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 1.0, 12.09.2025

SATURS

1. IZMANTOTIE TERMINI

1.1. Jēdzieni

Termins	Apraksts
Kriptogrāfija	Zinātne par drošas komunikācijas un datu aizsardzības metodēm, izmantojot matemātiskus algoritmus.
Konfidencialitāte	Īpašība, ka informācija ir pieejama tikai autorizētām personām.
Integritāte	Īpašība, ka dati nav modificēti neautorizēti.
Autentiskums	Īpašība, ka identitāte vai avots ir patiess un pārbaudāms.
Nenoliedzamība (*Non-repudiation*)	Īpašība, 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 resursa vai informācijas drošības klasi (apdraudējuma mērogu).
Kriptogrāfiskā elastība	Spēja operatīvi nomainīt kriptogrāfiskos algoritmus un atslēgu parametrus, ņemot vērā tehnoloģisko attīstību un jaunākos standartus.

Termins	Apraksts
Data at rest	Dati, kas tiek glabāti kādā vietā (diskā, datu bāzē, rezerves kopijā u.tml.), bet aktīvi netiek pārsūtīti vai apstrādāti.
Data in transit	Dati, kas tiek pārsūtīti starp sistēmām, lietotājiem vai ierīcēm, piemēram, pārvietojoties pa tīklu (internetu, iekšējo tīklu, VPN).
Data in use	Dati, kas tiek aktīvi apstrādāti sistēmas atmiņā vai lietotāja darba vidē, piemēram, tiek skatīti, rediģēti vai izmantoti aplikācijas darbības laikā.

1.2. Algoritmi un protokoli

Termins	Apraksts
AES	*Advanced Encryption Standard* – simetrisks šifrēšanas algoritms, izmantojams datu konfidencialitātes nodrošināšanai.
DES/3DES	*Data Encryption Standard/Triple DES* – veci simetriskie šifrēšanas algoritmi, kurus mūsdienās uzskata par nedrošiem.
SHA-256/SHA-3	*Secure Hash Algorithm* – jaucējfunkcijas, kuras nodrošina datu integritāti.
MD5/SHA-1	Vecas jaucējfunkcijas, kuras mūsdienās uzskata par nedrošām un vājiem.
HMAC	*Hash-based Message Authentication Code* – mehānisms ziņu autentiskuma pārbaudīšanai.
AES-CMAC	*Cipher-based Message Authentication Code* – ziņu autentifikācijas kods, kas balstās uz AES algoritmu.

RSA	*Rivest-Shamir-Adleman* – nodrošina drošu datu šifrēšanu un digitālo parakstu izveidošanu. Piemēram, RSA tiek plaši izmantots, lai nodrošinātu drošu datu pārraidi internetā (TLS protokolos), kā arī elektronisko dokumentu autentificēšanu un parakstīšanu.
ECDSA/ECDH	*Elliptic Curve Digital Signature Algorithm/Elliptic Curve Diffie-Hellman* – publiskās atslēgas algoritmi, kas balstās uz eliptisko līkņu matemātiku.
TLS	*Transport Layer Security* – protokols, kas nodrošina drošu datu pārraidi tīklā.
SSL	*Secure Sockets Layer* – TLS protokola priekštecis, kuru mūsdienās uzskata par nedrošu.
PFS	*Perfect Forward Secrecy* – īpašība, ka atslēgas, kuras tiek izmantotas sesijas laikā, nevar tikt izmantotas, lai atšifrētu iepriekšējos datus, ja tās tiek kompromitētas.
AEAD	*Authenticated Encryption with Associated Data* – šifrēšanas režīms, kas vienlaicīgi nodrošina konfidencialitāti, autentiskumu un integritāti.
AES-GCM	*AES-Galois/Counter Mode* – AEAD režīms, kas izmantojams datu aizsardzībai.
ChaCha20-Poly1305	AEAD (Authenticated Encryption with Associated Data) shēma, kas vienlaikus nodrošina datu šifrēšanu un integritātes pārbaudi - balstās uz ChaCha20 (šifrētājs) un Poly1305 (MAC algoritms).
X.509	Standarts publisko atslēgu sertifikātu struktūrai un pārvaldībai.

