KIBERNETINIO SAUGUMO EKSPERTŲ ASOCIACIJA

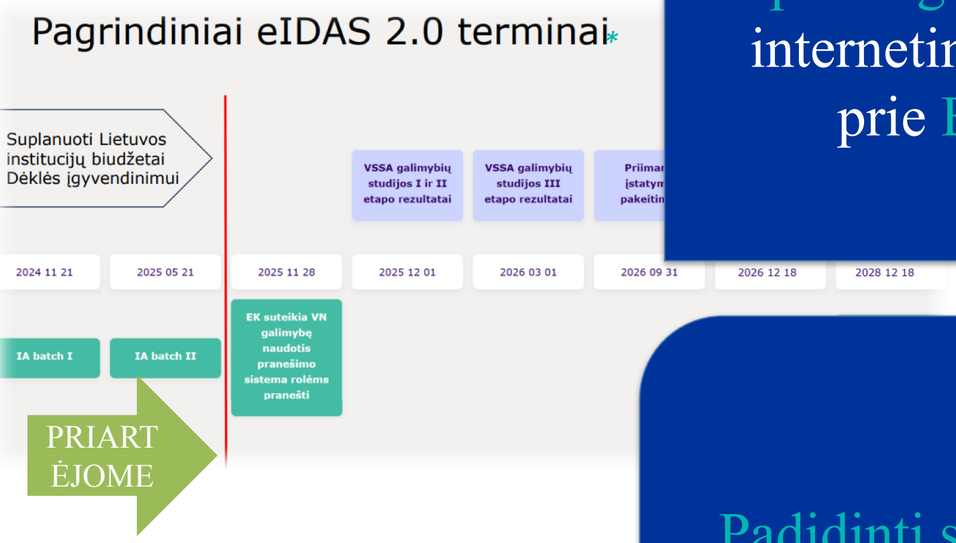
ARŪNAS GIRDZIUŠAS, Kibernetinio saugumo ekspertų asociacijos narys, KSEA

Kibernetinio saugumo ir privatumo užtikrinimas ES dėklės sistemoje

VIEŠA

KIBERNETINIO SAUGUMO EKSPERTŲ ASOCIACIJA

eIDAS 2.0 PAGRINDINIAI IŠŠŪKIAI



Atverti prieigą prie viešųjų paslaugų ir užtikrinti saugias internetines operacijas, prieigą prie ES valstybių narių

Įgalinti tarpvalstybinį pasitikėjimą

Padidinti saugumą ir patogumą vykdant verslą internetu

Skatinti skaitmeninių sandorių augimą ir dematerializaciją

VIEŠA

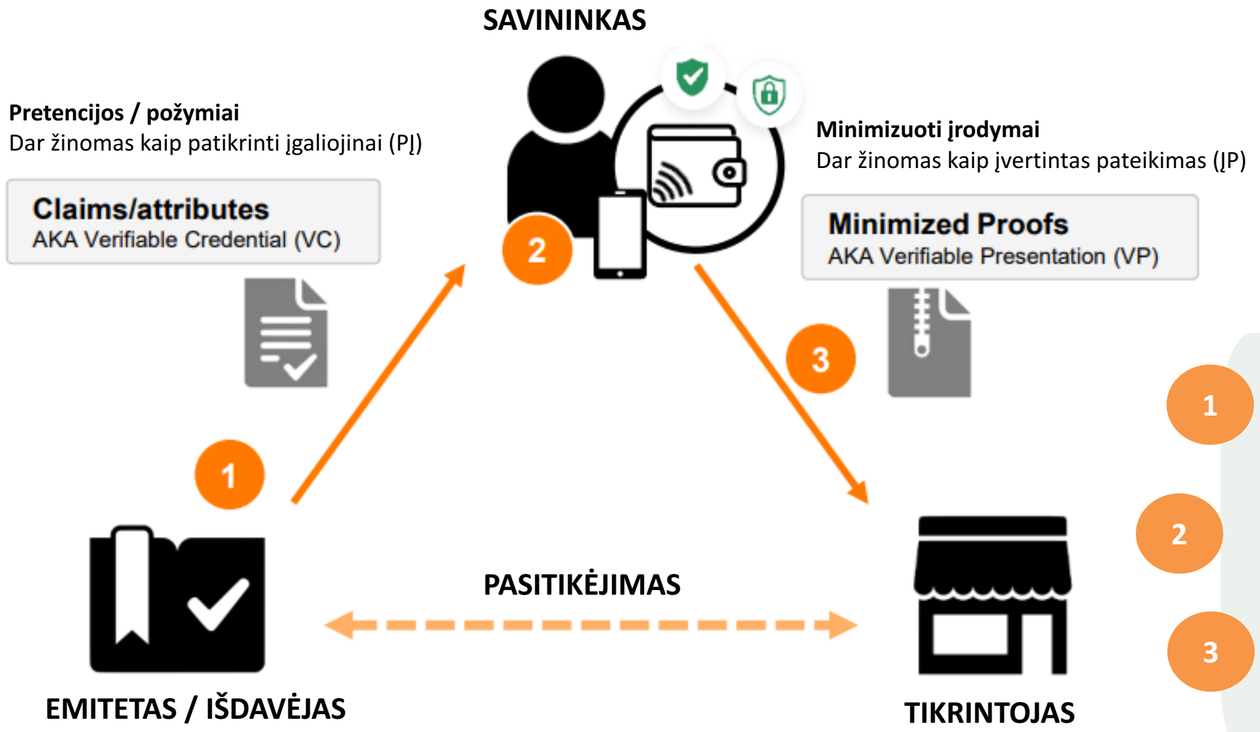
**Lietuvos pasirengimas įgyvendinti eIDAS 2.0, Vyr. patarėjas Arūnas Cijūnaitis 2025-05-30*

KIBERNETINIO SAUGUMO EKSPERTŲ ASOCIACIJA

AUKŠTO LYGIO eIDAS 2.0 FUNKCINĖ APŽVALGA

eIDAS: *Elektroninė atpažintis, tapatumo nustatymo ir patikimumo užtikrinimo paslauga* yra ES reglamentas, kuriuo nustatoma saugios ir patikimos elektroninės sąveikos teisinė sistema ir nustatoma europinė skaitmeninės tapatybės dėklė, leidžianti piliečiams saugiai patikrinti savo tapatybę ir naudotis paslaugomis visoje ES.

ARF: *Architektūros orientacinė sistema* yra standartizuota sistema, kurioje pateikiamos gairės ir geriausia praktika, - kaip kurti ir valdyti architektūrą pagal eIDAS reikalavimus. Pagrindinis jos tikslas – užtikrinti skirtingų sistemų sąveikumą, išlaikant nuoseklumą ir derinimą su verslo tikslais.



1. Emitentas sukuria rizikos kapitalą, kuriame yra požymių apie turėtoją ir jo viešąjį raktą, kurie visi pasirašyti su emitento privačiuoju raktu.
2. Savininkas saugo šias rizikos kapitalo priemones ir gali jas naudoti bei derinti parengti įrodymus, kurie turi būti pateikti tikrintojams.
3. Gavęs prašymą, savininkas savarankiškai pateikia šį įrodymą tikrintojui, kuris gali jį patvirtinti naudodamas Emitento viešąjį raktą ir Savininko viešąjį raktą, integruotą į PĮ.

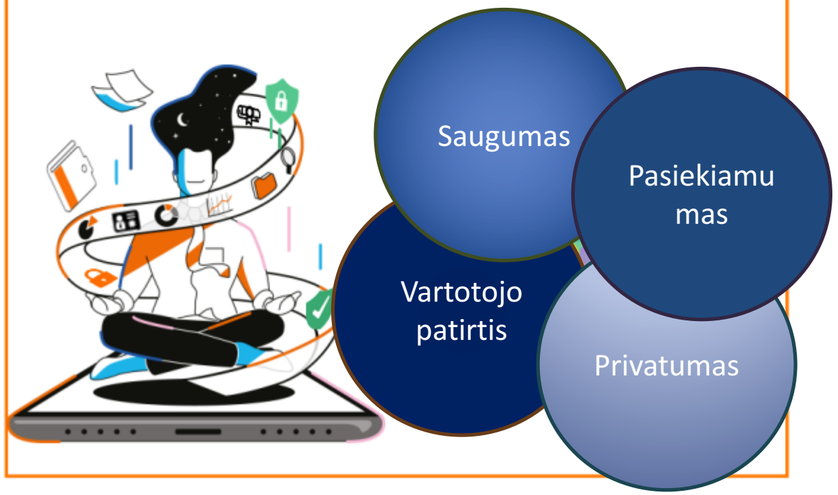
VIEŠA

KIBERNETINIO SAUGUMO EKSPERTŲ ASOCIACIJA

PAGRINDINĖS eIDAS 2.0 DIDŽIAUSIAS IŠŠŪKIS

Dėklių sėkmės sąlygos

- Kad eIDAS būtų sėkmingas, jis vienu metu turi turėti visas pagrindines savybes: saugumą, privatumą, pasiekiamumą ir vartotojo patirtį.
- Pilietinė visuomenė tikisi valstybės atitinkančių sprendimų.



