NACIONĀLAIS ATTĪSTĪBAS PLĀNS 2020

EIROPAS SAVIENĪBA
Eiropas Reģionālās attīstības fonds

IEGULDĪJUMS TAVĀ NĀKOTNĒ

Kriptogrāfija Latvijā

Rokasgrāmata

Sastādītāji: R.Balodis, I.Opmane, u.c.

Rīga, 2022

© Latvijas Universitātes Matemātikas un informātikas institūts
Dokumenta autortiesības pieder ERAF projekta "Kvantu kriptogrāfijas iekārtu un programmatūras risinājumu pielietojumi Latvijas skaitļošanas resursu infrastruktūrā" Nr. 1.1.1.1/20/A/106 projekta izpildītājiem

Ikdienas datu konfidencialitātes lietojuma scenāriji

SATURS

1. Ievads

ERAF projekta izpildītāji ir iezīmējuši kriptogrāfijas izmantošanas aktualizāciju un centienus visaptveroši kopā ar IKT industriju attīstīt kriptogrāfijas lietojumus Latvijā. Tas tiek pasniegts kriptogrāfijas digitālās ekosistēmas koncepcijas ietvarā. Darbs balstīts uz autoru un nozares ekspertu personīgo pieredzi un literatūras analīzi.

Rokasgrāmatas uzdevums ir parādīt, izvērtēt, apkopot un prognozēt ieteicamos kriptogrāfijas lietojumus Latvijas digitālajā vidē. Tāpat Rokasgrāmatas mērķis ir ieteikt risinājumus/ uzdevumus un metodiskas pieejas kriptogrāfijas lietošanai ar mērķi uzlabot IT drošību Latvijā.

Rokasgrāmatas saturs tiek sadalīts trīs sadaļās ar sekojošu uzdevumu:

- Kriptogrāfija mums ikdienā: ikdienas datu konfidencialitātes lietojuma scenāriji, klientu aptauja;
- Latvijas industrijas gatavība realizēt kriptogrāfijas, kvantu kriptogrāfijas platformas - no industrijas partneru intervijām uz risnājumu projektiem;
- Kriptogrāfijas tehnoloģiskie aspekti: kriptogrāfija komunikāciju tīklos un datu apstrādes protokolos.

Rokasgrāmatas pirmā daļa ir vispārlietojama, publiska, tajā tiek izskatīti šifrēšanas (kriptogrāfijas) ikdienas lietojuma scenāriji. Tie tiek apkopoti tematiskās problemātiskajās grupās, analizējot Eiropas regulējamus vai tiek aplūkotas ikdienas lietojuma grupas, kuras analizē un monitorē starptautiskas institūcijas, piemēram, ENISA (The European Union Agency for Cybersecurity) vai ICO. (The UK Information Commissioner's Office).

Lietojuma scenārijos izvirzītās tēmas (uzdevumi, jautājumi) var kalpot aptaujas (anketēšanas) organizēšanai, kā arī pirmajā sadaļā aplūkotos jautājumus var izmantot lasītājs personīgai rīcības argumentācijai ikdienas darbībā – "uz jautājumu it kā atbildot pašam".

Pirmajā sadaļā sagatavotie jautājumi orientēti individuālām atbildēm digitālajā vidē strādājošiem cilvēkiem. Atbildes tiek saņemtas kā šī darbinieka personīgs viedoklis, nevis institūcijas viedoklis, kā arī atbildes var neattēlot situāciju par darba vidi, ja darbinieks nav par to informēts. Aptaujas jautājumi tāpat neskar kriptogrāfijas izmantošanas novērtējumu darbībās, kuras būtu nepieciešams veikt institucionāli, piemēram, institūcijas kiberdrošības politikas vai stratēģijas esamība. Kiberdrošības un kriptēšanas institucionālo novērtējuma metodoloģija izstrādāta [4]. Realizējot Eiropā digitālās transformācijas programmu [5], labā prakse prasa institūcijai veikt digitālā brieduma testu. Digitālā brieduma pašnovērtējums palīdz institūcijām noteikt galvenās stiprās puses un nepilnības digitālo pakalpojumu nodrošināšanā un no datu kopsavilkuma pārskata var iegūt datus par progresu valstī kopumā.

Ieteicams būtu papildināt digitālā brieduma testu ar sadaļu par kiberdrošības un kriptogrāfijas lietojuma novērtējumu, bet rokasgrāmatas 1. sadaļa šiem jautājumiem nepieskaras.

Tādejādi šīs aptaujas mērķis aprobežojas ar uzdevumu identificēt tos ikdienas šifrēšanas lietojumus, kuriem ikdienas lietotāja skatā ir nepieciešams izmantot kriptogrāfijas visjaunākos tehnoloģiskos risinājumus.

Aptaujā atbildes uz visiem jautājumiem tiek plānotas pēc vienveidīgas shēmas:

- tēmai nav saistības ar kriptogrāfiju;
- esošie tehnoloģiskie risinājumi mani apmierina;
- nepieciešama kriptogrāfijas tehnoloģiju aktīvāka izmantošana;
- nepieciešams modernizēt kriptogrāfiskos risinājumus.

Informācijai mūsu sabiedrībā ir visaptveroša un ļoti būtiska loma. Mums nepieciešams informāciju iegūt, pārraidīt, apstrādāt, bet vienlaicīgi mums nepieciešams arī liegt/slēpt piekļuvi informācijai.

Kāpēc digitālā vidē pieeja datiem ir jāslēpj:

- datiem ir vērtība un tā ir jāpārvalda, lai to izmantotu noteiktiem mērķiem;
- datiem ir cilvēka/organizācijas privātuma īpašības/tiesības;

- datu pieejamība nodrošina digitālās vides funkcionalitātes patiesumu/drošību.

Digitālā vidē pieeju informācijai var liegt, aizslēdzot informācijas apstrādes iekārtas (datorus), piemēram, fiziski vai izmantojot paroles. Bet visplašāk informācijas pieejamības kontrolei izmanto datu kriptogrāfijas / datu šifrēšanas (kriptēšanas) tehnoloģijas.

Šifrēšana ir matemātiska funkcija, kas izmanto slepenu vērtību — atslēgu —, kas kodē datus, lai informāciju varētu lasīt tikai adresāts, kuram ir piekļuve šai atslēgai. Šifrēšana nodrošina atbilstošu aizsardzību pret neatļautu vai nelikumīgu datu apstrādi.

Informācija tiek šifrēta un atšifrēta, izmantojot vienu slepeno atslēgu (paroli). Daži algoritmi šifrēšanai un atšifrēšanai izmanto atšķirīgas atslēgas.

Divi galvenie darbības veidi, kuriem ir nepieciešams novērtēt šifrēšanas izmantošanu, ir datu glabāšana un datu pārsūtīšana fiziskos datu pārraides tīklos.

Kriptogrāfijas termins ir atvasināts no grieķu vārda kryptos, kas nozīmē apslēpts.

Izšķir trīs kriptogrāfijas lietojuma metodes: secret-key, public key, and hash function (slepenā atslēga, publiskā atslēga un jaucējfunkcija).

Kriptogrāfijas (Cryptography) jēdziens, neiedziļinoties mūsdienīgās kriptogrāfijas lietojuma niansēs, pēc būtības ir sinonīms jēdzienam kodēšana, šifrēšana (encryption), kas nodrošina cilvēkam saprotamas informācijas pārveidi uz tās neizprotamu saturu (unintelligible nonsens).

Mūsdienu kriptogrāfija atrodas matemātikas, datorzinātņu, elektrotehnikas, komunikācijas zinātnes un fizikas disciplīnu krustpunktā un risina datu konfidencialitātes, datu integritātes, darbību autentifikācijas, klienta autorizācijas problēmas. Kriptēšanas lietojumi (skat the General Council of the Bar's guidance on information security (PDF), which includes a section on encryption) ietver elektronisko tirdzniecību, mikroshēmu maksājuma kartes (skat the Payment Card Industry Data Security Standard (PCI-DSS)), digitālās valūtas, datoru paroles, elektronisku dokumentu parakstīšanu (skat the Attorney General's guidance on information security, which includes a section on the the storage and handling of electronic material), valsts noslēpuma / militāro sakaru informācijas uzglabāšanu un izmantošanu. Vispārīgāk runājot, kriptogrāfija ir tāda protokolu izveide un analīze, kas neļauj trešajām pusēm vai sabiedrībai lasīt aizsargātas ziņas.

Vieni un tie paši ievadītie dati, pielietojot šifrēšanu, vienmēr radīs vienu un to pašu rezultatīvo datu virkni. Apstrādājot rezultatīvo datu virkni, atkarībā no izmantotā šifrēšanas algoritma, ir sarežģīti vai pat neiespējami iegūt šifrēšanas atslēgu.

Datus šifrē, izmantojot atslēgu un jaukšanas algoritmus, piemēram, SHA (Secure Hashing Algorithm), tādejādi izveidojot nejaušu, unikālu, fiksēta garuma virkni no dotās atslēgas un ievadīto datu virknes.

