Nacionālais kiberdrošības centrs

https://cyber.gov.lv, NIS2@mod.gov.lv, 67335131

KRIPTOGRĀFIJAS VADLĪNIJAS

Šīs kriptogrāfijas vadlīnijas iesaka principus, algoritmus, procedūras un prasības, kas nodrošina datu konfidencialitāti, integritāti, autentiskumu un nenoliedzamību.

Versija 1.1 (+PQC), 17.03.2026

SATURS

1. IZMANTOTIE TERMINI

1.1. Jēdzieni

Termins	Apraksts
Kriptogrāfija	Zinātne par drošas komunikācijas un datu aizsardzības metodēm, izmantojot matemātiskus algoritmus.
Konfidencialitāte	Īpašība, kas nodrošina, ka informācija ir pieejama tikai autorizētām personām.
Integritāte	Īpašība, kas nodrošina, ka dati nav modificēti neautorizēti.
Autentiskums	Īpašība, kas nodrošina, ka identitāte vai avots ir patiess un pārbaudāms.
Nenoliedzamība (*Non-repudiation*)	Īpašība, kas nodrošina, ka darbības autors nevar noliegt savas darbības.
Riska novērtējums	Process, kurā tiek noteikts iespējamo apdraudējuma līmenis (iespējamība x ietekme) un izstrādāti atbilstoši aizsardzības pasākumi, ņemot vērā samērību, izvērtējot sekas riskam iestājoties un IKT resursa vai informācijas sistēmas drošības klasi (apdraudējuma mērogu).
Kriptogrāfiskā elastība	Spēja operatīvi nomainīt kriptogrāfiskos algoritmus un atslēgu parametrus, ņemot vērā tehnoloģisko attīstību un jaunākos standartus.
Post-kvantu kriptogrāfija (PQC)	Kriptogrāfijas algoritmi, kas ir droši pret uzbrukumiem, izmantojot kvantu datorus.
KEM (Key Encapsulation Mechanism)	Atslēgu apmaiņas mehānisms, ko izmanto PQC algoritmos. Nodrošina drošu simetriskās atslēgas izveidi starp pusēm.
Hybrid mode (Hibrīdais režīms)	Kriptogrāfijas režīms, kurā vienlaikus tiek izmantots klasiskās kriptogrāfijas algoritms un PQC algoritms, lai nodrošinātu pārejas drošību. NIST un ENISA to iesaka migrācijas periodā.
Harvest-Now-Decrypt-Later (HNDL)	Uzbrukuma modelis, kurā uzbrucējs šobrīd iegūst šifrētus datus ar mērķi tos atšifrēt nākotnē, izmantojot kvantu datorus. ENISA to piemin kā galveno PQC ieviešanas motivatoru.

1.2. Algoritmi un protokoli

Termins	Apraksts
AES	*Advanced Encryption Standard* – simetrisks šifrēšanas algoritms datu konfidencialitātei. NIST un ENISA to uzskata par drošu arī kvantu "laikmetā" (ar pietiekamu atslēgas garumu, piemēram, AES-256).
DES/3DES	*Data Encryption Standard/Triple DES* – veci simetriskie šifrēšanas algoritmi, kurus mūsdienās uzskata par nedrošiem.
SHA-256/SHA-3	Modernas jaucējfunkcijas datu integritātei. SHA-3 ir jaunākā NIST standarta funkcija, izturīga pret kvantu uzbrukumiem.