1.3. Atslēgu pārvaldība

Termins	Apraksts
Atslēga	Unikāla bitu virkne, kas tiek izmantota kriptogrāfiskos algoritmos datu šifrēšanai un atšifrēšanai.
CSPRNG	*Cryptographically Secure Pseudorandom Number Generator* – drošs gadījumu skaitļu ģenerators, kas piemērots atslēgu ģenerēšanai.
HSM	*Hardware Security Module* – fiziska ierīce, kas nodrošina drošu atslēgu glabāšanu un kriptogrāfisko operāciju veikšanu.
TRSM	*Trusted Security Module* – programmatūras vai aparatūras modulis, kas nodrošina drošu atslēgu glabāšanu.
Kriptoperiods	Noteikts laika posms, kāda laikā konkrēta kriptogrāfiskā atslēga tiek uzskatīta par drošu un derīgu tās paredzētajam izmantojumam, ņemot vērā pašreizējo drošības līmeni un potenciālās apdraudējumu riskus.
Atslēgu rotācija	Regulāra atslēgu maiņa, lai samazinātu tās kompromitēšanas risku.

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 informācijas drošības un privātuma novērtēšanai, kas nosaka principus un metodes drošības līmeņa un privātuma aizsardzības efektivitātes noteikšanai organizācijās
ISO/IEC 18033	Starptautisks standarts, kas definē kriptogrāfisko algoritmu specifikācijas un to pielietojumu, iekļaujot simetriskās un asimetriskās šifrēšanas, digitālo parakstu un jaucējfunkcijas algoritmus.
NIST	*National Institute of Standards and Technology (ASV)* – valsts institūcija, kas izstrādā un publicē kriptogrāfijas, kiberdrošības un informācijas tehnoloģiju standartus, tostarp publikācijas.
ENISA	*European Union Agency for Cybersecurity* – Eiropas Savienības Tīklu un informācijas drošības aģentūra, kas veicina kiberdrošības standartu un labākās prakses rekomendāciju izstrādi, sniedz vadlīnijas un atbalsta dalībvalstis kriptogrāfijas un kiberdrošības jautājumos.
EPC	*European Payments Council* – Eiropas maksājumu padome, kas koordinē un izstrādā vienotus maksājumu drošības un interoperabilitātes standartus, tostarp SEPA (*Single Euro Payments Area*) noteikumus.

2. VISPĀRĒJĀ INFORMĀCIJA

2.1. Mērķis

Kriptogrāfijas vadlīnijas un procedūras ir izstrādātas, lai nodrošinātu datu konfidencialitāti, autentiskumu un integritāti, atbilstoši aktīvu klasifikācijai un riska novērtējumam. Vadlīnijas iekļauj prasības datu aizsardzībai visos stāvokļos: "*data at rest*", "*data in use*" un "*data in transit*".

2.2. Kriptogrāfisko pasākumu tips, stiprums un kvalitāte

— ***Data at rest***: jāizmanto atbilstoši stiprs šifrēšanas algoritms (piemēram, AES-256), lai nodrošinātu datu konfidencialitāti un integritāti.

— ***Data in use***: jāizmanto drošas piekļuves kontroles un autentifikācijas mehānismi, piemēram, TPM moduļi vai drošas atmiņas zonas.

— ***Data in transit***: jāizmanto TLS 1.2 vai jaunāka versija, iespējams, ar iespēju pāriet uz jaunākām versijām (*cryptographic agility*).

2.3. Protokolu, algoritmu un kriptogrāfisko risinājumu izmantošana

— Jāizmanto tikai atzītus un drošus protokolus un algoritmus (piemēram, RSA, ECC, SHA-3).

— Jāievēro kriptogrāfiskā elastība, lai ātri varētu pāriet uz jaunākām un drošākām tehnoloģijām.

— Jāizmanto atbilstoši sertificēti kriptogrāfiskie risinājumi, piemēram, ar FIPS 140-2/3 sertifikāciju.