Kriptējot izmanto iesālīšanas (salt) metodi. Jaukšanas algoritmi ir piemēroti, lai padarītu atslēgas nelasāmas, taču, tā kā tie vienmēr rada vienu un to pašu izvadi, tie nav īpaši droši. Sāls ir nejauša virkne, kas tiek pievienota ievadei pirms jaukšanas. Tas padara hash unikālāku un ir grūtāk uzminēt atslēgas.

Populāru kriptogrāfijas skaidrojumu skat, piemēram, https://fireship.io/lessons/node-crypto-examples/

1.1. Rokasgrāmata un skaidrojumi par to

Kriptogrāfija aptver nozīmīgu un ļoti plašu jautājumu un uzdevumu spektru. Rokasgrāmatas satura izklāsta strukturēšanai izmantotas vairākas sabiedrībā populāras informācijas pasniegšanas metodes, un tās ir sekojošas:

1. **Skatpunkts** (*Point of View*)- Rokasgrāmatas autoru aprakstošas situācijas izklāsts. Mēs aprakstām kriptogrāfijas un ar to saistītu risinājumu specifiskus aspektus (sistēmu sadalām). **Apraksta dekompozīciju** raksturo daudzveidība un tā nav pilnīga. Izmantotā dekompozīcijas skatapunkta metode būtiski atšķiras no matemātiskās, funkcionālās vai hierarhiskās dekompozīcijas.
   "Rakstot stāstu, ir jāizlemj, kurš stāsta un kam viņš to stāsta. Stāstu var stāstīt varonis, kas ir iesaistīts stāstā, vai arī no perspektīvas, kas redz un pazīst visus varoņus, bet nav viens no tiem. Skatījumu mēs piedāvājam kā autori pirmajā personā, atsaucoties uz citu viedokli (kā trešās puses viedokli vai noteiktu faktu)".
   Tuvāk skat,
   Complete Guide to Different Types of Point of View: Examples of Point of View in Writing, Written by MasterClass, Last updated: Sep 2, 2021 *https://www.masterclass.com/articles/complete-guide-to-point-of-view-in-writing-definitions-and-examples*
   Point of view State Definition & Meaning - Merriam-Webster *https://www.merriam-webster.com/words-at-play/point-of-view-first-second-third-person-difference*
2. **Satura prezentācijas veids "aktuālais"** (*State of the Art*). "Tehniskā situācija (dažreiz progresīvākā vai aktuālā) attiecas uz ierīces, tehnikas vai zinātnes nozares augstāko vispārējās attīstības līmeni, kas sasniegts noteiktā laikā. Tomēr dažos kontekstos tas var attiekties arī uz attīstības līmeni, kas sasniegts jebkurā konkrētā laikā, izmantojot tajā laikā izmantotās kopīgās metodoloģijas."(*Wikipedia. State of the Art, https://en.wikipedia.org*). Vai arī: " Attīstības līmenis (kā ierīce, procedūra, process, tehnika vai zinātne), kas sasniegts jebkurā noteiktā laikā, parasti mūsdienu metožu rezultātā" (*State of the art Definition & Meaning - Merriam-Webster,* https://www.merriam-webster.com/dictionary/state%20of%20the%20art).
3. **Kontrolsaraksts** (*Checklist*). Kontrolsaraksts ir darba atbalsta veids, ko izmanto, lai samazinātu neveiksmes, kompensējot iespējamos cilvēka atmiņas un uzmanības ierobežojumus. Tas palīdz nodrošināt konsekvenci un pilnīgumu uzdevuma veikšanā. Pamatpiemērs ir "darāmo darbu saraksts". Kontrolsaraksta primārais uzdevums ir uzdevuma dokumentēšana un dokumentācijas salīdzināšana. (*https://en.wikipedia.org/wiki/Checklist*).
4. **Anketa, anketēšana** (*Survey*). Cilvēku pētījumos aptauja ir jautājumu saraksts, kuru mērķis ir iegūt konkrētus datus no noteiktas cilvēku grupas. Aptauju pētījumi bieži tiek izmantoti, lai novērtētu domas, viedokļus un jūtas. Aptaujas var būt specifiskas un ierobežotas, vai arī tām var būt globālāki, plaši izplatīti mērķi. Aptauja sastāv no iepriekš noteikta jautājumu kopuma, kas tiek uzdota izlasei. Izmantojot reprezentatīvu izlasi, var aprakstīt iedzīvotāju grupas attieksmi, no kuras tika izveidota izlase. Turklāt var salīdzināt dažādu iedzīvotāju attieksmi, kā arī meklēt attieksmju izmaiņas laika gaitā. Svarīgi nodrošināt, lai aptaujas jautājumi būtu objektīvi, piemēram, netiek lietoti suģestējoši vārdi. Tas novērš neprecīzus rezultātus aptaujā.(*https://en.wikipedia.org/wiki/Survey_(human_research)*).
5. **Kontrolsaraksts vai Anketa.** (*Checklist vs Survey*). Gan anketa, gan kontrolsaraksts ir vērtēšanas instruments, taču atšķirība starp tiem ir tā, ka kontrolsaraksta mērķis ir novērtēt pašreizējo realitāti, bet anketēšanas mērķis ir izvērtēt nākotni. (*skat, piemēram, diskusiju: Ali A. Naeem. What is the scientific difference between the checklist and the questionnaire?*

When and why is each tool used? https://www.researchgate.net/post/What-is-the-scientific-difference-between-the-checklist-and-the-questionnaire).
Rokasgrāmatā nav ievērota konsekventa kontrosarakta un anketas lietošana: aprakstīts ir uzdevums- tēma, kuru var pārveidot vai nu Anketā vai kontrolsarakstā.

6. **Rokasgrāmata**. Par šī dokumenta nosaukumu varētu diskutēt. Ieceres ideja ir aizgūta no ENISA (https://www.enisa.europa.eu/). ENISA ir Savienības aģentūra, kuras mērķis ir sasniegt augstu kopējo kiberdrošības līmeni visā Eiropā, sniedzot ieguldījumu ES kiberpolitikā visām Eiropas Savienības dalībvalstīm, uzlabojot IKT uzticamību produktiem, pakalpojumiem, un procesiem ar kiberdrošības sertifikācijas shēmām un rekomendējošiem dokumentiem, sadarbojas ar dalībvalstīm un palīdzot sagatavoties nākotnes kiberproblēmām. Jau no 2013.gada ENISA publicē ikgadēju dokumentu " ENISA THREAT LANDSCAPE" (*piemēram, ENISA THREAT LANDSCAPE 2021. April 2020 to mid-July 2021,* https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021/@@download/fullReport) , kura uzdevums ir lasītājam sniegt apkopojošas ziņas par kiberdrošības situāciju. Rokasgrāmatas autori līdzīgā veidā vēlas Latvijas sabiedrībai iedibināt pārskatu par kriptogrāfijas lietojumu, kā galveno kiberdrošībās nodrošināšanas risinājumu.
ENISA daudzu garumā šāda dokumenta sagatavošanā ir uzkrājis bagātu pieredzi un formalizējis dokumenta sagatavošanas procesu, sagatavojot darbībai paredzētu metodoģiju (ENISA CYBERSECURITY THREAT LANDSCAPE METHODOLOGY JULY 2022, https://www.enisa.europa.eu/publications/enisa-threat-landscape-methodology/@@download/fullReport).
Politikas veidotājiem, riska pārvaldītājiem un informācijas drošības speciālistiem ir nepieciešama atjaunināta un precīza informācija par jaunākajiem IKT drošības risinājumiem. ES Kiberdrošības aģentūra (ENISA) sniedz rekomendācijas kiberdrošības jomā, bet mēs vairāk centrējamies uz kiberdošības realizācijas vienu no komponentēm- kriptogrāfiju.
Rokasgrāmatas sagatavošanā esam plaši izmantojuši ENISA rekomendācijas un publikācijas, tomēr satura izklāsta stils ir vispārīgāks, vairāk balstīts uz iepriekš nosauktām pieejām (approach)- mainot satura izklāsta stilu no "landscape" uz " point of view" un "state if the art".
Lai vienkāršotu lasītāja turpmākas iniciatīvas noteiktu kriptogrāfisko uzdevumu risināšanai, Rokasgrāmatā analizēto dokumenta saturu esam izvērsuši un iekļāvuši norādes uz rekomendētiem informācijas avotiem turpmākam lasītāja darbam.

1.2. Dažu būtiskāko terminu skaidrojumi

Plašam tehnoloģiju lokam tiek lietotas dažādas terminu variācijas, mēs piedāvāsim terminus, kas būtu adekvātāki mūsu reālajai situācijai.

- **Kiberdrošība** ir tehnoloģiju, procesu un vadības ierīču pielietojums, lai aizsargātu sistēmas, tīklus, programmas, ierīces un datus no kiberuzbrukumiem. Tā mērķis ir samazināt kiberuzbrukumu risku un aizsargāties pret sistēmu, tīklu un tehnoloģiju neatļautu izmantošanu (*It Governance. Cyber security, Cyber security.* https://www.itgovernance.co.uk/what-is-cybersecurity).
- **Kriptogrāfija** ir drošu saziņas metožu izpēte, kas ļauj tikai ziņojuma sūtītājam un paredzētajam saņēmējam skatīt tā saturu. Termins ir atvasināts no grieķu vārda kryptos, kas nozīmē slēpts (*Kaspersky. Definition, What is Cryptography. https://www.kaspersky.com Kaspersky*).
- **Atšķirība starp kodēšanu un šifrēšanu ir šāda**: lai gan kodēšana ir nepieciešama, lai informācija būtu saprotama ikvienam, šifrēšana tiek izmantota pretējam mērķim. Tas ir paredzēts, lai aizsargātu datus no jebkuras datu izlasīšanas bez atšifrēšanas atslēgas

(*Practicum Bootcamp, https://medium.com/practicum-by-yandex/what-is-the-difference-between-encoding-and-encryption-5e509c9a33fc*).

