VILNIAUS UNIVERSITETO

KAUNO FAKULTETAS

SOCIALINIŲ MOKSLŲ IR TAIKOMOSIOS INFORMATIKOS

INSTITUTAS

Finansų technologijų studijų programa

Kodas 6211BX022

TOMAS KAREIVA

MAGISTRO BAIGIAMASIS DARBAS

ES SKAITMENINĖS TAPATYBĖS DĖKLĖS TAIKYMO METODAS KLIENTŲ ĮVEDIMO PROCESO GREIČIO DIDINIMUI IR PINIGŲ PLOVIMO PREVENCIJAI

Kaunas, 2025

VILNIAUS UNIVERSITETO

KAUNO FAKULTETAS

SOCIALINIŲ MOKSLŲ IR TAIKOMOSIOS INFORMATIKOS INSTITUTAS

TOMAS KAREIVA

MAGISTRO BAIGIAMASIS DARBAS

ES SKAITMENINĖS TAPATYBĖS DĖKLĖS TAIKYMO METODAS KLIENTŲ ĮVEDIMO PROCESO GREIČIO DIDINIMUI IR PINIGŲ PLOVIMO PREVENCIJAI

Magistrantas_____
(parašas)

Darbo vadovas_____
(parašas)

Doc. Partn. Audrius Ramoška
(darbo vadovo mokslo laipsnis, mokslo pedagoginis vardas, vardas ir pavardė)

Darbo įteikimo data

Registracijos Nr.

Kaunas, 2025

TURINYS

PAVEIKSLŲ SĄRAŠAS

SANTRUMPŲ SĄRAŠAS

STD – Skaitmeninė Tapatybė Dėklė

eIDAS – (eIDAS 1.0) Europos Parlamento ir Tarybos reglamentas (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų užtikrinimo paslaugų vidaus rinkoje, kurio panaikinama Direktyva 1999/EB

eIDAS – (eIDAS 2.0) Europos Parlamento ir Tarybos reglamentas (ES) Nr. 2024/1183, kurio iš dallies keičiamas Reglamentas (ES) Nr. 910/2014, kiek tai susiję su Europos skaitmeninės tapatybės sistemos nustatymu

ES – Europos Sąjunga

PPP – Pinigų plovimo prevencija

KYC – Pažink savo klientą (angl. Know Your Customer)

AML – kova su pinigų plovimu (angl. Anti-Money Laundering)

SEPA – Europos Sąjungos bendras naudojamas pervedimų standartas (angl. Single Euro Payments Area)

SWIFT – tarptautinė tarpbankinė finansinės informacijos perdavimo ir mokėjimų sistema (angl. Society for Worldwide Interbank Financial Telecommunication)

DI – Dirbtinis intelektas

Kareiva Tomas (2025). *The method of using the European Union's Digital Identity Wallet to speed up a customer onboarding process and money laundering prevention*. MBA Graduation Paper. Kaunas: Vilnius University, Kaunas Faculty, Institute of Social Sciences and Applied Informatics. 71 p.

SUMMARY

Money laundering is a global threat to financial stability. The rapid evolution of digital technologies and the virtual economy exacerbates these risks, creating new opportunities for criminal activity while making it more difficult to detectability. In view of the new regulatory environment of the European Union, together with the Digital Identity Wallet, which is dedicated to secure digital identity verification, a secure digital identity environment that can increase trust in accessing and providing services to both the public and private sectors. Aim of this case to assess the use of the European Union Digital Identity wallet for the prevention of money laundering, focusing on the processes of onboarding a new customer in financial institutions. This study aims to thoroughly examine the theoretical and practical foundation of anti-money laundering (AML) prevention, highlighting its significance, associated challenges, and the procedures involved in client identification. And finally, the analysis focus on the client onboarding process, comparing the currently remote onboarding with EU Digital Identity Wallet and what benefits it brings. Experimental study an in-depth analysis of the scientific literature and the updated eIDAS Regulation (No. 2024/1183) which legitimizes the European Digital Identity ecosystem, is conducted and compared with current client onboarding procedures. Through experimental research, this study aims to demonstrate that the EU Digital Identity Wallet can effectively optimize and accelerate the personal identity data entry process, ensuring anti-money laundering (AML) prevention from the earliest stages of integration into financial institutions. The main findings show that the use of Digital Identity Wallet significantly improves client's identification by enabling the rapid, secure, efficient and fair sharing of personal data, and digital documents in one environment.

Use of Digital Identity Wallet can improve and speed up financial transactions and reduce the risk of fraud and prevent money laundering. The European Union Digital Identity Wallet simplifies the identification of a person, completely abandons the need for manual work, provides security and privacy, and helps to more effectively identify individuals and their financial transactions, while at the same time ensuring anti-money laundering prevention.

This paper has 62 pages, 9 pictures.

ĮVADAS

Temos aktualumas. Pinigų plovimas išlieka viena didžiausių nacionalinio ir tarptautinio lygmens grėsmių finansinei sistemai, kuri ne tik skatina nusikalstamą veiką ir terorizmą, bet ir daro žalą ekonomikos stabilumui bei augimui (Wang, 2023). Pinigų plovimas didina bankininkystės riziką, daro neigiamą poveikį teisėtoms verslo operacijoms, prekių ir paslaugų kainodarai, santaupoms, užimtumo lygį ir ekonomikos augimą (Kot, 2021). Globalūs duomenys atskleidžia, kad kasmet į oficialią rinką patenkančios neteisėtos pajamos siekia nuo 800 mlrd. iki 2 trln. JAV dolerių (Isolauri ir Ameer, 2022).

Sparčiai kintančių informacinių technologijų ir skaitmeninės ekonomikos kontekste, ypač elektroninių ir virtualių sandorių srityje, dėl pinigų plovimo ženkliai auga grėsmės susijusios su finansų sistemų vientisumu, funkcionalumu, reputacija ir stabilumu (Bodescu, Achimb ir Rus, 2022). Manytina, kad sparti finansinių technologijų pažanga skatina globalios kovos su pinigų plovimu komplikuotumą.

Europos Sąjunga (ES), kaip viena iš lyderių kovoje su pinigų plovimu, nuolat ieško naujų, efektyvių ir ekonomiškų būdų, stiprinti esamas prevencines sistemas. ES siekis yra ne tik identifikuoti ir sustabdyti pinigų plovimo veiklą, skatinti finansinių sistemų skaidrumą, atsparumą nusikalstamų veikų poveikiui ir patikimumą vartotojams bei investuotojams (Grigaitė, Dias ir Magnus, 2021).

Skaitmeninės Tapatybės Dėklė (STD), kaip instrumentas atitinkantis atnaujintą eIDAS reglamentą (Nr. ES 2024/1183), yra esminius pokyčius ES finansų sistemoje skatinti priemonė, kuri palies kiekvieną. Šia priemone siekiama reikšmingai tobulinti skaitmeninių tapatybių valdymo ir panaudojimo praktiką visoje ES (Lietuvos Respublikos vidaus reikalų ministerija, 2024). STD suteiks galimybę piliečiams ir įmonėms ES teritorijoje saugiau ir patikimiau patvirtinti duomenis, suteikiant galimybę naudotis įvairiomis elektroninėmis viešomis ir privačiomis paslaugomis, tuo pačiu užtikrinant aukšto lygio tapatybės patikrinimą ir saugumą, suteikiant vartotojams galimybę kontroliuoti savo asmeninę informaciją (European Comission, 2023). Teigtina, kad ši iniciatyva atspindi skaitmeninių technologijų taikymo ES finansinių sistemų tobulinimui prioritetus ir gali sėkmingai prisidėti prie kovos su pinigų plovimu užtikrinimo.

Atnaujintas eIDAS reglamentas apibrėžia trys reikšmingos naujovės: naujo tipo tapatybės dokumentas (eID), pritaikytas naudoti skaitmeninėje aplinkoje, galimybė keistis skaitmeniniais, kompiuteriui suprantamu formatu pateikiamais duomenimis (pvz.: identifikacinis dokumentas, vaistų receptas, mokslo diplomas, socialinio draudimo pažymėjimas) ir tam yra pritaikytas instrumentas – Skaitmeninė Tapatybės Dėklė. Visos šios naujovės suteikia galimybę greitai ir patikimai identifikuoti asmenis bei jų finansines operacijas, todėl tai gali būti naudinga identifikuojant ir užkardant pinigų plovimo atvejus (Podgorelec, Alber ir Zefferer, 2022).

Problemos ištyrimo lygis. Pinigų plovimo prevencija (toliau – PPP) mokslinėje literatūroje plačiai nagrinėta tiek teoriniu, tiek praktiniu aspektu. Zavoli ir King (2021) tyrė kovos su pinigų plovimu priemonių įgyvendinimą nekilnojamojo turto sektoriuje. Vijeyan ir Rahmat (2022) siekė įvertinti kontrolės aplinkos, rizikos vertinimo, informavimo ir komunikacijos praktikos bei stebėsenos poveikį kovos su pinigų plovimu priemonių veiksmingumui. Durguti ir kt. (2023) gilinosi į kovos su pinigų plovimu taisyklių veiksmingumą vertinant Vakarų Balkanų šalių bankų sektoriaus stabilumą.

Moksliniuose šaltiniuose nustatyta, kad sparčiai tobulėjančios technologijos gali padėti finansų įstaigoms, kovoti su finansiniais nusikaltimais (Akhtar, Khan ir Raza, 2023). Bodescu ir kt. (2022) atskleidė, kad technologijų integravimas turi įtakos pinigų plovimo rizikos mažėjimui. Wang (2023) nustatė, kad integruojant technologijas didinamas kovos su pinigų plovimu priemonių ir sistemų veiksmingumas (Wang, 2023).

Nepaisant didelių kovai su pinigų plovimu skiriamų pastangų, finansinių įstaigų dalyvavimas neteisėtoje veikloje, korupcija ir finansiniai nusikaltimai vis dar yra egzistuojantis reiškinys. Kartu yra poreikis reaguoti į nuolatinę nusikalstamą veiklą vykdančių asmenų elgesio ir metodų kaitą (Krsteski, 2020; Wang, 2023; Kot, 2021). Pažymėtina, kad kibernetiniai nusikaltimai tapo svarbia nusikaltėlių veiklos dalimi (Rocha-Salazar ir Segovia-Vargas, 2024; Bodescu et al., 2022), daugėja pinigų plovimo atvejų panaudojant kriptovaliutas (Kolachala et al., 2021). Be to, Džafarovos (2022) teigimu, nusikaltėliams sumaniai naudojant išmaniąsias technologijas augančioms finansinių technologijų (FinTech) įmonėms vis sudėtingiau nuotoliniu būdu nustatyti klientų tapatybę.

Nors dauguma tyrimų koncentruojasi į gerai žinomas pinigų plovimo prevencijos priemones (pvz., „pažink savo klientą“ - KYC, atsiskaitymų stebėjimą ir tarptautinį bendradarbiavimą), literatūroje trūksta išsamesnės Europos Sąjungos Skaitmeninės Tapatybės Dėklės analizės pinigų plovimo prevencijos kontekste. Analizės trūkumą pirmiausiai sąlygoja tai, kad STD yra naujovė, kurios diegimas dar tik planuojamas. Todėl egzistuoja aiški mokslinės literatūros spraga, kuria siekiama užpildyti šiuo darbu.

Šiuo mokslinio darbo metu bus siekiama ištirti Skaitmeninės Tapatybės Dėklės potencialą ir galimybes pinigų plovimo prevencijos srityje, nustatant konkrečias naudas, galimybes ir iššūkius, su kuriais susidurs finansų sektorius, taip pat rekomendacijas dėl STD integracijos į esamas prevencijos sistemas.

Darbo problema. Kokią įtaką ES Skaitmeninės Tapatybės Dėklės panaudojimas gali turėti pinigų plovimo prevencijos efektyvumui, kliento įvedimui į finansų įstaigą?

Darbo objektas. Europos Sąjungos Skaitmeninės Tapatybės Dėklės panaudojimo pinigų plovimo prevencijoje, galimybių analizė, klientų įvedimo procese.

Darbo tikslas. Įvertinti klientų įvedimo greitį, panaudojant ES Skaitmeninės Tapatybės Dėklę galimybes taikant finansų įstaigose lyginant, kaip yra šiuo metu, užtikrinant pinigų plovimo prevenciją.

Darbo uždaviniai. Siekiant tikslo yra iškelti tokie uždaviniai:

1. Išnagrinėti pinigų plovimo prevencijos teorinius ir praktinius pagrindus, svarbą ir iššūkius bei procesą susijusi su klientų įvedimo į finansų įstaigą.
2. Įvertinti ES STD reguliacinę aplinką, analizuojant pritaikymo galimybes, pinigų plovimo prevencijai, siūlant sprendimus šioje srityje.
3. Analizuoti ES STD taikymo efektyvumą finansų įstaigų, klientų įvedimo procese, lyginant dabartinį procesą, kuris atliekamas nuotoliu ir kokią naudą tai suteikia.

Darbo struktūra. Pirmoje darbo dalyje „Pinigų plovimo prevencijos aktualumas ir problematika“ nagrinėjama su pinigų plovimo prevencijos problematika susiję aspektai: pinigų plovimo ypatumai skaitmeninių technologijų kontekste, pinigų plovimo prevencijos tipai, finansinių institucijų vaidmuo kovoje su pinigų plovimu bei tarptautinio bendradarbiavimo reikšmės siekiant užkardyti pinigų plovimą. Šioje darbo dalyje yra pagrindžiamas pinigų plovimo prevencijos efektyvinimo poreikis.

Antroje darbo dalyje „Europos Sąjungos Skaitmeninės Tapatybės Dėklės galimas vaidmuo pinigų plovimo prevencijoje. Siūlomi sprendimai“ nagrinėjamas ES STD galimas panaudojimas užtikrinant pinigų plovimo prevenciją tam skirtuose procesuose. Atsižvelgiant į temos naujumą šioje dalyje atliekama detali STD taikymo galimybių analizė. Aptariamos STD teikiamos galimybės efektyviai atpažinti (identifikuoti) asmenis ir jų finansines operacijas, analizuojami įvairūs technologiniai privalumai ir iššūkiai susiję su duomenų saugumu ir privatumu.

Trečioje darbo dalyje „Skaitmeninės Tapatybės Dėklės efektyvumo vertinimas pinigų plovimo prevencijoje“ pristatomos STD taikymo strategijos realiose situacijose. Nagrinėjant praktinius panaudojimo atvejus bei lyginant su šiuo metu vykdomomis procedūromis, atskleidžiamas STD taikymo poveikis, didinant klientų įvedimo (angl. *onboarding*) greitį ir kartu efektyvinant pinigų plovimo prevenciją.

Darbo ir tyrimo metodai. Darbe naudojama mokslinės literatūros ir atnaujinto eIDAS reglamento (Nr. 2024/1183) įteisinančio ES STD analizė, lyginant šiuo metu taikomu klientų įvedimo procesu, galimais sprendimais, vertinant pritaikymo galimybes finansų įstaigose.

1. PINIGŲ PLOVIMO PREVENCIJOS AKTUALUMAS IR PROBLEMATIKA

Šioje darbo dalyje nagrinėjama pinigų plovimo prevencijos problematika, skiriant ypatingą dėmesį su naujausiomis skaitmeninėmis technologijomis susijusioms problemoms. Šiandieną daugelis pinigų plovimo prevencinių priemonių ir veiksmų vis dar atliekami rankiniu būdu. Tačiau sparčiai augant kriptovaliutų ir skaitmeninių finansinių operacijų populiarumui, tradicinių rankinių metodų veiksmingumas ženkliai mažėja.

1.1. Pinigų plovimas skaitmeninių technologijų kontekste

Skaitmeninių mokėjimo sistemų paplitimas, interneto platformų plėtra tapo svarbiu šiuolaikinių finansinių paslaugų patogumo ir veiksmingumo veiksniu (Subbagari, 2023). Dėl visuotinio skaitmeninimo proceso tarptautiniu mastu mažėjo nacionalinių sienų reikšmė, vyko prekybos liberalizacijos procesai. Skaitmeninis amžius sietinas ir su tokiomis naujovėmis kaip nuotolinis darbas, mobilioji bankininkystė ir e. prekyba (Bodescu et al., 2022). Technologinis išsivystymas ir Fintech inovacijos turėjo įtakos ekonominei integracijai, kapitalo liberalizavimui ir finansinių sandorių spartai (Durguti et al., 2023). Pasak Lieonov ir kt. (2021), sparti technologinė pažanga lėmė transformacinę finansinių sandorių revoliuciją, kuri suteikė klientams neregėtą patogumą ir operacijų greitį. 2016 m. Pasaulio ekonomikos forume buvo pripažinta ketvirtosios pramonės revoliucijos pradžia. Svarbiausios šią revoliuciją charakterizuojančios technologinės inovacijos – dirbtinis intelektas, blokų grandinė, biotechnologijos, virtuali ir papildyta realybė, debesų kompiuterija, biometrija, DevOps, daiktų internetas (IoT), išmaniosios taikomosios programos (I-Apps), didieji duomenys ir analizė, robotų procesų automatizavimas (Rocha-Salazar ir Segovia-Vargas, 2024). Šiame poskyryje bus siekiama atskleisti, kokią įtaką skaitmeninių technologijų tobulėjimas daro pinigų plovimo reiškiniui.

Pinigų plovimas – nusikalstama veika, kurios metu neteisėtų būdu įgytos lėšos yra integruojamos į legalią ekonomiką, slepiant jų tikrąją kilmę ir žinant, kad šis turtas yra gautas iš nusikalstamos veikos arba dalyvaujant tokioje veikoje (LR pinigų plovimo ir teroristų finansavimo prevencijos įstatymas, 1997). Panašiai pinigų plovimas apibūdinamas ir mokslininkų. Remiantis Krsteski (2020), pinigų plovimas yra sudėtingas procesas, kurio metu neteisėtai gautos lėšos paverčiamos teisėtu turtu, siekiant nuslėpti jų neteisėtą kilmę, taip pat sąmoningas tokio turto, gauto iš nusikalstamos veiklos, įgijimas, laikymas ar naudojimas. Waleed, Gadsen ir Yawney (2022) pinigų plovimą apibūdina kaip procesą, kurio metu nusikaltėliai ir teroristinės organizacijos įteisina pajamas, gautas iš neteisėtos veiklos, dažnai susijusios su sunkiais nusikaltimais, tokiais kaip prekyba

narkotikais ir terorizmas. Visuose apibrėžimuose akcentuojamas pagrindinis pinigų plovimo tikslas – nuslėpti neteisėtą turto kilmę (Kot, 2021).

Elektroninėje erdvėje vykdomas pinigų plovimas patenka į kibernetinių nusikaltimų sritį. Kibernetiniai nusikaltimai – nusikaltimai, kuriems įvykdyti buvo panaudotos kompiuterinės technologijos (Nacionalinė kibernetinio saugumo būklės ataskaita, 2022). Pinigų plovimas elektroninėje erdvėje yra praktika, kai naudojami internetiniai sandoriai, pasižymintys dideliu pasiekiamumu, greičiu ir mažomis sąnaudomis bei anonimiškumu (Handa ir Ansari, 2022). Vykdydami pinigų plovimą nusikaltėliai dažnai pasitelkia skaitmenines priemones, pvz., įsilauždami pavagia prieigos raktus ar slaptažodžius. Įgiję šiuos finansinius išteklius nusikaltėliai gali manipuliuoti finansų sistema, kad „išplautų" pavogtas lėšas. Pinigų plovimas naudojant finansines technologijas yra palyginti nauja nusikaltimų rūšis, todėl tyrimų vykdymą apsunkina teisėsaugos pareigūnams reikalingų specialių žinių ir tikslumo stoka (Pratomo, Zainal ir Hakim, 2023). Pinigų plovimas gali apimti įvairias veikimo schemas, tačiau paprastai galima išskirti tris pinigų plovimo procesą apimančius etapus (Rocha-Salazar ir Segovia-Vargas, 2024):

- ✓ patalpinimą – neteisėtų lėšų įvedimą į finansų sistemą;
- ✓ sluoksniavimą – lėšų šaltinio nuslėpimą atliekant keletą operacijų;
- ✓ integravimą – pakartotinį išplautų pinigų kaip teisėtų įvedimą į ekonomiką.

Neteisėtos lėšos cirkuliuoja visame pasaulyje, dažnai kelis kartus pereidamos įvairių sektorių įmones, kol yra investuojamos į nekilnojamąjį turtą, prabangias transporto priemones ir kitą brangų turtą (Durguti et al., 2023).

Naujosios skaitmeninės technologijos netiesiogiai išplečia priemones, kuriomis tokia veikla gali būti vykdoma, transformuojama ir slepiama (Rocha-Salazar, ir Segovia-Vargas, 2024). Pasak Subbagari (2023), pinigų plovimo metodai vystomi siekiant pasinaudoti skaitmeninių technologijų silpnosiomis vietomis. Šiuolaikinės technologijos, nors ir naudingos, pritraukia kibernetinius nusikaltėlius, kurie naudojasi neteisėtais būdais siekdami finansinės naudos, todėl didėja kibernetinių nusikaltimų skaičius. Vykdant kibernetinius nusikaltimus naudojamasi informacinėmis technologijomis skirtingose jurisdikcijose ir skirtingomis tapatybėmis, todėl juos aptikti itin sudėtinga (Achim et al., 2021). Pasak Gerbrands ir kt. (2022), reaguodami į kovos su pinigų plovimu griežtinimą nusikaltėliai vis dar geba kurti sudėtingas ir sunkiai atsekamas nusikaltimo strategijas. Tobulėjant finansinėms technologijoms finansų įstaigos tapo pagrindiniais pinigų plovimo taikiniais, kadangi dėl plataus teikiamų paslaugų spektro suteikia įvairių galimybių nuslėpti finansinių operacijų lėšų kilmę (Pratomo et al., 2023).

Virtualių platformų, tokių kaip kriptovaliutų keityklos, žaidimų platformos ir virtualių valiutų prekybos vietos atsiradimas, suteikė nusikalstamoms organizacijoms naujų galimybių plėsti savo neteisėtą veiklą, įskaitant pinigų plovimą. Nusikaltimams vykdyti pasitelkiama įvairi, išmani

technologinė ir (arba) programinė įranga. Nepaisant reglamentavimo griežtinimo ir kovai su pinigų plovimu skirtų teisės aktų, vis dar įmanoma steigti ofšorines sąskaitas. Mokėjimo technologijų, tokių kaip mobilioji bankininkystė ir išmaniosios kortelės, pažanga pakeitė verslo operacijas ir suteikė dar daugiau mokesčių vengimo galimybių. Be to, finansinės technologijos išnaudojamoms sukčiavimui, turto prievartavimui, pinigų plovimui ir neteisėtam kriminalinės veiklos finansavimui (Bodescu et al., 2022). Reaguojant į naujus finansinių nusikaltimų iššūkius reikalingi tyrimai, kurie pasižymi dideliais kaštais bei reikalauja nuolatinio įgūdžių ir infrastruktūros atnaujinimo, todėl paprastai atsilieka nuo tobulėjančių finansinių nusikaltimų (Lieonov et al., 2021). Šiuolaikinių pinigų plovimo metodų, kuriuos skatina globalizacija ir technologinė pažanga, sudėtingumas rodo, kad būtina imtis pažangių pinigų plovimo prevencijos strategijų.

Remiantis Subbagari (2023), verta išskirti šiuos finansinių sandorių skaitmeninimo aspektus, kurie apsunkina kovą su pinigų plovimu:

1. Anonimiškumas – daugelis skaitmeninių platformų, įskaitant kriptovaliutų keityklas, socialinius tinklus, e. prekybos svetaines, virtualius žaidimus, virtualias valiutas ir kt., suteikia galimybę veikti anonimiškai arba naudoti privatumo funkcijas, skirtas paslėpti tikrąją tapatybę. Dėl anonimiškumo valdžios institucijoms sunku atsekti lėšų kilmę. Neturint galimybės nustatyti sandoriuose dalyvaujančių šalių tapatybės, sunkiau nustatyti ir įrodyti neteisėtą veiką, pvz., pinigų plovimą.
2. Globalumas – skaitmeniniai sandoriai atliekami tarptautiniu mastu ir nereikalauja fizinio pinigų judėjimo, todėl suteikia galimybę pasinaudoti skirtingų jurisdikcijų reguliavimo sistemų skirtumais ir spragomis. Siekdami paslėpti pėdsakus ir sumažinti neteisėtos veiklos rizikas, pinigų plovėjai gali nukreipti pinigus į šalis, kuriose galioja mažiau griežtos taisyklės.
3. Greitis ir efektyvumas – skaitmeniniu būdu vykdomus sandorius galima atlikti itin greitai. Vykstant sparčiam lėšų judėjimui ypač sunku susekti ir sustabdyti įtartinas finansines operacijas. Pinigų plovėjai gali greitai pervesti dideles pinigų sumas.

Ypač didelis kovoje su pinigų plovimu turi būti skirtas su kriptovaliutomis susijusiai problematikai. Galima teigti, kad per paskutinius keletą metų kriptovaliutos išsivystė į reikšmingą ekonomikos ir finansų rinkos inovaciją. Pradžioje šis valiutos tipas nebuvo plačiai analizuojamas dėl trūkstamo aiškaus apibrėžimo. 2012 m. Europos centrinis bankas kriptovaliutą apibrėžė kaip naudojamą išimtinai virtualioje aplinkoje, tai reiškia, kad su ja galima įsigyti tik virtualias prekes ir (ar) paslaugas. Šis apibrėžimas padidino susidomėjimą kriptovaliuta ir galimomis specifinėmis funkcijomis. Nors kriptovaliuta yra investavimo galimybes praplečianti technologinė naujovė, šiandien pripažįstama, kad naudojant ją spekuliaciniais tikslais finansinėms institucijoms kyla papildomų iššūkių (Marcinkevičiūtė, 2023).