3. PĀRVALDĪBA

3.1.Dati un paroles

Tēma	Prasības un ieteikumi	Normatīvais/standarta avots
Droša paroles glabāšana	***Hash* + *salt* (paroļu aizsardzība):** – ***Hash* (jaucējfunkcija):** parole tiek pārvērsta garā ciparu/burtu virknē, izmantojot vienvirziena algoritmu. No šī rezultāta nav iespējams tieši atjaunot sākotnējo paroli. – **Salt (sāls):** pirms paroles sajaukšanas (*hash+salt)* tai pievieno nejaušu un unikālu virkni. Tas nodrošina, ka pat tad, ja divi lietotāji izvēlas vienādu paroli, glabātais hash būs atšķirīgs. – **Ieteicamā ieviešana:** lietot Argon2id (ieteicams). Ja nav iespējams – *scrypt* vai *bcrypt*. **Operētājsistēmu mehānismi:** — **Linux / Unix (etc/shadow)** paroļu fails – izmantotais algoritms atkarīgs no sistēmas konfigurācijas — **Windows** – pēc noklusējuma paroles tiek glabātas kā **NT hash** (NTLM – *NT LAN Manager* hash, kura pamatā ir MD4 algoritms). Šo iekšējo formātu nav iespējams aizstāt ar mūsdienu atvasināšanas funkcijām, piemēram, **Argon2** vai **bcrypt**. — Ja organizācijas drošības prasības nosaka, ka paroles obligāti jāglabā, izmantojot modernu **Key Derivation Function (KDF)**, piemēram, **Argon2** vai **scrypt**, jāizmanto **ārējs identitātes nodrošinātājs** (*Identity Provider, IdP*). Šādā scenārijā paroles tiek pārvaldītas ārpus Active Directory, un tieši IdP ir atbildīgs par to drošu uzglabāšanu. — Papildus var ieviest Password Filter DLL (Dynamic Link Library), kas tiek instalēta uz domēna kontrolieriem (DC – Domain Controller). Šāds filtrs ļauj realizēt	OWASP *Password Storage Cheat Sheet*; NIST SP 800-63B

	papildu paroles validācijas mehānismus (piemēram, pārbaudi pret aizliegto paroļu sarakstiem), lai gan nemaina paroles glabāšanas algoritmu.	
Maskēšana un šifrēšana (GDPR 32. pants)	- Personas dati (īpaši paroles, identifikatori) jāapstrādā ar pseidonimizāciju, maskēšanu vai šifrēšanu. - Paroles glabāt tikai drošā, neatgriezeniski slēptā veidā. - Ja nepieciešama pagaidu datu atainošana, jāpiemēro daļēja maskēšana (piem., tikai pirmie/ pēdējie simboli).	GDPR 32. pants ("pseidonimizācija un šifrēšana" kā drošības pasākumi)
Papildu ieteikumi	- Atbalstīt daudzfaktoru autentifikāciju (MFA). - Ieviest kontu bloķēšanu vai aiztures pēc vairākiem neveiksmīgiem mēģinājumiem.	ENISA, OWASP ASVS

3.2.Atslēgu pārvaldība

Procedūra	Apraksts
Ģenerēšana	Atslēgas jāveido, izmantojot drošus un atzītus kriptogrāfiskos algoritmus ar pietiekamu stiprumu un nejaušību (saskaņā ar *National Institute of Standards and Technology* (NIST) un *International Organization for Standardization* (ISO) standartiem vai tml.).
Izdošana	Publiskās atslēgas sertifikātus drīkst izdot tikai starpniecībā ar sertificētu sertifikātu autoritāti (*Certificate Authority* – CA), ievērojot publisko atslēgu infrastruktūras (*Public Key Infrastructure* – PKI) standartus un organizācijas noteikumus.
Izplatīšana	Atslēgas jānodod tikai drošos, autentificētos un šifrētos kanālos (piemēram, *Transport Layer Security* (TLS) protokols vai droša failu pārraide).
Glabāšana	Atslēgas jāuzglabā drošās ierīcēs, piemēram, aparatūras drošības modulī (*Hardware Security Module* – HSM), kas pasargā no nesankcionētas piekļuves un manipulācijām.
Maiņa	Atslēgas regulāri jāmaina, balstoties uz noteikto kriptoperiodu un riska novērtējumu.
Kompromitēšana	Jābūt procedūrām kompromitētu atslēgu atsaukšanai, aizstāšanai un iekļaušanai incidentu reaģēšanas un nepārtrauktības plānā.
Atsaukšana	Kompromitētas, zaudētas vai nevajadzīgas atslēgas nekavējoties jāatsauc un jāatjauno sertifikātu atsaukšanas sarakstu (*Certificate Revocation List* – CRL).
Atjaunošana	Zaudētas atslēgas jāatjauno no drošām, šifrētām rezerves kopijām, ievērojot autentifikācijas un autorizācijas prasības.

Iznīcināšana	Atslēgas un ar tām saistītie dati jāiznīcina neatgriezeniski, ievērojot noteiktos standartus (piemēram, *National Institute of Standards and Technology* (NIST) SP 800-88) utt.
Auditēšana	Visas darbības ar atslēgām jāreģistrē un jāauditē, nodrošinot pilnu pārskatāmību un atbilstību drošības prasībām.
Aktivizācija/deaktivizācija	Atslēgas jāaktivizē vai jādeaktivizē noteiktos termiņos, saskaņā ar organizācijas politiku un drošības prasībām.