- **Klasiskās kriptogrāfijas** drošība balstās uz matemātiskās problēmas augsto sarežģītību liela skaita gadījumu faktorizēšanai. Kvantu kriptogrāfijas pamatā ir fizika, un tā balstās uz kvantu mehānikas likumiem (*Geeksforgeeks. Differences-between-classical-and-quantum-cryptography. (2022, June 22). https://www.geeksforgeeks.org/differences-between-classical-and-quantum-cryptography/*) .
- **Pēckvantu kriptogrāfija (PQC, Post-Quantum Cryptography)**, ko sauc arī par kvantu šifrēšanu, ir klasisko datoru kriptogrāfijas sistēmu izstrāde, kas var novērst sekmīgus kvantu datoru uzbrukumus (*Techtarget. Definition. Post-quantum cryptography. (n.d.).., from https://www.techtarget.com*) .

2. Vispārēja rakstura jautājumi par kriptogrāfijas lietojumu

2.1. Kriptogrāfija un kiberdrošība

Jēdzieni kriptogrāfija un kiberdrošība ir cieši saistīti un to atšķirība ir niansēs.
Kiberdrošība attiecas uz datu drošības nodrošināšanas procesu, savukārt kriptogrāfija ir viena no metodēm sensitīvas informācijas aizsardzībai. Tomēr kiberdrošība un kriptogrāfija ir divi termini, kurus nevajag lietot savstarpēji aizstājot. Šo terminu būtiskākās atšķirības attēlotas tabulā 1.

Kriptogrāfija	**Kiberdrošība**
- Sistēma, ko izmanto, lai šifrētu/atšifrētu datus, kurus nevar saprast neautorizēti lietotāji.	- Uzdevums attiecināms uz dažādiem pasākumiem, ko veic institūcijas organizācijas, lai atklātu un novērstu ļaunprātīgas darbības tīklos vai digitālajās ierīcēs.
- Metode, kurā ierobežo nevēlamo personu piekļuvi informācijai. Šifrēšanas kods un metode ir konfidenciāla.	- Metode ne vienmēr ir efektīva kibernoziedzības ierobežošanai, jo uzbrucēji joprojām var "apiet" vājas drošības sistēmas.
- Tehnoloģija, ko izmanto, lai uzlabotu kiberdrošību.	- Darbību kopums, kurā kriptogrāfija ir tikai viena no iespējām.
- Kriptogrāfija mazina kibernoziegumus, izmantojot speciālus tehnoloģiskos risinājumus.	- Kiberdrošība nozīmē īpašu procedūru uzturēšanu, lai nodrošinātu datu drošību.
- Tehnoloģija ietver personīgu zināšanu aspektu, jo sūtītājs un saņēmējs zina viens otra identitāti un bieži arī pārzina izmantoto tehnoloģisko rīku.	- Kiberdrošība nav personiska, jo tās nodrošinājuma politika tiek piemērota plašam lietojuma kontingentam.
- Kriptogrāfijas mērķi: 1. **Autentifikācija:** sūtītājs un saņēmējs zina viens otra identitāti. Viņi abi zina, kā šifrēt/ atšifrēt ziņojumu. 2. **Integritāte**: dati ir droši glabāti un droši pārsūtīti, jo neviens cits lietotājs tam nevar piekļūt, nevar atšifrēt kodu un izmantot vai izmainīt informāciju.	- Kiberdrošības mērķi: 1. Tīkla drošība 2. Datu drošība 3. Lietojumprogrammu drošība 4. Mobilo digitālo ierīču drošība 5. Mākoņdatošanas drošība

3. **Konfidencialitāte**: nepilnvarots lietotājs nevar piekļūt datu saturam.
4. Tāpat kriptogrāfijas mērķim pievieno **atbildību:** sistēmas darbībās vai to izcelsmē darītāju pēc tam var saukt pie atbildības par nodarījumu.

Tabula 1. Kriptogrāfijas unKiberdrošības tetminu būtiskākās atšķirības

"Kriptogrāfija ikdienas dzīvē" ietver vairākas situācijas, kurās kriptogrāfijas izmantošana atvieglo droša pakalpojuma sniegšanu: skaidras naudas izņemšana no bankomāta, maksas TV, e-pasta un failu glabāšana, izmantojot Pretty Good Privacy (PGP) bezmaksas programmatūru, droša tīmekļa pārlūkošana, un GSM mobilā tālruņa lietošana.

5 kriptogrāfijas ikdienas pielietojumi:

- Uzņēmuma ierīču šifrēšana.
- E-pasta sakaru nodrošināšana.
- Sensitīvu uzņēmuma datu aizsardzība.
- Datu bāzu šifrēšana.
- WEB vietnes nodrošināšana.

Rokasgrāmatā tiek pētīts kriptogrāfijas lietojums, tātad tematiski mēs esam saistīti gan ar tiešu kriptogrāfijas jēdzienu, gan ar kiberdrošību. Mēs veiksim aptauju lietotājiem ikdienas scenāriju ietvarā. Tādejādi tematiski pētījums var tikt attiecināts arī uz kiberdrošību, tomēr mūsu aptauja ierobežota ar personīgo viedokli un aptauja mazāk skar institucionālos risinājumus.

2.2. Drīkst/nedrīkst datus šifrēt (kriptēt). Regulēšanas principi : drīkst/nedrīkst, pēc pieprasījuma jāatkodē

Mūsdienu sabiedrībā cilvēkiem dati ir nozīmīgi, tāpēc datu apstrādes iespējas regulē. Dažādās valstīs datu apstrādes iespējas tiek regulētas ar dažādām prasībām. Datu kriptogrāfijas tiesības nosaka starptautiski līgumi un vienošanās, kriminālprocesa kodeksi, likumi par kibernoziegumiem, sakaru/telekomunikāciju likumi, informācijas pārtveršanas/novērošanas likumi un citi dekrēti, akti, rezolūcijas, darbības politikas un darba labās prakses dokumenti. Normatīvie akti parasti galvenokārt skar sakaru nodrošinātājus, interneta pakalpojumu sniedzējus vai ir attiecināmi uz datiem, kas tiek glabāti datoros.

Kriptogrāfijas tehnoloģijām ir valsts stratēģiska nozīme un tāpēc arī tiek regulēta datu drošības industrijas preču apmaiņa.

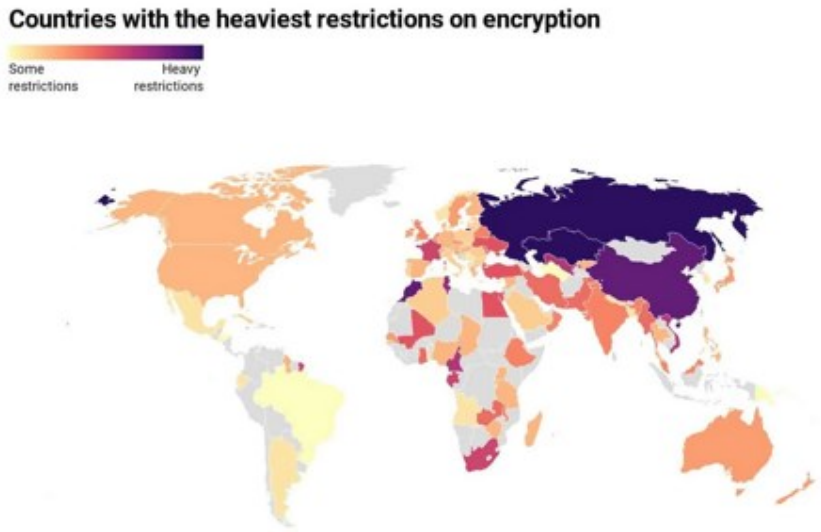
Starpvalstu vienošanos par preču apmaiņu, tai skaitā datu drošības risinājumus regulē Vasenāras vienošanās (Wassenaar Arrangement), kuru parakstījušas 42 valstis (2017):