DIDŽIAUSIAS IŠŠŪKIS

ARF trūksta sprendimo, kuris visiškai atitiktų šiuos reikalavimus, visų pirma teikiant moderniausią būdą derinti privatumą ir saugumą.

Iki Lapkričio 2026

Diegimas *SSI Dėklių

Valstybės narės privalo teikti SSI dėkles piliečiams iki 2026 m. lapkričio mėn.

Aukšto saugumo Reikalavimai

eIDAS Dėklės turi atitikti griežtus saugumo standartus ir pasiekti aukštą sertifikavimo lygį.

Laikomasi modernios privatumo politikos

Svarbu laikytis naujausių privatumo standartų, užtikrinti visišką atsiejimą, tikėtiną paneigimą ir amžiną privatumą.

Pasiekiamumas ir vartotojų patirtis

Dėklės turi užtikrinti platų pasiekiamumą ir sklandžią vartotojo patirtį su minimaliu operacijų laiku.

Pastaba: *Europos Komisija pasirinko ISO mDL (ISO/IEC 18013-5) kaip pagrindinį protokolą.*

VIEŠA

* Self-Sovereign Identity (SSI)

KIBERNETINIO SAUGUMO
EKSPERTŲ ASOCIACIJA

NACIONALINĖS RIZIKOS IR SILPNYBĖS ĮGYVENDINANT EUDI DĖKLĖS PROGRAMĄ

Kritiniai valdymo, resursų, teisės ir pasitikėjimo iššūkiai

Valdymo spragos:

Aiškios atsakingos institucijos nebuvimo išskaido atsakomybę ir lėtina reagavimą į incidentus.

Resursų trūkumas:

ribotas biudžetas ir kibernetinio saugumo ekspertų stygius silpnina auditų ir testavimo kokybę. (Pateiktas poreikis – 10,3 mln. Eur.)

Teisiniai iššūkiai:

Vėluojanti teisinė bazė kelia riziką dėl atsakomybės, duomenų apsaugos ir incidentų valdymo.

Viešojo pasitikėjimo rizika:

baimė dėl sekimo ar duomenų netinkamo naudojimo mažina sistemos priėmimą ir naudotojo patirtį.

Šios silpnybės reikalauja skubių sprendimų ir koordinuoto valdymo, užtikrinant sistemos patikimumą ir efektyvumą.

VIEŠA

PAGRINDINĖS GRĖSMĖS LIETUVOS MASTU - KS

1. SERTIFIKATŲ TEIKIMO FRAGMENTACIJA

- Kai sertifikatų išdavimą ir prieigos valdymą vykdo kelios institucijos, atsiranda:
- **Techninės rizikos**: nesuderinti standartai, skirtingos technologinės bazės, didesnė konfigūracijos klaidų tikimybė.
- **Teisinės rizikos**: neaišku, kuri institucija atsakinga už incidentą, pvz., suklastotą sertifikatą.
- **Kibernetinės pasekmės**: padidėja **man-in-the-middle** atakų ir neteisėto sertifikatų panaudojimo tikimybė.

2. KRITINIŲ REGISTRŲ APSAUGA

- Institucijos, saugančios jautrius asmens ir juridinių asmenų duomenis, taps pirmo lygio taikiniu užsienio žvalgyboms ir kibernetiniams nusikaltėliams.
- **Grėsmė**: šios institucijos taps prioritetiniu taikiniu užsienio žvalgyboms, kibernetiniams nusikaltėliams.
- **Pasekmės**: duomenų nutekėjimas gali pakenkti visai EUDI ekosistemai – nes nutekėję duomenys leidžia apeiti autentifikaciją ar kurti fiktyvias tapatybes.

3. REGULIATORIAUS PAJĖGUMAI

- Priežiūros institucija gali turėti interesų konfliktą, jei tuo pačiu metu sertifikuoja ir prižiūri rinką.
- **Grėsmė**: interesų konfliktas tarp priežiūros (reguliuoti) ir įgyvendinimo (sertifikuoti).
- **Pasekmės**: sprendimų šališkumas, lėtesnė reakcija į pažeidimus.

4. KOORDINAVIMO STOKA

- Nėra aiškaus centrinio SOC (Security Operations Center) ar nacionalinio EUDI incidentų valdymo centro veiklos.
- **Grėsmė**: incidentai gali būti pastebėti pavėluotai arba nesuvaldyti, koordinuotai.
- **Pasekmės**: lėtas reagavimas, grandininės atakos tarp institucijų, visuomenės pasitikėjimo praradimas.

5. PASIKLIAUJANČIŲJŲ ŠALIŲ REGISTRAVIMAS

- Jei registracija ir priežiūra nebus griežtai centralizuota, gali atsirasti **netikrų paslaugų teikėjų**.
- **Grėsmė**: kenkėjiški subjektai įsiterpia į ekosistemą.
- **Pasekmės**: piliečių duomenų vagystės, reputacinis smūgis visai sistemai.

KIBERNETINIO SAUGUMO EKSPERTŲ ASOCIACIJA

Europos skaitmeninė tapatybė Lietuvoje: saugumo iššūkiai ir galimybės

Įgyvendinimas pagal eIDAS 2.0 iki 2027 m. – svarbus žingsnis skaitmeninei visuomenei

Lietuvos mastu matoma, kad:

- **Dėklės (EUDI Wallet) teikėjas** galimai gali tapti nacionalinis skaitmeninių sprendimų centras, atsakingas už piniginės kūrimą, palaikymą ir jos techninį vystymą.
- **Dėklės pasikliaujančiųjų šalių registruotojai / priežiūros įstaiga** galimai gali tapti ryšių ir skaitmeninių paslaugų reguliatorius, užtikrinantis registraciją, priežiūrą ir atitiktį reikalavimams.
- **Asmens tapatybės duomenų teikėjai** galimai gali tapti institucija, valdanti fizinių asmenų duomenis (pvz., gyventojų registras) ir institucija, valdanti juridinių asmenų duomenis (pvz., įmonių registras).
- **Dėklės pasikliaujančiosios šalies prieigos sertifikatų teikėjas** galimai gali atlikti funkcija, pasidalinta tarp kelių subjektų, atsakingų už pasikliaujančiųjų šalių sertifikatų išdavimą ir valdymą.