MD5/SHA-1	Vecas jaucējfunkcijas, kuras mūsdienās uzskata par nedrošām un vājām.
HMAC	*Hash-based Message Authentication Code* – mehānisms ziņu autentiskuma pārbaudei. Drošs, ja izmanto modernu jaucējfunkciju (piem., SHA-256).
AES-CMAC	*Cipher-based Message Authentication Code* – MAC mehānisms, kas balstās uz AES.
RSA	*Rivest-Shamir-Adleman* – klasisks publiskās atslēgas algoritms šifrēšanai un digitālajiem parakstiem.
ECDSA/ECDH	*Elliptic Curve Digital Signature Algorithm/Elliptic Curve Diffie-Hellman* – eliptisko līkņu algoritmi digitālajiem parakstiem un atslēgu apmaiņai.
TLS	*Transport Layer Security* – Transport Layer Security – protokols drošai datu pārraidei. NIST un ENISA iesaka izmantot TLS 1.3 ar AEAD režīmiem un gatavoties PQC hibrīdajiem profiliem.
SSL	*Secure Sockets Layer* – TLS protokola priekštecis, kuru mūsdienās uzskata par nedrošu.
PFS (Perfect Forward Secrecy)	*Perfect Forward Secrecy* – īpašība, kas nodrošina, ka sesijas atslēgas nevar izmantot iepriekšējo datu atšifrēšanai. PQC migrācijā PFS ir kritisks, jo mazina "*harvest-now-decrypt-later*" risku.
AEAD	*Authenticated Encryption with Associated Data* – šifrēšanas režīms, kas nodrošina konfidencialitāti, integritāti un autentiskumu.
AES-GCM	*AES-Galois/Counter Mode* – AEAD režīms, kas izmanto AES un Galois/Counter Mode. Plaši izmantots TLS 1.3 un tiek uzskatīts par drošu arī kvantu "laikmetā" (ar AES-256).
ChaCha20-Poly1305	AEAD (*Authenticated Encryption with Associated Data)* shēma, kas nodrošina augstu veiktspēju un drošību, īpaši ierīcēs bez AES paātrinājuma. NIST un ENISA to atzīst par drošu alternatīvu AES-GCM.
X.509	Standarts publisko atslēgu sertifikātu struktūrai un pārvaldībai. PQC migrācijā X.509 sertifikāti tiks paplašināti ar PQC parakstiem un hibrīdajiem parakstiem.
CRYSTALS-Kyber ML-KEM (*Module-Lattice-Based Key-Encapsulation Mechanism*)	NIST izvēlētais PQC atslēgu apmaiņas (KEM) algoritms. Drošs pret kvantu uzbrukumiem - paredzēts aizstāt RSA/ECDH.
CRYSTALS-Dilithium ML-DSA (*Module-Lattice-Based Digital Signature Algorithm*)	NIST ieteiktais PQC digitālo parakstu algoritms. Paredzēts aizstāt RSA/ECDSA.
Falcon (*FFT over NTRU-Lattice-Based Digital Signature Algorithm*)	NIST ieteiktais PQC digitālo parakstu algoritms ar mazāku izmēru parakstiem - piemērots ierobežotu resursu sistēmām.

SPHINCS+ SLH-DSA (*Stateless Hash-Based Digital Signature Algorithm*)	Hash-based PQC parakstu algoritms. Lēnāks, bet ļoti drošs.

1.3. Atslēgu pārvaldība

Termins	Apraksts
Atslēga	Unikāla bitu virkne, ko izmanto kriptogrāfiskos algoritmos datu šifrēšanai, atšifrēšanai, parakstīšanai vai autentifikācijai. PQC kontekstā atslēgas bieži ir ievērojami garākas, kas ietekmē glabāšanas un pārvaldības prasības.
CSPRNG	*Cryptographically Secure Pseudorandom Number Generator* – drošs gadījumu skaitļu ģenerators, kas piemērots atslēgu, "*salt*" un citu kriptogrāfisku parametru ģenerēšanai.
HSM	*Hardware Security Module* – specializēta fiziska ierīce drošai atslēgu glabāšanai un kriptogrāfisko operāciju veikšanai. PQC migrācijā svarīgi, lai HSM atbalstītu hibrīdos un post-kvantu algoritmus.
TRSM	*Trusted Security Module* – aparatūras vai programmatūras modulis, kas nodrošina drošu atslēgu glabāšanu un aizsardzību pret manipulācijām. Izmantojams sistēmās, kur HSM nav praktiski ieviešams.
Kriptoperiods	Laika posms, kurā konkrēta atslēga tiek uzskatīta par drošu un derīgu. PQC kontekstā kriptoperiodi bieži tiek saīsināti, lai mazinātu "*harvest-now-decrypt-later*" risku un nodrošinātu savlaicīgu migrāciju uz kvantu drošiem algoritmiem.
Atslēgu rotācija	Regulāra atslēgu nomaiņa, lai samazinātu kompromitēšanas risku.
Atslēgu dzīves cikls (Key Lifecycle)	Process, kas ietver atslēgu ģenerēšanu, glabāšanu, izplatīšanu, izmantošanu, rotāciju un drošu iznīcināšanu. PQC migrācijā būtiski nodrošināt, ka dzīves cikls atbalsta gan klasiskos, gan PQC algoritmus.
Atslēgu inventarizācija (Crypto Inventory)	Process, kurā organizācija identificē visas izmantotās atslēgas, algoritmus, sertifikātus un protokolus. NIST un ENISA to definē kā pirmo un kritiski svarīgo soli PQC migrācijā.
Atslēgu atjaunošana (Key Renewal)	Atslēgas nomaiņa pirms kriptoperioda beigām vai pēc drošības incidenta. PQC ieviešanā bieži nepieciešama atjaunošana, lai pārietu uz hibrīdajiem vai PQC algoritmiem.
Atslēgu sadale (Key Distribution)	Drošs mehānisms atslēgu nodošanai starp sistēmām vai lietotājiem. PQC algoritmi (piem., Kyber) aizstās RSA/ECDH tradicionālajā atslēgu apmaiņā.
Atslēgu glabāšana (Key Storage)	Metodes un tehnoloģijas drošai atslēgu uzglabāšanai (HSM, TRSM, droši *enclaves*). PQC atslēgu lielums var prasīt infrastruktūras pielāgošanu.