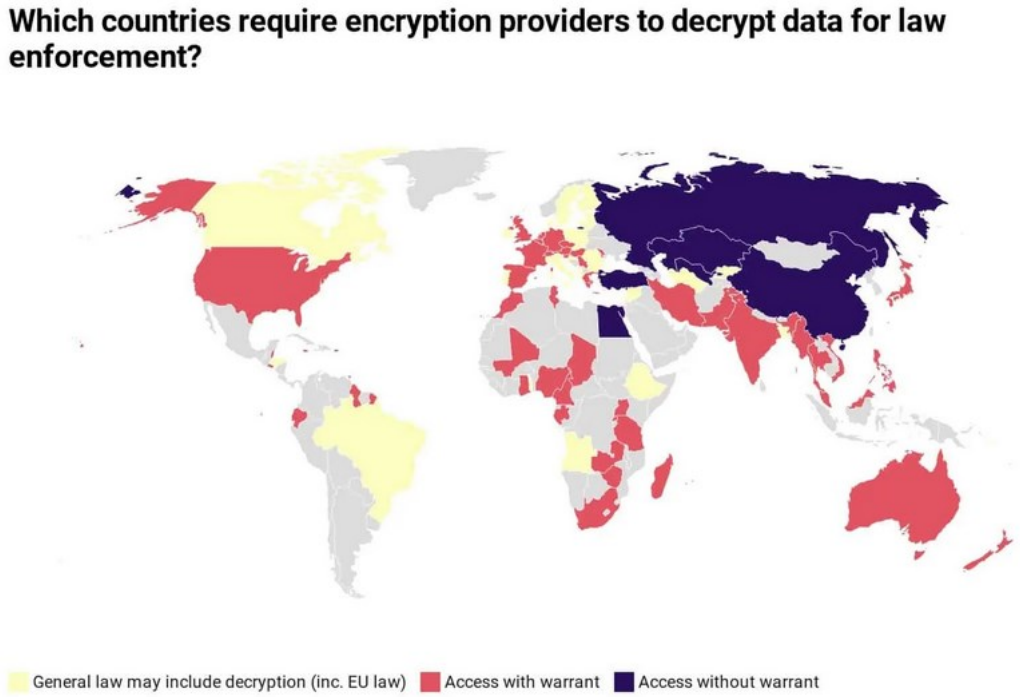
Argentīna, Austrālija, Austrija, Beļģija, Bulgārija, Kanāda, Horvātija, Čehija, Dānija, Igaunija, Somija, Francija, Vācija, Grieķija, Ungārija, Indija, Īrija, Itālija, Japāna, Latvija, Lietuva, Luksemburga, Malta, Meksika, Nīderlande , Jaunzēlande, Norvēģija, Polija, Portugāle, Korejas Republika, Rumānija, Krievijas Federācija, Slovākija, Slovēnija, Dienvidāfrika, Spānija, Zviedrija, Šveice, Turcija, Ukraina, Apvienotā Karaliste un Amerikas Savienotās Valstis.

Vienlaicīgi jāatzīmē, ka ikviena valsts nacionāli un starptautiski attīsta datu drošības risinājumu industriju [1], [2].

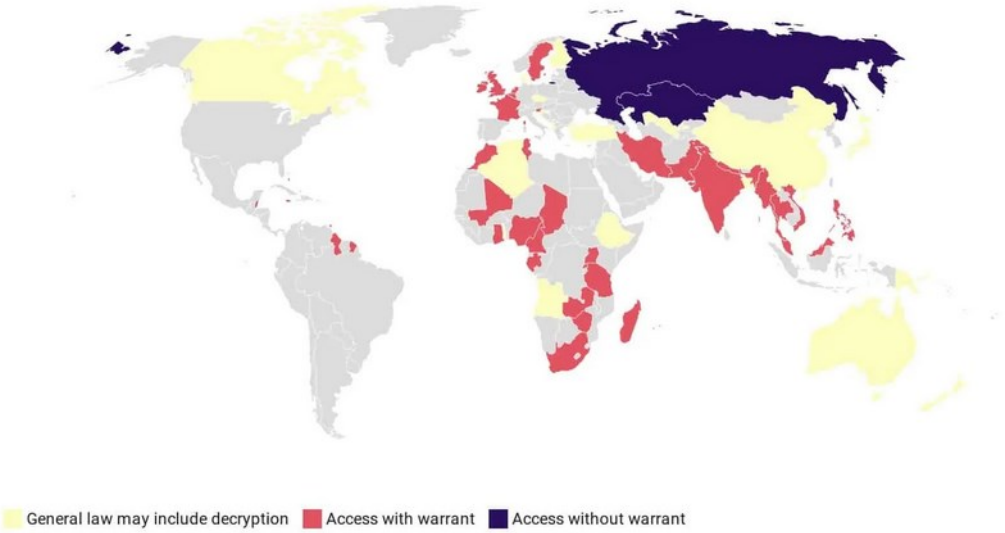
Eiropā DIGITAL EUROPE [3] atzinīgi vērtē iespējas izstrādāt Komerciālās kriptogrāfijas administratīvo noteikumu projektu (2020). Šifrēšanas politika nosaka, kad šifrēšana ir vai nav jāizmanto, un šifrēšanas tehnoloģijas vai algoritmi, kas ir pieņemami. Piemēram, politika var likt izmantot īpašus pārbaudītus algoritmus, piemēram, 3DES, RSA vai IDEA, un aizliegt izmantot patentētus vai nestandarta algoritmus.

Kriptogrāfijas likumi ir tiesību aktu kopums, kas attiecas uz informācijas nodrošināšanu un aizsardzību pret nesankcionētu piekļuvi. Kriptogrāfijas likumi aizsargā personas no viņu personīgās informācijas izplatīšanas bez viņu piekrišanas. Kriptogrāfijas likumi aizsargā nacionālos (valsts) un militāros noslēpumus. Dažas valstis aizliedz kriptogrāfijas programmatūras un/vai šifrēšanas algoritmu vai kriptoanalīzes metožu eksportu. Dažas valstis pieprasa, lai atšifrēšanas atslēgas būtu atkopjamas policijas izmeklēšanas gadījumā.
Kriptogrāfijas starptautisko tiesisko regulējumu raksturosim no [4]
Vājākie- smagākie ierobežojumi ir:

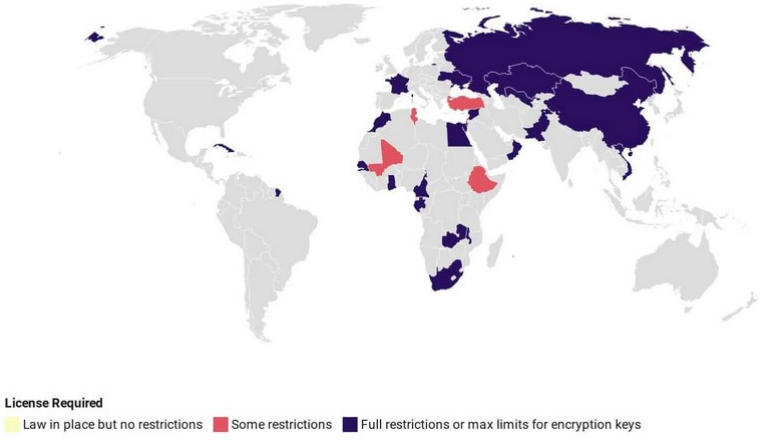


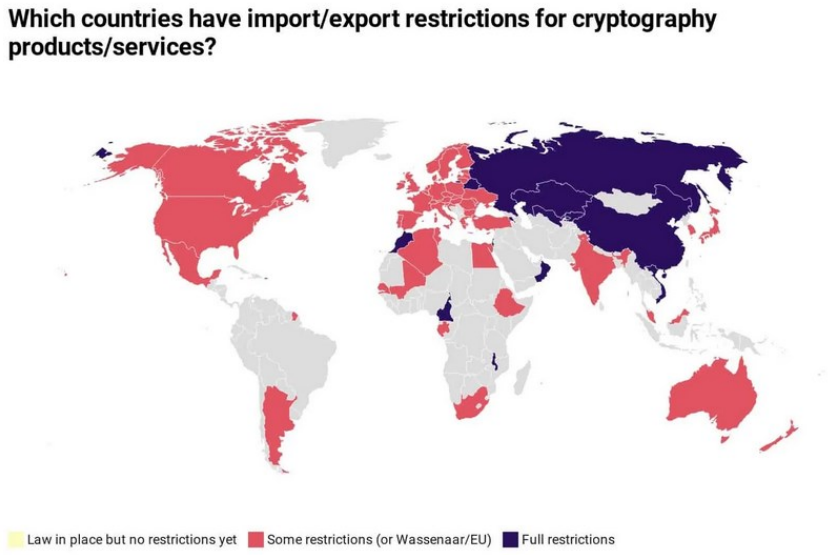


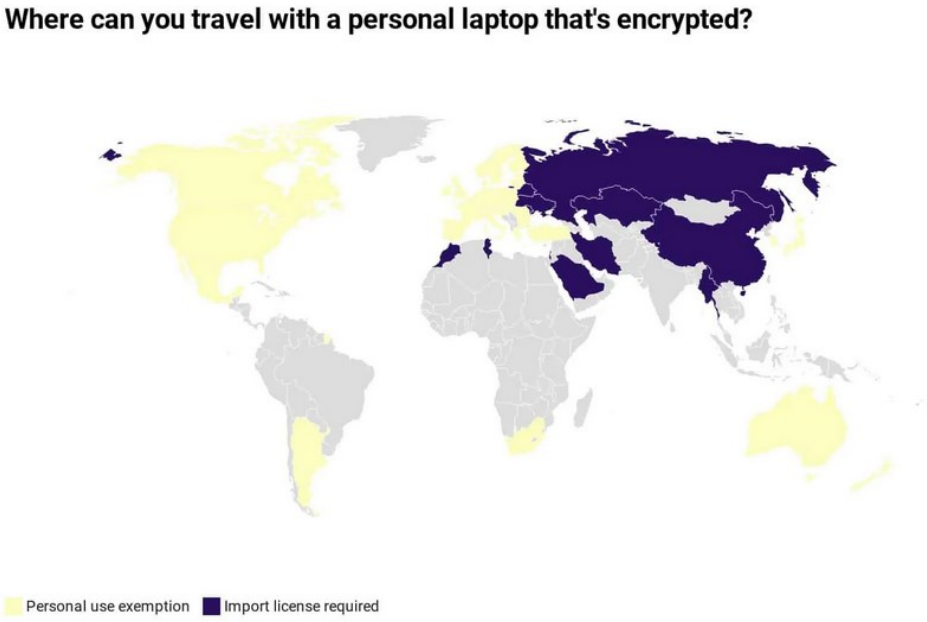
Which countries require encryption users to decrypt data for law enforcement?