Palyginimas su Europos praktika

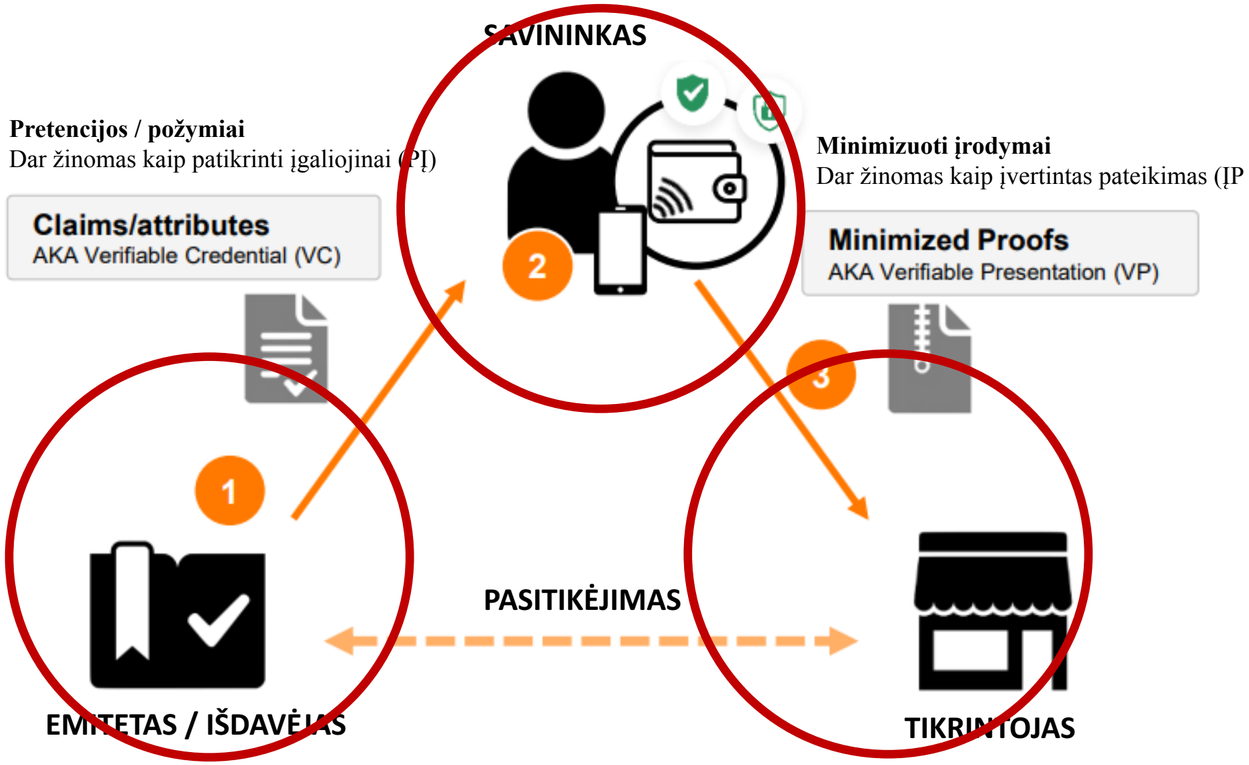
•Tokia schema atitinka bendrą ES logiką – nacionalinis skaitmeninių sprendimų centras kaip **techninis teikėjas**, ryšių ir skaitmeninių paslaugų reguliatorius, užtikrinantis registraciją, priežiūrą ir atitiktį reikalavimams kaip **reguliatorius ir priežiūros institucija**, o pagrindinės registrų institucijos – kaip **tapatybės duomenų teikėjas**.

•Tačiau ES pilotuose ir gairėse akcentuojama, kad vaidmenys turi būti **aiškiai atskirti**, **kad būtų išvengta interesų konfliktų ir atsakomybės dubliavimo**. **Lietuvoje kai kurios funkcijos yra persidengiančios, ypač dėl sertifikatų teikimo**.

VIEŠA

PAGRINDINĖS GRĖSMĖS KIBERNETINIO SAUGUMO EUDI DĖKLEI

Identifikuokite ir supraskite svarbiausias rizikas, keliančias pavojų vartotojų saugumui ir patikimumui



KIBERNETINIO SAUGUMO
EKSPERTŲ ASOCIACIJA

PAGRINDINĖS GRĖSMĖS KIBERNETINIO SAUGUMO EUDI DĖKLEI (USE CASE)

Identifikuokite ir supraskite svarbiausias rizikas, keliančias pavojų vartotojų saugumui ir patikimumui

Piniginės pažeidimas (įrenginio ar privataus rakto vagystė)

Kas: užpuolikas gauna privačius raktus, kuriuos naudoja vartotojo EUDI dėklė (per kenkėjiškas programas, sukčiavimą, pamestą / pavogtą įrenginį arba silpną saugų elementą).

Atakos vektorius: mobilioji kenkėjiška programa, kuri išfiltruoja raktus, sukčiavimas, kuris apgaudinėja vartotoją eksportuoti raktus, fizinė atrakinto įrenginio vagystė, nesaugios saugyklos / atsarginės kopijos išnaudojimas.

Poveikis: visiškas apsimetinėjimas vartotoju (autentifikavimas, pasirašymas, finansinis prisijungimas), tapatybės vagystė, apgaulingos operacijos, reputacijos ir reguliavimo pasekmės.

Aptikimo signalai: neįprasti autentifikavimo / parašo bandymai, naujos RP registracijos iš netikėtų vietų / įrenginių, vartotojų skundai, neįprasti operacijų modeliai.

Švelninimas: privaloma aparatūra pagrįsta raktų saugykla / sertifikuotas saugus elementas arba patikima vykdymo aplinka (TEE); stiprus prietaiso patvirtinimas; kelių veiksnių / operacijų patvirtinimo srautai; greičio apribojimai ir geografinių anomalijų aptikimas; vartotojų švietimas; raktų atšaukimo ir greito piniginės sustabdymo darbo eigos.

Ištaisymas: nedelsiant sustabdytas piniginės sustabdymas, rakto atšaukimas / CRL atnaujinimas, teismo ekspertizės fiksavimas, vartotojo ID pakartotinis išdavimas / **verifikuojamo įgaliojimo** rotacija, reguliatoriaus pranešimas (jei reikia).

PAGRINDINĖS GRĖSMĖS KIBERNETINIO SAUGUMO EUDI DĖKLEI (USE CASE)

Identifikuokite ir supraskite svarbiausias rizikas, keliančias pavojų vartotojų saugumui ir patikimumui

Apsimetimas apsimetant kitu asmeniu ir/ar kenkėjiška RP (pasikliaujančiąja šalimi)

Kas: vartotojai apgaudinėjami atskleisti sertifikatus netikriems RP arba kenkėjiškoms programoms, kurios atrodo kaip teisėtos paslaugos.

Atakos vektorius: sukčiavimo el. laiškai, typosquatting domenai (*goggle.lt vs. google.lt or swedbank.lt, sw[e]d[a]nk.lt, Cyrillic letters*), netikros mobiliosios programos, deepfake palaikymo skambučiai. Užpuolikai prašo pateikti sertifikatus / sutikimą suklastotoje vartotojo sąsajoje.

Poveikis: sertifikatų atskleidimas, neteisėtas atributų bendrinimas, paskyrų perėmimas, sukčiavimas keliose paslaugose.

Aptikimo signalai: didelis nepavykusio sutikimo patvirtinimo skaičius, keli sertifikatų pateikimai naujiems / neregistruotiems RP, vartotojų pranešimai apie įtartinas svetaines.

Poveikio mažinimo priemonės: RP registracija ir privalomi patikimi sąrašai; vizualūs RP tapatybės indikatoriai piniginės vartotojo sąsajoje; sukčiavimui atsparūs vartotojų srautai (patvirtinimai už juostos ribų, tiesioginiai pranešimai į registruotus įrenginius); naršyklės / programų smėlio dėžė; stiprus kovos su sukčiavimu švietimas.

Ištaisymas: atšaukti kenkėjišką RP registraciją, jei ji yra nacionaliniame registre; informuoti paveiktus vartotojus; atnaujinti juoduosius sąrašus; reguliavimo veiksmų.

PAGRINDINĖS GRĖSMĖS KIBERNETINIO SAUGUMO EUDI DĖKLEI (USE CASE)

Identifikuokite ir supraskite svarbiausias rizikas, keliančias pavojų vartotojų saugumui ir patikimumui

Emitento kompromitavimas (tapatybės požymio suteikimas)

Kas: sertifikatų išdavėjas (pvz., nacionalinis registras, universitetas, bankas) yra pažeistas ir išduoda apgaulingus atributus ar sertifikatus.

Atakos vektorius: išdavėjo vidinės sistemos išnaudojimas, vidinė grėsmė, silpni CI/CD arba netinkamai sukonfigūruoti API raktai, pavogti pasirašymo raktai.

Poveikis: plačiai paplitęs suklastotų sertifikatų išdavimas, sukčiavimas, pasitikėjimo visa ekosistema erozija, tarpvalstybinis poveikis.

Aptikimo signalai: sertifikatų išdavimo rodiklių šuolis, išdavimas iš neįprastų IP / vietų, atestavimo modelių neatitikimai, tolesnės patikros klaidos.

Švelninimas: HSM / sertifikuoto rakto apsauga emitento pasirašymo raktams, stiprus ALM ir pataisymas, vaidmenimis pagrįsta prieiga, daugiašalė pasirašymo kontrolė, emitento atestacijos stebėsena, emisijos metrikos anomalijų aptikimas, periodiniai trečiųjų šalių auditai.

Ištaisymas: atšaukti pažeistus išdavėjo raktus / sertifikatus, paskelbti incidentą, užšaldyti naują išdavimą iki saugumo, jei reikia, pakartotinai išduoti paveiktus sertifikatus.