Kriptovaliuta apibrėžiama kaip tik skaitmeninė valiutos forma, neturinti centralizuoto pinigų leidimo ar reguliavimo institucijos. Ji veikia decentralizuotoje sistemoje, kuri registruoja sandorius ir valdo naujų vienetų kūrimą. Pinigų plovimo procesas per kriptovaliutas, prasideda nuo sąskaitų atidarymo skaitmeninių valiutų keityklose, taip sudaromos sąlygos į kriptovaliutų sistemą įvesti savo neteisėtus pinigus. Tada pinigai perkeliami sistemoje naudojant įvairius kriptografinius metodus, kuriais nuslepiama jų kilmė. Dažnai tai apima pradinės kriptovaliutos sumaišymą su kitomis lėšomis ir mažesnių sumų paskirstymą konkrečiais adresais. Dėl santykinio kriptovaliutų naujumo su pinigų plovimu kovojančioms finansinėms institucijoms kyla nemažai iššūkių, nes oficialios reguliavimo sistemos dar tik kuriamos (Javor, 2020).

Dėl savo gebėjimo veikti už tradicinio finansų sektoriaus ribų skaitmeninės valiutos reiškia reikšmingą finansinės aplinkos pokytį. Naudojantis tokiomis kriptovaliutomis kaip „Bitcoin", ar „Ethereum" nereikia tradicinių finansų įstaigų dalyvavimo, todėl įmanoma visiškai apeiti reguliuojamą finansų sistemą. Tai yra nusikalstamai veiklai palanki savybė. Yra žinoma apie šių valiutų naudojimo nusikalstamoje veikloje, pvz., prekyboje narkotikais ir turto prievartavime, atvejus (Bodescu et al., 2022). Kaip teigia Tiwari, Gepp ir Kumar (2020), vienas iš pagrindinių virtualiųjų valiutų traukos objektų yra anonimiškumas, leidžiantis vykdyti tarpvalstybines bankines operacijas be griežtos stebėsenos, vykdomos tradicinėse bankų sistemose. Dėl anonimiškumo kriptovaliutos ypač patrauklios asmenims, siekiantiems nuslėpti neteisėtais būdais įgytas lėšas. Skirtingai nuo tradicinės dekretinės valiutos, kuri yra fizinio pobūdžio, virtualiosios valiutos egzistuoja tik skaitmenine forma internete ir veikia nepriklausomai nuo vyriausybės ar centrinio banko priežiūros. Ši decentralizuota sistema kartu su virtualiosioms valiutoms būdingu anonimiškumu yra didelis iššūkis teisėsaugos institucijoms, bandančioms atsekti neteisėtus sandorius. Be to, greitis ir paprastumas, kuriuo didelės pinigų sumos gali būti pervedamos virtualiomis valiutomis, dar labiau vilioja pinigų plovėjus, todėl jie gali greitai ir saugiai perkelti lėšas, išlaikydami savo anonimiškumą viso proceso metu.

Kolachala et al. (2021) akcentuoja, kad vykdant struktūrizavimą sandoriai skaidomi į mažesnius, o vėliau paskirstomi įvairiems vartotojams, valiutoms ir geografinėms vietovėms. Pasak Subbagari (2023), virtualiųjų valiutų naudojimas iš tiesų tapo paplitusiu pinigų plovimo metodu. Naudojantis virtualiomis valiutomis sukuriamas sudėtingas tinklas, slepiantis lėšų kilmę ir srautą, todėl tampa itin sudėtinga aptikti pinigų plovimo atvejus. Dar sudėtingiau tampa dėl painių mokėjimo tinklų, kuriuose pirmenybė teikiama vartotojų anonimiškumui, todėl atsekti operacijas iki jų šaltinių arba nustatyti galimą jų ryšį su neteisėta veikla itin sunku. Sprendžiant šiuos iššūkius finansų sektoriaus subjektams būtina naudotis pažangiausiomis priemonėmis ir technologijomis, kurios padėtų sumažinti sandorių struktūrizavimui ir anonimiškumui būdingą riziką. Pažangios priemonės reikalingos siekiant gerinti sandorių, kurie gali būti susiję su neteisėta veikla, stebėseną ir nustatymą.

Šių sandorių stebėseną dar labiau apsunkina tokios maišymo paslaugos kaip „Bitcoin Mixers" naudojimas, siekiant sulieti pinigų srautą, sumaišant neteisėtas pajamas su teisėtomis lėšomis. Naudojant šį metodą nusikaltėliams dar lengviau paslėpti neteisėtas operacijas bendroje virtualiųjų valiutų ekosistemoje. Anot Kenneth (2022), „Bitcoin Mixer" (kriptovaliutų maišymo paslauga) kelia didelių iššūkių reguliavimo ir teisėsaugos institucijoms. Maišytuvams būdingos decentralizuotos technologijos, trukdo valdžios institucijoms veiksmingai konfiskuoti ar peržiūrėti sandorių įrašus.

Kenneth (2022) pažymi, kad maišytuvai taip pat tobulėja, atsiranda tokios funkcijos kaip atsitiktinių sandorių sumų įtraukimas ir uždelstas vykdymas, todėl jie pranoksta įprastus stebėjimo metodus, dar labiau apsunkindama reguliavimo priežiūrą. Dėl to kovos su pinigų plovimu standartų vykdymo užtikrinimas tampa vis sudėtingesnis. Reguliavimo aplinka susiduria su kliūtimis kovojant su pinigų plovimu per maišytuvus, daugiausia dėl decentralizuotų blokų grandinės technologijos ypatybių. Nors kai kurios priemonės yra susijusios su sankcijomis maišytuvų paslaugoms, surinkti svarių įrodymų, tiesiogiai susiejančių šias paslaugas su konkrečiais neteisėtais sandoriais, itin sudėtinga. Norint išspręsti pinigų plovimo problemą kriptovaliutų srityje, reikia visapusiškos strategijos, kuri užtikrintų privatumo teises ir saugumą. Be to, skaitmeninėje aplinkoje nusikaltėliai gali užsiimti papildoma neteisėta veikla, pvz., kriptovaliutų vagystėmis ir (arba) plovimu per internetines prekybos platformas (Rocha-Salazar ir Segovia-Vargas, 2024).

Yra žinoma, kad kriptovaliutos, ypač bitkoinai, nuo pat jų atsiradimo pradžios, buvo siejamos su neteisėtais sandoriais, kuriuos galimai vykdo ekstremistinės grupuotės. Tokias kriptovaliutas, kaip „Bitcoin", "Solana" arba "Ethereum" teroristinės organizacijos išnaudojo siekdamos palengvinti neteisėtus sandorius, įskaitant prekybą narkotikais, ginklais ir kitomis nelegaliomis prekėmis pogrindinėse rinkose. Be to, daugėja su kriptovaliutomis sietinų bylų dėl turto prievartavimo schemų. Regionuose, kuriuose nepakankamai išvystytos arba nestabilios finansų sistemos, kriptovaliutos suteikia teroristams realią galimybę pritraukti lėšų. Be to, kriptovaliutos pasitelkiamos kibernetinio terorizmo veikloje siekiant palengvinti neteisėtus sandorius "tamsiajame internete" (angl. *Dark web*) (Padalkar, 2023). „Tamsusis internetas" yra interneto dalis, neprieinama naudojantis įprastinėmis naršyklėmis ir reikalaujanti specialių įrankių, prieigos. Ši interneto sritis suteikia itin aukštą anonimiškumo laipsnį tiek svetainių kūrėjams, tiek lankytojams. Dėl šios savybės tamsusis internetas tapo populiariu ne tik tarp įvairių nusikalstamų veiklų vykdytojų, pvz., narkotikų prekybos, ginklų pardavimo, neteisėtos informacijos platinimo ar pinigų plovimo, atžvilgiu (Omar ir Ibrahim, 2020).

Galima teigti, kad pagrindiniai finansinių sandorių skaitmeninimo privalumai, nors ir naudingi teisėtiems naudotojams, taip pat suteikia daugiau pinigų plovimo galimybių, kadangi apsunkina finansinių sandorių reguliavimą ir teisėsaugos institucijų pastangas veiksmingai kovoti su finansiniais nusikaltimais. Remiantis Handa ir Ansari (2022), galima išskirti pagrindinius kovos su pinigų plovimu skaitmeninėje aplinkoje susijusius sunkumus:

1. Jurisdikciniai iššūkiai – kibernetiniai nusikaltimai ir pinigų plovimas yra tarptautinė problema, dėl to sudėtinga užtikrinti teisės aktų vykdymą skirtingose jurisdikcijose. Dėl reglamentavimo skirtumų finansų įstaigoms neretai sunku gauti reikiamus duomenis arba veiksmingai veikti tarpvalstybiniu mastu. Globalus nusikalstamos veiklos pobūdis riboja pinigų plovimo užkardymo koordinavimą.
2. Sandorių apimtis – ekonominės globalizacijos kontekste didėja ir internetu atliekamų finansinių sandorių skaičius bei mastas. Kartu visame pasaulyje steigiamos naujos finansų įstaigos, aptarnaujančios vis daugiau klientų. Dėl augančios operacijų internete apimties vis sunkiau nustatyti, kurios iš jų yra įtartinos ar galimai susijusios su pinigų plovimo veikla.
3. Taisyklių ir reglamentų nenuoseklumas – visame pasaulyje skiriasi su pinigų plovimu glaudžiai susijusių veiklos sferų reglamentavimas. Pavyzdžiui, kibernetiniai nusikaltėliai dažnai yra linkę naudotis lažyboms ir kazino žaidimams internete palankesne aplinka.
4. Konkurencinis spaudimas internetinės bankininkystės srityje – finansų įstaigų konkurencinė aplinka internetinės bankininkystės srityje gali trukdyti veiksmingai įgyvendinti "pažink savo klientą" (angl. *Know Your Customer – KYC*) praktiką. Siekdamos pritraukti ir išlaikyti klientus finansų įstaigos gali sumažinti savo budrumą ar deramą atidumą, nes siekia konkurencinį pranašumą įgyti ne saugumo priemonėmis, o siūlydamos paprastumą bei didesnį operacijų vykdymo greitį. Remiantis Padalkar (2023), netinkamai vykdant KYC kyla sunkumų sekant ir užkertant kelią finansiniams nusikaltimams kriptovaliutų erdvėje.

Taip pat daug iššūkių kyla dėl šifravimo ir privatumo technologijų naudojimo, kuris suteikia galimybes nusikaltėliams veiksmingai nuslėpti savo tapatybę ir finansines operacijas. Tokios technologijos, kaip šifruoti komunikacijos kanalai, virtualūs privatūs tinklai (VPN) sudaro sąlygas itin sudėtingai nusikalstamos veikos schemai. Anonimiškumas ne tik apsunkina teisėsaugos institucijų gebėjimą rinkti reikšmingus įrodymus, bet ir trukdo atskleisti neteisėtų lėšų kilmę bei pinigų srautų judėjimą.

Finansinių sandorių skaitmeninimo kontekste atsiskleidžia ir tradicinių kovos su pinigų plovimu metodų ribotumas. Tačiau pripažįstama, kad diegiant skaitmenines technologijas galima padidinti kibernetinių nusikaltimų, įskaitant ir pinigų plovimą, užkardymo galimybes. Pereinant prie technologiškai pažangių metodų kaip anomalijų aptikimas galima veiksmingai apdoroti didžiulius duomenų kiekius ir padidinti kovos su finansiniais nusikaltimais rezultatyvumą (Waleed, Gadsen ir Yawney, 2022). Skaitmeninių technologijų taikymas padeda padidinti besivystančių šalių mokesčių administracijų pajėgumus, kadangi tobulinamas mokesčių pareigūnų turimos informacijos valdymas. Dėl optimizuoto informacijos srauto ir geresnių paslaugų, auga mokesčių administravimo sistemos veiksmingumas, kartu mažėja mokesčių vengimo atvejų ir auga mokesčių surinkimas (Achim, Borlea ir Văidean, 2021). Vis dėlto pripažįstama, kad egzistuoja su pažangių duomenų mokslo metodų

naudojimu kovai su pinigų plovimu susijusios literatūros ir mokslinių tyrimų trūkumas (Waleed et al., 2022). Gausesni ir išsamesni tyrimai reikalingi siekiant pagerinti nusikalstamų veiklų aptikimo metodikas ir stiprinti kovą su pinigų plovimu sistemų atsparumą.

Apibendrinant galima teigti, kad šiuolaikinės technologijos pakeitė finansinių operacijų pobūdį, teikdamos patogumą ir veiksmingumą, tačiau tuo pačiu metu jos sukėlė naujus iššūkius pinigų plovimo prevencijai ir kontrolės metodams. Fintech inovacijos, skaitmeninės mokėjimo sistemos ir kitos technologijos, tokios kaip blokų grandinės ir dirbtinis intelektas, viena vertus padeda gerinti finansinių operacijų skaidrumą ir efektyvumą, kita vertus – suteikia pinigų plovėjams priemones, kaip veikti greičiau, anonimiškiau ir globaliau. Skaitmeninės technologijos keičia pinigų plovimo schemas, apsunkina lėšų kilmės nustatymą ir neteisėtos veiklos sekimą. Kartu šių technologijų dinamiškumas reikalauja nuolat atnaujinti kovai su pinigų plovimu būtinas žinias ir technologijas. Kovojant su pinigų plovimu svarbu palaikyti pusiausvyrą tarp naujųjų technologijų teikiamų naudų ir keliamų pavojų. Tai reikalauja inovatyvių ir dinamiškų strategijų, kurios apima ir technologinę plėtrą, griežtą atitikimo ir stebėsenos sistemų reguliavimą.

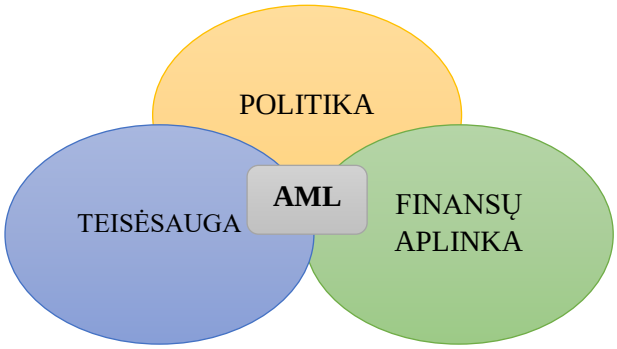
1.2. Pinigų plovimo prevencijos principai

Pinigų plovimo prevencija gali tapti valstybės saugumo ir stabilumo veiksniu, kadangi ne tik padeda stiprinti finansų įstaigų sąžiningumą, bet ir atlieka gyvybiškai svarbų vaidmenį puoselėjant teisinę valstybę, skatinant etišką verslo praktiką ir išsaugant visuomenės pasitikėjimą finansų sistema (Kurniawan, 2023). Spręsdamos daugialypes pinigų plovimo problemas valstybės gali padidinti savo atsparumą ekonominėms ir politinėms grėsmėms, kurias kelia neteisėti finansiniai srautai. Šiame poskyryje bus siekiama atskleisti pagrindinius pinigų plovimo prevencijos principus.

Visame pasaulyje skiriama daug pastangų kovoti su šiuo nusikalstamu reiškiniu, kadangi pinigų plovimas daro tiesioginį neigiamą poveikį gamybai ir investicijoms, didina makroekonominės destabilizacijos riziką. Lėšos, nepriklausančius oficialiai finansų sistemai, dažnai nukeliauja į ekonomikos sritis, kurios minimaliai prisideda prie nacionalinio biudžeto pajamų (Kot, 2021). Be to, pinigų plovimas, skatina tiek viešojo, tiek privataus sektoriaus korupciją. Korupcinės veiklos atžvilgiu jautrios šalys tampa mažiau patrauklios užsienio investuotojams ir įtvirtina nuolatinę nelygybę (Waleed et al., 2022). Pinigų plovimo padariniai juntami ne tik finansų sistemose, bet ir teisinei padėčiai (Steblianko et al., 2020).

Pinigų plovimo prevencijai yra įgyvendinama taikant AML principus (angl. *Anti-Money Laundering*). AML gali būti apibūdinama kaip priemonių, teisės aktų ir procedūrų visuma, nukreipta užkirsti kelią pinigų plovimui. AML apima įvairias teisines, finansines ir operacines priemones,

taikomas pinigų plovimo rizikos atpažinimui ir stebėjimui (Demetis, 2008). Galima išskirti tris pagrindinius struktūrinius AML komponentus (žr. 1 pav.).



Šaltinis: Demetis (2008). A Systems Theoretical approach for Anti-Money Laundering informed by a Case Study in a Greek Financial Institution. https://etheses.lse.ac.uk/2571/1/U615520.pdf

1 pav. AML komponentai

AML kaip priemonių, teisės aktų ir procedūrų visumą charakterizuoja šie principai (Demetis, 2008):

- Klientų tapatybės nustatymas („Pažink savo klientą“, KYC) – veiksmai skirti nustatyti kliento tapatybę ir įsitikinti, kad yra naudojamos teisėtai įsigytos lėšos.
- Sandorių stebėjimas – veiksmai, kuriais siekiama identifikuoti įtartinus sandorius.
- Rizikos vertinimas – identifikuojamos veiklos arba klientų kategorijos, kurios kelia didžiausią riziką ir turi sulaukti atidesnės kontrolės.
- Vidinės kontrolės sistemos – finansų organizacijos vadovaujasi procedūrų ir taisyklių visuma, skirta pinigų plovimo užkardymui.
- Tarpinstitucinis bendradarbiavimas – informacija apie įtartinus sandorius yra pateikiama atitinkamoms teisėsaugos institucijoms.

Vienas svarbiausių AML principų, aktualių ir šio darbo kontekste, yra jau minėta KYC praktika. KYC praktiką įpareigotos taikyti daugelis įvairių finansinių institucijų – bankai, elektroninių pinigų ir paslaugų teikėjai, investiciniai fondai, draudimo bendrovės, kriptovaliutų biržos ir kt. KYC patikrinimai reikalingi, nes padeda patikrinti klientų tapatybę ir užtikrinti, kad finansų sistema nebūtų naudojama neteisėtais tikslais. KYC procesai paprastai apima asmeninės informacijos, pvz., oficialių asmens tapatybės dokumentų, adresų, o kartais ir lėšų šaltinių, rinkimą ir tikrinimą. Nepaisant šių patikrinimų svarbos, kai kurios kriptovaliutų biržos dėl įvairių priežasčių vengia taikyti griežtas KYC priemones, pvz., nereikalauja atlikti KYC patikrinimų, kai klientai atsiima arba perveda savo lėšas. Dėl to gali atsirasti spragų, kai neteisėtos lėšos naudojamos be tinkamo patikrinimo (Padalkar, 2023). Internetinėje aplinkoje ypač sudėtinga užtikrinti nuoseklią KYC politiką. KYC politikoje paprastai reikalaujama, kad kliento tapatybė būtų patvirtinta

dokumentais. Tai yra nesudėtinga bendraujant akis į akį, tačiau skaitmeniniame kontekste, kai naudotojas nebūtinai pateikia tikslią asmeninę informaciją, patikrinti tapatybę pagal KYC standartus yra daug sudėtingiau (Handa ir Ansari, 2022).

Pol (2020) teigimu, nepaisant kelių dešimtmečių aktyvios kovos su pinigų plovimu, rodant globalią politinę valią užkardyti šią nusikalstamą veiklą, AML išlieka pačia neefektyviausia teisėsaugos funkcija. Remiantis autoriaus pateiktais skaičiavimais, taikant AML priemones kasmet pavyksta užkardyti maždaug tik 0,05 proc. globaliai plaunamų pinigų srauto. Tai reiškia, kad apie 99,95 proc. pinigų ir toliau sėkmingai plaunama. Todėl kyla klausimas, kuria kryptimi AML vystėsi pastaruosius kelerius metus susiduriant su dar didesniais nelegalių sandorių skaitmenizavimo iššūkiais.

Kaip pastebi Bodescu ir kt. (2022), iki 2018 m. AML taisyklėse trūko mechanizmų, kurie galėtų veiksmingai išspręsti virtualių valiutų naudojimą pinigų plovimui riziką. Virtualių valiutų decentralizacija ir sudėtingas atsekimas kelią didelį susirūpinimą dėl jų panaudojimo finansiniuose nusikaltimuose. Nepaisant to, kai kurie tyrėjai mano, kad virtualių valiutų technologijos gali prisidėti prie naujoviškų kovos su pinigų plovimu sprendimų banko sektoriuje. Tačiau, norint praktiškai įgyvendinti tokius sprendimus, reikia išsamesnių tyrimų ir konkrečių atvejų analizės, nes veiksmingos kovos su pinigų plovimu priemonės virtualių valiutų srityje dar nėra ištobulintos.

Reikšmingi pokyčiai sietini su 2023 m. gegužės 31 d. priimtu ES reglamentu (2023/1114) dėl kriptovaliutų rinkos (MiCA), kuris nuo 2024 m. gruodžio 30 d. bus taikomas pilna apimtimi. Šiuo reglamentu siekiama nustatyti vieningas kriptoturto veiklos reguliavimo taisykles visoje ES, užtikrinant didesnį skaidrumą ir saugumą rinkoje. Lietuvoje MiCA reikalavimai bus taikomi be pereinamojo laikotarpio, todėl po 2024 m. gruodžio 30 d. visos kriptoturto paslaugas teikiančios įmonės privalės turėti atitinkamą licenciją. Iki šiol Lietuvos Respublikos pinigų plovimo ir teroristų finansavimo prevencijos įstatymas (Nr. VIII-275) reglamentavo tik depozitinių virtualių valiutų piniginių ir virtualių valiutų keityklos operatorių veiklą. Depozitinių virtualių valiutų piniginių operatoriai yra juridiniai asmenys, teikiantys paslaugas, susijusias su virtualių piniginių valdymu klientų vardu, o virtualių valiutų keityklų operatoriai – juridiniai asmenys, teikiantys mokamas paslaugas, susijusias su virtualios valiutos keitimu, pirkimu ar pardavimu (LR pinigų plovimo ir teroristų finansavimo prevencijos įstatymas, 1997). Kitų kriptoturto paslaugų teikėjų veikla Lietuvoje iki šiol nebuvo reglamentuojama. Tačiau MiCA reglamentas reiškia esminį pokytį – nuo 2024 m. gruodžio 30 d. kriptoturto paslaugų teikėjai bus reguliuojami ženkliai platesne apimtimi. Kriptoturto paslaugų sąvoka apims ne tik virtualių valiutų keityklas ir depozitinių piniginių operatorius, bet ir kitus susijusius paslaugų teikėjus, įpareigojant juos laikytis griežtų reguliavimo ir licencijavimo reikalavimų („MiCA reglamentas: ką turėtų žinoti Lietuvos kriptoturto paslaugų teikėjai“, 2024).

Apibendrinant galima teigti, kad globali pinigų plovimo prevencija įgyvendinama pasitelkiant priemonių, teisės aktų ir procedūrų visumą, kuri dar apibūdinama kaip AML (angl. anti-money laundering). AML kaip sistema apima politinį, teisinį ir finansinį komponentą. Vienas iš svarbiausių principų įgyvendinant AML praktiką yra finansinių institucijų taikomas KYC – kliento tapatybės nustatymas yra vienas pirmųjų žingsnių užtikrinant, kad finansinis sandoris vykdomas naudojant teisėtas lėšas. Daugelis finansinių institucijų, pvz., bankai ar kriptovaliutų biržos, yra įpareigotos vykdyti KYC. Plačiau finansinių institucijų įsipareigojimai dalyvaujant pinigų plovimo prevencijoje bus atskleisti kitame poskyryje.

1.3. Finansinių institucijų vidaus kontrolės mechanizmai ir nuotolinio tapatybės nustatymo reikšmė pinigų plovimo prevencijoje

Finansinių institucijų vidaus kontrolė apima įvairias strategijas, mechanizmus ir procedūras, kurias organizacijos taiko, siekdamos patikrinti savo finansinių ataskaitų pagrįstumą ir tikslumą (Musyoki, 2023). Patikima vidaus kontrolė padeda sumažinti klaidas, manipuliacijas ir sukčiavimą, taip ribojant nusikaltimų plitimą ir užtikrinant rinkos konkurencingumą (Malahim et al., 2023). Vidaus kontrolės stiprinimui skirtos kelios priemonės ir principai:

1. Pareigų atskyrimas – ši kontrolės priemonė užtikrina, kad nė vienas asmuo nekontroliuotų visų finansinės operacijos aspektų, todėl mažėja tikimybė, kad sukčiavimo atvejai liks nepastebėti.
2. Nepriklausomos kontrolės funkcijos – šias kontrolės priemones įgyvendina departamentai, veikiantys nepriklausomai nuo prižiūrimų departamentų ir užtikrinantys objektyvią priežiūrą.
3. Kelios gynybos linijos – kelių skirtingų atsakomybės sritį turinčių priežiūros ir kontrolės lygmenų derinimas, siekiant užtikrinti, kad problemos būtų užfiksuotos įvairiais lygmenimis, kol jos dar neišsiplėtė.
4. Atsakomybė ir atskaitomybė – aiškumas apibrėžiant atsakomybes ir atskaitomybes padeda užtikrinti, kad visi darbuotojai žinotų, ko iš jų tikimasi.
5. Struktūrizuotas karjeros kelias – aiškios karjeros galimybės gali motyvuoti darbuotojus laikytis etikos standartų ir įmonės politikos, nes jie žino, kad asmeninis augimas ir pažanga priklauso nuo sąžiningumo ir darbo rezultatų.
6. Organizacinė struktūra – kontrolės priemonės turi būti įtrauktos į organizacinę struktūrą. Taip sukuriama sistema palaikanti skaidrumą, efektyvumą ir įstatymų bei kitų teisės aktų laikymąsi.

7. Aktyvi priežiūra – vidaus kontrolė yra suprantama kaip bendra visos organizacijos atsakomybė. Reguliariai atliekami patikrinimai padeda ankstyvoje fazėje nustatyti ir šalinti pažeidžiamumo veiksnius. Vidaus auditai leidžia padaliniams nuolat vertinti, kaip jie laikosi kontrolės procedūrų, ir atlikti reikiamus pakeitimus.
8. Technologinė integracija – integruojant technologijas į vidaus kontrolę gerokai padidinimas kontrolės veiksmingumas ir efektyvumas. Technologijos pagerina informacijos apdorojimo savalaikiškumą ir tikslumą.
9. Valdymas ir komunikacija – akcentuojamas vadovybės vaidmuo struktūrizuojant minėtas kontrolės priemones per aiškią politiką ir procedūras. Siekiant veiksmingai įgyvendinti šias kontrolės priemones, svarbu užtikrinti darbuotojų informuotumą ir įtrauktį. Komunikacijos kanalai ir informacijos srautas stiprina finansinių institucijų gebėjimą kovoti su pinigų plovimu.