1.4.Standarti

Termins	Apraksts
ISO/IEC 27001	Starptautisks standarts informācijas drošības pārvaldības sistēmu (ISMS) izveidei, ieviešanai, uzturēšanai un uzlabošanai, nodrošinot riska pārvaldību un atbilstošu kontroles pasākumu ieviešanu.
ISO/IEC 19790	Starptautisks standarts kriptogrāfisko moduļu drošības prasībām (atbilst FIPS 140 principiem). Lietots HSM un TRSM sertifikācijai.
ISO/IEC 18033	Starptautisks standarts, kas definē kriptogrāfisko algoritmu specifikācijas (simetriskie, asimetriskie, paraksti, jaucējfunkcijas).
NIST	*National Institute of Standards and Technology (ASV)* – izstrādā kriptogrāfijas standartus, tostarp PQC algoritmus (Kyber, Dilithium, Falcon, SPHINCS+), SP 800 sērijas vadlīnijas un migrācijas rekomendācijas.
ENISA	*European Union Agency for Cybersecurity* – izstrādā kiberdrošības vadlīnijas, PQC migrācijas ceļvežus, kriptogrāfijas mehānismu rekomendācijas un Eiropas sertifikācijas shēmas (EUCC).
EPC	*European Payments Council* – izstrādā maksājumu drošības un SEPA standartus, kas ietver kriptogrāfijas prasības finanšu sektoram.

2. VISPĀRĒJĀ INFORMĀCIJA

2.1. Mērķis

Kriptogrāfijas vadlīnijas un procedūras ir izstrādātas, lai nodrošinātu informācijas konfidencialitāti, integritāti, autentiskumu un nenoliedzamību, atbilstoši aktīvu klasifikācijai, riska novērtējumam un organizācijas drošības prasībām. Vadlīnijas aptver datu aizsardzību visos dzīves cikla posmos:

— **data at rest** (dati glabāšanas stāvoklī);

— **data in use** (dati apstrādes laikā);

— **data in transit** (dati pārraides laikā).

Šīs prasības veidotas saskaņā ar Eiropas Savienības kiberdrošības regulējumu, tostarp EUCC shēmu, kā arī ENISA ieteikumiem par piekritīgiem kriptogrāfiskiem mehānismiem (European Cybersecurity Certification Group Agreed Cryptographic Mechanisms v2.0, 2025).

2.2. Kriptogrāfisko pasākumu tips, stiprums un kvalitāte

Kriptogrāfisko pasākumu izvēle jābalsta uz riska novērtējumu, IKT resursu un informācijas sistēmu sensitivitāti un paredzēto aizsardzības līmeni.

— **Data at rest**:
datu glabāšanas aizsardzībai jāizmanto simetriskās šifrēšanas algoritmi, kas nodrošina augstu drošības līmeni un atbilst starptautiskajiem standartiem.

— **Data in use**:
datu apstrādes laikā jānodrošina stingri piekļuves kontroles, autentifikācijas un izolācijas mehānismi, kas samazina risku, ka sensitīva informācija tiek nopludināta vai kompromitēta apstrādes procesā.

— **Data in transit**:
datu pārraidei jāizmanto moderni, starptautiski atzīti protokoli, kas nodrošina spēcīgu šifrēšanu un aizsardzību pret mūsdienu uzbrukumiem. Par ieteicamo standartu tiek uzskatīts TLS 1.3, kas nodrošina uzlabotu drošības modeli, samazinātu uzbrukuma laukumu un obligātu *Perfect Forward Secrecy*.

Jāizmanto tikai atzīti un droši (*agreed*) kriptogrāfiskie mehānismi saskaņā ar European Cybersecurity Certification Group Agreed Cryptographic Mechanisms, kas ietver NIST standartizētus algoritmus un PQC mehānismus.

Prioritāri jāizmanto ENISA un NIST ieteiktie kriptogrāfiskie algoritmi un protokoli, kas nodrošina augstu drošības līmeni un atbilst mūsdienu starptautiskajiem standartiem. Šajā kategorijā ietilpst:

— **Simetriskā šifrēšana:**
jāizmanto AES-256 AEAD režīmos (piemēram, AES-GCM vai AES-GCM-SIV**),** kas nodrošina gan konfidencialitāti, gan integritāti un ir atzīti par drošiem ilgtermiņa lietošanai.

— **Jaucējfunkcijas:**
datu integritātes nodrošināšanai jāizmanto modernas un drošas jaucējfunkcijas, piemēram, SHA-3 vai SHA-512/256, kas nodrošina augstu drošības rezervi un atbilst NIST rekomendācijām ilgtermiņa aizsardzībai.

— **Asimetriskā kriptogrāfija:**
pārejas posmā jāizmanto mehānismi ar pietiekamu drošības rezervi, izvēloties NIST P-384 (atbilst secp384r1) vai augstāku līmeni (piem., P-521).