PAGRINDINĖS GRĖSMĖS KIBERNETINIO SAUGUMO EUDI DĖKLEI (USE CASE)

Identifikuokite ir supraskite svarbiausias rizikas, keliančias pavojų vartotojų saugumui ir patikimumui

QTSP / Atitikties įstaigos kompromitavimas (pasitikėjimo inkaro ataka)

Kas: atakuojamas kvalifikuotas patikimumo užtikrinimo paslaugų teikėjas arba atitikties vertintojo sistema, leidžianti suklastoti knygos įrašus, sertifikatus ar patikimumo sąrašus.

Atakos vektorius: tiekimo grandinės ataka, QTSP infrastruktūros pažeidimas arba protokolo / paslaugos pažeidžiamumo išnaudojimas.

Poveikis: sisteminis pasitikėjimo pažeidimas: suklastoti liudijimai, priimti visose RP sistemose, masiniai apgaulingi sandoriai, dideli teisiniai / reguliavimo padariniai.

Aptikimo signalai: netikėti patikimumo sąrašų pakeitimai, priimami nauji / netikėti sertifikatai, DK neatitikimai.

Švelninimas: griežtos QTSP apsaugos priemonės: nepriklausomi auditai, pertekliniai QS / vertintojų modeliai, kelių jurisdikcijų priežiūra, kelių tikrintojų nekintamumo įrodymai, kritinių pokyčių patikrinimas už juostos ribų.

Ištaisymas: Neatidėliotinas nepasitikėjimas pažeistais QTSP, atšaukimas arba karantinas, knygos įrašai, jei įmanoma perjungimas į alternatyvius pasitikėjimo inkarus (*anchors angl.*).

PAGRINDINĖS GRĖSMĖS KIBERNETINIO SAUGUMO EUDI DĖKLEI (USE CASE)

Identifikuokite ir supraskite svarbiausias rizikas, keliančias pavojų vartotojų saugumui ir patikimumui

DK (EBSI) vientisumo (*Leger integrity angl.*) ir privatumo rizika

Kas: Piktnaudžiavimas blokų grandinės / DLT didžiąja knyga kuri naudojama kaip auditas / Tarpinių (P2P) ryšio protokolų arba pranešimų magistralės (*backplane angl.*) – privatumo nutekėjimas arba bandymai jais manipuliuoti.

Atakos vektorius: koreliacijos atakos visuose knygos įrašuose, atskleidžiančios vartotojo elgseną; prastas dizainas, kaupiantis PII grandinėje; bando išsišakoti arba vykdyti 51% stiliaus atakas prieš nepakankamai decentralizuotus tinklus.

Poveikis: privatumo pažeidimai, BDAR nesilaikymas, naudotojų operacijų susiejimas tarp paslaugų, reputacinės / reguliavimo baudos.

Aptikimo signalai: netikėtos duomenų koreliacijos užklausos, DK skaitymo / peržvalgos apimties šuoliai, bandymai pasiekti ribotus duomenis.

Švelninimas: vengti saugojimo PII grandinėje (tik saugoti maišas / rodykles), naudokite atrankinį atskleidimą (patikrinamus sertifikatus, ZKP), griežtą prieigos prie DK mazgų kontrolę, skaitymo užklausų greičio ribojimą, leidimą turinčių DLT naudojimą su gerai valdomais mazgų operatoriais, privatumą pagal dizainą.

Ištaisymas: jei nutekėjo PII, BDAR procesai (pranešimas apie pažeidimą, DPIA), knygos pertvarkymas, raktų pasukimas maišos rodyklėms.

PAGRINDINĖS GRĖSMĖS KIBERNETINIO SAUGUMO EUDI DĖKLEI (USE CASE)

Identifikuokite ir supraskite svarbiausias rizikas, keliančias pavojų vartotojų saugumui ir patikimumui

Pakartojimo ir perdavimo atakos (autentifikavimo pakartojimas)

Kas: užpuolikas atkuria perimtus autentifikavimo / patvirtinimo atpažinimo ženklus arba perduoda seansą, kad apsimestų vartotoju.

Atakos vektorius: tinklo perėmimas (MITM), pakartotinis žetonų, neturinčių nece / laiko žymos ar susiejimo su kanalu, naudojimas.

Poveikis: neteisėta prieiga be kriptografinio rakto pažeidimo.

Aptikimo signalai: pasikartojantys teiginiai iš tų pačių atpažinimo ženklų, pakartotinai naudojamas nonce aptikimas, neįprasti IP šuoliai.

Švelninimas: atpažinimo ženklo susiejimas su kanalu / įrenginiu, trumpasis atpažinimo ženklas TTL, nonces, iššūkis-atsakas, transportavimo lygmens saugumas su mTLS, TLS prisegimas, įrenginio kilmės patvirtinimas.

Ištaisymas: anuliuokite žetonus, priverstinai atsijungkite, pasukite sesijos raktus, praneškite paveiktiems RP / vartotojams.

PAGRINDINĖS GRĖSMĖS KIBERNETINIO SAUGUMO EUDI DĖKLEI (USE CASE)

Identifikuokite ir supraskite svarbiausias rizikas, keliančias pavojų vartotojų saugumui ir patikimumui

Tarpvalstybinis politikos neatitikimas ir piktnaudžiavimas LoA (*Level of Assurance angl.*)

Kas: Valstybių narių saugumo užtikrinimo lygio ar aiškinimo skirtumai leidžia užpuolikams pasinaudoti silpnesnėmis jurisdikcijomis privilegijų eskalavimui.

Atakos vektorius: sertifikatų registravimas žemo patikimumo būsenoje ir jų naudojimas didelės vertės RP kontekste; išnaudoti politikos derinimo spragas.

Poveikis: sukčiavimas, teisiniai ginčai, nenuosekli tarpvalstybinė saugumo būklė.

Aptikimo signalai: tarpvalstybinio tikrinimo neatitikimai, pakartotiniai tarpvalstybiniai prašymai naudojant mažus LoA sertifikatus.

Švelninimas: suderintas minimalus LoA žemėlapis, politikos vykdymas RP lygmeniu, privalomų požymių atestavimo taisyklių sąvadai, federacijos pasitikėjimo politika.

Ištaisymas: blokuoti arba pažymėti tarpvalstybinius srautus, kurie neatitinka RP LoA reikalavimų; reikalauti laipsniško autentifikavimo.

PAGRINDINĖS GRĖSMĖS KIBERNETINIO SAUGUMO EUDI DĖKLEI (USE CASE)

Identifikuokite ir supraskite svarbiausias rizikas, keliančias pavojų vartotojų saugumui ir patikimumui

Vidinė grėsmė ir piktnaudžiavimas privilegijuotomis paskyromis

Kas: įgalioti darbuotojai (emitento administratorius, QTSP operatorius, SOC analitikas) piktnaudžiauja prieiga išduotais sertifikatais, gali atšaukti raktus arba manipuliuoti žurnalais.

Atakos vektorius: piktavališki ketinimai, prievarta, aplaidus sertifikatų tvarkymas, pažeistų administratoriaus sertifikatų naudojimas.

Poveikis: apgaulingas išdavimas, nesekamas atšaukimas, žurnalų ištrynimas, ilgalaikis neaptiktas netinkamas naudojimas.

Aptikimo signalai: neįprasti administratoriaus veiksmai, prieiga ne įprastomis valandomis, nepatvirtinti konfigūracijos pakeitimai, audito žurnalų spragos.

Švelninimas: mažiausios privilegijos, pareigų atskyrimas, daugiašalis leidimas slaptoms operacijoms, nekintami audito žurnalai, privilegijuotos prieigos stebėjimas (PAM), biografijos patikrinimai.

Ištaisymas: privilegijų atšaukimas, teismo medicinos tyrimas, paveiktų sertifikatų rotacija, drausminiai / teisiniai veiksmai.

KIBERNETINIO SAUGUMO
EKSPERTŲ ASOCIACIJA

PAGRINDINĖS GRĖSMĖS KIBERNETINIO SAUGUMO EUDI DĖKLEI (USE CASE)

Identifikuokite ir supraskite svarbiausias rizikas, keliančias pavojų vartotojų saugumui ir patikimumui

Paslaugų atsisakymas (DoS) prieš piniginės infrastruktūrą / AP

Kas: Didelio masto DoS veikia RP/AP galinius punktus arba piniginės vidines sistemas, neleisdama autentifikuoti ar atšaukti.