Pažymėtina, kad ne visi subjektai (finansų įstaigos), įgyvendinančios pinigų plovimo ir teroristų finansavimo prevencijos priemones, susiduria su vienoda rizika. Rizikos skirtumai kyla dėl klientų įvairovės, produktų, paslaugų, operacijų ypatumų bei šalių ar geografinių regionų rizikos. Įmonės, teikiančios buhalterinės apskaitos ar mokesčių konsultavimo paslaugas, įmonių steigimo bei administravimo paslaugų teikėjai, taip pat nekilnojamojo turto agentai, asmenys, užsiimantys ekonomine komercine veikla, įtraukiant prekybą turtu su grynaisiais pinigais, nėra licencijuojami ir jiems netaikomas registracijos (įtraukimo į sąrašą) režimas. Tai reiškia, kad kai kuriems nurodytas paslaugas teikiantiems subjektams yra privalomos numatytos veiklos priemonės, tačiau jie nepatenka į priežiūros institucijų akiratį (Finansinių nusikaltimų tyrimo tarnybos ataskaita, 2023).

Pasak Lienov ir kt. (2021), reaguojant į inovacijų teikiamas galimybes bankų sektoriui reikia laikytis atsargaus ir į ateitį orientuoto požiūrio. Siekiant integruoti pažangiausias skaitmenines inovacijas būtina išlaikyti subtilią pusiausvyrą tarp sandorių spartos ir geresnės prieigos prie finansinių paslaugų bei būtinybės užkardyti pinigų plovimo veiklą. Šią pusiausvyrą galima pasiekti kuriant strateginę sistemą, kurioje būtų naudojamos naujos technologijos, pvz., blokų grandinė. Kartu svarbu išlaikyti pamatinę bankininkystės praktiką, kuri ilgą laiką palaikė finansų sistemos vientisumą. Siekdamos įveikti iššūkius, kylančius dėl naujų pinigų plovimo galimybių, finansų įstaigos turi skirti daugiau išteklių savo atitikties pajėgumams stiprinti. Šis įsipareigojimas apima pažangių stebėsenos sprendimų diegimą, griežtą klientų tikrinimo procedūrų nustatymą ir partnerystės su finansines operacijas reguliuojančiomis institucijomis glaudinimą. Kruopščiai subalansuodami du tikslus – inovacijas ir saugumą – bankai gali užtikrinti, kad jų vykdoma skaitmeninė transformacija sustiprintų, o ne susilpnintų jų kovos su pinigų plovimu protokolus.

Ypač svarbus žingsnis užkertant kelią skaitmeniniam nusikalstamumui – efektyvus, patikimas ir saugus naujų klientų įvedimo (angl. *onboarding*) procesas. Šis procesas yra jau minėtos kovoje su

pinigų prevencija finansinėms institucijoms tenkančios prievolės pažinti savo klientą (KYC) dalis. Vykdant naujų klientų įvedimą yra siekiama užtikrinti, kad finansinės paslaugos būtų prieinamos tik teisėtai jomis pasinaudoti ketinantiems asmenims. Klientų įvedimo procesas prasideda nuo registracijos ir asmens tapatybės nustatymo (Gumus ir Cekerekli, 2024). Kai teikiamos nuotolinės finansinės paslaugos, reikalingi nuotolinio tapatybės nustatymo metodai. Būdai, kuriais finansinės institucijos gali identifikuoti vartotojo asmens tapatybę, yra griežtai reglamentuojami. Remiantis Štitiliu ir kt. (2011), teoriškai asmens autentiškumo patvirtinimas elektroninėje erdvėje gali būti atliekamas taikant vieną ar daugiau iš šių principų: 1) žinojimo (tai, ką vartotojas žino, pvz., slaptažodis); 2) turėjimo (tai, ką vartotojas turi, pvz., e. parašas); 3) būdingumo (tai, kas vartotojui būdinga, t. y., biometriniai duomenys). Finansinių institucijų veikloje žinojimo principo nepakanka, todėl yra taikomi turėjimo arba būdingumo principai.

Pastebima, kad iki 2016 m. Lietuvoje galiojo itin griežtas nuotolinio tapatybės nustatymo reglamentavimas pripažįstant tik asmens dokumentus (ar tinkamas jų kopijas), gaunamus iš trečiųjų asmenų, kol buvo konstatuota, kad griežta teisinė bazė neatitinka šiuolaikinės skaitmenizuotos verslo aplinkos poreikių. Nuotolinio tapatybės nustatymo ribojimai lėmė verslo vėlavimo ir neveiksnumo problemas, todėl buvo įteisinti nauji nuotolinio tapatybės nustatymo būdai. Nuotolinio tapatybės nustatymo reglamentavimas remiasi dviem kertiniais Europos Parlamento ir Tarybos direktyvoje 2014/92/ES įtvirtintais principais. Visų pirma, tapatybės nustatymo reguliavimas turi būti proporcingas pinigų plovimo rizikai. Antra, taikomos reguliavimo priemonės negali diskriminuoti teisėtai ES gyvenančių vartotojų, kai tie vartotojai prašo ES atidaryti mokėjimo sąskaitą arba ja naudojasi. 2016 m. spalio 26 d. Lietuvos Respublikos Vyriausybė įteisino šiuos naujus nuotolinio asmens tapatybės identifikavimo būdus: a) kvalifikuotas elektroninis parašas; b) ES išduotos aukšto arba pakankamo saugumo elektroninės atpažinties priemonės, c) tiesioginio vaizdo perdavimas. Taigi, iš viso Lietuvos atsirado penkios nuotolinio asmens tapatybės identifikavimo galimybės.

Skirtingi nuotolinio tapatybės nustatymo būdai gali būti charakterizuojami išskiriant tris kriterijus – tikslumo, saugumo ir prieinamumo. Taip pat svarbu atsižvelgti į tris taikymo aspektus – esamą paplitimą, taikymo problemas ir plėtros tendencijas. 2019 m. Mokėjimų Tarybos iniciatyva buvo atlikta galimybių studija, kuri apėmė visų reglamentuotų nuotolinio tapatybės nustatymo priemonių lyginamąją analizę atskleidžiant jų privalumus ir trūkumus („Naujų tapatybės patvirtinimo priemonių galimybių galimybių ir atitikties pinigų plovimo prevencijos tikslams problematika“, 2019):

- **Tiesioginio vaizdo perdavimas** – pagrindiniai šios priemonės privalumai yra susiję su tapatybės nustatymo kaštais ir pasiekiamumu. Taikydamos šią priemonę finansinės institucijos patiria mažiau sąnaudų, procesas gali būti pilnai automatizuotas. Be to, yra galimybė lengviau pasiekti užsienio klientus. Ši tapatybės nustatymo priemonė yra patraukli

vartotojams, todėl padeda sukurti gerą vartotojo patirtį. Tiesioginio vaizdo perdavimo kaip priemonės trūkumai yra susiję su saugumo aspektais – paslaugų teikėjai nėra sertifikuoti, stokojama priemonių patikimumo kontrolei.

- **El. parašas** – ši nuotolinio tapatybės patvirtinimo priemonė turi pranašumą būtent saugumo ir patikimumo srityje. E. parašams būdingas aukštas saugumo ir informacijos tikslumo lygis, taikymo reglamentavimas bei kontrolė, sertifikuotų paslaugos teikėjų veikimas. Be to, finansų įstaigos patiria sąlyginai mažai sąnaudų, nes tapatybės duomenis renka patikimumo užtikrinimo paslaugų teikėjai. Nepaisant šių privalumų e. parašai neįgijo masinio populiarumo, pasigendama šiai priemonei skirto viešinimo. E. parašų populiarumą galimai riboja tai, jog tai yra paslauga, už kurią tiesiogiai moka vartotojas. Taip pat trūksta techninių galimybių pasiekti užsienio klientus.
- **Pervedimas ir dokumentas** – tapatybės nustatymo priemonė, kuri nereikalauja specialių techninių priemonių, tačiau išlieka poreikis atlikti fizinio kontakto reikalaujančią procedūrą sudarant ir pateikiant tinkamą kopiją. Taip pat nėra galimybės valdyti riziką, kuri gali kilti dėl netinkamo tapatybės nustatymo kredito įstaigoje, iš kurios gautas mokėjimo pavedimas.
- **Trečiosios šalys** – priemonė pasižymi patogumu klientams, kadangi nėra poreikio papildomų klausimynų pildymui ir dokumentų pateikimui. Kartu tai yra priemonė, kuri leidžia finansų įstaigoms sumažinti duomenų ir dokumentų tikrinimo bei valdymo sąnaudas. Tačiau ši priemonė taip pat turi nemažai reikšmingų trūkumų. Pirmiausiai nėra patikimo trečiųjų šalių sąrašo, taip pat trūksta standartizuotos aplikacijų programavimo sąsajos. Antra, Lietuvos rinka yra per maža, kad užsienio šalyje veikiančios trečiosios šalys būtų suinteresuotos adaptuotis prie Lietuvos teisės normų. Be to, šių paslaugų kaina gali būti ekonomiškai nepagrįsta.
- **Elektroninė atpažintis** – priemonė, kuri pasižymi potencialiai aukštu saugumo ir informacijos tikslumo lygiu. Šios paslaugos teikimą reglamentuoja ir prižiūri atitinkamos institucijos. Be to, paslaugas teikia sertifikuoti paslaugų teikėjai (jei veikiama pagal eIDAS). Kadangi paslaugas taip pat teikia sertifikuotas paslaugų teikėjas, finansinės institucijos patiria mažiau su duomenų tikrinimu ir valdymu susijusių sąnaudų. Vis dėlto kol kas šių priemonių paplitimas taip pat išlieka žemas, trūksta verslo ir techninių galimybių pasiekti užsienio klientus. Be to, kai kurios e. atpažinties paslaugos yra mokamos ir reikalauja papildomos techninės įrangos (skaitytuvo). Taip pat pažymėtina, kad yra reikalingas bent vienas fizinis kontaktas, kai pasirašoma sutartis ir suteikiami personalizuoti saugumo požymiai.

Apibendrinant galimybių studijos rezultatus galima teigti, kad didžiausiu saugumo lygiu pasižymi e. pašto ir e. atpažinties priemonės. Nesaugiausios priemonės – mokėjimo pavedimas ir vaizdo perdavimo priemonės. Kartu vaizdo perdavimo priemonės laikomos mažiausiai tiksliomis. Vis dėlto būtent vaizdo perdavimo priemonės buvo įvardintos kaip populiariausios ir pasižyminčios

didžiausiu plėtros potencialu. Mažiausiai prieinama ir populiari priemonė – trečiųjų šalių informacija. Todėl daroma išvada, kad labiausiai prieinamos yra priemonės, kurios pasižymi automatizacija ir nereikalauja specialios įrangos. Tai skatina manyti, kad nuotolinio tapatybės nustatymo srityje prioritetas teikiamas paprastumui ir gerai vartotojo patirčiai, kuri lemia konkurencinį finansinės įstaigos pranašumą. Kaip pastebima galimybių studijoje skaitmeninimas yra finansinių institucijų konkuravimo strategija, todėl vadybiniu požiūriu šioms institucijoms svarbu taikyti nuotolinio tapatybės identifikavimo priemones, kurios tenkina vartotojų interesus ir užtikrina konkurencingumą rinkoje. Čia vėlgi susiduriama su Malahim (2023) pastebėjimu, jog finansinės įstaigos paprastai yra privataus sektoriaus subjektai, todėl konkurencinis pranašumas ir tapatybės nustatymo kaštai yra svarbesnis prioritetas nei procedūros saugumas ir tikslumas.

Tiek mokslinėje literatūroje, tiek viešajame diskurse pripažįstama, kad pinigų plovimas tebėra plačiai paplitusi finansų sektoriaus problema (Malahim et al., 2023). Išanalizavus literatūrą išskiriami šie finansinių institucijų įsipareigojimus kovoje su pinigų plovimu silpninantys ribotumai:

1. vidaus kontrolės statiškumas;
2. priklausomybė nuo rankinio duomenų apdorojimo;
3. išteklių trūkumas;
4. nepakankamas vadovybės įsipareigojimas vykdyti AML;
5. darbuotojų šališkumas;
6. rekomendacijų trūkumas.

Vidaus kontrolės sistemų statiškumas. Finansų įstaigų prevencinės veiklos skyriai jau taiko taisyklėmis pagrįstas sistemas, skirtas aptikti įtartinas bankines operacijas, kurioms būdingi pinigų plovimo požymiai. Šiame kontekste taisyklė – tai iš anksto nustatytas sąlygų rinkinys, kurį įvykdžius įspėjama, kad sandoris gali būti įtartinas. Kiekviena taisyklė atspindi įvairius kriterijus apimantį rizikos profilį. Tačiau vienas iš esminių šių taisyklėmis grindžiamų sistemų trūkumų yra jų statiškumas. Kartą nustatytos taisyklės dažnai ilgą laiką lieka nepakitusios, net jei nusikaltėliai prisitaiko ir atranda veiksmų seką, kaip apeiti tokias kontrolės priemones. Statiškomis taisyklėmis pagrįsta sistema gali greitai pasekti ir tapti neveiksminga. Mažėjant sistemos efektyvumui gali būti daug klaidingai teigiamų atvejų, kai įprastos, teisėtos operacijos pažymimos kaip įtartinos, ir klaidingai neigiamų atvejų, kai tikroji neteisėta veikla lieka nepastebėta (Rocha-Salazar ir Segovia-Vargas, 2024). Siekiant užtikrinti, kad kontrolės sistemos efektyviai pasiektų numatytus tikslus, būtina nuolatinė jų stebėsena ir atnaujinimas (Aminat, Ezekiel ir Obafemi, 2023). Kai stebėsenos mechanizmai yra silpni arba nepakankami, tampa lengviau nepastebėtai vykdyti sukčiavimo veiklą. Abei (2021) teigimu, finansinės institucijos nesugeba reguliariai atnaujinti savo vidaus kontrolės sistemų ir todėl atsiranda pažeidžiamų vietų, kuriomis gali pasinaudoti sukčiai. Pastebėtina, kad nusikaltėliams nėra sudėtinga apčiuopti finansinių institucijų vidaus kontrolės trūkumus. Visuomenės

spaudimas paskatino bankus skaidrinti kovos su pinigų plovimu strategijas. Nors šis skaidrumo siekis padeda geriau formuoti politiką, kartu atskleidžiami galimi bankų apsaugos mechanizmų trūkumai, o ši informacija gali būti naudinga ir nusikaltėliams (Lannoo ir Parlour, 2021).

Priklausomybė nuo rankinio duomenų apdorojimo. Abei (2021), pasiremdamas Baker et al. (2017) tyrimu, kuriame buvo nagrinėjami vidaus kontrolės trūkumai didelio Prancūzijos banko „Société Générale“ prekybos sistemose, pažymėjo, kad dėl pernelyg didelio pasitikėjimo rankiniu duomenų apdorojimu, kurį atlieka pagalbinių tarnybų darbuotojai, atsiranda kontrolės trūkumas, įskaitant vadovų aplaidumą atliekant operatyvinius patikrinimus, neefektyvų bendravimą, nepakankamą sukčiavimo rizikos suvokimą ir netinkamą priežiūrą – visa tai sudaro dideles galimybes sukčiauti.

Kartu pastebėtina, kad bankų vidaus kontrolės sistemos yra ganėtinai sudėtingos, todėl jas kuriant ir prižiūrint gali atsirasti klaidų. Šios klaidos gali sutrikdyti vidaus kontrolę ir suteikti dar daugiau sukčiavimo galimybių (Aminat, Ezekiel ir Obafemi, 2023).

Išteklių trūkumas. AML praktikų įgyvendinimas yra nemažai finansinių ir žmogiškųjų išteklių reikalaujantis procesas (FATF, 2021). FATF (2019) ataskaitoje nurodoma, kad nepakankamas biudžetas ir nepakankamas darbuotojų skaičius gali trukdyti vidaus auditoriams atlikti išsamų pinigų plovimo ir (arba) teroristų finansavimo kontrolės auditą arba vykdyti tolesnius auditus, kad būtų patikrintas taisomųjų priemonių įgyvendinimas. Iš dalies dėl išteklių trūkumo pastebimas nepakankamas vidaus audito ir kitų finansų įstaigų skyrių bendradarbiavimas. Dėl nepakankamo vidaus audito bei kitų organizacijos skyrių veiklos koordinavimo gali lemti fragmentišką ir nepakankamai integruotą požiūrį į pinigų plovimą ir (arba) teroristų finansavimo kontrolę. Esant tokiai situacijai, skirtingi padaliniai gali veikti skirtingai, o tai sumažina bendrą kontrolės priemonių efektyvumą. Toks komunikacijos lygis gali ne tik apsunkinti problemų identifikavimą ir sprendimų priėmimą, bet ir padidinti riziką, kad svarbūs veiksniai bus ignoruojami ar tinkamai neįvertinti. Vadovybės spaudimą arba interesų konfliktus patiriantiems vidaus auditoriams gali būti sunku užtikrinti savo nešališkumą vertinant pinigų plovimo kontrolės priemones (Akinteye et al., 2023). Taip pat Akinteye (2023) nurodo, kad vidaus auditoriams dažnai trūksta specialių žinių ir specifinių įgūdžių, reikalingų veiksmingai nustatyti pinigų plovimo riziką ir trūkumus. Šis kompetencijos trūkumas gali sumažinti vidaus audito poveikį pinigų plovimo kontrolės tobulinimui.

Pastebėtina, kad senų technologijų pakeitimas naujomis reikalauja didesnių investicijų. Ypač mažesnėms finansų įstaigoms dažnai trūksta vidinių išteklių ar gebėjimų įvertinti naujų technologijų tinkamumą, todėl tampa sunku nustatyti, ar jos atitinka įstaigos rizikos profilį, klientų bazę ir verslo operacijas, arba veiksmingai įgyvendinti ir valdyti šiuos naujus sprendimus (FATF, 2021). Be to, pastebėtina, kad dėl nepakankamo koordinavimo AML technologijų srityje sudėtinga diegti technologijas plačiu mastu, todėl yra slopinamas jų ekonominis efektyvumas. Neturint galimybės

didinti mastą, tam tikrų technologijų atnaujinimas gali būti ekonomiškai neperspektyvus (FATF, 2021).

Nepakankamas vadovybės įsipareigojimas įgyvendinti AML. Pažymėtina, kad bankai yra įdiegę mokėjimo operacijų stebėsenos sistemas, tačiau kai kurie iš jų atlieka tik paviršutinišką lėšų kilmės šaltinio patikrinimą, remdamiesi vien kliento pateiktais atsakymais, t. y., jie nesireikalauja jokių papildomų dokumentų, patvirtinančių lėšų šaltinį. Bankai naudoja mokėjimo operacijų stebėsenos sistemas, kurios dažnai remiasi bendraisiais nustatymais, pvz., pervedimo sumos limitais. Taip stebėsenos sistemose atsiranda daug klaidingų signalų (angl. *false positives*). Veikdami SEPA ir SWIFT sistemose bankai nėra priversti patikrinti, ar lėšų gavėjo vardas atitinka sąskaitos numerį, todėl nusikaltėliams leidžiama manipuliuoti šia informacija. Taip nusikaltėliai išvengia tikrosios gavėjo identifikacijos ir tarptautinių finansinių sankcijų. Be to, finansinėms institucijoms yra sudėtinga patikrinti nerezidentų naudos gavėjus, remiantis patikimais ir nepriklausomais šaltiniais, o nerezidentai sudaro apie 3,5 proc. visų banko klientų (Finansinių nusikaltimų tyrimo tarnyba, 2020). Taip pat pastebima, kad kai kurie bankai atnaujina mažos rizikos klientų KYC informaciją tik kartą per metus arba dar rečiau, per tą laiką neatliekant jokių automatinės patikros procedūrų, pvz., ar naudos gavėjas išliko tas pats. Tokia praktika suteikia galimybę nusikaltėliams naudotis banko sąskaita bent jau metus, kol bus atnaujinta KYC informacija (Finansinių nusikaltimų tyrimo tarnyba, 2020).

Galima teigti, kad AML teisinis reguliavimas atspindi tik minimalias finansinių institucijų prievoles, tačiau praktiniame lygmenyje institucijų įsitraukimas į pinigų plovimo prevencija priklauso nuo vadybos įsipareigojimo taikyti griežtas KYC ir kitas prevencines praktikas. Iš viso galima išskirti tris problemas, kurios kyla, kai finansinėse institucijose stokojama įsipareigojimo AML įgyvendinimui – paviršutiniškas lėšų kilmės patikrinimas, atitikties tarp sąskaitos numerio ir gavėjo tapatybės tikrinimo stoka, retas KYC informacijos atnaujinimas. Aminat, Ezekiel ir Obafemi (2023) taip pat pastebi, kad finansinių institucijų vidaus kontrolės procesai neretai pasižymi nestabilumu, kuris leidžia klestėti sukčiams ir daro žalą bankų sektoriui. Šių kontrolės priemonių veiksmingumas priklauso nuo kontrolės aplinkos patikimumo, kuris apima ir vadovybės įsipareigojimą laikytis griežtų standartų.

Darbuotojų šališkumas. Aminat, Ezekiel ir Obafemi (2023) teigimu, įvairiose šalyse daugėja kontrolės priemonių pažeidimų ir manipuliacijų finansiniais dokumentais, siekiant asmeninės naudos. Šališki apskaitos pareigūnai, vedami godumo ir asmeninių interesų, gali klastoti sandorius. Todėl prieš patikint darbuotojams itin svarbias pareigas reikalinga atidžiai patikrinti vidaus kontrolės skyrių pareigūnus (Musyoki, 2023). Abei (2021) akcentuoja, kad darbuotojai labiau linkę racionalizuoti sukčiavimą, kai jaučia, kad su jais darbe elgiamasi neteisingai, todėl sąžiningumo palaikymas ir

vertybių skatinimas kontrolės aplinkoje gali gerokai sumažinti netinkamo darbuotojų elgesio ir nesąžiningo veikimo riziką.

Rekomendacijų trūkumas. Viena iš objektyvių priežasčių lemiančių finansinėms institucijų vykdomos pinigų plovimo prevencijos ribotumus yra rekomendacijų trūkumas, kaip identifikuoti fiktyvias įmones ar paslaugas. Finansinės institucijos kyla iššūkis neatsilikti nuo besikeičiančių kovos su pinigų plovimu ir teroristų finansavimu taisyklių ir kontrolės priemonių. Finansų įstaigoms sudėtinga nuolat susipažinti su naujais rizikos veiksniais ar konkretaus sektoriaus problemomis, todėl jie gali nepastebėti kylančių grėsmių (Akinteye et al., 2023).

Apibendrinant galima teigti, finansinių institucijų vidaus kontrolės mechanizmai yra būtini siekiant sustabdyti pinigų plovimą. Yra sukurta ir taikoma daug įvairių į pinigų plovimo prevenciją orientuotų vidaus kontrolės principų bei priemonių, tačiau praktinį jų įgyvendinimą riboja statiškumas, žmogiškųjų ir finansinių išteklių stoka, priklausomybė nuo rankinio duomenų apdorojimo, nepakankamas vadovybės įsipareigojimas įgyvendinti AML, darbuotojų šališkumas, rekomendacijų trūkumas. Visos privačiame sektoriuje veikiančios finansinės institucijos siekia pelno, todėl vadybiniu požiūriu teikiamas prioritetas vartotojų patirčiai ir konkurencingumui, taip pat ir nuotolinio klientų tapatybės nustatymo srityje. Galima manyti, kad perspektyviausia laikoma tapatybės nustatymo priemonė, kuri yra patogiausia ir prieinamiausia vartotojams, t. y., tiesioginis vaizdo perdavimas, nors tai būtent ši priemonė pasižymi mažiausiu saugumo ir tikslumo lygiu. Visa tai suponuoja, kad finansinės institucijoms reikalingos priemonės, kurios dar labiau pagerintų duomenų saugumo, tikslumo ir ekonominio efektyvumo kriterijus.

1.4. Tarptautinio bendradarbiavimo reikšmė pinigų plovimo prevencijoje

Vienas iš svarbiausių pinigų plovimo skaitmenizacijos kontekste aspektų – šių nusikaltimų globalumas. Išnaudojant globalų interneto tinkle ir skaitmeninių finansų privalumus finansiniai sandoriai neretai peržengia valstybių sienas. Teisinių sistemų skirtumai įvairiose šalyse sudaro galimybes pasinaudoti teisinėmis spragomis. Teisinių sistemų ir reguliavimo procedūrų skirtumai leidžia nusikaltėliams lengviau perkelti lėšas į šalis, kurioms būdingas silpnesnis finansinių operacijų reguliavimas. Nusikaltėliai naudojasi biurokratiniais susikirtimais, valstybių suvereniteto apsauga ir visišku valstybių nepajėgumu, įskaitant korumpuotą ar silpną teisėsaugos sistemą, politinės valios nebuvimą. Pati suvereniteto sąvoka ir valstybės savarankiškumas užtikrinant įstatymų vykdymą kelia sunkumų kovojant su tarptautiniu nusikalstamumu. Šie iššūkiai reikalauja koordinuoto, savalaikio ir veiksmingo atsako, kuris reikalauja stiprinti tarptautinio bendradarbiavimo sistemas (Iftikhar ir Iqbal, 2021). Todėl tikslinga atskirai aptarti tarptautinio bendradarbiavimo reikšmę pinigų plovimo prevencijoje.