3.3.Aktīvu pārvaldība

— Aktīvi (kiberdrošības riskam pakļautie IKT resursi un informācija un to sistēmas) jāklasificē pēc to veida, sensitivitātes, riska līmeņa un drošības klases un prasībām.
— Jāpiemēro atbilstoši kontroles pasākumi: šifrēšana, piekļuves kontrole, perimetra aizsardzība, fiziskā un loģiskā piekļuve, dublēšana, reģistrācija, uzraudzība, glabāšana un likvidēšana.
— Jāveic ietekmes un seku analīze, lai noteiktu aktīvu klasifikācijas līmeni.

3.4. Personāla apmācība

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

3.5. Politiku pārskatīšana

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

3.6. Saskaņošana ar normatīvajiem aktiem

— Vadlīnijas ir izstrādātas, ņemot vērā Direktīvas (ES) 2022/2555 21. panta 2. punkta h) apakšpunktu un ENISA tehniskās ieviešanas vadlīnijas.

4. FUNDAMENTĀLIE DROŠĪBAS PRINCIPI

Princips	Kontrole
Konfidencialitāte	Datus jāaizsargā no neautorizētas piekļuves.
Integritāte	Datus jāaizsargā no neautorizētām izmaiņām.
Pieejamība	Datiem un sistēmām jābūt pieejamiem autorizētiem lietotājiem laikā, kad tie ir nepieciešami, nodrošinot pakalpojumu nepārtrauktību.
Autentiskums	Jāpārbauda identitāte un avota patiesība.
Nenoliedzamība (*Non-repudiation*)	Jānodrošina darbību un transakciju autentiskuma pierādījums.
Riska balstīta pieeja	Kriptogrāfiskie risinājumi jāizvēlas balstoties uz aktīvu klasifikāciju un riska novērtējumu, ņemot vērā drošības un lietojamības samērību

	pret kiberriskam pakļautā resursa vai informācijas drošības klasi kā arī iespējamību un ietekmi.
Kriptogrāfiskā elastība	Jānodrošina spēja operatīvi nomainīt algoritmus un atslēgu parametrus, ņemot vērā tehnoloģisko attīstību un jaunākos standartus.

4.1. Simetriskā šifrēšana

— AES (*Advanced Encryption Standard*): Minimāli pieņemamās atslēgas garums ir 128 biti; ieteicams izmantot 256 bitu atslēgas, lai nodrošinātu ilgtspējīgu aizsardzību pret potenciālām uzbrukumu metodēm.

— Vājie algoritmi: DES un 3DES tiek uzskatīti par nepiemērotiem mūsdienu drošības prasībām un ir izņemti no lietošanas.

4.2. Jaucējfunkcijas (*Hash function*)

— SHA-256 vai stiprāki algoritmi (piemēram, SHA-3).

— Vājie algoritmi: MD5 un SHA-1 vairs netiek uzskatīti par drošiem un nav ieteicami lietošanai.

4.3. Ziņu autentifikācijas kodi (MAC)

— HMAC (*Hash-based* MAC), izmantojot SHA-2 vai SHA-3, vai AES-CMAC: ieteicamie risinājumi ziņu autentiskuma nodrošināšanai.

— Vājie algoritmi: DES/TDES bāzētie MAC algoritmi vairs netiek uzskatīti par drošiem.

4.4. Asimetriskā šifrēšana – publiskās atslēgas kriptogrāfija (PKI).

— RSA: minimālais pieņemamais atslēgas garums ir 2048 biti. Ieteicams pāriet uz 3072 vai 4096 bitu atslēgām, ņemot vērā mūsdienu drošības prasības.

— ECDSA/ECDH: minimālais pieņemamais atslēgas garums ir 224 biti. Ieteicams izmantot 256 bitu atslēgas, lai nodrošinātu drošību pret pašreizējiem un nākotnes apdraudējumiem.

Gatavošanās postkvantu *(Post-quantum*) kriptogrāfijai: ieviešana hibrīdajiem risinājumiem, kas kombinē klasiskos algoritmus (piemēram, RSA vai ECDSA) ar postkvantu kriptogrāfijas algoritmiem, lai sagatavotos nākotnes drošības izaicinājumiem.