— Vienlaikus organizācijai jānodrošina gatavība post kvantu periodam, ieviešot NIST PQC standartizētos algoritmus, piemēram:
  - ✓ ML KEM (CRYSTALS Kyber) atslēgu apmaiņai,
  - ✓ ML DSA (CRYSTALS Dilithium) digitālajiem parakstiem,
  - ✓ SLH DSA (SPHINCS+) kā *hash-based* (uz jaucējfunkcijām balstītu) alternatīvu.

Informācijas sistēmas jācenšas projektēt ar modulāru arhitektūru, kas ļauj operatīvi nomainīt algoritmus un parametrus, reaģējot uz jauniem apdraudējumiem vai standartu izmaiņām (European Cybersecurity Certification Group Agreed Cryptographic Mechanisms un NIS2 tehniskās vadlīnijas).

Jāizmanto sertificēti kriptogrāfiskie moduļi, kas atbilst Eiropas Savienības drošības prasībām, tostarp EUCC sertifikācijas shēmai un EN 419 221-1 (HSM) standartam, vai arī ekvivalentiem ASV FIPS 140-3 kriptogrāfisko moduļu drošības standartiem.

Organizācijām jāveic kriptogrāfisko aktīvu inventarizācija un migrācijas plānošana uz PQC hibrīdiem risinājumiem (Eiropas Komisijas koordinētais ieviešanas ceļvedis).

3. PĀRVALDĪBA

3.1.Dati un paroles

Tēma	Prasības un ieteikumi	Aavots
Droša paroles glabāšana	Paroles drīkst glabāt tikai neatgriezeniski jaucējfunkciju balstītā formā, izmantojot modernu *Key Derivation Function* (KDF) un unikālu, kriptogrāfiski droši ģenerētu sāli (salt). Šī pieeja nodrošina, ka paroles nav iespējams atjaunot pat tad, ja paroles datubāze tiek kompromitēta. **Galvenie principi:** Paroles jaucējfunkcijai jābūt vienvirziena un izturīgai pret atjaunošanas mēģinājumiem, nodrošinot, ka pat pēc *hash* noplūdes parole nav rekonstruējama. "Salt" vērtībai jābūt unikālai katram lietotājam, nejauši ģenerētai ar kriptogrāfiski drošu pseido-nejaušo skaitļu ģeneratoru (CSPRNG) un vismaz 128 bitu garai, kā to nosaka NIST un ENISA labā prakse. Izmantotajam KDF jābūt noturīgam pret GPU/ASIC *brute-force* uzbrukumiem, nodrošinot pietiekamu iterāciju skaitu, atmiņas prasības un izturību. **Ieteicamā ieviešana:** *Argon2id* (ieteicamais mūsdienu standarts, atbilstošs NIST un ENISA rekomendācijām), *scrypt*, ja *Argon2id* nav pieejams, *bcrypt* ar pietiekami augstu sarežģītības parametru (*cost factor* ≥ 12), ja nav iespējams izmantot modernākus KDF. **Operētājsistēmu specifika:** Linux/Unix sistēmās paroles jāglabā /etc/shadow failā, izmantojot Argon2id vai bcrypt, atbilstoši sistēmas iespējām un drošības konfigurācijai. Windows vidē *NTLM hash* (balstīts uz MD4) tiek uzskatīts par novecojušu un nedrošu, jo tas neatbilst mūsdienu kriptogrāfijas prasībām. Ieteicams izmantot federētu identitātes nodrošinātāju (IdP), piemēram, *Microsoft Entra ID, Okta* vai *Keycloak*, kur paroles tiek glabātas un	OWASP Password Storage Cheat Sheet NIST SP 800-63B Digital Identity Guidelines ENISA Technical Implementation Guidance

	apstrādātas, izmantojot modernus KDF ārpus *Active Directory*. Papildus iespējams izmantot Password Filter DLL, lai ieviestu aizliegto paroļu sarakstu un politikas, taču tas nemaina Windows iekšējo glabāšanas algoritmu un tāpēc neuzlabo NTLM hash kriptogrāfisko drošību.	
Maskēšana un šifrēšana **(GDPR 32. pants)**	Personas dati, īpaši paroles un unikālie identifikatori, jāapstrādā ar pseidonimizāciju, anonimizāciju vai šifrēšanu. Paroles sistēmā jāglabā tikai neatgriezeniski "hashētā" veidā. Lietotāja saskarnē sensitīva informācija jāataino tikai daļēji maskētā formā, piemēram, parādot ierobežotu simbolu skaitu vai aizstājot tos ar maskējošiem simboliem, lai novērstu nejaušu vai ļaunprātīgu datu atklāšanu. Ja personas dati tiek glabāti ārpus specializētas paroļu jaucējfunkciju datu (*hash*) krātuves, jāievēro datu minimizācijas princips un jānodrošina šifrēšana glabāšanas stāvoklī (*data at rest*).	Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (GDPR), 32. pants
Papildu autentifikācijas un aizsardzības pasākumi	Organizācijai ir jāievieš daudzfaktoru autentifikācija (MFA) visiem lietotājiem un administratīvajiem kontiem, dodot priekšroku *phishing-resistant* autentifikācijas metodēm, kas nodrošina augstāko aizsardzības līmeni pret identitātes kompromitēšanu. Par drošākajām metodēm tiek uzskatīti FIDO2/passkeys risinājumi, aparatūras autentifikatori (piemēram, drošības atslēgas ar kriptogrāfisku aizsardzību) vai biometrikas un PIN kombinācijas, kas tiek apstrādātas lokāli un nekad netiek pārsūtītas tīklā.	ENISA Tips for Secure User Authentication ENISA Technical Implementation Guidance OWASP Application Security Verification Standard (ASVS) NIST SP 800-63B

