar numatytas pereinamasis laikotarpis, kad klientai galėtų saugiai migruoti?
8. Ar galėsite įsipareigoti sutartyje, kad šis produktas bus atnaujintas PQC palaikymui per nustatytą laiką?
9. Ar galite užtikrinti, kad klientai, įsigiję produktą dabar, gaus PQC palaikymą be būtinybės pirkti naują licenciją ar įrangą?

Perėjimo prie postkvantinės kriptografijos gairių
3 priedas

PAGRINDINIAI METODINIAI DOKUMENTAI PERĖJIMUI PRIE POSTKVANTINĖS KRIPTOGRAFIJOS

1. **NIST IR 8547 – *Transition to Post-Quantum Cryptography Standards***[17]
   Dokumentas apibrėžia perėjimo prie postkvantinės kriptografijos kryptį, kvantinėms grėsmėms pažeidžiamų viešojo rakto kriptografinių algoritmų statusą (įskaitant „deprecated“ ir „disallowed“ kategorijas), pereinamojo laikotarpio taikymo principus bei hibridinių sprendimų vaidmenį pereinant prie postkvantinių standartų.

2. **NIST SP 1800-38B – *Migration to Post-Quantum Cryptography: Cryptographic Discovery***[18]
   Dokumente pateikiama praktinė metodika, kaip atlikti organizacijoje naudojamų kriptografinių priemonių inventorizaciją, identifikuoti taikomus algoritmus, protokolus, raktų ilgius, sertifikatus, kriptografines bibliotekas ir jų priklausomybes nuo tiekėjų. Dokumentas taip pat padeda įvertinti organizacijos pasirengimo perėjimui lygį.

3. **NIST SP 1800-38C – *Migration to Post-Quantum Cryptography***[19]
   Dokumente pateikiami praktiniai perėjimo prie postkvantinės kriptografijos scenarijai, įgyvendinimo pavyzdžiai ir rekomendacijos, padedančios planuoti, testuoti ir vykdyti migraciją organizacijos mastu, įskaitant pereinamojo laikotarpio sprendimus.

4. **POSTKVANTINIAI KRIPTOGRAFIJOS STANDARTAI:**

   4.1 NIST FIPS 203 – *ML-KEM (CRYSTALS-Kyber)*[20]
   Postkvantinis raktų kapsuliavimo mechanizmo (KEM) standartas, skirtas saugiam raktų nustatymui ir naudojamas kaip postkvantinė alternatyva klasikiniams Diffie–Hellman ir ECDH sprendimams.

   4.1 NIST FIPS 204 – *ML-DSA (CRYSTALS-Dilithium)*[21]
   Gardelių pagrindu veikiantis postkvantinis skaitmeninio parašo algoritmas, skirtas pakeisti klasikinius ECDSA, EdDSA ir RSA parašų sprendimus.

   4.1 NIST FIPS 205 – *SLH-DSA (SPHINCS+)*[22]
   Maišos pagrindu veikiantis postkvantinis skaitmeninio parašo algoritmas be būsenos, skirtas naudoti tais atvejais, kai reikalinga alternatyva gardelių pagrindu veikiantiems parašams.

[17] IR 8547, Transition to Post-Quantum Cryptography Standards | CSRC
[18] SP 1800-38, Migration to Post-Quantum Cryptography: Preparation for Considering the Implementation and Adoption of Quantum Safe Cryptography | CSRC
[19] SP 1800-38, Migration to Post-Quantum Cryptography: Preparation for Considering the Implementation and Adoption of Quantum Safe Cryptography | CSRC
[20] FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard | CSRC
[21] FIPS 204, Module-Lattice-Based Digital Signature Standard | CSRC
[22] FIPS 205, Stateless Hash-Based Digital Signature Standard | CSRC

5. **NIST CSWP 39 – *Considerations for Achieving Cryptographic Agility: Strategiesand Practices***[23]
   Dokumente pateikiamos strateginės ir techninės kriptografinio lankstumo įgyvendinimo gairės, apimančios sistemų architektūrą, kriptografinių komponentų atskyrimą, konfigūruojamumą bei valdymo procesus. Šios rekomendacijos ypač aktualios organizacijoms, planuojančioms perėjimą prie postkvantinės kriptografijos ir siekiančioms sumažinti būsimų kriptografinių pokyčių kaštus bei rizikas.