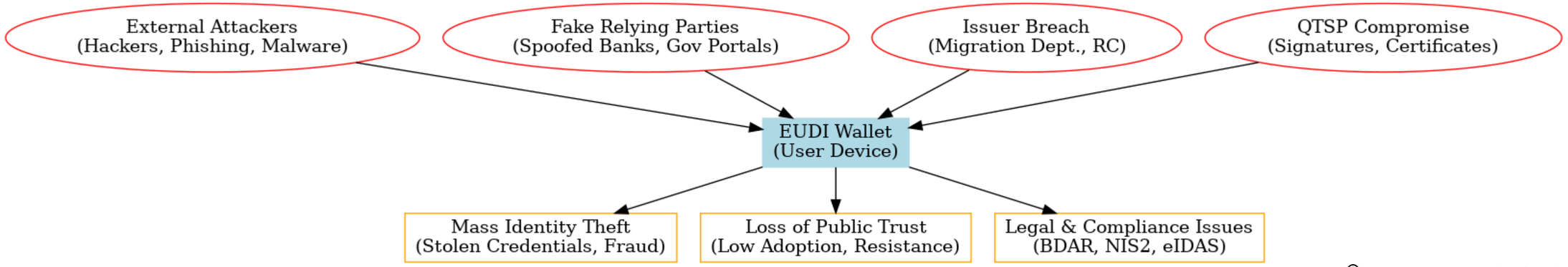
Atakos vektorius: tūrinės atakos, programų lygmens potvyniai, API ribojimo silpnybių išnaudojimas.

Poveikis: paslaugų sutrikimai, nesugebėjimas autentifikuoti ar atšaukti piniginių, galimi pakopiniai gedimai visuose RP.

Aptikimo signalai: srauto šuoliai, API galinių punktų prisotinimas, padidėjęs klaidų lygis.

Švelninimas: DDoS apsauga (šveitimas, CDN), automatinis mastelio keitimas, API greičio ribojimas ir laipsniškas degradavimas, atsarginiai autentifikavimo maršrutai neprisijungus, SLA su debesijos paslaugų teikėjais.

Ištaisymas: suaktyvinkite DDoS mažinimą, perjungimą į alternatyvius galinius punktus, aiškų ryšį su vartotojais ir RP.



VIEŠA

KIBERNETINIO SAUGUMO EKSPERTŲ ASOCIACIJA

PAGRINDINĖS eIDAS 2.0 GALIMOS LIETUVOS SĖKMĖS SAVYBĖS

*Blockchain nėra tik finansų sektoriaus technologija – ji tampa kertine priemone **kibernetiniam saugumui**, **duomenų apsaugai** ir **skaitmeninės ekonomikos vystymui**. Lietuvoje ji gali padėti įgyvendinti **eIDAS 2.0**, atitikti **BDAR**, **NIS2** ir **DORA** reikalavimus, bei sustiprinti nacionalinį atsparumą.*

Sveikatos priežiūra ir ePrescription

Naudojant blockchain galima kurti **nekintamą sveikatos duomenų registrą**, leidžiantį pacientams saugiai dalintis receptais, diagnozėmis ar tyrimų rezultatais tarp skirtingų šalių gydymo įstaigų. Lietuvoje, sujungus blockchain su **MyHealth@EU** sistema, pacientas galėtų patikimai įsigyti vaistus užsienio vaistinėje, o gydytojai turėtų garantiją, kad duomenys yra tikri.

Viešieji pirkimai ir antikorupcija

Blockchain užtikrina, kad **viešųjų pirkimų konkursų duomenys būtų skaidrūs ir nekintami**. Tai padėtų sumažinti korupcijos riziką Lietuvoje ir užtikrinti didesnį pasitikėjimą valstybės institucijomis.

Tapatybės valdymas ir EUDI piniginė

Naudojant blockchain galima užtikrinti saugų, nekintamą ir patikimą tapatybės duomenų saugojimą bei dalinimąsi. **Europos skaitmeninės tapatybės piniginės (EUDI Wallet)** atveju blockchain gali būti naudojamas kaip **patikimumo registras**, leidžiantis tikrinti ar skaitmeniniai atributai ir pažymėjimai (pvz., diplomas, vairuotojo pažymėjimas) yra galiojantys ir neišduoti netikros institucijos. Tai sumažina **sukčiavimo riziką** ir padidina **pasitikėjimą tarpvalstybiniu mastu**.

Finansinės paslaugos ir atsiskaitymai

Blockchain suteikia galimybę naudoti **išmaniąsias sutartis (smart contracts)** finansų sektoriuje. Lietuvos bankai ir fintech įmonės galėtų pritaikyti blockchain klientų identifikacijai pagal **KYC/AML reikalavimus**, bei realaus laiko tarptautiniams mokėjimams. Tai sumažina operacijų kaštus, pagreitina procesus ir užtikrina **DORA reglamento reikalavimus dėl IT atsparumo**.

Tiekimo grandinės skaidrumas

Įmonės gali naudoti blockchain technologiją, kad **sektų prekių kilmę** nuo gamintojo iki galutinio vartotojo. Tai itin aktualu maisto, farmacijos ir energetikos sektoriuose. Pavyzdžiui, Lietuvos pieno pramonė galėtų naudoti blockchain, kad pirkėjas parduotuvėje skenuodamas QR kodą matytų visą produkto kelią – nuo ūkio iki lentynos. Tai didina **vartotojų pasitikėjimą** ir užtikrina **atitiktį ES reglamentams**.

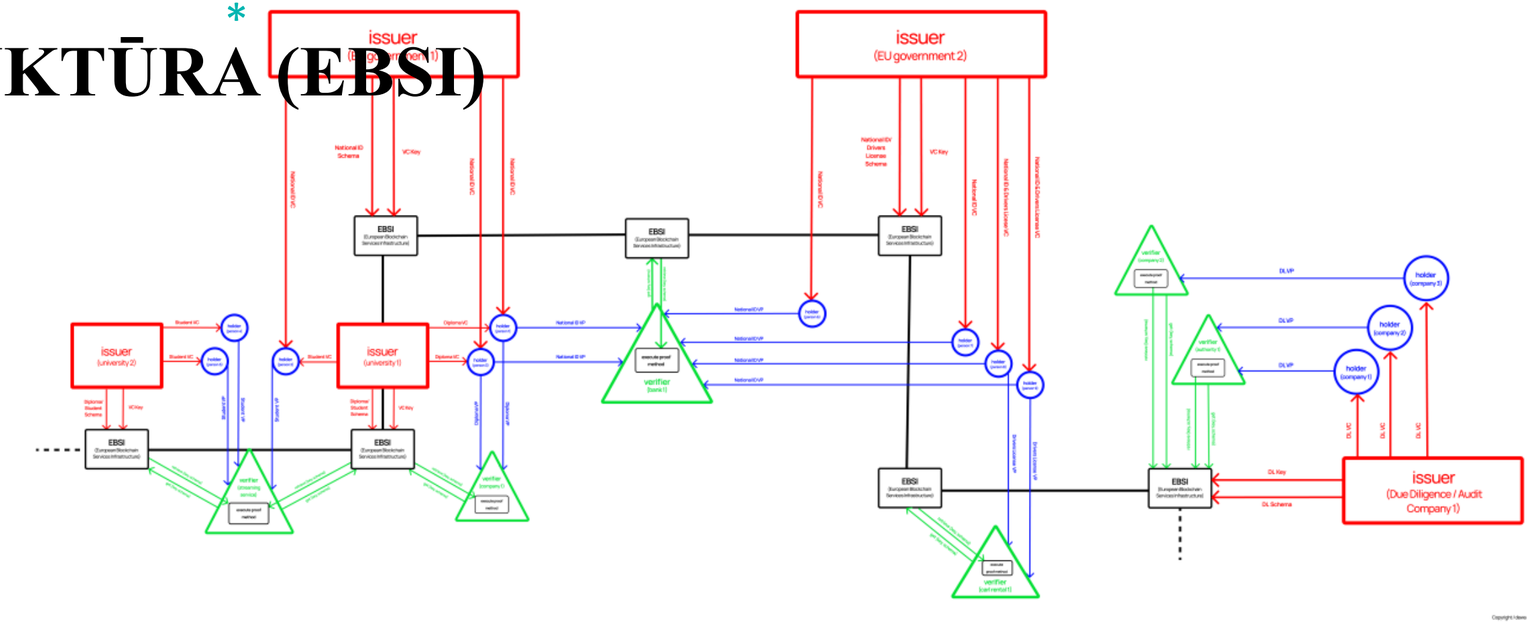
VIEŠA

KIBERNETINIO SAUGUMO EKSPERTŲ ASOCIACIJA

EUROPOS BLOCKCHAIN PASLAUGŲ INFRASTRUKTŪRA (EBSI)*

EBSI kaip pagrindinė infrastruktūra

Iš saugumo pusės **EBSI** jau sukurta **kaip pan-Europos DLT tinklas**, kuriame dalyvauja valstybių narės. **EBSI** veikia su vyriausybių valdomomis mazgų (*node angl.*) infrastruktūromis, kurios suteikia pasitikėjimo pagrindą (*trust anchor angl.*) **decentralizuotoms paslaugoms, tokioms kaip verifiable credentials, smart contracts, audito įrašai**.