3.2.Atslēgu pārvaldība

Procedūra	Apraksts un prasības (atjaunināts)
Ģenerēšana	Atslēgas jāģenerē, izmantojot kriptogrāfiski drošu nejaušo skaitļu ģeneratoru (CSPRNG) un algoritmus, kas nodrošina pietiekamu drošības līmeni. European Cybersecurity Certification Group Agreed Cryptographic Mechanisms nosaka, ka ieteicamajiem mehānismiem

	jānodrošina vismaz 125 bitu drošības līmenis, bet ieteicams ≥192 bitu ekvivalents. Atslēgu ģenerēšanā jāiekļauj post-kvantu algoritmi, piemēram, ML-KEM-512+, ML-DSA-44+ un SLH-DSA, kas atbilst NIST PQC standartiem. Jāizvairās no novecojušiem algoritmiem, piemēram, RSA ar atslēgām < 3000 bitiem.
Izdošana	Publiskās atslēgas sertifikāti jāizdod tikai sertificētām sertifikācijas iestādēm (CA), kas atbilst PKI standartiem un EUCC prasībām. Augsta riska sistēmām jāplāno pāreja uz hibrīdajiem PQC sertifikātiem līdz 2030. gadam, nodrošinot savietojamību un aizsardzību pret "*Harvest Now, Decrypt Later*" uzbrukumiem.
Izplatīšana	Atslēgas drīkst izplatīt tikai drošos, autentificētos un šifrētos kanālos, izmantojot modernus protokolus, piemēram, TLS 1.3. Ieteicams nodrošināt hibrīdo PQC atbalstu, apvienojot klasisko un post-kvantu atslēgu apmaiņu.
Glabāšana	Atslēgas jāglabā HSM vai TRSM ierīcēs, kas atbilst FIPS 140-3 vai EN 419 221-1 drošības prasībām. PQC atslēgas (piemēram, ML-KEM) ir būtiski lielākas, tāpēc jānodrošina atbilstoša infrastruktūra.
Maiņa / Rotācija	Atslēgu rotācija jāveic regulāri, balstoties uz kriptogrāfijas periodu. NIST SP 800-57 nosaka, ka simetriskajām atslēgām tas ir 1–2 gadi, bet asimetriskajām — līdz 3 gadiem, tomēr kvantu riska kontekstā rotācijas periodi var būt īsāki. Pārejas periodā prioritāri jārotē hibrīdās PQC atslēgas.
Kompromitēšana	Jāizstrādā skaidras procedūras kompromitētu atslēgu atsaukšanai, aizstāšanai un incidentu vadības integrācijai, kā to nosaka MK 397 šifrēšanas prasības. Procedūrās jāiekļauj arī PQC migrācijas scenāriji, lai nodrošinātu noturību pret kvantu draudiem.
Atsaukšana	Kompromitētas vai zaudētas atslēgas nekavējoties jāatsauc. Ieteicams ieviest automatizētu atsaukšanas procesu, lai samazinātu cilvēka faktora risku.
Atjaunošana	Atslēgas drīkst atjaunot tikai no šifrētām un autentificētām rezerves kopijām, izmantojot daudzfaktoru autorizāciju. Rezerves kopijām jābūt PQC saderīgām, lai nodrošinātu ilgtermiņa drošību.
Iznīcināšana	Atslēgas jāiznīcina neatgriezeniski. HSM ierīcēs jānodrošina gan fiziska, gan loģiska atslēgu iznīcināšana.
Auditēšana	Visas darbības, kas saistītas ar atslēgām, jāreģistrē un jāauditē, nodrošinot pilnu pārskatāmību. Rekomendējam līdz 2026. gada beigām veikt kriptogrāfisko aktīvu inventarizācija (*crypto inventory*), kā to nosaka ES PQC ceļvedis.
Aktivizācija / Deaktivizācija	Atslēgas jāaktivizē un jādeaktivizē saskaņā ar organizācijas politiku un riska novērtējumu. Novecojušie mehānismi jādeaktivizē līdz 2031. gadam, kā to nosaka European Cybersecurity Certification Group Agreed Cryptographic Mechanisms.
Inventarizācija un migrācija	Rekomendējam līdz 2026. gada beigām veikt kriptogrāfisko aktīvu inventarizāciju, identificējot visus algoritmus, atslēgas, sertifikātus un to izmantošanas vietas. Organizācijām pakāpeniski jāīsteno PQC migrācijas plāns, kas ietver hibrīdos risinājumus (klasiskie +

	ML-KEM/ML-DSA) un prioritizē augsta riska datus, kas ir pakļauti "*Harvest Now, Decrypt Later*" uzbrukumiem. Augsta kritiskuma informācijas sistēmās PQC hibrīdalgoritmi jāievieš prioritāri 24 - 36 mēnešu laikā. Vidēja un zema kritiskuma sistēmās migrācija tiek veikta atbilstoši piegādātāju gatavībai un infrastruktūras atbalstam, nodrošinot c*rypto agility* un savietojamību.