Pinigų plovimas skaitmeniniame amžiuje dažnai susijęs su tarpvalstybiniais elementais, kuriems naudingas tarptautinio bendradarbiavimo ir nenuoseklus reglamentavimo trūkumas. Reaguojant į minėtas pinigų plovimo globalumo problemas, pabrėžiama pasaulinio bendradarbiavimo būtinybė. Užuot izoliavus valstybes, kad jos spręstų nusikaltėlių padarytus nusikaltimus lokaliai, t. y., savo teritorijoje, naujos įvairių vyriausybinių subjektų bendradarbiavimo galimybės, palengvina kovą su tarptautiniu nusikalstamumu, nes sustiprinamas jo išaiškinimas, prevencija ir baudžiamasis persekiojimas. Tačiau jurisdikciniai skirtumai ir reguliavimo standartų trūkumas tampa kliūtimi veiksmingam tarptautinių teisėsaugos ir reguliavimo institucijų bendradarbiavimui ir koordinavimui. Dėl to gali būti sunku atsekti neteisėtų lėšų srautus ir imtis vieningų tarptautinių veiksmų prieš pinigų plovimo veiklą (Subbagari, 2023). Pasak Kao ir kt. (2023), nors tarptautiniai kovos su terorizmu ir terorizmo finansavimu teisiniai dokumentai yra plačiai ratifikuoti, tarp jų nuostatų ir praktinio įgyvendinimo šalies viduje dažnai egzistuoja didelis atotrūkis.

Terminas "tarptautinis bendradarbiavimas" baudžiamosios justicijos srityje paprastai apima savitarpio teisinę pagalbą ir ekstradiciją – pagrindinės priemones, padedančias įveikti tarptautinio nusikalstamumo keliamas kliūtis. Kartu bendradarbiaujančios šalys vykdo įvairius susitarimus, kurie leidžia keistis informacija apie nusikalstamą veiklą (Iftikhar ir Iqbal, 2021). Tarptautinio bendradarbiavimo aspektai apima sąveiką, tiesiogiai susijusią su teisiniais procesais arba neteisiniais bendradarbiavimo aspektais, įskaitant keitimąsi informacija tarp įvairių kompetentingų institucijų. *Keitimasis informacija* yra labai svarbus nustatant ir sekant neteisėtą finansinę veiklą, renkant duomenis ir rengiantis galimiems teisiniams veiksmams ar politikos formavimui. Tuo tarpu teisminis bendradarbiavimas yra susijęs su keitimusi informacija arba įrodymų rinkimu specialiai teisminiam nagrinėjimui. Teisminis bendradarbiavimas apima tokius procesus kaip savitarpio teisinė pagalba ir ekstradicijos prašymai, t. y., oficialūs procesai, kai viena šalis prašo kitos šalies padėti tirti nusikalstamas veikas arba vykdyti baudžiamąjį persekiojimą. Teisminis bendradarbiavimas būtinas nagrinėjant tarptautines sienas peržengiančius nusikaltimus, nes jame dalyvauja skirtingų jurisdikcijų teisiniai subjektai. Struktūriniai klausimai turi būti sprendžiami taip, kad atitiktų kiekvienos jurisdikcijos oficialius įsipareigojimus (Kao et al., 2023).

Kovoje su terorizmo finansavimu dalyvauja platus institucijų spektras – įskaitant muitines, žvalgybos tarnybas, priežiūros institucijas (Finansinių nusikaltimų tyrimo tarnybos, antstolių rūmai, prabavimo rūmai, Lošimų priežiūros tarnyba ir kt.) bei teismų sistemas (Finansinių nusikaltimų tyrimo tarnyba, 2020). Kiekviena jurisdikcija gali būti veikti pagal savitus procedūrinius ypatumus, kurie daro įtaką bendradarbiavimo pobūdžiui (Kao et al., 2023). Įvairiose jurisdikcijose skiriasi kovos su pinigų plovimu taisyklės, todėl pasaulinė reguliavimo aplinka yra fragmentiška. Kaip jau minėta, dėl suderintų kovos su pinigų plovimu standartų trūkumo nusikaltėliai gali pasinaudoti reguliavimo spragomis ir lengviau pervesti lėšas per jurisdikcijas, kuriose galioja silpnesni įstatymai arba ne taip

griežtai įgyvendinami įstatymai (Subbagari, 2023). Dabartinės kovos su pinigų plovimu taisyklės yra pernelyg plačios ir nepakankamai konkrečios, kad būtų veiksmingos tarp skirtingų jurisdikcijų. Toks bendrumas gali sumažinti jų veiksmingumą, todėl reikalingas universalus požiūris, kuris leistų atsižvelgti į unikalius kiekvienos šalies aspektus ir palengvintų visapusišką valstybių bendradarbiavimą užkardant pinigų plovimą (Svensson, 2021).

Steblianko ir kt. (2020) akcentuoja, kad šalys, kuriose kovos su pinigų plovimu priemonės yra nepakankamos, yra ypač pažeidžiamos, o jų pažeidžiamumas labiau didina pasaulio ekonominį nesaugumą. Naujų technologijų, tokių kaip kriptovaliutos, atsiradimas dar labiau apsunkino neteisėtų lėšų sekimą, todėl vis sunkiau veiksmingai kovoti su šia nusikalstama veikla. Pastebimas poreikis stiprinti tarptautinį bendradarbiavimą pinigų plovimo prevencijos srityje. Anot Silvana (2021), stokojant tarptautinio bendradarbiavimo ir neužkardanti globalaus pinigų plovimo yra skatinamas organizuotas nusikalstamumas ir didinama terorizmo grėsmė. Atsižvelgiant į tai, kad pinigų plovimas peržengia tarptautines ribas, pasinaudojant nacionalinių teisinių sistemų trūkumais, tarptautiniuose susitarimuose ir konvencijose pabrėžiama būtinybė sudaryti kolektyvines teisines ir procedūrines sistemas. Šios sistemos yra orientuotos į pinigų plovimo praktikos kriminalizavimą, savitarpio teisinę pagalbą ir laikinųjų priemonių, tokių kaip turto įšaldymas, priėmimą.

Išanalizavus literatūrą galima išskirti kelis vyraujančius tarptautinio bendradarbiavimo pinigų plovimo prevencijoje ribotumus:

- **Pasitikėjimo tarp valstybių trūkumas.** Nepasitikėjimas gali kilti dėl įvairių priežasčių – teisinės valstybės požymių trūkumo, korupcijos, valstybės užvaldymo, politinio nestabilumo, žmogaus teisių problemų, nesaugius ryšių kanalus, netinkamos konfidencialios ar neskelbtinos informacijos apsaugos (Iftikhar ir Iqbal, 2021). Stokojant pasitikėjimo šalys ar agentūros gali nesiryžti dalytis svarbia informacija su savo partneriais.
- **Pernelyg griežtas dvigubo nusikalstamumo principo taikymas.** Pagal šį principą reikalaujama, kad įtariama nusikalstama veika būtų laikoma nusikalstama ir prašančiojoje, ir prašomojoje valstybėje. Nors šis principas yra labai svarbus tarptautinėje baudžiamojoje teisėje, įskaitant ekstradiciją, jo griežtumas gali sulėtinti procedūras, kurios nėra tiesiogiai susijusios su priverstinėmis teisinėmis priemonėmis, trukdyti greitesniam procedūrų vykdymui ir kelti grėsmę teisminiams procesams (Iftikhar ir Iqbal, 2021).
- **Išteklių ir informuotumo trūkumas.** Daugelyje šalių trūksta kovai su pinigų plovimu reikalingų išteklių, pvz., aukštos kvalifikacijos darbuotojų ir informacijos valdymo sistemų. Šis trūkumas daro didelę įtaką valstybės galimybėms reaguoti į pagalbos prašymus ir aktyviai ieškoti informacijos tarptautinio teroristų finansavimo bylose. Be to, neretai teisėsaugos institucijos apskritai yra nepakankamai informuotos apie tarptautinę pagalbą ir neteikia jai prioriteto, nes vengia ilgai trunkančių teisinių procesų. Specializuoti darbuotojai galėtų spręsti

šias problemas, skatindami naudotis turimomis bendradarbiavimo priemonėmis ir kanalais (Kao et al., 2023).

- **Politinis nestabilumas ir silpna teisinė aplinka**. Pasak Kao ir kt. (2023), patirtis patvirtina, kad teroristų ir nusikaltėlių ryšiai stipriausi yra būtent nestabiliose ir konfliktų paveiktose valstybėse. Konfliktai lemia valdymo trūkumus – sukuria aplinką, kurioje teisinė valstybė yra silpna, todėl sudaromos idealios sąlygos nusikalstamai ir teroristinei veiklai susilieti.

Apibendrinant galima teigti, kad skaitmeniniai sandoriai dažnai peržengia nacionalines sienas, todėl apsunkina neteisėtų lėšų srautų sekimą, kadangi stokojama jurisdikcijų ir reguliavimo standartų ir tarptautinio bendradarbiavimo. Teisinių sistemų ir reguliavimo procedūrų skirtumai leidžia nusikaltėliams lengviau perkelti lėšas į šalis, kurioms būdingas silpnesnis finansinių operacijų reguliavimas. Tarptautinį bendradarbiavimą kovoje su pinigų plovimu riboja pasitikėjimo, išteklių ir informuotumo, politinės valios tarp šalių trūkumas. Egzistuoja sudėtinga teisinė pagalba ir ekstradicijos procesai, kurie kartais sulėtina arba trukdo operatyviems veiksmams.

2. EUROPOS SĄJUNGOS SKAITMENINĖS TAPATYBĖS DĖKLĖS GALIMAS VAIDMUO PINIGŲ PLOVIMO PREVENCIJOJE. SIŪLOMI SPRENDIMAI

Šioje darbo dalyje aptariami teisiniai aspektai, susiję su skaitmeninės tapatybės įteisinimu ir reguliavimu, apžvelgiant pakeitimus, kurie įvyko įsigaliojus atnaujintai eIDAS reglamento redakcijai. Europos Parlamento ir Tarybos reglamento 2024/1183, kuriuo iš dalies keičiamas Reglamentas Nr. 910/2014. Taip pat nagrinėjamas elektroninės atpažinties, skaitmeninis asmens tapatybę patvirtinantis dokumentas (Asmens identifikavimo duomenys, angl., PID), t. y., trečias visoje ES įteisintas tapatybės įrodymo dokumentas, papildantis asmens pasą ir asmens tapatybės kortelę. Išskirtinis dėmesys bus skiriamas STD ir su ja susijusiai ekosistemai, bei šių inovacijų taikymo galimybėms pinigų plovimo prevencijoje.

2.1. Skaitmeninės Tapatybės Dėklės teisinė reguliacinė aplinka

Nauja Europos skaitmeninės tapatybės sistema papildo 2014 m. liepos 23 d. Europos Parlamento ir Tarybos reglamento Nr. 910/2014 versiją, kuri reglamentavo elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugas ES vidaus rinkoje. Šios sistemos atsiradimą lėmė skaitmeninių paslaugų, DI pagrindu sukurtų paslaugų poreikio augimas bei didėjančios kibernetinės grėsmės.

Siekiant sukurti ES skaitmeninės tapatybės ekosistemą 2024 m. balandžio 30 d. Europos Parlamento ir Tarybos priimtas reglamentas, kuriuo iš dalies pakeičiamas 2014 m. reglamentas (ES) Nr. 910/2014. Šiame reglamente pripažįstama didėjanti vartotojų svarba suteikiant jiems daugiau galimybių valdyti savo asmens duomenis, neteikti perteklinės informacijos ir naudotis skaitmeninėmis paslaugomis. Reglamentas nustato teisinį pagrindą ir sąlygas, kuriais remiantis asmenys ir organizacijos įgalinti naudotis sukurtomis skaitmeninėmis tapatybėmis visose ES valstybėse narėse. Pagal šią reglamento (Nr. 2024/1183) versiją pagrindinis tikslas išlieka, užtikrinti naudotojui visišką mobilią, saugią ir patogią skaitmeninę aplinką – Europos Skaitmeninės Tapatybės Dėklę (toliau – STD). Remiantis reglamentu (Nr. 2024/1183), STD – tai elektroninė priemonė, leidžianti saugiai laikyti ir valdyti asmens tapatybės duomenis (angl. PID), taip pat ir elektroninius požymių liudijimus (angl. *electronic attestation of attributes*), kad galėtų juos pateikti pasikliaujančioms šalims (angl. *relying party*).

Atnaujintoje reglamento (Nr. 2024/1183) versijoje teigiama, kad asmenys yra įgalinami būti atsakingais už savo tapatybės atskleidimą internete, kartu užtikrinant jiems saugią prieigą prie viešųjų, privačių ir tarpvalstybinių skaitmeninių paslaugų. Kartu su reglamentu panaikinamos

administracinės ir institucinės kliūtys, apsunkinančios piliečių galimybę naudotis viešosiomis paslaugomis internetu (Sjöholm, 2023). Reglamento tikslas – reglamentuoti ir įtvirtinti STD, kurioje vartotojai galėtų talpinti asmeninius duomenis ir taip geriau kontroliuoti jų atskleidimą. Dėklėje esantys asmeniniai duomenys gali būti naudojami ir tarpvalstybiniu mastu, tokiais tikslais kaip naudojimasis viešosiomis paslaugomis, medicinos paslaugomis, adreso pakeitimui, banko sąskaitos atidarymui, deklaruojant mokesčius, amžiaus patvirtinimui ar skaitmeninio vairuotojo pažymėjimo išdavimui bei naudojimui. Naudodamasis šia priemone asmuo turės galimybę patvirtinti savo tapatybę internetu arba net neprisijungęs prie interneto, pateikti reikalingą informaciją viešosioms ar privačioms paslaugoms gauti. STD, turėtų palengvinti vienkartinio duomenų pateikimo principo įgyvendinimą, taip sumažinant administracinę naštą bei skatinant tarpvalstybinį Europos Sąjungos piliečių, gyventojų ir įmonių mobilumą visoje Sąjungoje, taip pat prisidėti prie sąveikių e. valdžios paslaugų plėtos visoje bendrijoje.

Europos Parlamento ir Tarybos Reglamentas (Nr. 910/2014 su papildyta reglamento versija Nr. 2024/1183), nustatė bendras taisykles dėl elektroninės atpažinties ir pasitikėjimo paslaugų, siekiant užtikrinti saugią ir efektyvią elektroninę sąveiką tarp piliečių, verslo ir valdžios institucijų visoje ES. Naujoji reglamento (Nr. 910/2014) versija papildo reglamentą valstybėms skirtu įpareigojimu išleisti bent vieną oficialią skaitmeninę dėklę, kurioje būtų naujasis asmens tapatybę patvirtinantis dokumentas, galimas susieti su kitais skaitmeniniais asmens dokumentais (pvz., vairuotojo pažymėjimu, profesiniu kvalifikacijos pažymėjimu, socialinio draudimo pažymėjimu ar banko sąskaita). Naudodamiesi mobiliaisiais įrenginiais su STD piliečiai galės patvirtinti savo tapatybę ir dalytis elektroniniais dokumentais. Dėklių išdavimo taisyklių nustatymo prerogatyva paliekama šalims narėms.

Atnaujinto eIDAS reglamento (Nr. 2024/1183) papildymo preambulė aiškiai apibrėžia ir išdėsto ES skaitmeninės tapatybės sistemos ir skaitmeninės aplinkos plėtros tikslus – užtikrinti ne tik skaitmeninės infrastruktūros saugumą, bet ir palengvinti viešųjų ir privačiųjų paslaugų prieinamumą, stiprinant pasitikėjimą skaitmenine erdve ir skatinti skaitmeninės ekonomikos augimą. Akcentuotinos šios reglamento nuostatos:

1. ES piliečiams ir kitiems gyventojams turi būti užtikrinta teisė kontroliuoti savo skaitmeninę tapatybę, suteikiant galimybę naudotis ir dalyvauti skaitmeninėje ekonomikoje. Dėl to sukurta skaitmeninės tapatybės sistema, leidžianti naudotis viešosiomis ir privačiosiomis paslaugomis visoje ES, tiek prisijungus, tiek neprisijungus prie interneto.
1. Visiems ES gyventojams užtikrinama teisė saugiai tvarkyti su jų tapatybę susijusius duomenis bei kontroliuoti jų naudojimą. Reglamentu užtikrinamas aukščiausias saugumo, privatumo lygis, kartu laikomasi pagrindinių teisių ir nediskriminuojami tie, kurie

nepasirinks naudotis STD. Siekiant išvengti diskriminacijos ir priverstinio naudojimo šia sistema, į reglamentą įtrauktos apsaugos priemonės, kurios garantuoja, kad asmenys nusprendę nesinaudoti skaitmenine tapatybės dėkle, nepatirs jokių neigiamų pasekmių. Naudojimas STD išliks savanoriškas ir neprivalomas.

2. Naudojantis ES STD asmenys turės galimybę kurti ir visoje bendrijoje, naudoti pripažįstamus kvalifikuotus elektroninius parašus ir spaudus (angl. *qualified electronic seals*). Tai turės galimybę automatiškai ir nemokamai naudotis kvalifikuotais elektroniniais parašais, be jokių papildomų administracinių procedūrų taikymo, patvirtinti jų pačių pateiktus teiginius ar požymius.
3. Valstybės narės įpareigojamos teikti europines STD, grindžiamas bendrais standartais ir techninėmis specifikacijomis, kurios padės užtikrinti IT saugumą ir atsparumą prieš kibernetinius išpuolius bei sumažinti bendrijos gyventojams bei įmonėms kylantį skaitmenizacijos pavojų.
4. Stiprinant PID apsaugą šiuo reglamentu nustatomi kibernetinio saugumo reikalavimai.
5. Užtikrinamas STD veikimo skaidrumas – sudaromos sąlygos asmens duomenų tvarkymo patikrai, kartu valstybės narės įpareigojamos atskleisti STD naudotojo taikomas programos, programinė įrangos komponentų, įskaitant su asmens ir juridiniais duomenimis taikymo, pirminį kodą. Siekiama, kad visuomenė, naudotojai ir kūrėjai, suprastų STD veikimą ir atliktų kodo peržiūrą. Skaidrumas yra svarbus užtikrinant visuotinį naudotojų pasitikėjimą STD ekosistema bei stiprinant saugumą, kadangi visiems suteikta galimybė informuoti apie kodo klaidas ar pažeidžiamumą. Tačiau valstybėms narėms palikta prerogatyva apriboti šio produkto naudojamų bibliotekų, kitų elementų pirminio kodo atskleidimą visuomenės saugumo tikslais.
6. Skatinant STD diegimą ir naudojimą, valstybės narės įpareigojamos bendradarbiauti su privačiuoju sektoriumi, akademine bendruomene. Bendradarbiavimas yra svarbus kuriant mokymo programas, kuriomis būtų siekiama sustiprinti piliečių, pažeidžiamų grupių (asmenų su negalia ar vyresnio amžiaus asmenų) skaitmeninius įgūdžius. Taip pat valstybės narės įpareigojamos vykdyti švietėjišką veiklą, kuria būtų informuotumas apie STD naudą ir riziką.

Kol bus prieinami sertifikuoti nuo klastojimo apsaugantys sprendimai, siūloma naudoti sertifikuotus išorinius saugius elementus arba aukšto lygio saugumo priemones, siekiant apsaugoti duomenis, bet šis reglamentas neturėtų paveikti nacionalinių teisių dėl sertifikuotų išorinių saugių elementų naudojimo pereinamuoju laikotarpiu.

Atnaujinto reglamento versija (Nr. 2024/1183) numato, kad elektroniniai registrai turėtų sukurti chronologinę duomenų įrašų seką. Kartu su kitomis technologijomis STD prisidės prie

veiksmingesnių ir transformatyvių viešųjų paslaugų, tokių kaip e. balsavimas, muitinių tarpvalstybinis ir akademinių institucijų bendradarbiavimas, nekilnojamojo turto nuosavybes registravimas decentralizuotuose žemės registruose ir t. t. Kvalifikuoti elektroniniai registrai (angl. *Qualified electronic ledger*) sukurs teisinę prezumpciją, skirtą užtikrinti unikalią, tikslią ir nuoseklią chronologinės registro duomenų įrašų tvarką bei vientisumą.

Užtikrinant teisinį tikrumą ir skatinant inovacijas teisinė sistema kuriama visos ES mastu - teisinė sistema, pagal kurią numatomas patikimumo užtikrinimo paslaugų, skirtų registruoti duomenis elektroniniuose registruose pripažinimas tarpvalstybiniu mastu. Šis žingsnis galimai padės užkirsti kelią skaitmeninio turto kopijavimui ir pardavimui skirtingoms šalims daugiau nei vieną kartą.

Svarbu pažymėti, kad nepaisant reglamentavimo tarptautiškumo atnaujintu reglamentu nėra daromas poveikis jokioms teisinėms elektroninių registrų naudotojų pareigoms pagal ES ar nacionalinę teisę. Atsižvelgiant į STD teikiamas galimybes tikslinga manyti, kad šis įrankis ne tik padės modernizuoti viešąsias paslaugas, bet ir pasitarnaus su tokiomis grėsmėmis kaip pinigų plovimas. Toliau bus aptariamos STD ypatybės susijusios būtent su kibernetinio saugumo stiprinimu.

Naujo tipo skaitmeninių dokumentų kūrimui naudojami nauji standartai ar specifikacijos, tenkinantys aukštus saugumo ir privatumo reikalavimus. Siekiama užtikrinti dokumentą patikimumą, lengvą patikrą ir atitiktį vartotojų bei institucijų poreikiams įvairiose situacijose.

1. Kvalifikuoti elektroniniai požymių liudijimai ((Q)EAA) – skaitmeniniai dokumentai, išduoti organizacijų, kurios imasi papildomų saugumo veiksmų, užtikrinančių dokumentų patikimumą. Tokios organizacijos vadinamos kvalifikuotais patikimumo užtikrinimo paslaugų teikėjais, kaip apibrėžta eiDAS reglamente EP ir Tarybos reglamentas (ES) 2024/1183). (Q)EAA dokumentams keliami aukščiausio patikimumo reikalavimai. Dažniausiai tai oficialūs dokumentai, tokie kaip socialinio draudimo pažymėjimas ar asmens tapatybę patvirtinantis dokumentas. Kvalifikuotas elektroninis požymių liudijimas turi tradiciniams popieriniams dokumentams prilygstančią teisinę galią.
2. Nekvalifikuoti elektroniniai požymių liudijimai (EAA) arba kvalifikuoti ir nekvalifikuoti sertifikatai – skaitmeniniai dokumentai, išduoti organizacijų, kurios nėra kvalifikuotos patikimumo užtikrinimo paslaugų teikėjos, todėl jiems taikomas mažesnės apimties taisyklių rinkinys. EAA skirti mažiau svarbiems dokumentams, pvz., traukinio, autobuso ar koncerto bilietai.
3. ISO/IEC 18013-5 standartas. Numatoma, kad elektroninių dokumentų formatas bus paremtas ISO18013 arba Verifiable Credentials (Verifikuojamų kredencialų duomenų modelis) specifikacijomis.

   ISO18013 yra tarptautinis standartas, kurio pagrindinis tikslas yra apibrėžti reikalavimus skirtus skaitmeniniams vairuotojo pažymėjimams (angl. *mobile Driving License, mDL*). Šis

standartas gali būti naudojamas ir kito tipo dokumentams. Pažymėtina, kad dokumentas, paruoštas pagal šią specifikaciją, gali būti patikrintas be skaitmeninio ryšio, naudojant tam pritaikytus įrankius, skirtus patikrinti dokumento autentiškumą ir galiojimą.

4. Asmens tapatybės duomenys (PID) – duomenų rinkinys, pagal kurį nustatoma fizinio arba juridinio asmens tapatybė. PID prieinami vienu iš pagrindinių formatų - (Q)EAA kvalifikuoto elektroninių požymių liudijimo standartą, atsižvelgiant į prieinamo ryšio būklę. Kai nėra galimybės užmegzti interneto ryšio ar tiesioginio tinklo prieigos, numatoma taikyti ISO18013 formatą (mDL). Esant interneto ryšiui, tapatybės patikrinimui bus naudojami Verifiable Credential, pagrįsti Selective Disclosure JSON Web Signature (SD JWS) technologija. Šis formatas leis saugiai patvirtinti tapatybės informaciją internetu, užtikrinant duomenų vientisumą ir autentiškumą. Šie formatai užtikrins PID saugumą ir prieinamumą, kai yra reikalingi. PID bus išduodami tik sertifikuotų viešųjų ir privačių organizacijų, kurias pripažins valstybės narės. Prieš įtraukiamos į patikimu PID teikėjų sąrašą šios organizacijos įsipareigos laikytis griežtų gairių. Sertifikavimo procesas užtikrins, kad PID ir susijusios savybės atitiks aukščiausius saugumo standartus, todėl jais gali būti pasikliaujama visoje ES.

Svarbu akcentuoti, kad kvalifikuotas elektroninių požymių liudijimas tobulina apsaugą nuo galimo skaitmeninių dokumentų klastojimo. Vartotojas gali patikrinti, ar gauta žinutė tikrai yra išsiųsta iš organizacijos, kuria prisistato. Tuo pačiu paprastėja naujų paslaugų kūrimas, klientų aptarnavimas ir užtikrinama geresnė prieiga prie įvairių internetinių paslaugų. Kuriamoje ekosistemoje numatomi elektroniniai registrai sukuria ekosistemos dalyvius jungiančius ir pasitikėjimu grįstus ryšius bei saugo skaitmeninių dokumentų ruošinius, kurie yra suprantami bet kurioje ES šalyje narėje. Reglamento 5A straipsnyje nurodoma, kad STD taikomosios programinės įrangos komponentų pirminis kodas privalės būti licencijuotas, kaip atviro kodo programinė įranga. Tai reiškia, kad visuomenė, įskaitant naudotojus ir kūrėjus, turės galimybę susipažinti su šiuo kodu, atlikti jo auditą ir įvertinti, taip didinant pasitikėjimą sistema. Atviro kodo licencija ne tik užtikrins skaidrumą, bet ir suteiks galimybę pranešti apie kodo pažeidžiamumą bei klaidas, taip prisidedant prie Europinės STD saugumo ir kokybės. Tačiau valstybės narės gali nustatyti išimtis ir dėl tinkamai pagrįstų priežasčių nuspęsti neatskleisti tam tikrų programinės įrangos komponentų kodo, ypač tų, kurie nėra įdiegti naudotojo įrenginyje. Tokie sprendimai gali būti priimti siekiant apsaugoti visuomenės saugumą arba dėl kitų tam tikrų svarbių interesų.