Which countries have licensing requirements for cryptography products/services?







2.3. Likumi Latvijā: atklātība, aizsardzība, publiskas informācijas atkal izmantošana

Informācijas pieejamību Latvijā regulē Informācijas atklātības likums, kas satur publiskas informācijas atkal izmantošanu, kā arī Fizisko personu datu apstrādes likums (www.likumi.lv). Šis likumu kopums atbilst Eiropas regulējumam.
Likumos un normatīvajos regulējumos atrunā specifiskus informācijas lietošanas nosacījumus:
- Datu apstrāde oficiālajā publikācijā (mēdiju informācija);
- Datu apstrāde statistikas nolūkos;
- Datu apstrāde arhivēšanas nolūkos sabiedrības interesēs;
- Datu apstrāde zinātniskās vai vēstures pētniecības nolūkos;
- Datu apstrāde saistībā ar vārda un informācijas brīvību;
- Nosacījumi bērna piekrišanai attiecībā uz informācijas sabiedrības pakalpojumiem;
- Datu apstrāde krimināltiesību jomā

Tāpat starptautiskā praksē tiek atrunāta informācijas izmantošanas prakse politiskās kampaņās.

2.4. Kriptēšana un cilvēktiesības

Mūsuprāt ļoti vērtīgs apkopojums par situāciju atspoguļots [5]. Kkriptogrāfiju plaši izmanto arī kriminālā pasaule. Šī apstākļa dēļ kriptogrāfijas likumdevējiem jārēķinās ar cilvēktiesību prasībām, kā arī ļaunprātīgu informācijas izmantošanu kriminālajās aprindās (Regulated encryption isn't possible — here's what is https://www.politico.eu/article/regulated-encryption-solution/). Tas attur ļoti stingru prasību iekļaušanu kriptogrāfijas likumos un aicina valstis noziedzības apkarošanai meklēt arī citus risinājumus, saistītus ar izmeklēšanas metožu izstrādi ļaunprātīgas kriptogrāfijas izmantošanas gadījumos.
Eiropas Komisija ierosināja 6 konkrētus neleģislatīvus risinājumus (https://ec.europa.eu/home-affairs/cybercrime/encryption_en), lai palīdzētu tiesībaizsardzības iestādēm pārvarēt problēmas, ko kriminālās izmeklēšanas kontekstā rada šifrēšana. Šie pasākumi atbilst stingrai prasību šifrēšanas uzturēšanai, kas nepieciešama digitālā vienotā tirgus darbībai, un nekādā veidā neaizliedz, neierobežo vai vājina šifrēšanu šajos lietojumos.
Komisija tuvākajā laikā neplāno sagatavot tiesību aktus specifiski par šifrēšanu.

3. Scenāriji ikdienas darbiem digitālajā vidē, kad jāizlemj kriptogrāfijas izmantošana

3.1. EU regulējums-eIDAS:

"eIDAS" [9] ir saīsinājums no "elektroniskās identifikācijas un uzticamības pakalpojumiem". Tas attiecas uz virkni pakalpojumu, kas ietver personu un uzņēmumu identitātes pārbaudi tiešsaistē un elektronisko dokumentu autentiskuma pārbaudi.

Elektroniskos uzticamības pakalpojumus var izmantot vairākos veidos, lai nodrošinātu elektronisko dokumentu, sakaru un darījumu drošību, piemēram, lai palīdzētu nodrošināt, ka elektroniski nosūtītie dokumenti nav nekādā veidā mainīti un ka sūtītāju var viegli atpazīt. Elektroniskie uzticamības pakalpojumi ļauj piemērot šādus drošības rekvizītus un pēc tam tos apstiprināt, tādējādi palīdzot nodrošināt pārliecību par informācijas elektronisku pārsūtīšanu.
"Kriptogrāfija ikdienas dzīvē" ietver vairākas situācijas, kurās kriptogrāfijas izmantošana atvieglo uzticama pakalpojuma sniegšanu: skaidras naudas izņemšana no bankomāta, maksas TV, e-pasta un failu glabāšana, izmantojot Pretty Good Privacy (PGP) bezmaksas programmatūru, droša tīmekļa pārlūkošanu, un mobilā tālruņa lietošanu.
Kriptogrāfijas ikdienas pielietojumu piemēri:

- Uzņēmuma ierīču šifrēšana.
- E-pasta sakaru nodrošināšana.
- Sensitīvu uzņēmuma datu aizsardzība.
- Datu bāzu šifrēšana.
- WEBlapas izmantošanas drošība.

eIDAS uzticamības pakalpojumiem un izveidots tiesiskais regulējums elektronisko parakstu, elektronisko zīmogu, elektronisko laika zīmogu, elektronisko dokumentu, elektroniskās reģistrētās piegādes pakalpojumu un vietņu autentifikācijas sertifikātu izsniegšanas pakalpojumus.
Ir pieci īpaši uzticamības pakalpojumu veidi, uz kuriem attiecas eIDAS noteikumi:

- elektroniskie paraksti;
- elektroniskie zīmogi;
- elektroniskie laika zīmogi;

- reģistrēti droši elektroniskie pakalpojumi;
- WEB vietņu autentifikācijas sertifikāti.

3.1.1. eIDAS lietojuma scenāriji

Autentifikācija un digitālie paraksti ir ļoti svarīgs publiskās atslēgas kriptogrāfijas lietojums. Piemēram, ja saņemat ziņojumu, ka esmu šifrējis ar savu privāto atslēgu, un jūs varat to atšifrēt, izmantojot manu publisko atslēgu, jums vajadzētu justies diezgan pārliecinātam, ka ziņojums tiešām ir no manis. Ja es uzskatu, ka ir nepieciešams paturēt ziņojumu noslēpumā, es varu šifrēt ziņojumu ar savu privāto atslēgu un pēc tam ar jūsu publisko atslēgu, tādējādi tikai jūs varat izlasīt ziņojumu un zināt, ka ziņojums ir no manis. Vienīgā prasība ir, lai publiskās atslēgas būtu saistītas ar to lietotājiem uzticamā veidā, piemēram, ar uzticamu direktoriju. Lai novērstu šo trūkumu, izmanto sertifikātu. Sertifikātā ir iekļauts sertifikāta izsniedzēja nosaukums, subjekta nosaukums, kuram sertifikāts tiek izsniegts, subjekta publiskā atslēga un daži laika zīmogi. Jūs zināt, ka publiskā atslēga ir laba, jo sertifikāts ir arī sertifikāta izsniedzējam.

Kas ir reģistrēta droša elektroniskā pakalpojuma sertifikāts
Elektroniskā paraksta vai zīmoga sertifikāts ir "elektroniskais apliecinājums", kas satur datus, kas apliecina paraksta vai zīmoga derīgumu un saista to ar konkrētu nosauktu personu (parakstiem) vai organizāciju (zīmogiem) un apstiprina parakstīto vai aizzīmogoto datu izcelsmi un autentiskumu.
Kvalificēts sertifikāts ir jāizsniedz kvalificētam uzticamības pakalpojumu sniedzējam, un tajā jāiekļauj īpaša informācija, kas norādīta eIDAS regulas pielikumos.
Elektroniskā paraksta vai zīmoga sertifikāts atšķiras no vietnes autentifikācijas sertifikāta
Vietnes autentifikācijas sertifikāti identificē personu vai uzņēmumu, kas uztur tīmekļa vietnes saturu, un palīdz pārbaudīt, vai vietne ir autentiska.

Elektroniskie paraksti
Elektroniskais paraksts ir jebkura metode, ko indivīds izmanto, lai "parakstītu" elektronisku dokumentu. Tas aptver plašu pasākumu klāstu, sākot no vienkārša teksta vai digitāla attēla piestiprināšanas līdz sarežģītākām augsto tehnoloģiju metodēm, kas atbilst īpašiem kritērijiem, kas noteikti eIDAS regulā uzlabotiem vai kvalificētiem elektroniskajiem parakstiem. Elektroniskie paraksti ir pieņemami kā pierādījums tiesā.

Elektroniskie zīmogi
Elektroniskie zīmogi ļauj uzņēmumiem un citām korporatīvajām struktūrām "apzīmogot" elektroniskos dokumentus un apliecināt tos kā īstus, tāpat kā privātpersona var izmantot elektronisko parakstu. Tie ir pieņemami kā pierādījumi tiesā. Tāpat kā ar elektroniskajiem parakstiem, ir uzlaboti un kvalificēti elektroniskie zīmogi, kas piedāvā papildu priekšrocības salīdzinājumā ar pamata elektroniskajiem zīmogiem.