3.3. Aktīvu pārvaldība

1) Aktīvi (IKT resursi, informācija un to apstrādes sistēmas) jāklasificē pēc to veida, sensitivitātes, kritiskuma, riska līmeņa un drošības klases, ņemot vērā organizācijas riska novērtējumu un normatīvās prasības.
2) Katrai aktīvu kategorijai jāpiemēro atbilstoši drošības kontroles pasākumi, piemēram - šifrēšana (data at rest / in transit / in use), piekļuves kontrole, perimetra aizsardzība, fiziskā un loģiskā piekļuve, rezerves kopijas, reģistrācija un uzraudzība, droša glabāšana, atjaunošana un likvidēšana.
3) Personāla apmācība un ietekmes un seku analīze jāveic ar regularitāti, kas nav retāka kā reizi gadā.

Visiem darbiniekiem, kuri strādā ar aktīviem (jeb riskam pakļautajiem IKT resursiem, informācijai un to sistēmām), jāpārzina un jāievēro aktīvu pārvaldības politika un norādījumi.

3.4. Politiku pārskatīšana

Kriptogrāfijas politika un procedūras jāpārskata un jāatjauno regulāri, ņemot vērā kriptogrāfijas attīstības līmeni un jaunākos standartus (piemēram, ENISA, ISO un NIST ieteikumus).

4. FUNDAMENTĀLIE DROŠĪBAS PRINCIPI

Princips	Kontrole
Konfidencialitāte	Dati jāaizsargā no neautorizētas piekļuves, izmantojot atbilstošus šifrēšanas, piekļuves kontroles un segmentācijas mehānismus.
Integritāte	Dati jāaizsargā no neautorizētām vai nejaušām izmaiņām, izmantojot digitālos parakstus, jaucējfunkcijas, auditēšanu un integritātes pārbaudes mehānismus.
Pieejamība	Informācijas sistēmām un datiem jābūt pieejamiem autorizētiem lietotājiem laikā, kad tie ir nepieciešami, nodrošinot pakalpojumu nepārtrauktību, rezerves kopijas, incidentu pārvaldību un aizsardzību pret DoS/DDoS uzbrukumiem.
Autentiskums	Jānodrošina identitātes un avota patiesuma pārbaude, izmantojot drošus autentifikācijas mehānismus, tostarp *phishing-resistant* MFA, digitālos sertifikātus un kriptogrāfiski drošus protokolus.
Nenoliedzamība (*Non-repudiation*)	Jānodrošina, ka darbības un pārsūtīšana ir pierādāma un to autori nevar tās noliegt. Tas tiek panākts, izmantojot digitālos parakstus, auditēšanas žurnālus un drošu laika zīmogošanu.

Riska balstīta pieeja	Kriptogrāfiskie risinājumi jāizvēlas, balstoties uz aktīvu klasifikāciju, riska novērtējumu un potenciālās ietekmes analīzi. Jāņem vērā drošības un lietojamības samērība, kā arī ilgtermiņa riski, tostarp "*Harvest Now, Decrypt Later*" scenāriji.
Kriptogrāfiskā elastība (Crypto Agility)	Jānodrošina spēja operatīvi nomainīt kriptogrāfiskos algoritmus, atslēgu garumus un protokolus, ņemot vērā tehnoloģisko attīstību, jaunas ievainojamības un starptautisko standartu izmaiņas. Šis princips ir būtisks pārejai uz post-kvantu kriptogrāfiju un hibrīdajiem risinājumiem.

Ieteicamās prakses kriptogrāfiskās elastības nodrošināšanai

— **Regulāra novērtēšana:**
Organizācijai vismaz reizi gadā vai pēc būtiskiem drošības incidentiem jāveic kriptogrāfijas riska novērtējums, izvērtējot izmantoto algoritmu stiprumu un to atbilstību aktuālajiem un prognozētajiem apdraudējumiem. Izmantotajiem atslēgu garumiem un algoritmiem jānodrošina vismaz 128 bitu ekvivalentais drošības līmenis, ņemot vērā arī *post-quantum* prasības ilgtermiņa datu aizsardzībai.