Viena iš svarbesnių atnaujinto eIDAS reglamento (Nr. 910/2014 su papildyta dokumento versija Nr. 2024/1183) reikalavimų yra suteikti reikiamą infrastruktūrą, kuri leistų įgyvendinti reglamentą. Specifikacijos apima skaitmeninės tapatybės ar kokio kito skaitmeninio dokumento išdavimo, jo priėmimo ir laikymo, bei tokių skaitmeninių dokumentų patikrinimo nuostatas. ES Skaitmeninės Tapatybės Dėklė (STD) mobiliems įrenginiams skirta programėlė, kurios pagalba

privatūs ir juridiniai asmenys galės priimti, laikyti ir pateikti skaitmeninį tapatybę patvirtinantį dokumentą ar kitus su asmenybe susijusius skaitmeninius dokumentus. Visa tai suteiks galimybę ES piliečiams ir įmonėms paprasčiau naudotis skaitmeniniu tapatybę patvirtinančiu dokumentu ar kitais skaitmeniniais dokumentais, reikalingais naudojantis įvairiomis paslaugomis bendrijos ribose. Naudodamiesi STD verslas ir (arba) valstybės institucijos galės saugiau, greičiau ir paprasčiau identifikuoti asmens tapatybę, gauti kitus asmeninius duomenis tiek internetu, tiek fizinėje aplinkoje.

Stiprinant vartotojų duomenų apsaugą atnaujinto reglamento 12 straipsnyje išsamiai aprašomos asmeninių duomenų kontrolės ir panaudojimo teisės. Numatoma, kad duomenys gali būti naudojami tik su vartotojo sutikimu. Šia nuostata taip pat sustiprina asmens duomenų apsauga.

Atnaujintas reglamentas nurodo, kad iki 2026 metų pabaigos kiekviena valstybė narė privalės išleisti bent vieną oficialią STD ir suteikti galimybę savo piliečiams jomis pasinaudoti užsakant paslaugas skaitmeninėje aplinkoje. Taip pat valstybės narės įsipareigos aptarnauti ir kitų ES šalių piliečius, besinaudojančius ES STD. Šis įrankis vartotojams bus suteikiamas nemokamai, kartu su nemokamais STD autentiškumo patvirtinimo mechanizmais. Šie mechanizmai taip pat turi užtikrinti pasikliaujančioms šalims, pagal reglamento 5b straipsnį (Europos skaitmeninės tapatybės dėklės pasikliaujančios šalys – Relying Party), patikrinti tapatybės autentiškumą ir galiojimą. Reglamentas reikalauja, kad valstybės narės nemokamai įdiegtų ir palaikytų patvirtinimo mechanizmus (angl. *validation verify mechanisms*), kurie leistų patikrinti skaitmeninės dėklės ir ją naudojančių subjektų tapatybės autentiškumą bei galiojimą. Šios priemonės turėtų padidinti pasitikėjimą skaitmeninėmis paslaugomis ir užtikrinti jų saugumą.

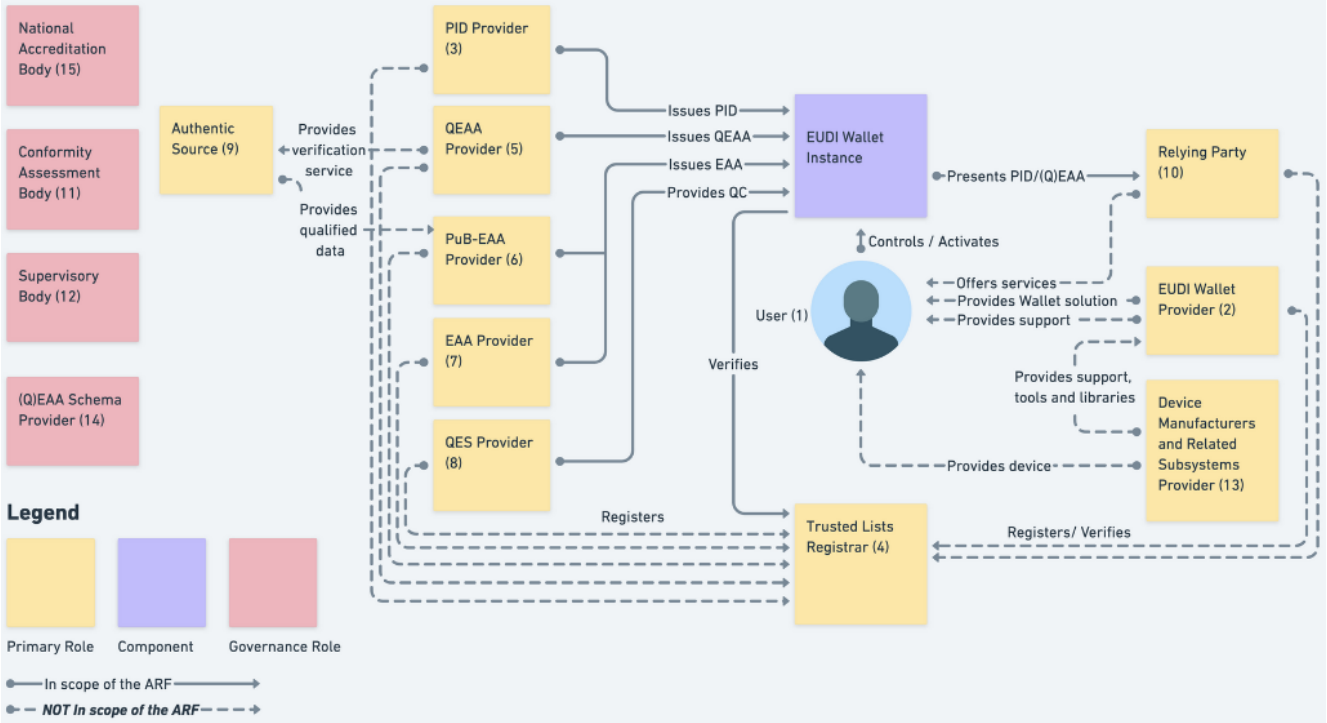
Apibendrinant galima teigti, kad bendras STD skaidrumas ir jų teikėjų atskaitomybė yra suvokiami kaip esminės visuomenės pasitikėjimo ir sistemos pripažinimo prielaidos. Atsižvelgiant į tai valstybės narės turėtų užtikrinti pirminio kodo, susijusio su asmens duomenų ir juridinių asmens duomenų tvarkymų, viešumą. Sistemos naudojai turi suprasti, kaip tvarkomi jų duomenys, kartu įvertinti sistemos patikimumą bei saugumą. Reglamentu siekiama užtikrinti nuoseklumą tarp skaitmeninės tapatybės dėklės, kaip elektroninės atpažinties formos ir schemos, pagal kurią ji bus išduodama. Taip siekiama užtikrinti efektyvų, saugų ir sklandų šios sistemos veikimą visose valstybės narėse.

2.2. Europos Sąjungos Skaitmeninės Tapatybės Dėklės ekosistema

Europos Sąjungos Skaitmeninės Tapatybės Dėklės *(*European Union Digital Identity Wallet) ekosistema apima saugų ir patikimą skaitmeninės tapatybės valdymo tinkle sudarančius subjektus – naudotojus, paslaugų teikėjus, tapatybės duomenų valdytojus ir kitas suinteresuotas šalis, kurios kartu

užtikrina, kad asmens tapatybės informacija būtų apsaugota ir efektyviai naudojama visoje ES. Kiekvienas subjektas atlieka specifinį vaidmenį, užtikrinant ekosistemos funkcionalumą ir vientisumą.

Žemiau pateiktame paveikslėlyje grafiškai atvaizduota visa ES STD ekosistema (2 pav.).



Šaltinis: Eu digital identity wallet. Prieiga per https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/1.4.0/arf/#3-ecosystem

2 **pav. ES STD ekosistema**

Remiantis techniniu standartu (angl. Architecture Reference Framework) STD ekosistemą sudaro šie komponentai:

- Skaitmeninės Tapatybės Dėklės naudotojai (angl. *Users of EUDI Wallets*) – fiziniai ir juridiniai asmenys, kurie dėklėje saugo, gauna ir pateikia asmeninę informaciją bei naudojasi PID. Taip pat naudotojai gali kurti kvalifikuotus elektroninius parašus ir spaudus (angl. *Qualified Electronic Signatures and Seals*).
- Skaitmeninės Tapatybės Dėklės paslaugų teikėjai (angl. *EUDI Wallet Provider*) - valstybės narės arba organizacijos, kurias įgaliojo arba pripažino valstybės narės, kurioms leidžia galutiniams naudotojams naudotis dėkle. Įgaliojimo sąlygas nustato kiekviena valstybė narė. Skaitmeninės Tapatybės Dėklės teikėjai, naudodamiesi savo dėklės sprendimu, pateikia naudotojui kelių teisės akto pasiūlyme numatytų produktų ir patikimumo užtikrinimo paslaugų derinį, kuris suteikia PID ir elektroninių požymių liudijimų (QEAA, PuB-EAA arba EAA) ir visų kitų asmens duomenų, esančių jo dėklės, naudojimo kontrolę. Techniniu požiūriu yra užtikrinta išskirtinė neskelbtinos

kriptografinės medžiagos (pvz., privačių raktų), susijusios su PID ir (ar) (Q)EAA kontrole, įskaitant naudojimo atvejus elektroninei atpažinčiai ir parašo ar antspaudo kūrimui. Skaitmeninės Tapatybės Dėklės paslaugų teikėjai yra atsakingi už tai, kad būtų laikomasi dėklėje taikomų reikalavimų.

- PID teikėjai (angl. Person Identification Data (PID) Providers) – yra patikimi subjektai, atsakingi už ES STD naudotojo tapatybę, laikantis aukštų reikalavimų, išduodant PID į dėklę suderintu bendru formatu ir pateikti informaciją pasikliaujančiosioms šalims, kad jos galėtų patikrinti PID galiojimo laiką. Šių paslaugų teikimo sąlygas nustato valstybės narės. PID teikėjais gali būti tos pačios organizacijos, kurioms išduodamos oficialūs tapatybės dokumentai arba išduodančios ES Skaitmeninės Tapatybės Dėklės paslaugas.
- Patikimų sąrašų registratorius (angl. *Trusted Lists Registrar*) – šalis, atsakinga už patikimo sąrašo tvarkymą, valdymą ir publikavimą STD ekosistemoje.
- (Q)EAA teikėjai (angl. *(Q)EAA) Providers*) – organizacijos atsakingos už patikimų elektroninių požymių liudijimų, patvirtinančių vartotojų tapatybės atributus (pvz., amžių, pilietybę, išsilavinimą) teikimą. Šiuos teikėjus pripažįsta ir licencijuoja kvalifikuoti patikimumo paslaugų teikėjai (angl. *Qualified Trust Service Providers, QTSP*), kurie užtikrina liudijimų saugumą bei atitiktį reglamentui. Taip pat (Q)EAA teikėjai palaiko sąsajas su STD, kuriose vartotojai gali laikyti įvairius savo tapatybės patvirtinimo atributus. Šios sąsajos leidžia vartotojams saugiai teikti prašymą ir gauti elektroninius liudijimus. Be to, (Q)EAA teikėjai užtikrina abipusį autentifikavimą tarp naudotojų ir patikimų šaltinių, reikalingų patikrinti pateiktus atributus.
- Viešo autentiško šaltinio elektroninio požymių liudijimo (PuB-EAA) teikėjai (angl. Public Body Authentic Source Electronic Attestation of Attributes (PuB-EAA) Providers) – yra už autentišką šaltinį atsakinga arba savo vardu jį išduodanti viešoji įstaiga. Autentiškų šaltinių reikalavimu dėl PuB-EAA išdavimo ir veikimo siekiama suteikti pasikliaujančiosioms šalims galimybę teisiniu lygmeniu pripažinti juos kvalifikuotais liudijimais ((Q)EAA).
- Nekvalifikuoti elektroninio požymių liudijimo (EAA) teikėjai (angl. *Non-Qualified Electronic Attestation of Attributes (EAA) Providers*) – gali teikti bet kuris patikimumo užtikrinimo paslaugų teikėjas (angl. *Trust Service Provider* – TSP). Nors šie paslaugų teikėjai yra prižiūrimi pagal eIDAS reglamentą, galima teigti, kad EAA teikimo, naudojimo ir pripažinimo taisykles dažniausiai gali būti pagrįstos ir kitomis teisinėmis, kurios papildo ar praplečia eIDAS reglamentavimo ribas. Šis požymių liudijimas apima įvairias sritis, pavyzdžiui vairuotojo pažymėjimų išdavimą, mokslo diplomo pažymėjimo išdavimą, atpažinimą arba skaitmeninius mokėjimus, tačiau kai kuriais atvejais gali būti

reikalaujama, kad paslaugos būtų grindžiamos kvalifikuotais elektroninio požymių liudijimų teikėjais – (Q)EAA. Norint užtikrinti efektyvų elektroninio požymių liudijimo (EAA) naudojimą, patikimumo užtikrinimo paslaugų teikėjai (TSP) suteikia vartotojams prieigą prie mechanizmo, leidžiančio pateikti prašymus dėl EAA gavimo. Tai reiškia, kad TSP privalo atitikti techninius reikalavimus, nustatytus Skaitmeninės Tapatybės Dėklės sąsajoje.

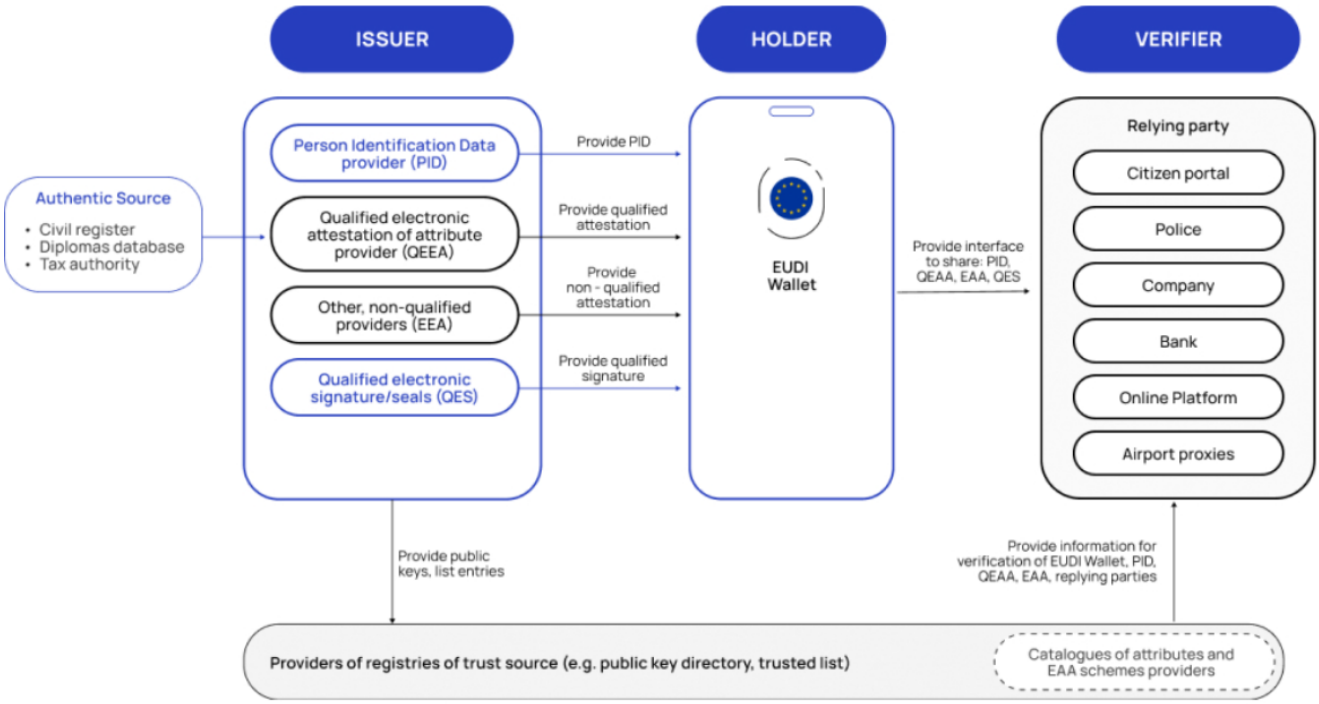
- QES nuotolinio kūrimo paslaugų teikėjai (angl. *Qualified Electronic Signatures Remote Creation Service Providers*) – šios įstaigos Skaitmeninės Tapatybės Dėklės naudotojui suteikia nemokamo kvalifikuotų elektroninių parašų kūrimo galimybę. Tai padidina pasirašymo naudojant STD patogumą. Kvalifikuotą elektroninį parašą arba spaudą naudojant dėklę galima sukurti keliais būdais: pati dėklė yra sertifikuota, kaip kvalifikuotas parašo/spaudo kūrimo įrenginys (QSCD) arba pačioje dėklėje yra įdiegtas saugus autentifikavimas ir elektroninis parašas arba elektroninio spaudo iškvietimo galimybė kaip vietinio QSCD arba nuotolinio QSCD, valdomo QTSP, dalis.
- Autentiški šaltiniai (angl. *Authentic Sources*) – teisės aktais pripažįstamos arba reikalaujamos viešosios arba privačios saugyklos ar sistemos, kuriose yra fizinių ir (ar) juridinių asmenų požymių. Autentiški šaltiniai, kuriems taikomas eIDAS reglamento 45e straipsnis, pvz., adreso, amžiaus, lyties, civilinės būklės, šeimos sudėties, pilietybės, išsilavinimo, mokymo kvalifikacijų ir licencijų, profesinių kvalifikacijų vardų ir licencijų, viešųjų leidimų ir licencijų, finansinių ir įmonių duomenų šaltiniai. Autentiški šaltiniai, kuriems taikomas 45e straipsnis, privalo teikti sąsajas su QEAA teikėjais, kad šie pirmiausiai galėtų patikrinti minėtų požymių autentiškumą tiesiogiai arba per nacionaliniu lygmeniu pripažintus bei paskirtus tarpininkus.
- Pasikliaujančiosios šalys (angl. *Relying Parties*) – fiziniai arba juridiniai asmenys, kurie naudojasi elektronine atpažintimi arba patikimumo užtikrinimo paslauga. ES STD, atveju šie asmenys prašo naudotojų pateikti būtinus atributus, esančius PID duomenų rinkinyje, t. y., QEAA, Pub-EAA ir EAA, kad galėtų pasikliauti dėkle. Pažymėtina, kad atributai pateikiami tik su dėklių savininkų (naudotojų) sutikimu ir laikantis numatytų teisės aktų bei taisyklių. Kad galėtų pasikliauti Skaitmeninės Tapatybės Dėkle paslaugai teikti, pasikliaujančiosios šalys turi informuoti valstybę narę, kurioje yra įsisteigusios, apie savo ketinimą tai daryti. Kad galėtų prašyti liudijimų su abipusiu autentiškumo patvirtinimu pasikliaujančiosios šalys turi išlaikyti sąsają su ES STD. Pasikliaujančiosios šalys yra atsakingos už PID ir (Q)EAA autentiškumo patvirtinimą.
- Atitikties įvertinimo įstaigos (angl. *Conformity Assessment Bodies, CAB*) – valstybių narių akredituotos viešosios arba privačiosios įstaigos, atsakingos už vertinimų, kuriais

valstybės narės turės remtis Europos Parlamento ir Tarybos reglamentu (EB) Nr. 765/2008, prieš išleisdamos ES STD arba suteikdamos patikimumo užtikrinimo paslaugų teikėjui kvalifikacijos statusą, atlikimą. Atitikties įvertinimo įstaigos reguliariai atlieka QTSP auditą. Standartai ir schemos, kuriuos atitikties įvertinimo įstaigos naudoja vykdydamos savo užduotis, sertifikuoti ES STD.

- Priežiūros įstaigos (angl. *Supervisory Bodies*) – priežiūros įstaigos atliekančios STD paslaugų teikėjų ir kitų susijusių subjektų priežiūrą. Šios įstaigos turi būti įsteigtos visose valstybėse narėse. Valstybės narės įpareigotos pranešti Komisijai apie visas priežiūros įstaigas.
- Įrenginio kūrėjai ir susiję posistemių teikėjai (angl. *Device Manufacturers and Related Subsystems Providers*) – STD ekosistemos komerciniai subjektai, prisidedantys prie saugaus ir sklandaus dėklės veikimo, pvz., įrenginio gamintojai ir susijusių posistemių teikėjai. Įrenginio gamintojai ir susiję posistemių teikėjai yra įpareigoti sukurti platformą, kurios pagrindas turi būti sukurtas Skaitmeninės Tapatybės Dėklės sprendimas. Pagrindiniai sprendimo veiksniai – tinkamumas naudoti, saugumas ir stabilumas. Įrenginių gamintojų ir susijusių posistemių tiekėjų teikiami komponentai apima ir aparatinę įrangą, operacines sistemas, saugią kriptografinę aparatinę įrangą, bibliotekas ir taikomųjų programų saugyklas.
- Kvalifikuoti ir nekvalifikuoti elektroninio požymių liudijimo schemos teikėjai (angl. *Qualified and Non-Qualified Electronic Attestation of Attributes Schema Providers*) – įstaigos skelbiančios schemas ir žodynus, kuriuose aprašoma (Q)EAA struktūra ir semantika. Šių įstaigų veikimas reikalingas siekiant sudaryti sąlygas kitiems subjektams, pvz., pasikliaujančiosioms šalims, atrasti ir patvirtinti (Q)EAA. Šiuo tikslu Europos Komisija nustato minimalias technines specifikacijas, standartus ir procedūras. Siekiant plataus (Q)EAA pritaikymo reikalingos bendros schemos tinkamos konkrečių sektorių organizacijoms.
- Nacionalinės akreditacijos įstaigos (angl. *National Accreditation Bodies* – NAB) – valstybių narių įstaigos, vykdančios akreditavimą pagal valstybės narės suteiktus įgaliojimus. Nacionalinės akreditacijos įstaigos akredituoja atitikties įvertinimo įstaigas kaip kompetentingas, nepriklausomas ir prižiūrimas profesinio sertifikavimo, atsakingas už produktų, paslaugų ir procesų sertifikavimą pagal norminį (-ius) dokumentą (-us), kuriuo (-iais) nustatomi reikalavimai (pvz., teisės aktai, specifikacijos, apsaugos profiliai). Nacionalinės Akreditacijos įstaigos atlieka ir subjektų, kuriems išdavė akreditacijos pažymėjimą, stebėseną.

Europos Sąjungos Skaitmeninės Tapatybės Dėklės naudotojai galės atsisiųsti, įsidiegti ir naudoti šią ekosistemą savo asmeniniuose išmaniuosiuose telefonuose ar kituose mobiliuosiuose įrenginiuose. Su dėkle bus leidžiama greitai ir paprastai, vienu mygtuko paspaudimu, perduoti reikiamą informaciją pasikliaujančioms šalims. Naudotojai galės atskleisti tik esminius, pasirinktus duomenis, pavyzdžiui, amžių ar pilietybę, užtikrinant asmens duomenų privatumą ir saugumą. Skirtingai nei naudojant fizinius dokumentus, STD padeda užtikrinti teisės į jų asmeninę informaciją suverenumą ir išvengti perteklinių duomenų atskleidimo.

Žemiau pateiktame paveikslėlyje pavaizduota pavyzdinio ES STD naudojimo proceso eiga (žr. 3 pav.).

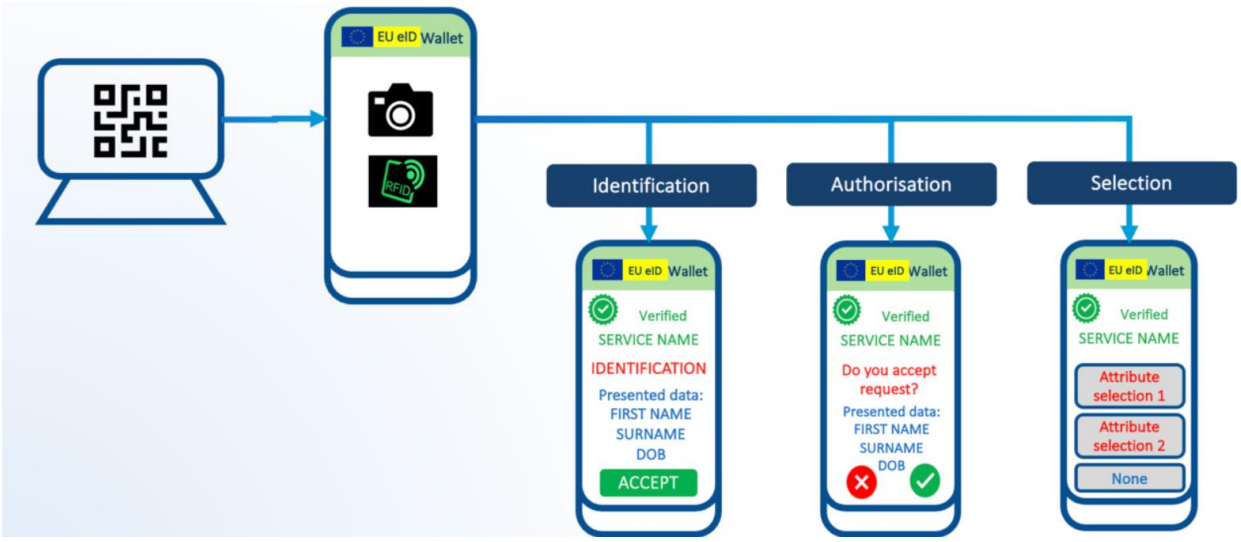


Šaltinis: EUDI wallet iliustration of the eIDAS roles and relationships. Prieiga per internetą: *https://www.lissi.id/blog/eudi-wallet-illustration-of-the-eidas-roles-and-relationships*

3 pav. ES STD naudojimo proceso eiga

Inicijavimo ir programėlės aktyvinimo etape naudotojas atsisiunčia aplikaciją į savo įrenginį, į kurį įkeliamas (šalies narės nustatyta tvarka) asmenybę tapatybę patvirtinantis dokumentas (angl. PID). Įkėlus PID naudotojas gali aktyviai naudotis programėlės funkcijomis ir paslaugomis įvairiems asmeniniams poreikiams (pvz., atsiskaitymui, tapatybės patvirtinimui ir (arba) naudotis kitoms skaitmeninėms paslaugoms). Skaitmeninėje Tapatybės Dėklėje esantis PID leidžia viešosioms įstaigoms, pvz., bankams, atlikti asmens identifikaciją.