4.5.Protokoli un to izmantošana

Protokols/Lietojums	Drošības kontroles prasības un ieteikumi
Datu pārraide	Jāizmanto TLS 1.2 vai TLS 1.3 (ieteicamais standarts), ievērojot, ka savienojumam jāatbalsta *Perfect Forward Secrecy* (PFS) ar atbilstošu šifrēšanu (piemēram, *Ephemeral Diffie-Hellman* — DHE vai ECDHE).
Vājie protokoli	SSL, TLS 1.0 un TLS 1.1 jāuzskata par nepiemērotiem. Jāizvairās no vājas šifrēšanas (piemēram, RC4, DES, 3DES) un pašdarinātu šifrēšanas algoritmu lietošanas.

Datu aizsardzība	Jāizmanto *sign-then-encrypt* pieeja vai AEAD (*Authenticated Encryption with Associated Data*) šifrēšanas režīmi, piemēram, AES-GCM vai ChaCha20-Poly1305, lai nodrošinātu gan konfidencialitāti, gan autentiskumu.
Sertifikāti	X.509 sertifikātiem jābūt spēkā esošiem, ar regulāru derīguma termiņa pārbaudi. Jānodrošina sertifikātu atsaukšanas statusa verifikācija, izmantojot Sertifikātu atsaukšanas sarakstus (CRL) vai Tiešsaistes sertifikātu statusa protokola (OCSP) atbildes.

DNSSEC (*Domain Name System Security Extensions*) – nodrošina domēna vārdu sistēmas (DNS) datu autentiskumu un integritāti, pasargājot no DNS viltošanas (DNS *spoofing*) un pāradresācijas uz ļaunprātīgiem resursiem.

IPSec (*Internet Protocol Security*) – paredzēts drošai datu pārraidei tīkla līmenī, nodrošinot šifrēšanu, autentifikāciju un datu integritāti starp komunikācijas partneriem. Bieži tiek izmantots virtuālo privāto tīklu (VPN) izveidei.

S/MIME (*Secure/Multipurpose Internet Mail Extensions*) – nodrošina e-pasta ziņojumu konfidencialitāti, autentiskumu un sūtītāja identitātes apliecināšanu, izmantojot digitālos sertifikātus un šifrēšanu.

SSH (*Secure Shell*) –protokols, kas nodrošina drošu attālinātu piekļuvi un sistēmu administrēšanu, izmantojot šifrētu sakaru kanālu. Autentifikācijai ieteicams izmantot mūsdienīgas publiskās atslēgas kriptogrāfijas shēmas, piemēram, **Ed25519** vai **ECDSA (Elliptic Curve Digital Signature Algorithm)**. Šīs metodes nodrošina augstāku kriptogrāfisko drošību un efektīvāku veiktspēju, salīdzinot ar tradicionālajām **RSA (Rivest–Shamir–Adleman)** atslēgām.

VPN (*Virtual Private Network*) – tehnoloģija, kas nodrošina drošu lietotāja vai organizācijas tīkla savienojumu ar citu tīklu, izmantojot publisko internetu. VPN izveido šifrētu datu tuneli starp galapunktiem, tādējādi aizsargājot datu plūsmu pret nesankcionētu pārtveršanu, noklausīšanos un satura modificēšanu.

Piemēram:

- **WireGuard** – jauns, viegls un ļoti ātrs VPN protokols. Izceļas ar modernu kriptogrāfiju (Curve25519, ChaCha20, Poly1305) un salīdzinoši vienkāršu kodu, kas padara to drošāku un vieglāk auditējamu.
- **OpenVPN** – atvērtā koda un plaši izmantots protokols, kas nodrošina spēcīgu šifrēšanu (AES-256, TLS 1.3) un elastību.
- **IKEv2/IPSec (*Internet Key Exchange* v2)** – drošs un ātrs protokols, īpaši noderīgs mobilajās ierīcēs, jo labi pārslēdzas starp dažādiem tīkliem (piemēram, no Wi-Fi uz mobilajiem datiem). Balstās uz IPSec šifrēšanu un nodrošina augstu drošības līmeni.

4.6.Atbilstība un uzraudzība

Darbība	Kontrole (prasība/ieviešana)	Nacionālais kiberdrošības likums un MK Nr. 397
Regulārs pārskatījums	Izvērtēt un atjaunināt šifrēšanas protokolus	Nacionālās kiberdrošības likuma 27. pants – subjekts veic samērīgus

	atbilstoši starptautiskām vadlīnijām.	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.