Elektroniskie laika zīmogi
Elektroniskais laika zīmogs pierāda, ka konkrēti dati pastāvēja noteiktā laikā un kopš tā laika nav mainīti.
Laika zīmogs ir paņēmiens, kas var apliecināt, ka noteikts elektroniskais dokuments vai saziņa pastāvēja vai tika piegādāts noteiktā laikā. Laika zīmogs izmanto šifrēšanas modeli, ko sauc par aklā paraksta shēmu. Aklā paraksta shēmas ļauj sūtītājam saņemt ziņojumu, ko saņem cita puse, neatklājot otrai pusei nekādu informāciju par ziņojumu.
Laika zīmogs ir ļoti līdzīgs ierakstītas vēstules nosūtīšanai pa pastu, taču tā nodrošina papildu pierādījumu līmeni. Tas var pierādīt, ka saņēmējs ir saņēmis konkrētu dokumentu. Iespējamie

pieteikumi ietver patentu pieteikumus, autortiesību arhīvus un līgumus. Laika zīmogs ir ļoti svarīga lietojumprogramma, kas palīdzēs padarīt iespējamu pāreju uz elektroniskiem juridiskiem dokumentiem.

Reģistrēti droši elektroniskie pakalpojumi
Reģistrēti droši elektroniskie pakalpojumi darbojas kā drošs tiešsaistes apliecinājums par izsūtīšanu vai ierakstītas piegādes pakalpojumu. Tie sniedz pierādījumus, ka informācija tika nosūtīta un saņemta elektroniski un ka tā nav pārtverta vai mainīta ceļā. Vairāk lasīt [6. 7, 8].

[10] ENISA,
Recommendations for technical implementation of the eIDAS Regulation
Towards a harmonised Conformity Assessment Scheme for QTSP/QTS
DECEMBER 2019

[11] www.enisa.europa.eu European Union Agency For Network And Information Security
eIDAS: Overview on the implementation and uptake of Trust Services
One year after the switch over
DECEMBER 2017

[12] European Union Agency for Network and Information Security www.enisa.europa.eu
Standardisation in the field of Electronic Identities and Trust Service Providers
Inventory of activities, Version 1.0, December 2014

3.1.2. Paroles datu aizsardzībai

Laba paroļu sistēma ir tāda, kas sniedz pietiekamu pārliecību, ka persona, kas mēģina pieteikties, ir lietotājs, par kuru viņa uzdodas. Praksē tas nozīmē, ka labai paroļu sistēmai ir jāaizsargā pret divu veidu uzbrukumiem:

- parolēm jābūt grūti pieejamām lietojamā formā;
- parolēm jābūt iespējami grūti uzminējamām, neskatoties uz dabīgu prasību, lai tieši paroles autoram būtu tās viegli atcerēties vai uzglabāt.

Paroles autors pats nosaka paroles izskatu un uzglabāšanu. Tomēr praksē būtu jāizmanto procedūra, ko sauc par SHA (Secure Hashing Algorithm) (detaļas skat **https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-132.pdf**). SHA funkcija ir vienvirziena metode, kas pārvērš paroli jauktā vērtībā, ko bieži sauc vienkārši par "jauktu", t.i., neglabājot paroli vienkāršā tekstā.

3.2. EU regulējums- NIS

NIS [6] ir paredzēts, lai izveidotu kopēju tīkla un informācijas sistēmu drošības līmeni. Lai gan NIS galvenokārt attiecas uz kiberdrošības pasākumiem, tā aptver arī fiziskos un vides faktorus. Tuvāk par NIS skat. [7].

Tehnoloģiski adekvātu drošības līmeni darbiem tīklā realizē aplikāciju un zemāku OSI standarta līmeņa datu apmaiņas protokolos.

Secure Socket Layer (SSL) protokolu izmanto, lai nodrošinātu datu drošību slāņos starp TCP/IP (interneta sakaru pamata protokols) un lietojumprogrammu protokoliem (piemēram, HTTP, Telnet, NNTP vai FTP). SSL atbalsta datu šifrēšanu, servera autentifikāciju, ziņojumu integritāti un klienta autentifikāciju TCP/IP savienojumiem.

SSL protokols autentificē katru savienojuma galu (serveri un klientu), un otrā vai klienta autentifikācija nav obligāta.
SSL izmanto RSA publiskās atslēgas kriptosistēmas autentifikācijas darbībām. Pēc atslēgu apmaiņas tiek izmantotas vairākas dažādas kriptosistēmas, tostarp RC2, RC4, IDEA, DES un triple-DES. Rokasgrāmatas 3. sadaļā tuvāk tiek aplūkota protokolu izmantošana.

3.3. Datu anomizācija – EU regulējums GDPR

Lai nodrošinātu personu datu aizsardzība atbilstoši GDPR [8] prasībām, ir jāizmanto datu anonimizācijas tehnoloģijas, kas savukārt satur kriptogrāfijas instrumentus.
Skat. [9], [10], [11].
Pseidonimizācija ir personas datu apstrāde tādā veidā, ka personas datus vairs nevar attiecināt uz konkrētu datu subjektu, neizmantojot papildu informāciju, ja šāda papildu informācija tiek glabāta atsevišķi un tai tiek piemēroti tehniski un organizatoriski pasākumi, lai nodrošinātu, ka personas dati netiek attiecināti uz identificētu vai identificējamu fizisku personu *(GDPR, art. 4(5))5.*
Anonimizācija ir process, kurā personas dati tiek neatgriezeniski izmainīti tā, ka datu subjektu vairs nevar tieši vai netieši identificēt ne datu pārzinis pats, ne sadarbībā ar jebkuru citu pusi (ISO/TS 25237:2017)6.
Sadzīviski runājot pseidonimizācijas mērķis ir aizsargāt personas datus, slēpjot personas identitāti, piemēram, aizstājot vienu vai vairākus personas datu identifikatorus ar tā sauktajiem pseidonīmiem un atbilstoši aizsargājot saikni starp pseidonīmiem un sākotnējiem personas datiem.
Izšķir vairākus anonimizācijas risinājumus:
1) Deterministiska pseidonimizācija – vienmēr vieniem un tam pašiem datiem lieto vienu un to pašu pseidonīmu;
2) Dokumentā gadījuma pseidonimizācija – izmantojot vienu un to pašu pseidonīmu
Vieniem un tiem pašiem datiem tikai dokumenta ietvarā;
3) Pilnībā gadījuma pseidonimizācija — vienmēr izmantojot citu pseidonīmu
tiem pašiem datiem.
Pseidoanonimizācijas pamata tehnoloģiju apskats (termini).

Tehnika Pseidonīma ģenerators

Skaitītājs (Counter) *Monotonisks skaitītājs, kas sākas ar noteiktu vērtību un tiek palielināts katru reizi, kad ir nepieciešams jauns pseidonīms*

Gadījuma skaitlis (Random number) *Nejauša vērtība, kas iegūta no minimuma līdz maksimumam robežām katru reizi, kad ir nepieciešams jauns pseidonīms*

Jaucējfunkcija (Hash function) *Vienvirziena (neatgriezeniska) kriptogrāfiskā funkcija lai pārveidotu personas datus fiksēta garuma vērtībās*

Uz jaucējkodu balstīts ziņojuma autentifikācijas kods Hash-based message authentication code (HMAC)

Vienvirziena (neatgriezeniska) kriptogrāfijas funkcija, kas pievieno atslēgu padarot ziņojumu mazāk paredzamu nekā jaucējfunkcija

Šifrēšana (Encryption) Divvirzienu (atgriezeniska) kriptogrāfijas funkcija, kas pārveido ievadītās personas datus, kuras iespējams atkārtoti pārveidot oriģinālajā formātā, izmantojot atslēgu

3.4.Valsts reģistri, publiskie dati, ģeotelpiskie dati, datu bāzes, internets

Virsrakstā minētie informācijas avoti un datu apstrādes iespējas pakļaujas vispārīgām prasībām un regulējumam. Realizētās tehnoloģijas nodrošina nepieciešamu aizsardzību un adekvātu

kriptogrāfijas metožu lietojumu. Rokasgrāmatas trešajā sadaļā ir aplūkoti kriptogrāfijas lietojumi protokolos, ierīcēs, tīklos, ar kuriem tad arī tiek nodrošināta nepieciešamā kiberdrošība un kriptogrāfijas tehnoloģiju lietojumus.
Šajā rokasgrāmatas sadaļā tēma ir iekļauta, lai aptaujā iegūtu ļoti vispārīgu kriptogrāfijas tehnoloģiju lietošanas novērtējumu.