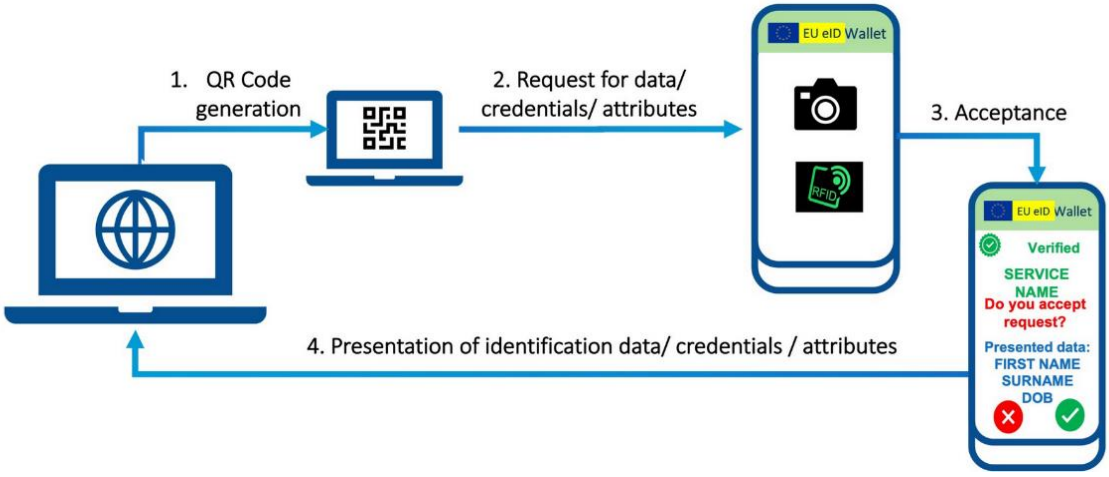
Trečioji schema apibūdina skaitmeninės tapatybės identifikacijos ir autentifikacijos procesą, naudojantis skaitmeninėmis paslaugomis (žr. 4 pav.).



Šaltinis: Prieiga per internetą: *https://obserwatorium.biz/en/raporty/*

4 pav. Skaitmeninės tapatybės identifikacijos ir autentifikacijos procesas

Pasirinkęs skaitmeninę tapatybę iš dėklės naudotojas pradeda autentifikaciją, pateikia asmenybę patvirtinančius duomenis (PID) arba kitą, skaitmeninį dokumentą tinkantį tai paslaugai gauti (pvz., kvalifikuotų elektroninių požymių liudijimų (Q)EAA formatu išduotą tinkantį paslaugos teikimui dokumentą). Šį skaitmeninį dokumentų formatą gali atitikti tokie dokumentai kaip šiuo metu yra studento ar senjoro pažymėjimai. Tuomet kriptografinius metodus naudojanti sistema apdoroja pateiktą skaitmeninį dokumentą, įrodantį asmens tapatybę (žr. 5 pav.).



Šaltinis: prieiga per internetą: https://obserwatorium.biz/en/raporty/

5 pav. Skaitmeninės tapatybės identifikacijos ir autentifikacijos procesas

Šio proceso metu patikrinami dokumento autentiškumas, galiojimas ir priklausomumas jį pateikiančiam asmeniui faktas. Prieš pateikiant STD esantį dokumentą, naudotojas turi patvirtinti, kokius duomenis nori atskleisti, ir duoti sutikimą jų panaudojimui prašomai paslaugai suteikti. Tokiu būdu asmuo, siekiantis gauti paslaugą, turi galimybę kontroliuoti asmeninius duomenis. Sistema atlieka saugų autentifikavimą. Stiprinant proceso saugumą naudotojo gali būti prašoma įvesti

papildomus patvirtinimo duomenis, pvz., PIN kodą, arba panaudoti biometrinę informaciją. Po sėkmingo patvirtinimo sistema suteikia naudotojui prieigą prie paslaugos.

Europos Sąjungos Skaitmeninės Tapatybės Dėklė yra platesnės ekosistemos, apimančios eilę ir kitų dalyvių, kurie prisideda prie visos ekosistemos patikimumo užtikrinimo dalies. Pagrindinis ir plačiai pripažintas skaitmeninės tapatybės ekosistemos modelis apima tris pagrindinius dalyvius: vartotoją, skaitmeninių dokumentų išdavėją ir paslaugų teikėją (Kubach ir Roßnagel, 2024). Vartotojai, pagrindiniai skaitmeninės tapatybės dėklės naudos gavėjai, yra ES piliečiai, įmonės (verslas). Naudotojai patys kontroliuoja savo asmens duomenis ir gali pasirinkti paslaugas, su kuriomis nori dalytis šiais duomenimis. Skaitmeninę tapatybę patvirtinantį dokumentą (angl., PID) išduodančios organizacijos privalo, patikrinti piliečių tapatybę pasikliaujant saugiais ir patikimais tapatybės patvirtinimo procesais. Paslaugų teikėjai, pavyzdžiui, vyriausybinės agentūros, finansų įstaigos ir e. prekybos platformos, gali pasinaudoti skaitmeninės tapatybės dokumentu identifikuodami naudotojus, kad patvirtintų naudotojų autentiškumą ir suteiktų saugią prieigą prie savo paslaugų.

Lukkien, Bharosa ir De Reuver (2023), teigia, kad skaitmeninės tapatybės dėklės ekosistemoje dalyvaujantys dalyviai, reikalingi įvairioms svarbioms šios sistemos funkcijoms užtikrinti:

1. Skaitmeninės tapatybės dėklės paslaugų teikėjai: viešieji arba privatieji subjektai, siūlantys naudotojams pačią skaitmeninę piniginę.
2. Pasitikėjimo paslaugų teikėjai: organizacijos, teikiančios patikimumo užtikrinimo paslaugas, pavyzdžiui, išduodančios skaitmeninius sertifikatus ar elektroninius parašus.
3. Tapatybės paslaugų teikėjai: subjektai, atsakingi už naudotojų tapatybės duomenų tikrinimą ir tvarkymą, bei skaitmeninio tapatybės dokumento (PID) išdavimą.
4. Kvalifikuotų ir nekvalifikuotų (EAA ir (Q)EAA) požymių liudijimo paslaugų teikėjai: organizacijos, išduodančios skaitmeninius dokumentus STD formatu, pvz., išsilavinimo kvalifikaciją patvirtinantį dokumentą arba licenciją.
5. Technologijų teikėjai: įmonės, teikiančios techninę ir programinę įrangą, reikalingą skaitmeninės tapatybės dėklės funkcijoms palaikyti.

Taip pat yra svarbu paminėti jog Skaitmeninės Tapatybės Dėklės ekosistemos kontekste svarbi sąvoka yra „patikimi sąrašai“ (angl. *trusted list*), kuriuose pateikiama informacija apie įvairius ekosistemos dalyvius ir kuri tikrinama kiekvieno santykio su STD atveju. Organizacija, kuri pageidaus būti įtraukta į sąrašą, turės užsiregistruoti šalies narės „patikimame sąraše“. Šiuos sąrašus tvarko „patikimų sąrašų registratorius“ (angl. *trusted list registrar*), kurio funkcija yra užtikrinti, kad į sąrašą įtraukti dalyviai atitiktų nustatytus saugumo reikalavimus ir su tuo susijusius standartus. Patikimų sąrašų registratorius atsakingas už sąrašo atnaujinimą, naujų dalyvių registravimą bei esamų

dalyvių informacijos tikrinimą ir patvirtinimą pagal atnaujinto reglamento (Nr. 2024/1183) versiją bei nustatytus techninius standartus (European Digital Identity Wallet Architecture and Reference Framework).

2.3. ES Skaitmeninės Tapatybės Dėklės ekosistemos panaudojimo galimybės pinigų plovimo prevencijoje

Kaip jau minėta, per kelerius ateinančius metus kiekviena ES valstybė narė visiems piliečiams, gyventojams ir įmonėms privalės pasiūlyti Skaitmeninės Tapatybės Dėklės (STD) mobiliąją aplikaciją, sukurtą vadovaujantis eIDAS reglamento bei kitų teisės aktų reikalavimais. Manoma, kad ši ekosistema užtikrins saugų ir patikimą skaitmeninės tapatybės valdymą visoje ES. Šiame poskyryje bus siekiama atskleisti STD pritaikymo kovoje su pinigų plovimu galimybes.

Automatizavimas. Pirmiausiai verta akcentuoti automatizuotų kontrolės procesų, kurie taikomi STD ekosistemoje, reikšmę. Kaip jau minėta, vienas iš pinigų plovimo prevenciją ribojančių veiksnių yra būtent rankinis patikros procedūrų pobūdis. Naudojant STD galima skaitmenizuoti daugelį kontrolės procesų, kurie anksčiau buvo atliekami rankiniu ir (ar) popieriniu būdu. Dėl vieningų ir kompiuterinėms sistemoms suprantamų dokumentų EAA ar (Q)EAA formatų duomenys atsiranda galimybė vykdyti automatizuotus finansinių operacijų kontrolės procesus. Galima išskirti kelis automatizuotos patikros privalumus lyginant su rankine patikra – tai duomenų tikslumas, apdorojimo greitis ir tikslumas, mažesnė klaidų tikimybė. Automatizuojant kontrolės procesus užtikrinama, kad visos operacijos būtų vykdomos pagal nustatytus standartus ir taisykles. Kartu yra tikėtina, kad didinant kontrolės procesų tikslumą ir mažinant žmogiškųjų klaidų rizika, didės vartotojų pasitikėjimas skaitmeninėmis paslaugomis.

Didelio duomenų masyvo apdorojimo sparta yra itin svarbi kovoje su pinigų plovimu, kadangi padeda identifikuoti pasikartojančius modelius, kuriems būdingi pinigų plovimo požymiai. STD padės tiksliau analizuoti finansinių sandorių istoriją, nes kiekvienas sandoris bus tiesiogiai susiejamas su patvirtinta vartotojo tapatybe. Sparčiai apdorojant didelį duomenų masyvą galima užfiksuoti finansines anomalijas. Be to, finansų sektoriaus skaidrinimo kontekste nemažiau svarbu yra tai, jog visos bankinės operacijos yra stebimos ir analizuojamos realiuoju laiku. Reaguojant į įtartinas bankines operacijas realiuoju laiku galima veikti prevenciškai ir užkirsti kelią įvairiems finansiniams nusikaltimams.

Kartu STD ekosistema padės didinti pinigų plovimo prevencijoje svarbios informacijos prieinamumą. Pažymėtina, kad būtent dėl riboto informacijos prieinamumo bei spartaus internetinių sandorių atlikimo tempo kyla sunkumų renkant detalią bankinių operacijų informaciją. Naudojant STD kiekviena finansinė operacija gali būti papildyta tiksliomis ir išsamiomis detalėmis, kurios padės

geriau suprasti operacijos esmę ir kilmę su lygiagrečiai susieta skaitmenine tapatybe. Visa tai yra būtina siekiant užtikrinti skaidresnius ir saugesnius sandorius.

Automatizuoti kontrolės procesai palengvina autentiškumo patikrą, kuri yra ypač reikšminga siekiant sumažinti sukčiavimo riziką. Kompiuteriai gali automatiškai patikrinti EAA ar (Q)EAA formatu pateikto skaitmeninio dokumento autentiškumą, nustatyti ar jis nėra suklastotas ir patvirtinti, kad yra atsiųstas iš patikimo šaltinio. Automatiškai tikrinant tapatybę sumažėja žmogiškųjų klaidų rizika. Kartu yra mažinamas ir finansinių operacijų kontrolei reikalingų išteklių poreikis – net ir didelio finansinių duomenų masyvo apdorojimui nereikia papildomų darbuotojų ir fizinių resursų, todėl mažėja tiek finansinių, tiek teisėsaugos bei priežiūros institucijų sąnaudos, reikalingos kovoje su pinigų plovimu.

Apibendrinant automatizuotų kontrolės procesų ypatybes galima teigti, kad STD gali efektyvinti kovą su pinigų plovimu, nes tampa lengviau aptikti nusikalstamas veiklas. Nagrinėjant STD galimybes pinigų plovimo prevencijoje galima įžvelgti kelias šios sistemos pritaikymo perspektyvas, kurias verta aptarti atskirai – finansų institucijos, priežiūros ir teisėsaugos institucijos bei vartotojai.

Finansų institucijos. Siekiant įvertinti ES STD galimybes pinigų plovimo prevencijoje galimybes pirmiausiai tikslinga atsižvelgti į pritaikymo finansų sektoriuje ypatybes. Kaip jau išsiaiškinti ankstesniuose skyriuose, dažnai būtent finansinių institucijų veiklos spragos sukuria pinigų plovimo galimybes. Iki šiol finansų sektoriaus sistema palieka nemažai pinigų plovimui palankių spragų. Viena iš akivaizdžiausių spragų yra susijusi su tapatybės identifikavimu. Veikdami SEPA ir SWIFT sistemose bankai nėra priversti patikrinti, ar lėšų gavėjo vardas atitinka sąskaitos numerį, todėl nusikaltėliai gali manipuliuoti šia informacija, tokiu būdu išvengdami tikrosios gavėjo identifikacijos ir galimai tarptautinių finansinių sankcijų. Naudojant STD kartu su kvalifikuotų požymių liudijimu atributu (Q)EAA, bankai galės automatiškai patikrinti, ar lėšų gavėjo vardas ir (ar) pavardė atitinka sąskaitos numerį. Tam pasitelkiami skaitmeniniai sertifikatai ir kriptografinė autentifikacija. Šis procesas užkirs kelią galimybei manipuliuoti informacija ir užtikrins, kad visi tarptautiniai pavedimai būtų vykdomi tik teisėtiems gavėjams ir teisėtais tikslais. Automatinis tapatybės patikros mechanizmas yra greitas ir nereikalauja daug sąnaudų, todėl bankams neprireiks aukoti finansinių sandorių spartos dėl didesnio saugumo ir skaidrumo. Be to, STD padės bankams lengviau laikytis reguliavimo reikalavimų, nes visi sandorių kontrolės procesai yra standartizuoti, t. y., suderinti su ES standartais.

Tapatybės identifikacija ir apsauga. Naujoviškas finansų sektoriaus institucijoms prieinamas asmens tapatybės bei įmonių identifikavimas yra vienas svarbiausių pinigų plovimo prevencijos aspektų. Šiuo metu finansų institucijoms trūksta rekomendacijų, kurios padėtų identifikuoti fiktyvias įmones ar paslaugas. Tarp tokių rekomendacijų galėtų būti reikalavimas visoms

įmonėms privalomai registruotis oficialiuose nacionaliniuose ar ES registruose, o registracijos procesą pagrįsti naudojant Skaitmenine Tapatybės Dėkle, kuri užtikrintų kokybišką ir tikslų duomenų autentifikavimą ir saugumą. Automatinis registracijos ir patikrinimo procesas sumažintų fiktyvių įmonių bei teikiamų paslaugų riziką. Šis metodas galėtų užtikrinti ne tik duomenų tikslumą, bet ir jų vientisumą bei apsaugą nuo informacijos manipuliavimo. Įvairūs audito procesai ir sertifikavimo mechanizmai gali prisidėti prie bendro sistemos patikimumo, o naudotojų kontrolės ir duomenų skaidrumo užtikrinimas padės stiprinti pasitikėjimą finansų sistema bei kovoti su finansiniais nusikaltimais.

Asmens duomenų vagystės iki šiol buvo sunkiai užkardoma kibernetinių nusikaltimų sritis. Nusikaltėliai vagia asmeninę informaciją (pvz., vardus, adresus ir (ar) biometrinius duomenis) vėliau naudoja juos internetinės bankininkystės aplinkoje, tokiu būdu siekdami gauti prieigą prie lėšų ir jomis pasinaudoti. Pasitelkiant Skaitmeninės Tapatybės Dėklę kiekviena finansinė operacija bus susieta su tiksliai patvirtinta asmens tapatybe. Tai užtikrins, kad operacijos gali būti atliekamos tik teisėto naudotojo, taip sumažinant riziką, kad asmeninę informacija pasinaudos nusikaltėliai. Jei tapatybės dokumentas yra pavogtas arba prarastas, jo galiojimas gali būti nedelsiant atšauktas, todėl juo nebus galima pasinaudoti net ir tolimiausiose šalyse.

Skaitmeninės Tapatybės Dėklės ekosistema suteikia papildomą asmens duomenų apsaugos lygmenį, kuris skatins vartotojų pasitikėjimą internetine bankininkyste ir skaitmeninėmis paslaugomis. Visi STD saugomi skaitmeniniai dokumentai (pvz., skaitmeninis asmens tapatybės dokumentas, mobilusis vairuotojo pažymėjimas) išliks privatūs. Kartu ir visi jų naudojimo atvejai, pvz., tapatybės patvirtinimas perkant prekes ar paslaugas, pasirašant sutartis arba gaunant prieigą prie skaitmeninių paslaugų, bus apsaugoti nuo neautorizuotos prieigos ar atskleidimo. Duomenų, kuriais bus dalijamasi, tvarkymas bus griežtai reglamentuojamas. Tai reiškia, kad paslaugų teikėjai taip pat privalės laikytis visų asmens duomenų saugumo nuostatų. STD integruotame valdymo skydelyje bus registruojamas kiekvieno paslaugų teikėjo, su kuriuo buvo pasidalinti duomenys, sąrašas, duomenų ištrynimo prašymas ir kt. Todėl bus fiksuojami duomenys apie asmenis ir įstaigas, kurie turėjo prieigą prie asmens duomenų. Vartotojų patogumui ir skaidrumui užtikrinti visi duomenų naudojimo įrašai bus prieinami realiu laiku per STD mobiliąją aplikaciją. Tai leis vartotojui greitai pasiekti informacija, kada tik bus reikalinga – pavyzdžiui, atsekant paslaugų teikėjus, turėjusius prieigą prie duomenų ar siekiant suprasti, kaip buvo naudojami jo duomenys. Šis funkcionalumas užtikrina, kad duomenų tvarkymo procesai išliks saugūs, skaidrūs ir patikimi.

KYC. Užtikrinant finansų srities skaidrumą ir saugumą ypač svarbios harmonizuotos KYC taisyklės. Internetinėje aplinkoje itin sudėtinga užtikrinti efektyvų KYC politikos vykdymą. KYC politikoje paprastai reikalaujama, kad kliento tapatybė ir pinigų plovimo prevencijos procesų eigos įgyvendinimas būtų patvirtinti dokumentais (.pdf formatu), telefoniniu skambučiu ar elektroniniu

laišku. Skaitmeniniame kontekste, kai naudotojas nebūtinai pateikia tikslią asmeninę informaciją, patikrinti tapatybę pagal KYC standartus yra daug sudėtingiau. Naudojant STD finansinės institucijos gali patikimai patikrinti kliento tapatybę nuotoliniu būdu, kai klientas aktyviai dalyvauja realiu laiku.

Tikrinant vartotojo tapatybę STD sistemoje taip pat išvengiama su rankine duomenų patikra susijusių trūkumų. Automatinis informacijos autentiškumo tikrinamas vykdomas naudojant inovatyvius **kriptografinius metodus.** Finansų institucijos gaus tikslesnį ir išsamesnį klientų profilį, nes identifikacija bus atliekama realiuoju laiku ir be rankinio darbo. STD taip pat suteikia galimybę keistis KYC informacija tarp finansinių institucijų be papildomų ir brangių API (angl. *Application programming interface*) integracijų. Tai leis efektyviau ir ekonomiškiau vykdyti KYC reguliavimo reikalavimus, sumažinti administracines išlaidas ir padidinti kontrolės procesų efektyvumą. Kartu automatizuojant ir standartizuojant kontrolės procesus finansinėms institucijoms taps lengviau laikytis teisės aktų reikalavimų, nes sumažinama klaidų tikimybė bei administracinė našta. Vienodai visoje bendrijoje taikomos KYC taisyklės padės greičiau ir efektyviau patikrinti klientų tapatybę, taip sumažinant sukčiavimo riziką. Tai padės išvengti problemos, finansų įstaigų konkurencinė aplinka internetinės bankininkystės srityje trukdo veiksmingai įgyvendinti KYC praktiką.

Pinigų srautai ir ofšorinės sąskaitos. Vienas iš svarbiausių STD taikymo kovoje su pinigų plovimu aspektų yra rizikos, susijusios su neteisėtos veiklos perkėlimu į kitas šalis, minimalizavimas. Kaip jau minėta, nusikaltėliai gali vykdyti neteisėtą veiklą vienoje šalyje, tačiau savo pelną pervesti į kitą, kurioje galioja aukštas bankų informacijos slaptumo lygis, todėl sunku atsekti lėšų kilmę. Tokią praktiką dar labiau palengvina teisinių sistemų skirtumai ir teisėsaugos institucijų tarptautinio bendravimo sunkumai. Šiuo atveju STD taikymas labai svarbus, nes padeda patikimai nustatyti tapatybę ir su ja susijusius skaitmeninius dokumentus nepriklausomai nuo to, kurioje šalyje veikiama. Todėl sudaromos prielaidos efektyviam ir paprastesniam neteisėtos veiklos bei lėšų kilmės atsekimui.

Užtikrinant efektyvesnį pinigų kilmės atsekimo mechanizmą užkardomos finansiniams nusikaltėliams būdingos didelių sumų skaidymo arba pervedimo į ofšorines sąskaitas praktikos. Kaip žinoma, pinigų plovėjai dažnai suskaldo dideles pinigų sumas į mažesnes dalis, kad išvengtų papildomų bankų sąskaitų patikrų atliekant vienkartinę didelę finansinę operaciją. Šios mažesnės sumos yra įnešamos į bankomatą per daugelį kartų ar atliekamos bankinės transakcijos internetu slepiant tikrąją mokėjimų paskirtį. Ofšorinės sąskaitos dažniausiai atidaromos užsienio šalyse, kuriose galioja silpnesnė finansinė priežiūra arba aukštas bankų informacijos slaptumo lygis. Naudojant STD galima užtikrinti kiekvieno finansinio srauto skaidrumą, nes visi finansinių operacijų duomenys susieti su patvirtintomis tapatybėmis, todėl tampa galima lengviau identifikuoti asmenis, atliekančius operacijas į ofšorines sąskaitas. Pažangios šifravimo technologijos leidžia iš anksto patvirtinti ir saugoti informaciją apie kiekvieną atliktą finansinį veiksmą. Be to, naudojant algoritmus realiu metu analizuojami įtartinų veiklų požymiai, pvz., keistai pasikartojančios bankinės operacijos.

Kiekvienos finansinės operacijos susietumas su konkrečia tapatybe reiškia ir tai, kad STD ekosistema padeda nustatyti ir analizuoti struktūrizuotus pinigų pervedimus. Nors visos bankinės operacijos, nepriklausomai nuo STD naudojimo, turi būti stebimos ir analizuojamos, STD suteikia papildomą saugumo sluoksnį, užtikrinantį, kad visi finansiniai srautai būtų tiksliai atsekami iki konkretaus asmens ar organizacijos. Todėl minimalizuojamos anonimiškai vykdomos nelegalios finansinės veiklos galimybės. Su skaitmenine tapatybe susietais duomenimis apie finansines operacijas gali pasinaudoti tiek finansų, tiek teisėsaugos ir priežiūros institucijos.

Kalbant apie STD taikymą finansų sektoriuje daugiausiai akcentuojamos bankinės operacijos, tačiau verta atkreipti dėmesį ir į kitas finansų sektoriaus institucijoms. Pritaikant STD virtualių valiutų keityklų veikloje bus išvengta situacijų, kai dėl aukšto anonimiškumo lygio ir greito lėšų pervedimo sąveikaujama su aukštos rizikos zonomis ir klientais, kurių tapatybė lieka nežinoma. STD ekosistemoje klientų tapatybė yra patikimai nustatoma net atliekant nuotolinį patikrinimą. Tapatybės identifikavimui naudojami biometriniai duomenys, dviejų faktorių autentifikavimas (MFA) ir kiti saugumo mechanizmai. STD ekosistema sukurta pagal vieningą tapatybės patikrinimo standartą, tinkamą visoms virtualių valiutų keitykloms. Todėl tikėtina, jog sumažės pinigų plovimo atvejų susijusių su virtualių valiutų keityklomis.

Taip pat svarbu akcentuoti STD galimybes užkertant kelią neteisėtų lėšų įvedimui per finansų sistemą naudojant grynuosius pinigus nekilnojamojo turto sandoriuose, lošimo namuose ar internetinėse kazino platformose. Internetinės kazino platformos ir lošimo namai yra gerai žinomos, tačiau sunkiai įveikiamos finansų sistemos spragos, padedančios vykdyti pinigų plovimo veiklą. Todėl svarbu, kad STD sistemoje ir tokie veiksmai kaip grynųjų pinigų įnešimas, lošimo namų ar kazino operacijos bei nekilnojamojo turto sandoriai būtų vykdomi tik patvirtinus vartotojo tapatybę ir pateikus su ta veikla susijusius elektroninius dokumentus. STD sistema gali užtikrinti, kad visos finansinės operacijos būtų atliekamos tik po, kai vartotojo asmens tapatybė yra patikrinta kriptografiškai saugesniu būdu. Kita vertus, svarbu akcentuoti, kad toks visapusiškas STD taikymas užkertant kelią kritiškai svarbioms finansinių srautų kontrolės spragoms galimas tik tuo atveju, jei visi rinkos dalyviai sutaria naudoti STD sistemą.

Vartotojai. Vartotojams ne mažiau kaip ir finansinėms institucijoms svarbi apsauga nuo kibernetinių sukčių ir tapatybės vagysčių. STD taikomi kriptografiniai metodai padeda užtikrinti duomenų vientisumą ir apsaugą nuo klastojimo ar duomenų perėmimo. Kiekvienas bankinis pavedimas gali būti autentifikuotas, tai reiškia, kad sistema patvirtina tiek siuntėjo, tiek gavėjo tapatybę. Suteikus papildomą saugumo sluoksnį duomenų perėmimas yra praktiškai neįmanomas.