Integracija su eIDAS 2 per „Qualified Electronic Ledgers (QTSP-EL)“

eIDAS 2 įveda kategoriją **Qualified Trust Service Providers – Electronic Ledger (QTSP for Ledger)**, pagal kurią tam tikros blockchain / DLT paslaugos gali oficialiai tapti kvalifikuotomis paslaugomis, jeigu jos atitinka reikalavimus (pvz. duomenų įrašų tvarkymas, pakeitimų aptikimas, chronologinis sekos užtikrinimas). EBSI gali būti naudojama kaip infrastruktūra tokioms paslaugoms (ledger kaip paslauga).

*Lorenz Carl Flechtenmacher
CEO & Co-founder @dewa | unlocking the next generation of digital identity

VIEŠA

KIBERNETINIO SAUGUMO EKSPERTŲ ASOCIACIJA

GALIMI IŠŠŪKIAI LIETUVOS MASTU

eIDAS 2.0 + BDAR (GDPR/BDAR)

Sąsajos: eIDAS 2.0 įveda EUDI dėklę kaip oficialų asmens duomenų ir atributų šaltinį. Tai reiškia, kad BDAR taisyklės dėl teisėto duomenų tvarkymo, minimizavimo ir duomenų subjektų teisių tampa kritiškai svarbios dėklės naudojime.

Pasekmės sektoriams

Universitetai: studentų tapatybės tikrinimas, diplomų ar pažymėjimų išdavimas per dėklę → būtina užtikrinti selektyvų duomenų atskleidimą, prieigos žurnalus ir BDAR atitikties mechanizmus.

Registrų centras: atsakingas už juridinių asmenų duomenis, kurie taps EUDI atributais → privalo užtikrinti aukštą BDAR atitiktį, nes pažeidimai turės tarpvalstybinį poveikį.

Medicinos įstaigos: pacientų ID ir sveikatos duomenys (ePrescription, Health ID) → taikomas griežčiausias BDAR režimas: šifravimas, griežtos prieigos teisės, audito žurnalai.

Bankai ir finansų įstaigos: bankai naudos EUDI atributus KYC/AML procedūroms → būtina užtikrinti, kad duomenų gavimas būtų teisėtas, minimalus ir dokumentuotas; būtini procesai duomenų saugumui ir subjekto sutikimui fiksuoti. Finansų institucijos turi papildomai įsitikinti, kad EUDI atributų naudojimas nepažeidžia BDAR reikalavimų ir kad šie srautai yra log‘inami bei prižiūrimi.

KIBERNETINIO SAUGUMO EKSPERTŲ ASOCIACIJA

GALIMI IŠŠŪKIAI LIETUVOS MASTU

eIDAS 2.0 + TIS2 (NIS2 / TIS2)

Sąsajos: eIDAS 2.0 įpareigoja dėkles, QTSP ir pasikliaujančias šalis laikytis aukštų saugumo standartų. Tai sutampa su TIS2 reikalavimais dėl kritinės infrastruktūros atsparumo, incidentų pranešimų ir rizikų valdymo.

Pasekmės sektoriams:

Universitetai: ypač valstybiniai — privalo įtraukti EUDI sąsajas į savo ISMS ir TIS2 rizikų valdymo procesus.

Registrų centras: priskiriamas prie ypatingos svarbos operatorių — trumpi incidentų pranešimo terminai, privaloma SOC sąveika ir aktyvus koordinavimas su NKSC.

Medicinos įstaigos: ligoninės ir eSveikatos sistemos — bet koks EUDI incidentas privalo būti praneštas NKSC/ENISA per TIS2 procesus.

Bankai ir finansų įstaigos: laikomi esminiais paslaugų teikėjais pagal TIS2 — bankų EUDI integracijos turi atitikti TIS2 reikalavimus (operacinis atsparumas, tiekimo grandinės sauga, incidentų pranešimai), todėl bankai privalo turėti SOC, rizikų valdymo procedūras ir greitus pranešimo mechanizmus.

VIEŠA

KIBERNETINIO SAUGUMO EKSPERTŲ ASOCIACIJA

GALIMI IŠŠŪKIAI LIETUVOS MASTU

eIDAS 2.0 + DORA

Sąsajos: DORA tiesiogiai taikoma finansų sektoriui. Kadangi EUDI dėklė taps vienu iš pagrindinių klientų identifikacijos įrankių (KYC, AML), eIDAS sertifikuoti sprendimai turės atitikti ir DORA reikalavimus dėl IT atsparumo, testavimo ir tiekimo grandinės valdymo.

Pasekmės sektoriams:

Universitetai: tiesioginis poveikis nedidelis, nebent teikiamos finansinės paslaugos (studentų paskolos).

Registrų centras: teikdamas duomenis bankams per EUDI atributus, įsilieja į finansų tiekimo grandinę → registrui gali tekti atitikti DORA reikalavimų reikalavimus, kai jis yra kritinis informacijos tiekėjas finansams.

Medicinos įstaigos: netiesioginė įtaka; jei eSveikata sąveikauja su draudimo ar mokėjimų sistemomis, per partnerystes taikomi DORA reikalavimai.

Bankai ir finansų įstaigos: tiesiogiai taikoma DORA — privalomi veiklos atsparumo planai, testavimas (pvz., streso scenarijai), tiekimo grandinės rizikų valdymas (Wallet tiekėjai, QTSP, RP paslaugų teikėjai), papildomi auditai ir atitikties reikalavimai.

KIBERNETINIO SAUGUMO EKSPERTŲ ASOCIACIJA

GALIMI IŠŠŪKIAI LIETUVOS MASTU

Bendrosios kibernetinės pasekmės Lietuvoje

Padidėjusi atakų rizika: EUDI infrastruktūra taps nacionaliniu taikiniu — ypač didelė rizika Registrų centrui, sveikatos sektoriui ir finansų institucijoms.

Pranešimų dubliavimas: incidentai turi būti pranešti pagal BDAR (72 val.), TIS2 (ankstyvas ir detalus pranešimas) ir eIDAS (dėklės suspendavimo procedūros); bankai papildomai privalo vykdyti DORA veiklos atsparumo pranešimus.

Resursų trūkumas: universitetams, medicinos įstaigoms ir Registrų centrui gali trūkti pajėgumų užtikrinti ir BDAR, ir TIS2, ir eIDAS reikalavimus; bankai turės papildomas atitikties išlaidas ir testavimo resursus.