3.5. Citi bieži kriptogrāfijas lietojumi ikdienā

3.5.1. Datu nosūtīšana pa e-pastu un šifrēti pielikumi

Šifrēts e-pasts var nodrošināt iespēju šifrēt e-pasta ziņojumu pamattekstu un pielikumus. Piemēram, OpenPGP un S/MIME standarti ir plaši izmantotas šifrēšanas metodes, kuras ir ieviesušas virkne bezmaksas un komerciālu programmatūras produktu.
Šifrēta e-pasta sūtīšanai un saņemšanai ir jāizmanto saderīga e-pasta klienta programmatūra un ir nepieciešama iepriekšēja konfigurācija. Ir daži specializēti tīmekļa pasta pakalpojumu sniedzēji, kas atbalsta šifrētu e-pastu, taču lielākā daļa tiešsaistes e-pasta pakalpojumu sniedzēju to parasti neatbalsta, lai gan ir daži pārlūkprogrammas spraudņi, kas var nodrošināt šo iespēju, un šajā jomā tiek panākts turpmāks progress.

Pēc nepieciešamības tiek lietoti šifrēti e-pasta pielikumi. Lai atšifrētu pielikumu, adresātam ir jābūt saderīgai programmatūrai un zināmai atslēgai. Parasti atslēga tiek iegūta no īsākas, neaizmirstamākas paroles, ko var pārsūtīt adresātam; tomēr parolei jābūt pietiekami garai un sarežģītai, lai izvairītos no kompromitēšanas.

3.5.2. Droša tīmekļa pakalpojuma lietošanas scenāriji

WEB tīmekļa lietojumus var izveido bez drošības ietekmes, kā drošas darba tehnoloģijas ar kriptogrāfijas risinājumiem, skat, piemēram,
Oracle® Application Server Web Services Security Guide
Understanding Web Services Security Concepts
https://docs.oracle.com/

Nedrošu tīmekļa pakalpojumu risinājumos ir ietverti vienkārši lietošanas gadījumi, kuros netiek izmantota tīmekļa pakalpojumu drošība, savukārt var tikt izmantoti dažādi drošibas risinājumi, piemēram::
• uz HTTP balstīta drošība
• WS-Security
• XML paraksts
• XML šifrēšana
• vārtejas
• identitātes pārvaldība
• sadarbspēja

3.5.3. Dublējumkopijas

Izplatīts scenārijs ir tāds, ka organizācija ieraksta dublējumkopijas lentē, diskā vai citā fiziskā datu nesējā, kas tiek pārvietota uz drošu vietu. Ja dati tiek glabāti šifrētā formātā, tie tiks aizsargāti pret nesankcionētu piekļuvi. Tomēr būs svarīgi nodrošināt labu atslēgu pārvaldību, lai nodrošinātu, ka datiem nākotnē var piekļūt, kad tas būs nepieciešams.
Ilgtermiņa dublēšanas vai arhīva gadījumā var būt svarīgi arī nodrošināt, lai datiem joprojām var piekļūt un izmantotā šifrēšana laika gaitā ir piemērota. Jums būs jāņem vērā arī "tiesības uz dzēšanu".

3.5.4. Mākoņdatošana

Datu apstrāde mākonī rada risku, jo jūsu datus pārvalda mākoņa pakalpojumu sniedzējs. Tāpēc jums ir nepieciešams novērtēt mākoņa nodrošinātāja veiktos drošības pasākumus, lai nodrošinātu, ka tie būtu jums piemēroti jūsu datu drošības politikai.

Homomorphic encryption

Homomorfā šifrēšana ļauj veikt šifrētu datu aprēķinus, tos vispirms neatšifrējot. Tipisks homomorfās šifrēšanas lietošanas gadījums ir tad, kad datu subjekts vēlas nodot savu personas datu apstrādi ārpakalpojumu sniedzējam, neatklājot personas datus vienkāršā tekstā. Ir skaidrs, ka šādas funkcijas ir ļoti piemērotas, ja apstrādi veic trešā puse, piemēram, mākoņpakalpojumu sniedzējs.

ENISA. Data Protection Engineering
https://www.enisa.europa.eu/publications/data-protection-engineering
DATA PROTECTION ENGINEERING
From Theory to Practice, JANUARY 2022

3.6. Aptaujas Anketa

Uz katru jautājumu tabulas rindā (iezīmētu ar BOLD) var izvēlēties vienu, divas, trīs vai četras atbildes, atzīmējot savu izvēli uz jautājumu atbilstošā kvadrātā zem jautājuma rindas.
Savas izvēlētās atbildes tekstu kvadrātā iekrāsojiet vai arī kvadrātā ielieciet kādu ķeksi pie teksta (tātad šī atbilde būs izvēlēta). Dzēsts teksts nozīmēs jautājuma/ secinājuma noraidīšanu. Ja Anketa ir uz papīra, tad ielieciet ķeksi pie teksta vai nosvītrojiet tekstu, ja Jums tas šķiet noraidāms. Pretrunīgas atbildes uz jautājumu tiks ignorētas. Atbilde uz jautājumu tiek sagaidīta personalizēta: man tā jādara/ es tā daru/ darīšu/ man tas ir vai šķiet svarīgi. Respondentam atbildes nav jāpamato - tās vien atspoguļo atbildētāja vispārinātas zināšanas, domas, izjūtas par tēmu jautājumā.
Aptaujas rezultāti tiks izmantoti, lai novērtētu respondenta inviduālas domas un viedokļus par datu kriptēšanas un kriptogrāfijas lietojumu un to nepieciešamību.
Atbildes lūdzam iesūtīt imcs@lumii.lv vai biedrības Latvijas Digitālais akselerators mājas lapā.

Kriptogrāfija un kiberdrošība ***Jūsu vērtējums par kiberdrošību valstī***			
kriptogrāfijas lietošana neietekmē kiberdrošību valstī	*esošie kriptogrāfijas tehnoloģiskie risinājumi nodrošina adekvātu kiberdrošību*	*nepieciešama kriptogrāfijas tehnoloģiju aktīvāka izmantošana*	*nepieciešams modernizēt kriptogrāfiskos risinājumus*
Drīkst/nedrīkst datus šifrēt (kriptēt). Regulēšanas principi: drīkst/nedrīkst, pēc pieprasījuma jāatkodē **Jūsu vērtējums par kriptogrāfijas lietošanas normatīvo regulējumu**			
nav nepieciešams kriptogrāfijas lietojuma politikas dokuments	*esošie kriptogrāfijas lietošanas dokumenti ir pietiekami*	*nepieciešama precīzāka un aktīvāka kriptogrāfijas labās prakses izmantošana*	*nepieciešams pieprasīt modernizēt kriptogrāfiskos risinājumus*
Likumi Latvijā: atklātība, aizsardzība, publiskas informācijas atkal izmantošana **Jūsu vērtējums par kriptogrāfijas normatīvo regulējumu Latvijā**			
nav nepieciešams kriptogrāfijas lietojuma tālāks regulējums	*esošie kriptogrāfijas lietošanas dokumenti Latvijā ir samērojami ar starptautisko labo praksi*	*nepieciešams iespējot kriptogrāfijas lietošanas starptautisko praksi privātās digitālās ierīcēs*	*normatīvos nepieciešams noteikt, ka jālieto pārbaudīti jaunākie kriptogrāfiskie risinājumi*
Kriptēšana un cilvēktiesības **Jūsu vērtējums par kriptogrāfiju un cilvēktiesībām**			