STD ekosistema padės vartotojams apsisaugoti nuo sukčiavimo taikant tarp kibernetinių nusikaltėlių paplitusį „phishing“ metodą, nes leis tiksliai patikrinti siuntėjo tapatybę ir gaunamo pranešimo autentiškumą, naudojant kriptografinius metodus. STD užtikrins, kad kiekvienas

siunčiamas elektroninis laiškas ar žinutė būtų pasirašyta skaitmeniniu būdu, o gavėjas galėtų patikrinti, ar siuntėjas yra autentiškas ir (ar) pranešimo turinys nebuvo pakeistas. STD sistema gali automatiškai identifikuoti įtartinus pranešimus ir įspėti vartotojus apie galimą grėsmę. Įtartini elektroniniai laiškai ar žinutės gali būti greitai atpažinti ir netgi automatiškai blokuojami, taip sumažinant kylančią sukčiavimo riziką ir apsaugant vartotojus nuo galimo pinigų praradimo. Naudojant STD patys vartotojai galės lengvai patikrinti e. laiškų ir kitų pranešimų autentiškumą, o tai padės apsisaugoti nuo „phishing“ atakų ir duomenų vagystės atvejų. Vartotojai turės galimybę įsitikinti, kad pranešimas tikrai yra iš teisėtos finansų institucijos. Tai mažins tikimybę apgauti vartotojus ir priversti juos atskleisti savo asmeninę informaciją.

STD gali būti efektyvi ir užkardant nusikaltimus vykdomus per mobiliąsias programėles. Mobiliosios programėlės (angl. *mobile application*) dažnu atveju tampa nusikaltėlių taikiniu, nes vartotojai nesugeba griežtai apsaugoti savo prieigos duomenų. Pažangios STD ekosistemos kriptografinės technologijos padės užtikrinti, kad naudotojų duomenys būtų saugūs ir neprieinami neteisėtam pasisavinimui.

Kalbant apie vartotojų interesus svarbu pabrėžti ir STD taikomą “self-sovereign identity” principą. Šis principas reiškia, kad pačiam vartotojui suteikiama tapatybės ir duomenų valdymo kontrolė. STD ekosistemoje tikrinant vartotojo tapatybę duomenys naudojami tik su vartotojo sutikimu. Tai reiškia, kad vartotojo duomenys nėra naudojami be jo žinios. Vartotojai gali pasirinkti, kada ir kokią informaciją atskleisti, taip sumažinant riziką, susijusią su duomenų nutekėjimu ar nusikalstamu panaudojimu. “Selective disclosure” funkcija leidžia vartotojams dalintis tik reikalinga informacija, nesuteikiant visų savo asmens duomenų, todėl naudojantiems STD suteikiamas aukšto lygio privatumas. Pabrėžtina, kad STD sistema naudoja decentralizuotų identifikatorių (DID) technologijas. Manoma, kad duomenų valdymo decentralizacija taip pat paskatins vartotojų pasitikėjimą skaitmeninėmis paslaugomis ir saugumą skaitmeninėje aplinkoje. Sistema užtikrina, kad asmens tapatybės informacija yra ne tik patvirtinama, bet ir apsaugoma nuo neteisėtos prieigos ar pakeitimo. Taikomas “High level of assurance” reikalavimas reiškia, kad tapatybės patikrinimai atliekami griežtai ir patikimai, užtikrinant aukščiausią saugumo lygį.

Teisėsaugos ir priežiūros institucijos. Kitas ne mažiau svarbus STD taikymo pinigų plovimo srityje aspektas – teisėsaugos ir priežiūros institucijų veikimo pokyčiai. Skaitmeninėje aplinkoje taikant STD teisėsaugos ir priežiūros institucijos įgyja daugiau galimybių užkardyti pinigų plovimo veiklą. Automatizuota informacijos identifikavimo ir (ar) analizės sistema leis greitai nustatyti tiek fizinius asmenis, tiek įmones, kurie kelia įtarimų, ir atitinkamai reaguoti, užkertant kelią manipuliacijoms bei sukčiavimui. Be to, automatiškai nustačius galimai kylančią riziką dėl duomenų klastojimo, sukčiavimo ir (ar) pinigų plovimo STD naudotojai turės galimybę operatyviai informuoti

teisėsaugos institucijas, kurios reaguodamos realiu metu galėtų atitinkamų veiksmų užkardyti nusikalstamą veiką.

Pinigų plovimo srityje veikiančioms viešojo sektoriaus institucijoms dažnai trūksta išteklių, tokių kaip profesionalūs darbuotojai ir informacijos valdymo sistemos, todėl svarbu paminėti, kad STD gali sumažinti pinigų plovimo prevencijai reikalingus išteklius. Išteklių taupymas susijęs ne tik su automatizuotais finansinių operacijų patikros ir stebėsenos procesais, bet ir su standartizuota tapatybės nustatymo ir informacijos valdymo sistema. Kitaip tariant, taikant vieningą tapatybės identifikavimo sistemą nėra reikalinga turėti skirtingas sistemas kiekvienoje šalyje. Naudojantis ta pačia infrastruktūra ženkliai mažėja profesionalių darbuotojų ir kitų išteklių poreikis. Mažėja kaštai ir reikalingi bendradarbiavimui tarp skirtingų šalių ir institucijų.

Bendradarbiavimas. STD yra svarbus įrankis, padedantis įveikti jurisdikcinius iššūkius susijusius su tarptautinio bendradarbiavimo trūkumu, nesuderintais kovos su pinigų plovimu standartais (ypač regionuose, kuriuose galioja silpna teisinė bazė). Kaip jau minėta, būtent vienodų reguliavimo standartų nebuvimas dažnai trukdo veiksmingam tarptautinių teisėsaugos ir reguliavimo institucijų bendradarbiavimui bei koordinavimui. Visos ES šalys turės vieningą ir suderintą taisyklių rinkinį, kuris padės sumažinti nenuoseklumus tarp skirtingų jurisdikcijų. Finansinės operacijos bus vykdomas laikantis vienodų standartų, nesvarbu, kurioje ES šalyje jos vyksta.

Visos ES šalys naudos tą pačią tapatybės nustatymo ir informacijos kaupimo sistemą, tai sumažins skirtingų teisinių sistemų keliamus sunkumus ir padės efektyviau kovoti su tarptautiniais nusikaltimais. Naudojant unifikuotą sistemą galima efektyviau nagrinėti tarptautinius prašymus suteikti informaciją ar apsikeisti duomenimis (dokumentais). Pavyzdžiui, dokumentai su EAA atributais galės būti tiesiogiai pasirašomi ir siunčiami kitoms ES šalims saugiu, tiksliu ir greitu būdu, taip užtikrinant efektyvesnį bendradarbiavimą tarp institucijų be poreikio kurti centralizuotas duomenų bazes. Vienodi standartai ir technologija sumažins informacijos apdorojimo laiką ir padidins tikslumą, nes duomenys bus lengvai prieinami ir suprantami visiems suinteresuotiems subjektams. Dėl to yra pagrįsta tikėtis, kad STD skatins geresnį tarptautinį bendradarbiavimą atliekant baudžiamąjį persekiojimą. Kartu turėdamos prieigą prie patikimos ir vieningos skaitmeninės tapatybės identifikavimo informacijos teisėsaugos institucijos gali greičiau ir efektyviau reaguoti į tarptautinius nusikaltimus.

Plėtojant tarptautinio teisėsaugos ir priežiūros institucijų bendradarbiavimą tikėtinas didesnis tarpusavio pasitikėjimas bei operatyvumas tiek tiriant jau įvykdytus nusikaltimus, tiek stiprinant pinigų plovimo prevenciją. Keičiantis informacija ir stiprinant tarptautinį bendradarbiavimą paprasčiau identifikuoti fizinius ir juridinius asmenis visoje ES, kadangi mažėja tikimybė tą patį asmenį ar juridinį vienetą laikyti skirtingu kitose jurisdikcijose. Taigi, vieninga skaitmeninė tapatybės

sistema ženkliai apribos galimybes kurti skirtingas tapatybes ir apeiti teisinį reguliavimą. Remiantis eIDAS reglamentu asmenys identifikuojami nuotoliniu būdu, nepriklausomai nuo jų buvimo vietos.

Svarbu pastebėti, kad STD pagrindu kuriama finansinių operacijų priežiūros standartizacija nebūtinai apsiribos tik bendrijos valstybėmis. STD gali veikti ir platesniu mastu, jei už bendrijos ribų esančios valstybės taip pat pripažins šį standartą. Nors prognozuojama, kad ES STD taps prieinamos iki 2027 m., jau esama pasiūlymų taikyti dėklę kaip pavyzdį būsimiems skaitmeninės tapatybės projektams už ES ribų. Dullaert ir kt. (2024) teigia, kad būtent ES STD turi potencialo tapti pasauliniu skaitmeninės tapatybės nustatymo standartu. Pažymėtina, kad nacionaliniu lygmeniu panašaus pobūdžio sistemos jau dabar yra įdiegtos įvairiose šalyse. Pavyzdžiui, Indija turi "Aadhaar" sistemą, Singapūras – "Singpass", Italija – savo skaitmeninės tapatybės sistemą, o JAV – skirtingas vairuotojų pažymėjimo sistemas.

Ribotumai ir išbandymai. Tolesnis eIDAS sistemos diegimas neatsiejamas nuo teisinės bazės kūrimo. Sistema jau yra patvirtinta EP, tačiau siekiant įtvirtinti ją kaip teisės aktą reikalingas ES Ministrų Tarybos patvirtinimas. Institucijoms priėmus galutinį reglamentą, įsigalios 6-12 mėnesių laikotarpis, per kurį bus parengti įgyvendinimo aktai (skirti ES šalims) ir deleguotieji aktai, kurie papildys pirminius teisės aktus. Numatoma, kad priimti 45 įgyvendinimo aktus ir 3 deleguotuosius aktus. Būtent šiems aktams įsigaliojus, ES valstybės narės privalės per 24 mėnesius suteikti savo piliečiams prieigą prie ES STD (Dullaert et al., 2024). Murray ir kt. (2024) teigia, kad siekiant sukurti visose valstybės narėse pripažįstamą skaitmeninės tapatybės sistemą, dar reikia įveikti nemažai barjerų. Skaičiuojama, kad šiuo metu tik 14 proc. svarbiausių ES viešųjų paslaugų palaiko tarpvalstybinį tapatybės nustatymą naudojantis skaitmenine tapatybe.

Dullaert ir kt. (2024) taip pat pabrėžia, kad STD yra svarbi inovacija skaitmeninės tapatybės srityje, tačiau šiuo metu valstybės narės yra tik pradiniame įgyvendinimo etape. Siekiant išbandyti ES STD ir užtikrinti saugų bei sklandų jos diegimą 2023 m. gegužės mėn. buvo pradėti keturi didelio masto bandomieji projektai. Šiuose bandomuosiuose projektuose dalyvauja apie 360 subjektų, įskaitant privačias bendroves ir valdžios institucijas iš 27 valstybių narių. Planuojama, kad šie bandomieji projektai bus vykdomi iki 2025 m. Bandomųjų projektų metu simuliuojamos kasdienės gyventojų situacijos, kai yra poreikis pasinaudoti STD, ir renkami atsiliepimai apie dėklės ekosistemos įgyvendinimą. Bandymuose renkama informacija, skirta padidinti skaitmeninės dėklės saugumą, sąveikumą ir bendrą dizainą. Bandomieji projektai padeda išsiaiškinti, kaip STD gali palengvinti prieigą prie vyriausybinių paslaugų (pvz., vairuotojo pažymėjimo paraiška, mokesčių deklaracija), siekiant atidaryti banko sąskaitą, įrodant tapatybę sudarant išankstinio ir vėlesnio apmokėjimo SIM kortelių sutartis, pasirašant sutartis, užsakant vaistų receptus, gaunant socialinės apsaugos išmokas ir kt.

Apibendrinant galima teigti, kad STD taikymas įvairiapusiškai praplėstų pinigų plovimo prevencijos galimybes, pirmiausiai dėl to, jog yra eliminuojami su rankine finansinių operacijų kontrolę susiję ribotumai. Automatinės analizės priemonės greitai nustatys neatitikimus ar įtartinus veiklos modelius su tiksliai nustatyta asmens tapatybe. STD leis efektyviai tikrinti lėšų kilmės šaltinius. Kartu automatizuoti patikrinimai ir standartizuoti metodai padidins finansų sektoriaus saugumą ir skaidrumą. Be to, STD sistema padės identifikuoti ir patikrinti įmones bei vartotojus, sumažinant fiktyvių įmonių ir anonimiškumo riziką. Informacijos apsauga ir jos apdorojimas naudojant dviejų faktorių autentifikaciją dar labiau sustiprina kovą su pinigų plovimu ir kitais finansiniais nusikaltimais. Remiantis eIDAS reglamentu visos ES šalys galės turėti vieningą reguliavimo standartą, kuris padės sumažinti jurisdikcinių skirtumų keliamus iššūkius. Tai ypač aktualu skatinant tarptautinį teisėsaugos ir priežiūros institucijų bendradarbiavimą, kuris yra būtina pinigų plovimo prevencijos prielaida. Siekiant išnaudoti STD privalumus pinigų plovimo prevencijoje svarbus tiek įvairių finansinių institucijų, tiek vartotojų suinteresuotumas naudotis šia ekosistema. Manytina, kad pažangios kriptografinės technologijos skatins vartotojų pasitikėjimą skaitmeninėmis paslaugomis. Išryškinant STD privalumus institucijoms akcentuojami saugumo, efektyvumo ir mažesnių kaštų aspektai.

3. SKAITMENINĖS TAPATYBĖS DĖKLĖS EFEKTYVUMO VERTINIMAS PINIGŲ PLOVIMO PREVENCIJOJE

Šioje darbo dalyje bus siekiama atsakyti į klausimą, ar STD taikymas gali pagerinti finansų įstaigų asmens tapatybės tikrinimo procesų efektyvumą. Antroje darbo dalyje buvo atskleista, kad STD ekosistema gali tapti vienu iš svarbių įrankių, siekiant pagerinti finansinių operacijų saugumą, kokybišką ir greitą klientų tapatybės identifikavimą, skaitmeninių dokumentų pateikimą ar pasirašymą, todėl bus siekiama palyginti vieną iš pagrindinių KYC metodų – klientų įvedimą (angl. "onboarding") ir įvertinti, koks yra STD poveikis tapatybės nustatymo greičiui, operacijų atlikimo efektyvumui ir tikslumui. 3.1 poskyryje, bus vertinama, kaip finansų institucijos vykdo nagrinėjamą procesą šiuo metu, nenaudodamos naujo skaitmeninio tapatybę patvirtinančio dokumento (PID) ir Skaitmeninės Tapatybės Dėklės. 3.2 poskyryje tas pats procesas bus vertinamas naudojant PID ir STD, kaip visos Europos Sąjungos skaitmeninės ekosistemos dalį.

3.1. Nuotolinio asmens tapatybės nustatymo vertinimas finansų įstaigose užtikrinant pinigų plovimo prevenciją

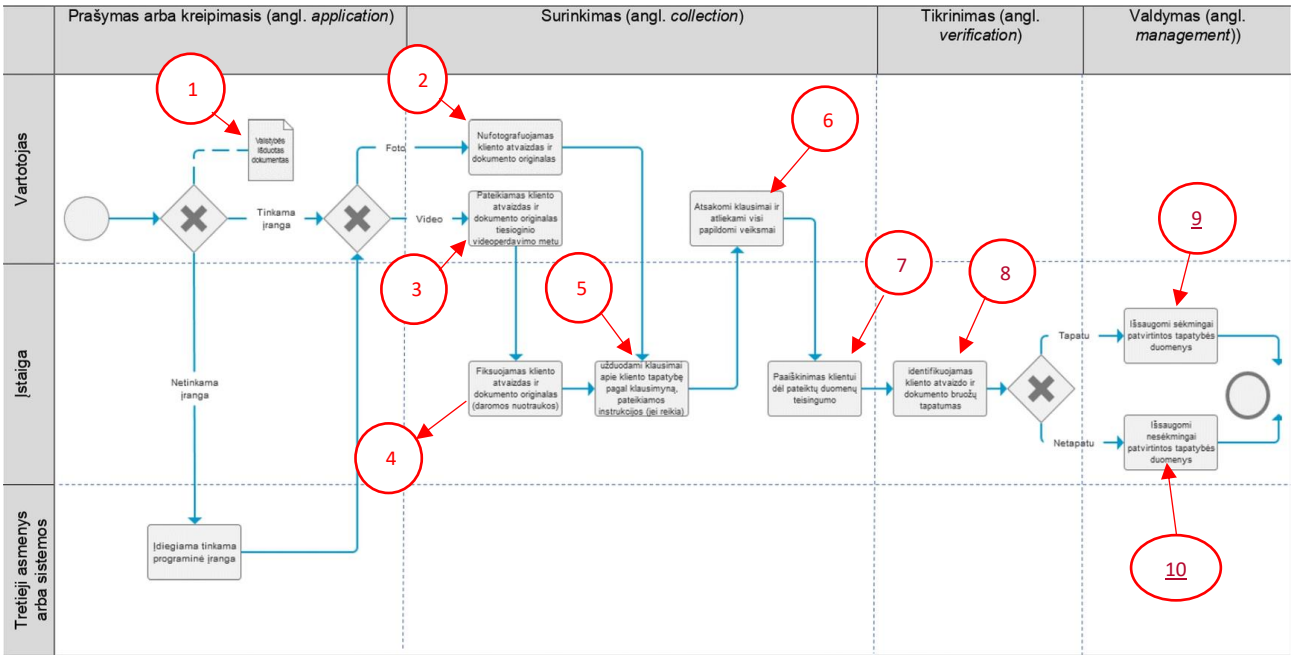
Asmens tapatybės nustatymas finansų įstaigose, tiek finansų technologijų (FinTech) startuoliuose, tiek tradiciniuose bankuose, yra viena iš pagrindinių priemonių, padedančių užtikrinti teikiamų paslaugų saugumą ir teisėtumą. Asmens tapatybės nustatymui ypatingą dėmesį skiria ir finansų rinkos reguliuotojai. Šis procesas nėra tik formalus žingsnis, bet ir kompleksinis veiksmas, reikalaujantis tikslumo ir patikimumo.

Finansų sektoriuje asmens tapatybės nustatymas vykdomas pagal griežtą nacionalinio ir tarptautinio lygmens reglamentavimą. Remiantis KYC principais reikalaujama, kad finansinės institucijos, identifikuotų savo klientus remiantis patikimais šaltiniais ir metodais, dar prieš pradedant bet kokius dalykinius santykius (pvz., banko sąskaitos atidarymą ar paskolos gavimą). KYC procedūros taikomos ne tik siekiant nustatyti tapatybę, bet ir įvertinant finansines rizikas, užkertant kelią neteisėtai veiklai, tokiai kaip pinigų plovimas ar terorizmo finansavimas.

KYC metodų veiksmų seka apima kelis žingsnius. Paprastai tapatybės nustatymo procesas prasideda kliento nuo asmens apsilankymo finansų įstaigoje arba atliekant tapatybės patikrinimo procedūras nuotoliu, t. y., internetu. Klientas visada turi pateikti tapatybę identifikuojantį dokumentą, tokį kaip asmens tapatybės kortelė ar pasas. Asmens tapatybės tikrinimo procesai gali vykti ir fiziškai klientui dalyvaujant finansų įstaigoje, pateikiant tapatybės patvirtinantį dokumentą, o vėliau rankiniu būdu yra tikrinami specialistų, t. y., kopijuojami ar skenuojami tolimesniam patikrinimui ir šių duomenų saugojimui. Jei procesas vyksta internetu, klientas turi įkelti skaitmenines dokumentų kopijas (įskaitant ir paso nuotrauką), o įkelti skaitmeniniai dokumentai (duomenys) turi būti

patikrinti, paprastai pasinaudojant trečiųjų šalių paslaugomis (pvz., „Ondato“ ar „Onfido“). Taip pat išsamesniam patikrinimui kliento gali būti prašoma pateikti papildomą informaciją, pvz., gyvenamosios vietos adreso patvirtinimą arba banko sąskaitų išrašus iš kitų finansinių įstaigų. Dėl sudėtingų reguliavimo reikalavimų bei didelio kiekio rankinio informacijos tikrinimo KYC procesai dažnai yra lėti ir sudėtingi. Tai gali sukelti klaidų riziką ir apsunkinti visą asmens tapatybės tikrinimo proceso sklandumą.

Šiuo metu finansų įstaigose tapatybės nustatymo procesai dažnai atliekami nuotoliu (kliento veido fotografavimas ir dokumentų fotografavimas iš abiejų pusių). Kaip jau minėta pirmoje šio darbo dalyje, šie procesai yra patogūs klientui, tačiau finansų įstaigoms vis dar prireikia atlikti nemažai rankinio darbo, susijusio su papildomais patikrinimais ar duomenų apdorojimu. Procesas iliustruojamas žemiau pateikiamoje schemoje (žr. 6 pav.)



Šaltinis: Prieiga per internetą: https://www.lb.lt/lt/media/force_download/?url=%2Fuploads%2Fdocuments%2Ffiles%2Fmusu-veikla%2Fmokejimai%2FApie-mokejimu-rinka%2FMokejimu-taryba%2FNaujos+tapatybes+patvirtinimo+priemones.pdf

6 pav. Nuotolinio asmens tapatybės nustatymo proceso schema

Pateiktoje schemoje yra identifikuoti pagrindiniai veiksmai, atliekami finansų įstaigose, vykdant asmens tapatybės nustatymą, kuris yra KYC procedūrų dalis, siekiant užtikrinti teisės aktų atitiktį ir saugumą. Pavaizduotas procesas taikomas ir tolimesnėje analizėje, hipotetiškai vertinant jo vykdymą, pasinaudojant ES 2024 m. gegužės mėn. įteisintu PID, panaudojant STD ekosistemą.

Analizuojamo proceso veiksmai atliekami šia seka:

Veiksmas Nr. 1 – Vartotojas kreipiantis į finansų įstaigą dėl paslaugų gavimo jo yra prašoma pateikti savo valstybės išduotą asmens tapatybę patvirtinantį dokumentą, t. y., pasą arba asmens tapatybės kortelę. Vykdomas pirminis tapatybės patikrinimo ir informacijos registravimo etapas.

Nuotoliu bendraujant su finansų įstaigos darbuotoju, klientas vykdo tolimesnius veiksmus, pateiktoje schemoje jo tapatybei patvirtinti ir paslaugų teikimui užtikrinti. Remiantis "Onfido" pateiktu paaiškinimu (KYC process steps, 2022), dokumentų pateikimo, tikrinimo ir įsitikinimo, ar yra bendraujama su tuo žmogumi, trukmė paprastai neviršija 10 sekundžių.

Veiksmas Nr. 2 – Klientas nufotografuoja savo veido atvaizdą ir asmens tapatybės dokumentą (iš abiejų pusių). Šis duomenų surinkimo veiksmas, remiantis "Ondato" paaiškinimu (Everything You Need to Know about KYC), tai gali trukti iki 60 sekundžių, tačiau su vaizdo kokybe susiję trikdžiai gali prailginti šį duomenų pateikimo etapą.

Veiksmas Nr. 3 – Realiuoju laiku vykdoma duomenų surinkimo proceso dalis, kai klientas vaizdo skambučio metu siekia įrodyti savo tapatybę, parodydamas savo asmens tapatybės dokumentą. Vaizdo skambučio duomenys yra analizuojamas dėl galimų bandymų apsimesti kitu asmeniu. Šis veiksmas padeda išvengti tapatybės klastojimo ir sukčiavimo atvejų.

Veiksmas Nr. 4 – Klientas vaizdo perdavimo metu pateikia savo atvaizdą ir asmens tapatybės dokumentą (veiksmas Nr. 3), finansų įstaiga per kelias sekundes, taip pat remiantis tuo pačiu "Onfido" pateiktu paaiškinimu (KYC process steps, 2022), užfiksuoja šiuos duomenis, siekiant užtikrinti kliento tapatybės tikslumą ir atitiktį teisės aktų reikalavimams.

Veiksmas Nr. 5 – Užfiksavus kliento pateiktus duomenis (schemos veiksmus Nr. 2 ir Nr. 4) finansų įstaiga klientui pateikia klausimyną, kuriuo siekiama surinkti papildomą informaciją apie jo tapatybę, finansinę istorija ir (ar) darbo veiklą. Remiantis „Keler CCP Ltd" atliktu tyrimu *(*User guide to completing the risk KYC questionnaire) ir „Visma Creditro" duomenimis, priklausomai nuo klausimų apimties ir sudėtingumo užduodamų klausimų trukmė gali trukti nuo 2 iki 4 minučių. Trukmė gali būti ilgesnė, jei kyla papildomų klausimų arba reikia daugiau laiko atsakymams pateikti.

Veiksmas Nr. 6 – Klientui atsakius į pateiktus klausimus ir finansų įstaigai iškilus abejonėms dėl pateiktų kliento duomenų (atsakymų) teisingumo, gali būti prašoma pateikti papildomus atsakymus arba pateikti papildomus dokumentus, padedančius patvirtinti asmens tapatybę. Šio etapo atlikimas klientui gali trukti nuo 2 iki 5 minučių. Remiantis Lietuvos banko studija „Naujų tapatybės patvirtinimo priemonių galimybių ir atitikties pinigų plovimo prevencijos tikslams problematika, 2019 m." pateiktų duomenų (pvz., klausimyno) teisingumas turi būti patvirtinamas bent pažangiuoju elektroniniu parašu, pagal eIDAS reglamentą (ES Nr. 910/2014), tai būtina atlikti nedelsiant, ne vėliau nei per 1 valandą.

Veiksmas Nr. 7 – Klientas informuojamas, ar jo pateikti duomenys yra teisingi ir teisėti, ir (ar) atitinka KYC reikalavimus. Finansų įstaiga nedelsiant praneša klientui apie bet kokius galimus neatitikimus ar klaidas pateiktoje informacijoje. Jei pateikti duomenys ar dokumentai yra netikslūs arba netinkamai pateikti, gali būti suteiktos rekomendacijos, kaip ištaisyti neatitikimus.