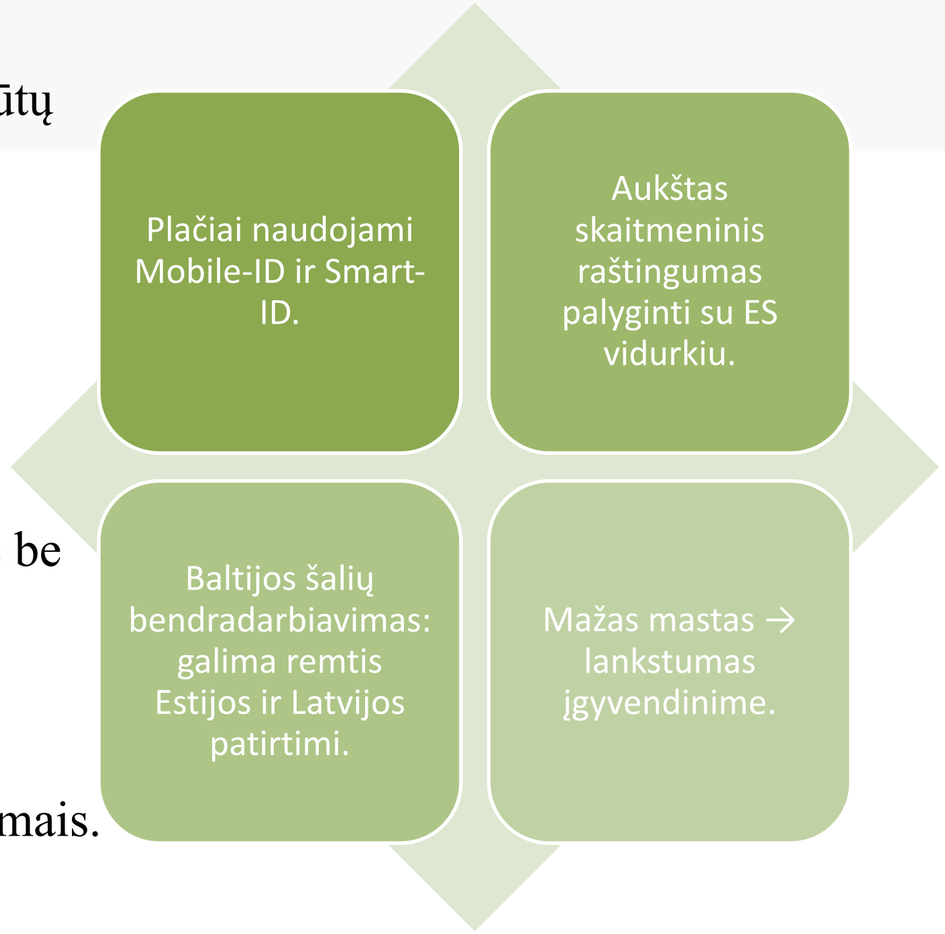
Atsakomybės pasidalinimas: be aiškios koordinacijos BDAR, TIS2, DORA ir eIDAS kontekste gali susidaryti „atsakomybės vakuumai“ incidentų metu — ypač tarp duomenų tiekėjų (RC), dėklės teikėjo ir finansų institucijų.

KIBERNETINIO SAUGUMO EKSPERTŲ ASOCIACIJA

GERIAUSIOS PRAKTIKOS IR REKOMENDACIJOS: EFEKTYVUS SAUGUMAS IR PERĖJIMAS PRIE eIDAS 2.0

Strategijos komunikacijai, incidentų valdymui ir sklandžiam Mobile-ID migravimui prie EUDI Wallet

- Aiškiai atskirti **techninį įgyvendinimą** nuo **reguliavimo ir priežiūros**.
- Konsoliduoti sertifikatų teikimo atsakomybę vienoje institucijoje, kad būtų išvengta dubliavimosi.
- Įsteigti **nuolatinę tarpžinybinę darbo grupę** koordinavimui, įtraukiant valstybės saugumo specialistus dėl kibernetinio saugumo.
- Numatyti papildomus resursus ryšių ir Asmens tapatybės ir migracijos duomenų valdytojams, kad šios institucijos galėtų atlikti savo vaidmenis be paslaugų kokybės suprastėjimo.
- Sukurti **aiškų incidentų valdymo planą** ir pasidalinti atsakomybę su Europos Komisijos koordinavimo, priežiūros ir įgyvendinimo mechanizmais.

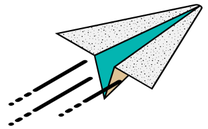


VIEŠA

KIBERNETINIO SAUGUMO EKSPERTŲ ASOCIACIJA

IŠVADOS: EUDI Wallet vaidmenys Lietuvoje






Rizika	Grėsmė	Galimos pasekmės	Rekomendacijos
Sertifikatų teikimo fragmentacija	Nesuderinti standartai, atsakomybės dubliavimas	Techninės klaidos, suklastotų sertifikatų rizika, man-in-the-middle atakos	Konsoliduoti sertifikatų teikimą vienoje institucijoje; aiškiai nustatyti atsakomybę
Kritinių registrų apsauga	Registrai tampa prioritetiniu taikiniu užsienio žvalgyboms ir kibernetiniams nusikaltėliams	Asmens ir juridinių duomenų nutekėjimas, neteisėtų tapatybių kūrimas	Sustiprinti ryšių ir skaitmeninių paslaugų reguliatorius, užtikrinantis registraciją, priežiūrą kibernetinio saugumo pajėgumams; reguliarios saugumo patikros
Reguliatoriaus pajėgumai	Interesų konfliktas tarp priežiūros ir įgyvendinimo funkcijų	Sprendimų šališkumas, pavėluota reakcija į pažeidimus	ryšių ir skaitmeninių paslaugų reguliatorius sutelkti tik į priežiūrą ir reguliavimą; sertifikavimo funkciją perkelti kitur
Koordinavimo stoka tarp institucijų	Nesuderintas incidentų valdymas	Lėtas reagavimas į atakas, grandininiai pažeidimai tarp institucijų	Įsteigti nacionalinį koordinavimo centrą / SOC EUDI ekosistemai; įtraukti NKSC
Pasikliaujančiųjų šalių registravimas	Neskaidri ar nepakankama priežiūra leidžia patekti netikriems paslaugų teikėjams	Piliečių duomenų vagystės, reputacinė žala	Griežta registracijos procedūra, sertifikavimas, centralizuotas prižiūrėtojas

VIEŠA

KIBERNETINIO SAUGUMO EKSPERTŲ ASOCIACIJA

IŠVADOS: eIDAS 2.0, BDAR, TIS2 ir DORA sąveika sektoriuose




Sektorius	eIDAS 2.0 + BDAR	eIDAS 2.0 + TIS2	eIDAS 2.0 + DORA	Galimos rizikos/pasekmės
Universitetai	Studentų tapatybės patikra, diplomų/pažymėjimų išdavimas → būtina duomenų minimizacija ir logai	Valstybiniai universitetai laikomi svarbia infrastruktūra → turi įtraukti EUDI į ISMS	Netiesioginis poveikis, nebent teikiamos paskolos	Nepakankami resursai IS saugumui, pranešimų dubliavimas
Registrų centras (RC)	Juridinių asmenų duomenys kaip EUDI atributai → BDAR pažeidimai turėtų tarpvalstybinį poveikį	RC priskiriamas ypatingos svarbos operatoriams → privaloma SOC sąveika, trumpi pranešimo terminai	RC kaip duomenų tiekėjas bankams tampa DORA grandinės dalimi	Kritinis taikinys atakoms, atsakomybės vakuumai tarp institucijų
Medicinos įstaigos	Pacientų ID, Health ID, ePrescription → griežčiausias BDAR režimas (šifravimas, prieigos ribojimas)	Ligoninės ir eSveikata jau yra kritinė infrastruktūra → visi incidentai privalo būti pranešti NKSC/ENISA	Netiesioginis poveikis, kai integruojasi su draudimo/finansų paslaugomis	Duomenų vagystės, reputacinė žala, pranešimų dubliavimas
Bankai ir finansų įstaigos	KYC/AML procesai per EUDI → būtina duomenų minimizacija, sutikimų dokumentavimas	Esminiai paslaugų teikėjai pagal TIS2 → būtini SOC, atsparumo planai, incidentų pranešimai	DORA taikomas tiesiogiai → testai, tiekimo grandinės valdymas, papildomi auditai	EUDI sutrikimai gali blokuoti onboardingą, tiekimo grandinės atakos, papildomi kaštai

VIEŠA

AČIŪ

KIBERNETINIO SAUGUMO
EKSPERTŲ ASOCIACIJA

VIEŠA

Intelektinės nuosavybės teisės

Visas šiame dokumente viešai skelbiamas skaitmeninis audiovizualinis turinys yra saugomas turtinėmis autorių bei gretutinėmis teisėmis Lietuvos Respublikos ir Europos Sąjungos teisės aktuose nustatyta tvarka. Bet koks šio skaitmeninio audiovizualinio turinio atgaminimas, platinimas, padarymas viešai prieinamu (viešas paskelbimas) ar kitoks turtinėmis autorių ar gretutinėmis teisėmis saugomas panaudojimas be teisėto šio turinio savininko sutikimo laikomas minėtųjų turtinių teisių į šiuos veiksmus pažeidimu, už kurį jas pažeidusiam asmeniui gali būti pritaikyta atsakomybė Lietuvos Respublikos ir Europos Sąjungos teisės aktuose nustatyta tvarka bei apimtimi.
Be teisėto savininko sutikimo, šiame dokumente viešai skelbiamas skaitmeninis audiovizualinis turinys trečiųjų asmenų gali būti panaudojamas tik išimtiniais Lietuvos Respublikos autorių teisių ir gretutinių teisių įstatyme reglamentuotais atvejais, pavyzdžiui, asmeninio naudojimo tikslais ir pan. Dėl šiame dokumente viešai skelbiamo skaitmeninio audiovizualinio turinio panaudojimo komerciniais tikslais ar kitais būdais, reikalaujančiais teisėto šio turinio savininko sutikimo (licencijos), kreiptis el. paštu: arunas.girdziusas@networkgate.lt