nav jāsaista kriptogrāfijas lietošana ar cilvēktiesību jautājumu	*kriptogrāfijas lietošana nerada pretrunas ar cilvēktiesībām*	*neapzināta jauno tehnoloģiju lietošana, piemēram, mākslīgais intelekts, radīs pretrunas ar cilvēktiesībām*	*tikai jaunāko kriptogrāfisko risinājumu lietojums var radīt pretrunas ar cilvēktiesībām*
EU regulējums par EiDAS [1] **Jūsu vērtējums par uzticamības pakalpojumu realizēto drošību**			
kriptogrāfijas lietošana eIDAS nav jāvērtē	*esošie rīki ar iekļautu kriptogrāfiju nerada bažas par drošības apdraudējumu*	*ir jāizvērtē katra rīka drošības riskus*	*jālieto rīki tikai ar jaunākajiem kriptogrāfiskajiem risinājumiem*
Paroles datu aizsardzībai **Jūsu vērtējums par paroļu lietošanas kultūru**			
tekstisku paroļu izmantošana ir pietiekama	*ieteicams izmantot paroles ar jaucējfunkciju aizsardzību, piemēram, SHA (Secure Hashing Algorithm)*	*paroles var tikt dažādotas atkarībā no lietošanas vides*	*jālieto paroles tikai ar jaunākajiem kriptogrāfiskajiem risinājumiem*
EU regulējums- NIS [2] **Jūsu vērtējums par NIS direktīvas ieviešanu**			
kriptogrāfijas lietošana NIS direktīvas ietvaros neinteresē	*esošie komunikāciju lietojumi nerada bažas par drošības apdraudējumu*	*ir jāizvērtē drošības riski*	*komunikācijās jālieto rīki tikai ar jaunākajiem kriptogrāfiskajiem risinājumiem*
Datu anomizācija EU regulējuma GDPR ietvarā [3] **Jūsu integrēts vērtējums par kriptogrāfijas lietošanu**			
personas datu anonimizācija neinteresē	*esmu saskāries ar personas datu visvienkāršāko anonimizācijas risinājumu*	*ir jāizvērtē drošības riski atklāt anonimizācijai pakļautos datus*	*personas datu anonimizācijai jālieto rīki tikai ar jaunākajiem kriptogrāfiskajiem risinājumiem*
Valsts reģistri, publiskie dati, ģeotelpiskie dati, datu bāzes, internets **Jūsu integrēts vērtējums par kriptogrāfijas lietošanu**			
pieņemu piedāvāto pakalpojumu un nevērtēju kriptogrāfijas vajadzību	*novērtēju, ka esošie kriptogrāfijas tehnoloģiskie risinājumi atbilst adekvāti manām vajadzībām*	*nepieciešama paša iniciatīva datu aizsardzības aktīvākai izmantošanai, piemēram, VPN izmantošana*	*nepieciešams modernizēt piedāvātos kriptogrāfiskos risinājumus*
Datu nosūtīšana pa e-pastu un šifrēti pielikumi **Jūsu vērtējums par drošības risinājumiem e-pasta izmantošanā**			
darbā ar e-pastu datu šifrēšanu nav jāizmanto	*esošie rīki un lietojumi nerada bažas par drošības apdraudējumu*	*ir jāizvērtē drošības riski nešifrēta e-pasta lietošanai*	*komunikācijās jānodrošina eIDAS prasības un jālieto rīki tikai ar jaunākajiem kriptogrāfiskajiem risinājumiem*
Droša tīmekļa pakalpojuma lietošanas scenāriji **Jūsu vērtējums par pieredzi par drošības risinājumiem darbā tīmeklī**			
darbam tīmeklī šifrēšanu nav jāizmanto	*esošie rīki un lietojumi nerada bažas par drošības apdraudējumu*	*ir jāizvērtē drošības riski nešifrēta tīmekļa lietošanai*	*komunikācijās jānodrošina eIDAS prasības un jālieto rīki tikai ar jaunākajiem kriptogrāfiskajiem risinājumiem*
Datu dublējumkopijas **Jūsu vērtējums par dublējumkopiju veidošanu**			
dublējumkopijās dati nav jāšifrē	*pietiek izmantot vienkāršāko datu šifrēšanu*	*ir jāizvērtē drošības riski nešifrētu datu glabāšanai*	*datu šifrēšanai rezerves kopijās jālieto jaunākie kriptogrāfijas risinājumi*

Mākoņdatošana **Jūsu vērtējums par mākoņdatošanas izmantošanas pieredzi**			
par datu šifrēšanu nerūpējos	*pietiek izmantot vienkāršāko datu šifrēšanu tikai vajadzības gadījumā*	*ir jāizvērtē drošības riski mākoņdatošanas ārpakalpojumam*	*jālieto jaunākie kriptogrāfijas risinājumi*

3.7. Aptauju analītika: literatūra (OECD un citi publiski atrodami materiāli).

Piedāvājam lasītāja analīzei atlasītus nozīmīgākos (gan tematiski gan reprezentatīvi) un plašākos pētījumus kiberdrošības un kriptogrāfijas jomā. Dažādos pētījumos ir analizēti dati par dažādien ģeogrāfiskiem reģioniem, bet šajos pētījumos nebija ietverta situācijas analīze par Latviju. Tipiski, ka aptaujas tiek veiktas par kiberdrošību, ietveroši arī par kriptogrāfiju.

Aptaujas: ieteicamā literatūra.

EY Global Information Security Survey 2021
Cybersecurity: How do you rise above the waves of a perfect storm?
https://www.ey.com/en_gl/cybersecurity/cybersecurity-how-do-you-rise-above-the-waves-of-a-perfect-storm

PWC 2022 Global Digital Trust Insights Survey: Simplifying cyber
https://www.pwc.com/gx/en/issues/cybersecurity/global-digital-trust-insights.html

ENISA ENISA THREAT LANDSCAPE 2021
April 2020 to mid-July 2021
https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021/@@download/fullReport

ISACA State of Cybersecurity 2020
https://www.isaca.org/go/state-of-cybersecurity-2020

Comparitech
300+ Terrifying Cybercrime and Cybersecurity Statistics (2022 EDITION)
https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/

https://purplesec.us/resources/cyber-security-statistics/

119 Impressive Cybersecurity Statistics: 2021/2022 Data & Market Analysis
https://financesonline.com/cybersecurity-statistics/

ACCENTURE State of Cybersecurity Resilience 2021, How aligning security and the business creates cyber resilience, https://www.accenture.com/_acnmedia/PDF-165/Accenture-State-Of-Cybersecurity-2021.pdf

ITU Global Cybersecurity Index
https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

Deloitte Global 2021 Future of Cyber Survey finds rapid increase in cyberattacks driven by organisations' embrace of digital transformation

https://www2.deloitte.com/mm/en/pages/risk/articles/deloitte-global-2021-future-of-cyber-survey-finds-rapid-increase-in-cyberattacks.html

Cyberattacks 2021: Phishing, Ransomware & Data Breach Statistics From the Last Year Jan 18 2022 BY Spanning Cloud Apps
https://spanning.com/blog/cyberattacks-2021-phishing-ransomware-data-breach-statistics/

Human rights, cryptography, survey, ieteicamā literatūra.

Human rights and encryption, Wolfgang Schulz Joris van Hoboken, Human rights and encryptionUNESCOPublishing
https://unesdoc.unesco.org/ark:/48223/pf0000246527?1=null&queryId=e05fdd78-68b9-4ff3-b7ce-b998b0c0cf01, ISBN: 978-92-3-100185-7 2016 83 p.

Konstantinos Limniotis, Cryptography as the Means to Protect Fundamental Human Rights Cryptography 2021, 5, 34, https://doi.org/10.3390/cryptography5040034
https://www.mdpi.com/journal/cryptography

Encryption laws and policies: Human rights assessment tool, December 2020,
https://www.gp-digital.org/wp-content/uploads/2020/12/encryption-human-rights-assessment-tool.pdf

Danaja Fabčič Povše Chapter 6. Protecting Human Rights through a Global Encryption Provision, Intersentia 129-159

Cryptography and Liberty 2000, An International Survey of Encryption Policy Electronic Privacy Information Center, Washington, DC, First edition 2000, ISBN: 1-893044-07-6, https://web.stanford.edu/class/msande91si/www-spr04/readings/week6/epic.htm

Encryption: finding the balance between privacy, security and lawful data access 16 Mar 2020, https://www.digitaleurope.org/resources/encryption-finding-the-balance-between-privacy-security-and-lawful-data-access/

KimmoHalunen Outi-MarjaLatvala, Review of the use of human senses and capabilities in cryptography, ELSEVIER Computer Science Review, Volume 39, February 2021, 100340
https://doi.org/10.1016/j.cosrev.2020.100340

Literatūra

1. Guiding Opinions on Stimulating the Development of the Cybersecurity Industry (Draft for the Solicitation of Public Comment), https://www.chinalawtranslate.com/en/guiding-opinions-on-stimulating-the-development-of-the-cybersecurity-industry-draft-for-the-solicitation-of-public-comment/
2. Nathan Saper. International Cryptography Regulation and the Global Information Economy, Northwestern Journal of Technology and Intellectual Property, Volume 11, Issue 7 Article 5, 2013
3. DIGITAL EUROPE comments to the Proposed Revision of Commercial Cryptography Administrative Regulation, 18 Sep 2020, https://www.digitaleurope.org/resources/digitaleurope-comments-to-the-proposed-revision-of-commercial-cryptography-administrative-regulation/
4. https://www.comparitech.com/blog/vpn-privacy/encryption-laws/
5. Danaja Fabčič Povše, Published online by Cambridge University Press: 23 January 2020 Chapter 6 - Protecting Human Rights through a Global Encryption Provision https://www.cambridge.org/core/books/abs/security-and-law/protecting-human-rights-through-a-global-encryption-provision/EF0C72C221365AC554ECC91518A83C84
6. The eIDAS Regulation is Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market
7. ENISA, Recommendations for technical implementation of the eIDAS Regulation Towards a harmonised Conformity Assessment Scheme for QTSP/QTS, DECEMBER 2019
8. www.enisa.europa.eu European Union Agency For Network And Information Security, eIDAS: Overview on the implementation and uptake of Trust Services One year after the switch over DECEMBER 2017
9. European Union Agency for Network and Information Security www.enisa.europa.eu Standardisation in the field of Electronic Identities and Trust Service Providers, Inventory of activities, Version 1.0, December 2014
10. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union
11. ENISA 2016 Technical guidelines for the implementation of minimum security measures for DSPs, www.enisa.europa.eu European Union Agency For Network And Information SecurityTechnical Guidelines for the implementationof minimum security measures for Digital Service Providers, DECEMBER, 2016, https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers/@@download/fullReport
12. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
13. ENISA proposes Best Practices and Techniques for Pseudonymisation, https://www.enisa.europa.eu/news/enisa-news/enisa-proposes-best-practices-and-techniques-for-pseudonymisation, December 03, 2019

14. Data Pseudonymisation: Advanced Techniques and Use Cases, https://www.enisa.europa.eu/publications/data-pseudonymisation-advanced-techniques-and-use-cases
15. Deploying Pseudonymisation Techniques, https://www.enisa.europa.eu/publications/deploying-pseudonymisation-techniques, The case of the Health Sector, MARCH 2022