Simetriskā šifrēšana, ņemot vērā *post-quantum*:

- ✓ AES-256 vai stiprāks — nodrošina ~256 bitu klasisko drošību un ~128 bitu drošību pret Grovera algoritmu ;
- ✓ SHA-256 — nodrošina aptuveni 128 bitu drošību pret kvantu laikmetu;
- ✓ HMAC-SHA-256 — praktiski nodrošina ≥128 bitu drošības līmeni, ja tiek izmantotas pietiekami stipras atslēgas

Publiskās atslēgas (atslēgu apmaiņa, paraksti), ņemot vērā *post-quantum*:

- ✓ ECC P-256 / secp256r1 (aptuveni 128 bitu ekvivalentais līmenis, P-384 ar rezervi);
- ✓ RSA 3072 (aptuveni 128 bitu ekvivalentais līmenis);
- ✓ FF-DH 3072 (aptuveni 128 bitu ekvivalentais līmenis).

— **Modulāra arhitektūra:**
Informācijas sistēmas jāprojektē ar nomaināmiem kriptogrāfijas moduļiem (piemēram, izmantojot OpenSSL vai līdzīgas bibliotēkas), lai nodrošinātu ātru algoritmu nomaiņu bez būtiskām izmaiņām infrastruktūrā.

— **Migrācijas plāns:**
ENISA iesaka izmantot **LATICE** ietvaru - **Locate** (identificēt algoritmus), **Assess** (novērtēt riskus), **Transition** (plānot pāreju), **Implement** (ieviest), **Certify** (nodrošināt atbilstību), **Evaluate** (regulāri pārskatīt).

— **Atslēgu pārvaldība:**
Jāievēro definēti "kripto-periodi" (parasti 1–2 gadi atslēgu rotācijai) un jānodrošina gatavība post-kvantu algoritmu integrācijai, lai mazinātu "*Harvest Now, Decrypt Later*" risku.

4.1.Post-kvantu kriptogrāfija

Post-kvantu kriptogrāfija (PQC) ietver kriptogrāfiskos algoritmus un protokolus, kas ir izturīgi pret uzbrukumiem, izmantojot kvantu datorus. Kvantu datoru spējas, īpaši izmantojot *Shor*

algoritmu, ļauj efektīvi salauzt pašreiz plaši izmantotos publiskās atslēgas algoritmus, piemēram, RSA, DSA, DH un ECC, padarot tos ilgtermiņā nedrošus. Šie algoritmi balstās uz matemātiskām problēmām (faktorizācija, diskrētā logaritma problēma, eliptisko līkņu diskrētais logaritms), kuras kvantu datoriem kļūst atrisināmas polinomiālā laikā (nozīmē, ka kāds uzdevums vai algoritms ir izpildāms efektīvi**,** proti — tā izpildes laiks pieaug ne ātrāk kā kāds polinoms (matemātiska izteiksme) no ievades lieluma).

Tā kā klasiskie algoritmi, piemēram, RSA-2048 vai ECC P-256, nodrošina aptuveni 128 bitu drošību pret klasiskajiem uzbrukumiem, bet kvantu uzbrukumu kontekstā to drošība samazinās līdz aptuveni 64 bitiem, tie vairs neatbilst mūsdienu drošības prasībām. Tāpēc pārejai uz PQC algoritmiem jānodrošina vismaz 128 bitu drošības līmenis pret kvantu uzbrukumiem, kā to nosaka NIST PQC standarti (FIPS 203/204/205) un European Cybersecurity Certification Group Agreed Cryptographic Mechanisms.

Saskaņā ar ENISA ieteikumiem, klasiskie protokoli jāpapildina ar hibrīdiem risinājumiem (klasiskais + post-kvantu), lai aizsargātos pret kvantu apdraudējumiem.

4.2.Klasiskie protokoli un drošības kontroles prasības

Tabula atspoguļo klasisko algoritmu minimālos parametrus, kas jāizmanto pārejas periodā līdz pilnai PQC ieviešanai.