Intellectual property rights

All digital audiovisual content made public in this document is protected by property copyright and related rights in accordance with the procedure established by the legal acts of the Republic of Lithuania and the European Union. Any reproduction, distribution, making available to the public of this digital audiovisual content (communication to the public) or other use protected by property copyright or related rights without the legitimate consent of the owner of this content shall be considered a violation of the above-mentioned property rights to these actions, for which the person who violated them may be held liable in accordance with the procedure and to the extent established in the legal acts of the Republic of Lithuania and the European Union. Without the consent of the rightful owner, the digital audiovisual content publicly available in this document may be used by third parties only in exceptional cases regulated by the Law on Copyright and Related Rights of the Republic of Lithuania, for example, for the purposes of personal use, etc. For the commercial use of the digital audiovisual content made public in this document or by other means requiring the legitimate consent (license) of the owner of this content, please contact us by e-mail: arunas.girdziusas@networkgate.lt

Intelektinės nuosavybės teisės

KIBERNETINIO SAUGUMO EKSPERTŲ ASOCIACIJA

VIEŠA

KIBERNETINIO SAUGUMO EKSPERTŲ ASOCIACIJA

GALIMI IŠŠŪKIAI LIETUVOS MASTU

Koordinavimas tarp skirtingų institucijų ir įmonių

- Išlieka rizika, kad atsakomybės tarp skirtingų vaidmenų nebus aiškiai paskirstytos. Reikalingas nuolatinis tarpžinybinis koordinavimas tarp dėklės teikėjo, priežiūros ir registracijos funkciją atliekančių subjektų bei tapatybės duomenų valdytojų.

Resursai ir kompetencija

- Tapatybės duomenų valdytojai jau dabar susiduria su IT resursų bei specialistų trūkumu. Nauji procesai gali sukelti delsimus diegiant sprendimus. Priežiūros institucijai teks plėsti kompetencijas į kibernetinio saugumo sritį, kuri iki šiol nebuvo pagrindinė veiklos kryptis.

Sertifikatų valdymo persidengimai

- Jeigu sertifikatų teikimo funkciją vykdys keli subjektai, gali kilti standartizacijos ir atsakomybės problemų. Neaišku, kas prisiims atsakomybę už klaidas ar galimą kompromitaciją.

Teisinės ir reguliacinės rizikos

- Nacionalinis reguliavimas turi būti greitai suderintas su visais eIDAS 2.0 įgyvendinamaisiais aktais. Bet kokie vėlavimai gali sukelti neapibrėžtumo dėl atsakomybės. Atsakomybės pasidalinimas tarp nacionalinių subjektų ir Europos Komisijos (ypač dėl incidentų valdymo, sertifikavimo, registravimo) gali būti painus.

Kibernetinio saugumo iššūkiai

- Kiekvienas vaidmuo taps potencialiu kibernetinių atakų taikiniu: duomenų valdytojai – dėl saugomų duomenų, priežiūros subjektai – dėl sertifikatų, piniginės teikėjas – dėl pačios infrastruktūros. Todėl būtina užtikrinti aukšto lygio incidentų valdymo mechanizmą ir koordinuotą nacionalinį SOC (Security Operations Center).

KIBERNETINIO SAUGUMO EKSPERTŲ ASOCIACIJA

EUROPOS BLOCKCHAIN PASLAUGŲ INFRASTRUKTŪRA (EBSI) USE CASE

Use case eksperimentai / prototipai

EBSI jau palaiko keletą pilotažinių projektų (pilots) tokiose srityse kaip:

- **diplomų / išsilavinimo pažymėjimai** (digital diploma)
- **traceability / supply chain** (prekių kilmės sekimas)
- **audit trail, integracija su eDelivery komunikacijos protokolais**
- **integracija tapatybės su transakcijomis**

  Šie eksperimentai demonstruoja, kaip identitetas ir transakcijos gali būti vienoje infrastruktūroje.

Kiekybiniai reikalavimai (Level of Assurance – LoA)

Vienas iš iššūkių – EUDI Wallets dažniausiai reikalauja aukšto lygio patikimumo (LoA „high“) tapatybės (PID). Tačiau, ne visiems naudojimo atvejams reikalingas toks lygis – daugumai atvejų gali užtekti „substantial“ lygio.

Klausimai dėl GDPR / duomenų apsaugos ir šalinimo

Vienas esminių iššūkių DLT kontekste – kaip suderinti **immutability** (nekintamumą) su BDAR („teisė būti pamirštam - vietoj fizinio duomenų šalinimo gali būti naudojama **logiškai išjungti įrašai arba blokavimas**, arba blacklisting (angl.) funkcija.

Atitikties vertinimas bei sertifikavimo integracija

EBSI infrastruktūra, jeigu ji bus naudojama kaip infrastruktūra QTSP / ledger paslaugoms, turi būti dalis atitikties vertinimo (conformity assessment) proceso pagal eIDAS 2 standartus. Tai reiškia, kad saugumas, privatumas ir techniniai aspektai turi būti patvirtinti nepriklausomų vertinimų.

KIBERNETINIO SAUGUMO EKSPERTŲ ASOCIACIJA

Liuksemburgo (*Use Care angl.*)

eIDAS 2.0 suteikia aiškų teisinį pagrindą blockchain sprendimams, kurie anksčiau buvo riboti dėl neaiškių taisyklių. Įvedus **Qualified Trust Service Providers – Electronic Ledgers (QTSP-ELs)** koncepciją, atsiranda galimybė blockchain panaudoti kaip patikimą įrašų saugojimo mechanizmą, kuris atitinka ES reguliacinius reikalavimus.

Use Case esmė

Liuksemburgas aprašomas kaip pavyzdys, kaip valstybė gali pasinaudoti eIDAS 2.0 tam, kad:

- skatintų **blockchain sprendimus finansų, sveikatos apsaugos, energetikos sektoriuose**,
- kurtų **viešojo ir privataus sektoriaus partnerystes**,
- steigtų **reguliacinius smėlio dėžės (sandbox) projektus**,
- ir virstų **Europos centru skaitmeninių paslaugų patikimumo srityje**.

Nauda ir rizikos valdymas

- **Nauda:** didesnis pasitikėjimas tarpvalstybiniais skaitmeniniais sandoriais, inovacijų pritraukimas, patikimos tapatybės ir duomenų valdymo sistemos.
- **Iššūkiai:** būtinybė derinti **sektorinius reglamentus (pvz., finansų, sveikatos)** su eIDAS 2.0, užtikrinti kibernetinį saugumą ir duomenų apsaugą, bei sukurti teisines kompetencijas interpretacijai.

KIBERNETINIO SAUGUMO EKSPERTŲ ASOCIACIJA

Šalys / projektai, siejami su blockchain / SSI + eIDAS 2 ambicijomis

- **Italija / PwC & SKChain Advisors**: kuriama blockchain pagrindu veikianti skaitmeninės tapatybės sistema, remianti SSI technologiją, kad būtų suderinta su eIDAS 2 reikalavimais.
- **Projekto mastu – 22 šalys Europoje**: Large-Scale Pilots (pvz. projektai POTENTIAL, DC4EU) tiria, kaip integruoti eIDAS mechanizmus su blockchain / EBSI (European Blockchain Services Infrastructure) + Norvegija ir Ukraina.
- **Europos Blockchain Paslaugų Infrastruktūra (EBSI):** bando ne viena valstybė, bet 27 ES šalys + Norvegija.
- **Lichtenšteinas ir pati Komisija** dalyvauja EBSI tinkle, kaip blokų infrastruktūros operatoriai. EBSI yra numatyta kaip įrankis, palaikyti patikimus blockchain pagrindu veikiančius skaitmeninius paslaugų mechanizmus, kurie bus naudingi eIDAS 2 kontekste. Kai kurios šalys leidžia arba ruošiasi įdiegti EBSI pilotus: Prancūzija, Suomija, Švedija, Danija, Nyderlandai, Liuksemburgas, Slovėnija ir kt.
- **Liuksemburgas**: minima kaip valstybė, kuri gali pasinaudoti eIDAS 2 pakeitimais siekiant skatinti blockchain sprendimus reguliuojamoje aplinkoje (QTSP-EL, interoperabilumas) – kaip koncepcinis pavyzdys, kur blockchain gali tapti nacionalinės skaitmeninės tapatybės ekosistemos dalimi.