6. **ETSI TR 103 619 – *Migration strategies and recommendations to Quantum-Safe schemes***[24]
   Dokumente aprašomos postkvantinės kriptografijos migracijos strategijos, pereinamojo laikotarpio sprendimai ir rekomendacijos, skirtos organizacijoms planuojant perėjimą prie kvantinėms grėsmėms atsparių schemų.

7. **ETSI TR 104 016 V1.1.1 – *CYBER; Quantum-Safe Cryptography (QSC); A Repeatable Framework for Quantum-Safe Migrations***[25]
   Dokumente pateikiamas kartotinas (repeatable) perėjimo prie postkvantinės kriptografijos karkasas, leidžiantis struktūruotai planuoti, prioritetizuoti ir valdyti migracijos veiklas organizacijos portfelio ir sistemų lygmeniu.

8. **The PQC Migration Handbook (2 leidimas)**[26]
   Praktinis vadovas, skirtas organizacijoms, ieškančioms detalių, žingsnis po žingsnio paaiškinimų, kaip įgyvendinti perėjimą prie postkvantinės kriptografijos, remiantis NIST ir ETSI metodinėmis gairėmis.

9. **NIST SP 800-208 – *Recommendation for Stateful Hash-Based Signature Schemes***[27]
   Dokumente pateikiamas postkvantinės kriptografijos taikymo kontekstas, įskaitant kvantinių kompiuterių keliamą grėsmę klasikinei viešojo rakto kriptografijai, pereinamojo laikotarpio aspektus bei bendruosius perėjimo prie postkvantinių sprendimų principus. Šis dokumentas naudojamas kaip papildomas metodinis pagrindas kvantinės rizikos pagrindimui ir perėjimo būtinumui argumentuoti.

[23] CSWP 39, Considerations for Achieving Cryptographic Agility: Strategies and Practices | CSRC
[24] TR 103 619 - V1.1.1 - CYBER; Migration strategies and recommendations to Quantum Safe schemes
[25] TR 104 016 - V1.1.1 - CYBER; Quantum-Safe Cryptography (QSC); A Repeatable Framework for Quantum-Safe Migrations
[26] TNO-2024-pqc-en.pdf
[27] SP 800-208, Recommendation for Stateful Hash-Based Signature Schemes | CSRC

10. **NIST SP 800-57 – *Recommendation for Key Management*[28]**
    Dokumente aprašomi kriptografinių raktų ir algoritmų gyvavimo ciklo valdymo principai, įskaitant raktų kūrimą, naudojimą, rotaciją, archyvavimą ir saugų nutraukimą. Šios gairės yra aktualios užtikrinant ilgalaikį postkvantinių kriptografinių sprendimų valdymą ir suderinamumą su kriptografinio lankstumo (crypto-agility) principais.

11. **ENISA – *Post-Quantum Cryptography: Current State and Quantum Mitigation*[29]**
    Ataskaitoje pateikiama Europos Sąjungos institucijų pozicija postkvantinės kriptografijos klausimu, apžvelgiama dabartinė technologinė situacija, kvantinių grėsmių poveikis bei galimos rizikos mažinimo kryptys. Dokumentas naudojamas kaip informacinis kontekstas, papildantis NIST ir ETSI metodines gaires Europos reguliacinėje ir strateginėje aplinkoje.

[28] Key Management | CSRC
[29] https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation

Esant klausimams, pastebėjus neaiškumų ar neatitikimų šiose gairėse, prašome kreiptis el. paštu: pqc@kam.lt

Išleido Lietuvos Respublikos krašto apsaugos ministerija,
Totorių g. 25, LT-01121 Vilnius, www.kam.lt

Maketavo Krašto apsaugos ministerijos bendrųjų reikalų departamento
Vaizdinės informacijos skyrius, Totorių g. 25, LT-01121 Vilnius