Protokols	Funkcija	Algoritms	Šobrīd	Ieteicamais	Mērķa algoritms (PQC)
TLS 1.3	Atslēgu apmaiņa	RSA / ECDHE	RSA-2048, ECDHE P-256	ECDHE P-384 (RFC 8446)	CRYSTALS-Kyber **ML-KEM** (*Module-Lattice-Based Key-Encapsulation Mechanism*) - (FIPS 203)
TLS 1.3	Paraksti	RSA / ECDSA	RSA-2048, ECDSA P-256	RSA-3072, ECDSA P-384 (RFC 8446)	CRYSTALS-Dilithium vai FALCON **ML-DSA** (*Module-Lattice-Based Digital Signature Algorithm*) – (FIPS 204)
SSH / SFTP	Servera autentifikācija	RSA	RSA-2048	RSA-3072 (RFC 4253)	Dilithium, SPHINCS+ **SLH-DSA** (*Stateless Hash-Based Digital Signature Algorithm*)
SSH / SFTP	Servera autentifikācija	ECDSA	ECDSA P-256	ECDSA P-384 (RFC 5656)	Dilithium, SPHINCS+
SFTP	Atslēgu apmaiņa	ECDH (SSH KEX)	ECDH P-256	ECDH P-384 (RFC 5656)	CRYSTALS-Kyber (FIPS 203)
IPSec / IKEv2	Atslēgu apmaiņa	DH / ECDH	DH-2048, ECDH P-256	DH-3072 / ECDH P-384 (RFC 7296, RFC 5903)	CRYSTALS-Kyber (FIPS 203)
VPN	Atslēgu apmaiņa	ECDH / RSA	ECDH P-256, RSA-2048	ECDH P-384, RSA-3072	CRYSTALS-Kyber (FIPS 203)
DNSSEC	Paraksti	RSA	RSA-2048 (RSASHA256)	RSA-3072 (RFC 5702)	SPHINCS+ (FIPS 205)
DNSSEC	Paraksti	ECDSA	ECDSA P-256	ECDSA P-384 (RFC 6605)	SPHINCS+ (FIPS 205)
S/MIME	E-pasta šifrēšana	RSA	RSA-2048	RSA-3072–4096 (RFC 8551)	CRYSTALS-Kyber (FIPS 203)
S/MIME	Paraksti	RSA	RSA-2048	RSA-3072–4096 (RFC 8551)	Dilithium, FALCON, SPHINCS+ (*FFT over NTRU-Lattice-Based Digital Signature Algorithm*) - FIPS 206

Izvērtejiet **"Harvest Now, Decrypt Later"** riskus, īpaši attiecībā uz datiem ar ilgu sensitivitātes periodu, kurus nākotnē varētu atšifrēt ar kvantu skaitļošanas palīdzību.

Veiciet **kriptogrāfiskā inventarizāciju**, pārskatot izmantotos protokolus, algoritmus un atslēgu drošības līmeni, lai savlaicīgi identificētu novecojušus vai neaizsargātus risinājumus.

4.3.Atbilstība un uzraudzība

Darbība	Kontrole (prasība/ieviešana)	Nacionālais kiberdrošības likums un MK Nr. 397
Regulārs pārskatījums	Izvērtēt un atjaunināt šifrēšanas protokolus atbilstoši starptautiskām vadlīnijām.	**Nacionālās kiberdrošības likuma 27. pants** – subjekts veic samērīgus tehniskus pasākumus kiberrisku pārvaldībai, tai skaitā šifrēšanai.
Drošības auditi	Veikt regulārus iekšējos vai ārējos auditus — infrastruktūras pārbaudi, veicot iekšējo vai ārējo auditu aizpildīt pašnovērtējuma anketas.	**Minimālo kiberdrošības prasību 8.3. nodaļa** - Pašnovērtējums un iekšējais audits saskaņā ar kārtību (līdz 2025. gada 1. oktobrim, pēc tam reizi 1–3 gados)
Personāla apmācība	Nodrošināt regulāras mācības par kiberdrošību un incidentu pārvaldību.	**Minimālo kiberdrošības prasību 78. punkts** – Subjekts nodrošina, ka apmācību saturs tiek pārskatīts un nepieciešamības gadījumā aktualizēts vismaz reizi gadā vai mainoties apstākļiem (piemēram, izceļoties jauniem kiberapdraudējumiem, mainoties kiberriska līmenim, notiekot kiberincidentam).
Dokumentācija	Izstrādāt un uzturēt dokumentāciju.	**Nacionālā kiberdrošības likuma 28. pants** – Subjektam ir pienākums izstrādāt kiberrisku pārvaldības un informācijas un komunikācijas tehnoloģiju darbības nepārtrauktības plānu un nodrošināt darbiniekiem regulāru apmācību efektīvai plānā iekļauto pasākumu īstenošanai **un Minimālo kiberdrošības prasību 3.2. nodaļa** - Subjekta kiberdrošības pārvaldības dokumentu kopumu veido kiberdrošības politika, IKT resursu un informācijas sistēmu katalogs, kiberrisku pārvaldības un IKT darbības nepārtrauktības plāns, kiberincidentu žurnāls.

Sertifikācija un atbilstība – EUCC shēma paredz, ka kriptogrāfijai jāatbilst ENISA "*recommended*" drošības līmenim, un PQC integrācija tiek uzskatīta par būtisku priekšnoteikumu ilgtermiņa sertifikācijas noturībai.

5. NODERĪGI RESURSI

Nr.	Nosaukums
1	Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography (EU)
2	A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography (EU)
3	EUCC Guidelines on Cryptography: Agreed Cryptographic Mechanisms, Version 2 (EU)
4	Post-Quantum Cryptography: Current state and quantum mitigation (EU)
5	PQC Standardization Process (USA)
6	Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms (USA)
7	NIST Migration to Post-Quantum Cryptography (USA)
8	Guidance on becoming cryptographically agile - ITSAP.40.018 (Canada)
9	Addressing the quantum computing threat to cryptography (ITSE.00.017) (Canada)