Veiksmas Nr. 8 – Finansų įstaigai nuotoliniu būdu surinkus visus pateiktus kliento duomenis, toliau pradedamas tikrinimas (angl. *Verification*), kliento atvaizdo ir dokumento bruožų tapatumo palyginimas. Finansų įstaigai naudojant specializuotas programines įrangas šis etapas, remiantis įvairių technologijų kompanijų, kurios kuria sprendimus, susijusius su KYC procedūromis, gali trukti iki kelių sekundžių, priklausomai nuo sistemos našumo ir pateiktų duomenų vaizdo kokybės. Tačiau jeigu specializuotos programos aptinka neatitikimus tarp kliento pateiktų duomenų, šis tapatybės tikrinimo etapas reikalauja papildomos patikros. Tokiu atveju gali būti reikalingas duomenų tikrinimas rankiniu būdu, t. y., įsikišant žmogui. Žmogiškasis faktorius įtraukiamas tik tuomet, kai specializuotos programos nėra pakankamos problemai išspręsti.

Veiksmas Nr. 9 – Kliento pateikti asmens tapatybės duomenys, tokie kaip vardas, pavardė, gyvenamasis adresas ir skaitmeniniai dokumentai yra išsaugomi finansų įstaigos duomenų bazėje, po to, kai jie yra sėkmingai patikrinti ir teisingi. Kliento tapatybės duomenų išsaugojimas finansų įstaigos duomenų bazėse vyksta iškart, ypač jei naudojama centralizuota duomenų bazė. Išsaugojimo trukmė gali nežymiai kisti priklausomai nuo sistemos našumo bei duomenų kiekio.

Veiksmas Nr. 10 – Jei tapatybės patvirtinimas nepavyksta dėl tam tikrų neatitikimų, tarp kliento pateiktų duomenų, tokia informacija apie neatitikimus taip pat yra nedelsiant išsaugoma, tačiau duomenys žymimi kaip “nepatvirtinti” arba “atmesti”. Šis duomenų tvarkymo veiksmas yra itin svarbus dėl būtinų reguliacinių reikalavimų, susijusių su pinigų plovimo prevencija ir kovos su terorizmo finansavimo įstatymais. Šis etapas taip pat įvykdomas iškart.

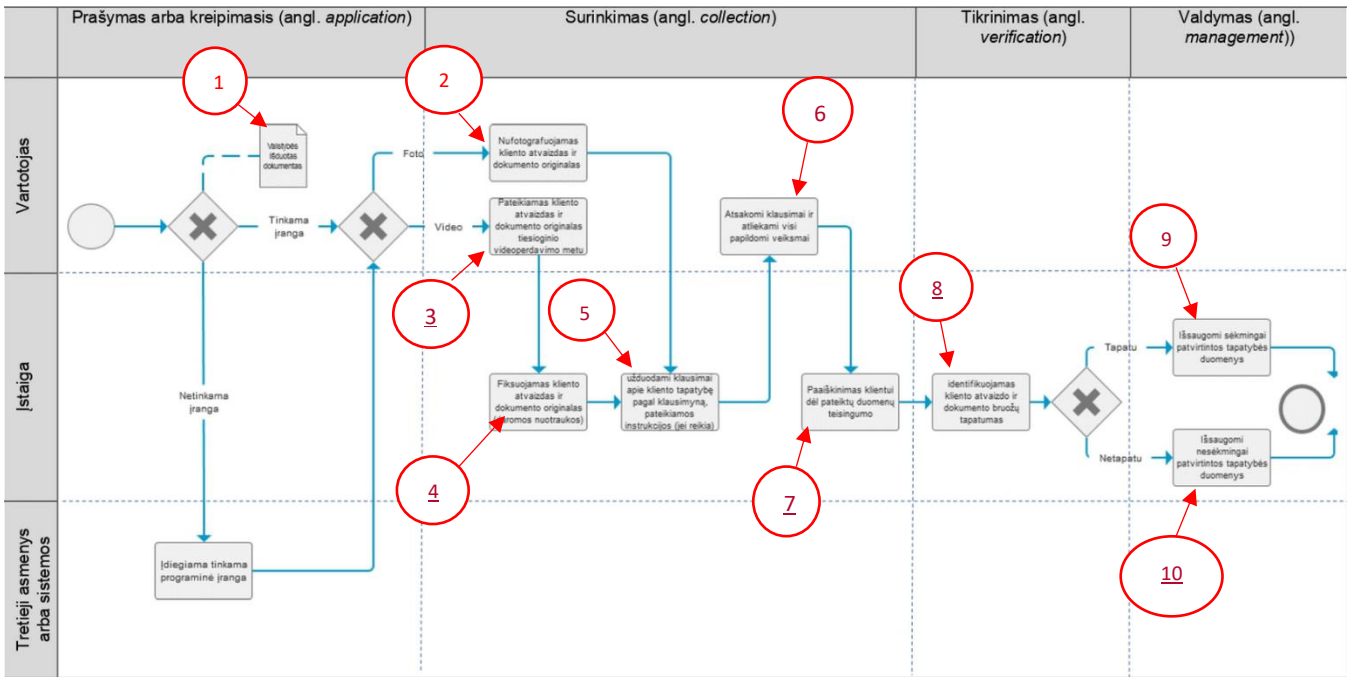
Apibendrinant galima teigti, kad asmens tapatybės nustatymas finansų institucijose yra esminis procesas, užtikrinantis teisėtą ir saugų finansinių paslaugų teikimą. Taikant šiuo metu paplitusius KYC metodus vis dar yra susiduriama su žmogiškojo faktoriaus klaidomis. Galimi rankinio darbo trūkumai ir klaidos kelia papildomų rizikų, susijusiu su sukčiavimu ir neteisėta veika. Taip pat ir šiuo metu atliekant nuotolinį asmens tapatybės identifikavimą reikalingos ilgos patikrinimo procedūros, įskaitant nuotolinį dokumentų kopijos pateikimą ir veido atvaizdo atpažinimą. Procesą dažnai prailgina techniniai trikdžiai ar papildomos patikros poreikis. Tokiems tapatybės patikrinimo procesams kaip dokumentų fotografavimas, veido atpažinimas ir kt., reikalingas darbuotojo įsitraukimas, dėl ko nėra užtikrinamas pakankamas efektyvumas, saugumas ir proceso įvykdymo greitis. Todėl KYC metodai ne visuomet padeda užtikrinti optimalų saugumo ir greičio balansą, ypač didelio masto finansų paslaugų sektoriuje. Todėl manytina, kad finansinėms įstaigoms reikalingi alternatyvūs, greitesni ir efektyvesni KYC sprendimai.

3.2. Asmens tapatybės nustatymo procesas naudojant Skaitmeninės Tapatybės Dėklę

Darant prielaida, kad STD naudojimas gali smarkiai pagerinti finansinių įstaigų klientų įvedimo procesą (angl. *onboarding*), bus atliekamas 3.1 skyriuje nagrinėto proceso vykdymo tyrimas naudojant STD. Klientų įvedimo metu atliekamas ne tik asmens tapatybės nustatymas, bet ir eigoje, vertinamos finansinės veiklos rizikos, kad būtų siekta užtikrinti, jog klientas nesinaudotų finansinėmis priemonėmis nelegaliai veiklai.

Atliekant STD tyrimą bei lyginant su šiuo metu finansų įstaigose taikomu KYC metodu – nuotoliniu asmens tapatybės nustatymu, pirmiausia būtina apibrėžti, kaip vyksta tapatybės nustatymo procesas, naudojant STD ekosistemą. Kaip jau minėta, naudojant STD ekosistemą kiekvienas tapatybės patvirtinimo žingsnis yra valdomas paties vartotojo. Per šią ekosistemą asmuo turi saugią prieigą prie savo asmens tapatybės duomenų skaitmeninu formatu ir gali savarankiškai nuspręsti, kokius duomenis jis nori dalintis su pasikliaujančia šalimi (angl., *Relying Party*), išvengiant perteklinės informacijos atskleidimo. STD ekosistema taip pat leidžia tapatybės nustatymo etapus atlikti ženkliai greičiau ir su mažesne klaidų rizika. Tai ne tik supaprastina tapatybės patikrinimo veiksmus, bet ir pagerina visų atliekamų etapų eiliškumo saugumą, užtikrindama, kad duomenys bus pasiekiami tik įgaliotų institucijų. Taip pat svarbu paminėti, kad ši ekosistema palengvina saugų vartotojo (kliento) identifikavimą ir autentifikavimą aukštu užtikrinimo lygiu (angl. *High Level of Assurance*, LoA) įvairioms viešosios ir privačiosioms internetinėmis paslaugomis, remiantis techniniu Europos Sąjungos Skaitmeninės Tapatybės Dėklės ARF (The Architecture and Reference Framework) dokumentu.

7 paveiksle pateikta schema atskleidžia galimus asmens tapatybės nustatymo proceso ypatumus naudojantis ES STD (žr. 7 pav.).



Šaltinis: Prieiga per internetą: https://www.lb.lt/lt/media/force_download/?url=%2Fuploads%2Fdocuments%2Ffiles%2Fmusu-veikla%2Fmokejimai%2FApie-mokejimu-rinka%2FMokejimu-taryba%2FNaujos+tapatybes+patvirtinimo+priemones.pdf

7 pav. Asmens tapatybės nustatymo procesas naudojant ES STD

Veiksmas Nr. 1 – Lyginant su šiuo metu atliekamu KYC etapu, kuris aprašomas 2.2. poskyryje, pagrindinis skirtumas yra tai, kad fiziniam asmeniui bus išduodamas skaitmeninis tapatybės patvirtinimo dokumentas (PID), naudojamas su STD norint gauti tiek viešas, tiek privačias paslaugas. Tapatybės identifikavimas, kuomet klientas, kreipdamasis į finansų įstaiga ir pateiks skaitmeninį tapatybės patvirtinimo dokumentą (PID), esantį savo mobiliajame įrenginyje (STD), gali užtrukti vos keletą sekundžių.

Veiksmas Nr. 2 – Naudojantis STD klientams nereikės pateikti savo veido atvaizdo ar atlikti asmens dokumentų nuotraukų, kaip tai yra daroma šiuo metu. STD ekosistema automatiškai identifikuos asmenį ir autentifikuos kliento tapatybę su pateiktu PID. Šis tapatybės identifikavimo etapas užtruks vos kelias sekundes.

Veiksmas Nr. 3 – Naudojant STD klientui nereikės atlikti asmens tapatybės identifikavimo etapo vaizdo skambučio metu. Su STD ekosistema taip pat bus leidžiama, vartotojo mobiliajame įrenginyje atlikus vos keletą paspaudimų, patikimai ir automatiškai identifikuoti asmenį ir jo tapatybę remiantis pateiktu PID. Šis etapas taip pat vyksta realiuoju laiku, užtikrinant tapatybės klastojimo ir sukčiavimo prevenciją.

Veiksmas Nr. 4 – Naudojant STD, finansinėms įstaigoms nereikia atlikti duomenų surinkimo etapo, nes visi būtini duomenys apie klientą yra saugiai pateikiami ir prieinami tiesiai per STD ekosistemą. Praleidus šiuos perteklinius žingsnius, kurie taikomi šiuo metu, kartu mažėja ir potenciali klaidų rizika. Dėl pažangių šifravimo technologijų klientui naudojantis STD finansinei įstaigai perduodami asmens duomenys yra patikimi ir saugūs.

Veiksmas Nr. 5 – Šio duomenų surinkimo etapas finansų įstaigoms gali būti ženkliai pagreitinamas, nes panaudojant STD ir jos ekosistemą, klientui suteikiama galimybė automatiškai iš STD pateikti visus reikiamus duomenis ar dokumentus. Visi klientui reikalingi papildomi duomenys (dokumentai) gali būti pateikti greitai ir saugiai užtrunkant vos kelias sekundes. Esant poreikiui klientai, pasinaudodami STD ekosistema, gali papildomai pasirašyti reikalingus dokumentus. Naudojantis STD sumažina šio etapo klaidų ir duomenų nutekėjimo rizika.

Veiksmas Nr. 6 – Naudojantis STD klientams nebus būtina atlikti šio etapo, nes visa reikalinga informacija automatiškai pasiekiama per STD, vos tik klientas atlieka tapatybės patvirtinimo procesą su PID. Papildomi dokumentai ar duomenys gali būti pateikti per STD ekosistemą ir pasirašyti kvalifikuoti elektroniniu parašu, kuris turi tokia pat teisinę galią kaip ir ranka pasirašyti dokumentai. Šis etapas trunka tik keletą sekundžių, nes papildomi veiksmai atliekami

pasinaudojant STD ir kvalifikuotu elektroniniu parašu yra tvarkomi saugiai ir patikimai atitinkant visus reikalavimus pagal eIDAS reglamentą (Nr. 2024/1183).

Veiksmas Nr. 7 – Naudojant STD finansinėms įstaigoms nereikės informuoti kliento apie jo pateiktų duomenų teisingumo, nes STD užtikrina tiesioginį ir patikimą duomenų prieinamumą. Klientas savo STD ekosistemos aplinkoje gali matyti, kokius dokumentus pateikė ir (ar) juos pasirašė naudojant kvalifikuotą elektroninį parašą, kuris atitinka eIDAS reglamentą (Nr. 2024/1183). Kartu klientas gali matyti, kokia informacija yra pateikta ir pasidalinta su finansinėmis įstaigomis ar kitoms pasikliaujančiomis šalimis. Šis etapas visiškai užtikrina aukštą skaidrumo ir privatumo lygį, atitinkant eIDAS (Nr. 2024/1183) reglamento reikalavimus bei techninį ES STD ARF (The Architecture and Reference Framework) dokumentą.

Veiksmas Nr. 8 – Šį veiksmą finansų įstaigoms atlikti su STD taip pat nebūtina, kadangi naudojant STD, asmens tapatybės duomenys (PID) yra patikimi ir saugūs, atitinkantys keliamus reikalavimus pagal atnaujintą eIDAS reglamento dokumento versiją (Nr. 2024/1183) ir techninį ARF (The Architecture and Reference Framework*)* dokumentą.

Veiksmas Nr. 9 – Finansinės įstaigos šį duomenų valdymo etapą gali atlikti automatizuotai ir efektyviai. Atitinkami finansinių įstaigų IT padaliniai pirmiausia patikrina iš STD gautus dokumentus ir jeigu visi duomenys atitinka keliamus reikalavimus, gali vykti automatizuotas dokumentų tvarkymas. Patvirtinti tapatybės duomenys yra automatiškai išsaugomi, o visa informacija realiu laiku užfiksuojama, užtikrinant aukštą apsaugos lygį.

Veiksmas Nr. 10 – Naudojant STD šiame etape pateikti kliento duomenys ir dokumentai, finansų įstaigoje yra tikrinami automatiškai, kaip tai yra daroma ir šiuo metu. Kiekvienas duomenų rinkinys gali būti priimtas arba atmestas, priklausomai nuo įvairių kriterijų, pvz., ar dokumentas išduotas kvalifikuoto teikėjo (Q)EAA, ir ar atitinka nustatytą patikimumo lygį. Jei tapatybės duomenys ar pateikti skaitmeniniai dokumentai, neatitinka reikalavimų, jie fiksuojami, kaip nepraėję automatinio patikrinimo. Tokiu atveju klientas realiu laiku yra informuojamas apie nepavykusį dokumento patvirtinimą, galimai pateikiant konkrečias priežastis, dėl kurių duomenys buvo atmesti. Klientui taip pat nurodoma, kokius papildomus veiksmus reikėtų atlikti, kad dokumentas atitiktų reikalavimus – pvz., pateikti dokumentą, išduotą kitos institucijos ar aukštesnio patikimumo lygio šaltinio, kaip numatyta eIDAS reglamento (Nr. 2024/1183) reikalavimuose. Šis duomenų valdymo etapas užtikrina, kad finansų įstaigos galėtų efektyviai tvarkyti tik patikimus ir teisėtus klientų duomenis, garantuojant aukštą saugumo ir atitikties standartą.

Apibendrinant galima teigti, kad STD naudojimas finansų įstaigose, atliekant klientų įvedimą, duomenų surinkimo ir tikrinimo etapus tampa greitesnis, tikslesnis ir saugesnis. STD leidžia atsisakyti tam tikrų šiuo metu atliekamų duomenų surinkimo etapų, kadangi klientai dalijasi patvirtintais, realiu laiku prieinamais duomenimis ir (ar) dokumentais, o finansų įstaigos gali greitai

patikrinti dokumentų patikimumą ir kilmę. Taip pat klientams suteikiamos galimybės kontroliuoti savo duomenis ir matyti informaciją, kuria buvo pasidalinta, taip užtikrinant aukštą skaidrumo lygį.

3.3. Eksperimentinio tyrimo eiga. STD panaudojimas KYC metoduose

Eksperimentinio tyrimo metu buvo surinkti ir panaudoti realūs finansinių įstaigų, klientų įvedimo (angl. *onboarding*) etapų duomenys, remiantis finansinių technologijų įmonių statistika, praktika bei viešai prieinama mokslinių šaltinių įžvalga, išdėstyta 3.1 skyriuje. Atkreiptinas dėmesys ir į papildomą, viešai pateiktą informaciją apie naujausius finansų technologijų (FinTech) atliktus statistinių tyrimų skaičiavimus. Pavyzdžiui, organizacija "Regula", kuri padeda įstaigoms (įskaitant ir finansų) palengvinti asmens dokumentų autentifikavimą ir tapatybės patvirtinimą, savo ataskaitoje (Digital Onboarding: Definition, Benefit & How It Works, 2023) pabrėžia, kad sėkmingas klientų įvedimas į finansų įstaigą užtrunka vos kelias minutes.

Remiantis „FinTech Global" pranešimu (UBS links with Regula to automate onboarding, 2022), Šveicarijoje esantis bankas „UBS", bendradarbiaudamas su „Regula", sukūrė skaitmeninio prisijungimo paslaugą, kuri automatizuoja klientų registraciją 24 valandas per parą, 7 dienas per savaitę. Šis sėkmingas klientų įvedimas į įstaigą taip pat trunka vos kelias minutes. Viešai prieinamoje „Innovatrics" ataskaitoje (Onboarding report, 2020) rodoma, kad sėkmingas kliento įvedimas į finansų įstaigą vidutiniškai trunka apie 2 minutes (į šį proceso diapazoną patenka kliento atvaizdo nuotrauka ir dokumento nuotrauka iš abiejų pusių).

Todėl remiantis šiame skyriuje aukščiau pateiktais duomenimis ir informacija, atliekant eksperimentinį tyrimą, pasirinktas preliminarus kliento įvedimo į finansų įstaigą laikas yra iki 5 minučių, tačiau atsižvelgiant į pinigų plovimo prevencijos reikalavimus, kurie taikomi finansų įstaigoms, šis laikas gali užtrukti ir ilgiau, priklausomai nuo kliento duomenų pateikimo, dokumentų tikrinimo iki sėkmingos tapatybės patvirtinimo. Taip pat atliekant eksperimentinį tyrimą buvo remtasi pagrįsta ataskaita iš "PwC" (Next-Generation Client Onboarding), kurioje pateikiami apklausos rezultatai apklausus 41 ekspertus iš 26 finansinių institucijų. Ataskaitoje atskleisti esminiai iššūkiai susiję su klientų įvedimo procesu. "PwC" tyrimo rezultatai parodo, kad net 49 proc. viso kliento įvedimo į finansų įstaigą laiko klientai skiria atsakinėdami į užduodamus klausimus pagal klausimyną. Taip pat 15 proc. laiko užtrunka pasikartojančių ar papildomų duomenų bei dokumentų pateikimas.

Atliekant eksperimentinį tyrimą surinkti duomenys apie pagrindinius etapus ir trukmę sekundėmis leido atlikti išsamią analizę atsižvelgiant į skirtingą procesų trukmės veiksmų diapazoną. Veiksmai, kurie pateikti 6 ir 7 paveiksluose, buvo identifikuoti kaip pagrindiniai klientų asmens dokumentų surinkimo ir duomenų tikrinimo veiksmų etapai, atliekami nuotolinio asmens tapatybės

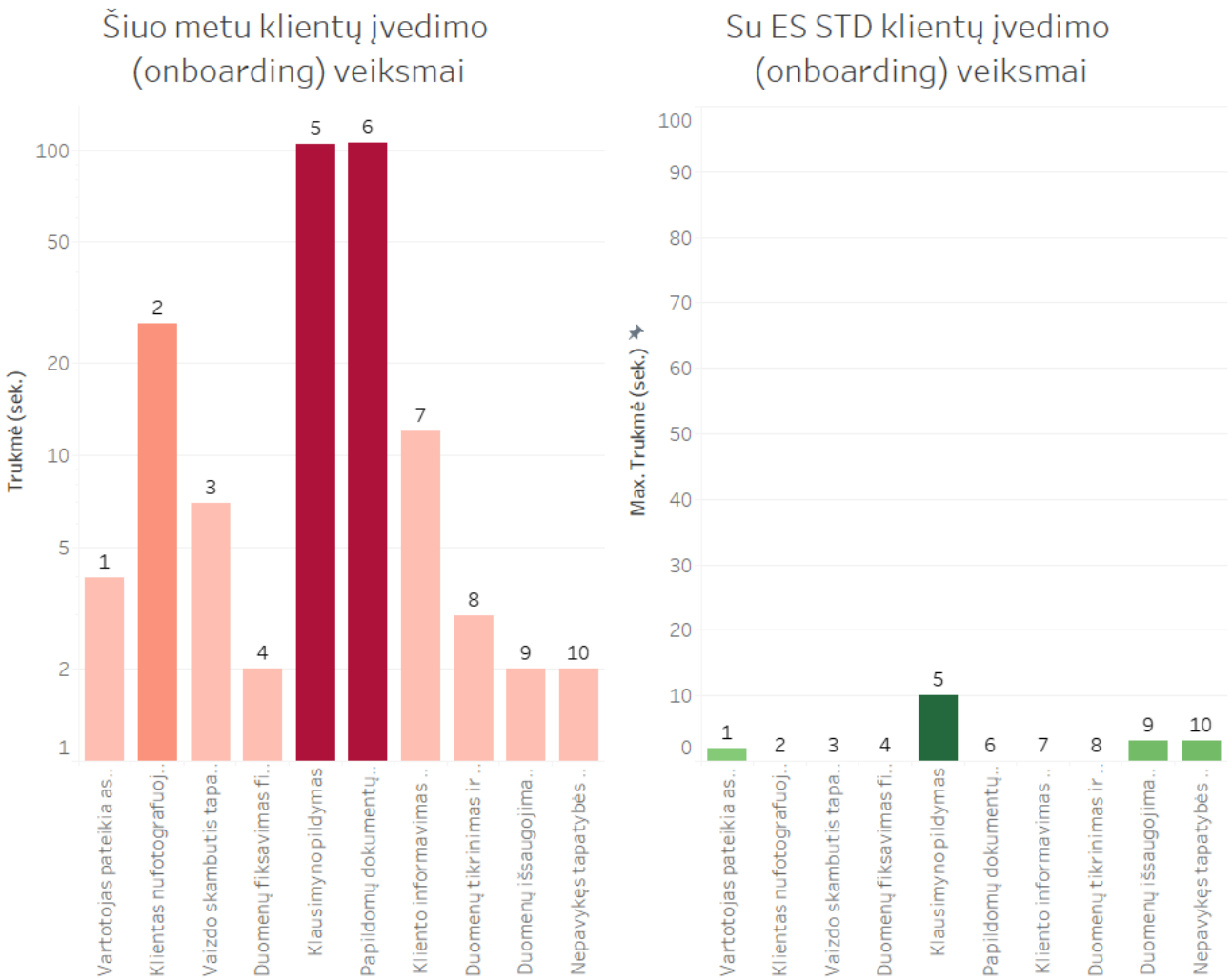
nustatymo metu. Žinoma, reikia atsižvelgti, kad kiekvieno atliekamo veiksmo etapo trukmė gali nežymiai varijuoti.

Eksperimentinio tyrimo eigoje klientų įvedimo į finansų įstaigą surinkti pirminiai duomenys iš įvairių šaltinių buvo nestruktūrizuoti, todėl pirmas žingsnis buvo juos struktūrizuoti, naudojant skaičiavimo ir analizės įrankį "Microsoft Excel". Šios programinės įrangos pagalba duomenys buvo susisteminti, suvienodinti pagal bendrą veiksmų seką, nuo veiksmas Nr. 1 iki veiksmas Nr. 10. Sukūrus vienodą duomenų rinkinį, vyko tolimesnis jų perkėlimas į duomenų vizualizavimo ir analizės įrankį "Tableau". Naudojant "Tableau" duomenys suskirstyti pagal kiekvieną atliekamą kliento įvedimo veiksmų etapų trukmę sekundėmis. Tai leido atlikti aiškią proceso veiksmų analizę.

Kiekvieno atliekamo kliento įvedimo veiksmų etapų reikšmės buvo pateiktos atskirai, siekiant išryškinti veiksmų trukmės skirtumus. Analizės rezultatai vaizduojami 8 paveiksle, atskleidžiant esminius skirtumus tarp šiuo metu atliekamo klientų įvedimo į finansų įstaigą veiksmų etapų (duomenų surinkimas ir tikrinimas) ir etapų, kurie būtų vykdomi pritaikius Europos Sąjungos STD.

Analizės rezultatai parodė, kad dabartiniai klientų įvedimo į finansų įstaigas etapai (Žr. 8 Pav., "Šiuo metu klientų įvedimo (onboarding) veiksmai") yra pastebimai ilgesni lyginant su ES STD funkcionalumu. Vidutiniškai visas kliento įvedimas į finansų įstaigą procesas šiuo metu užtrunka apie 4,5 minutes (~269 sekundės). Nustatyta, kad veiksmas Nr. 5 (klausimų pateikimas pagal klausimyną) ir veiksmas Nr. 6 (papildomų klausimų ar dokumentų pateikimas klientui) sudaro reikšmingą dalį ir prailgina visą proceso laiką, kartu užimdami apie 3,5 minutės (~210 sekundžių). Tai reiškia, kad abu šie veiksmai lemia apie 78 proc. viso šiuo metu atliekamo klientų įvedimo proceso laiko.

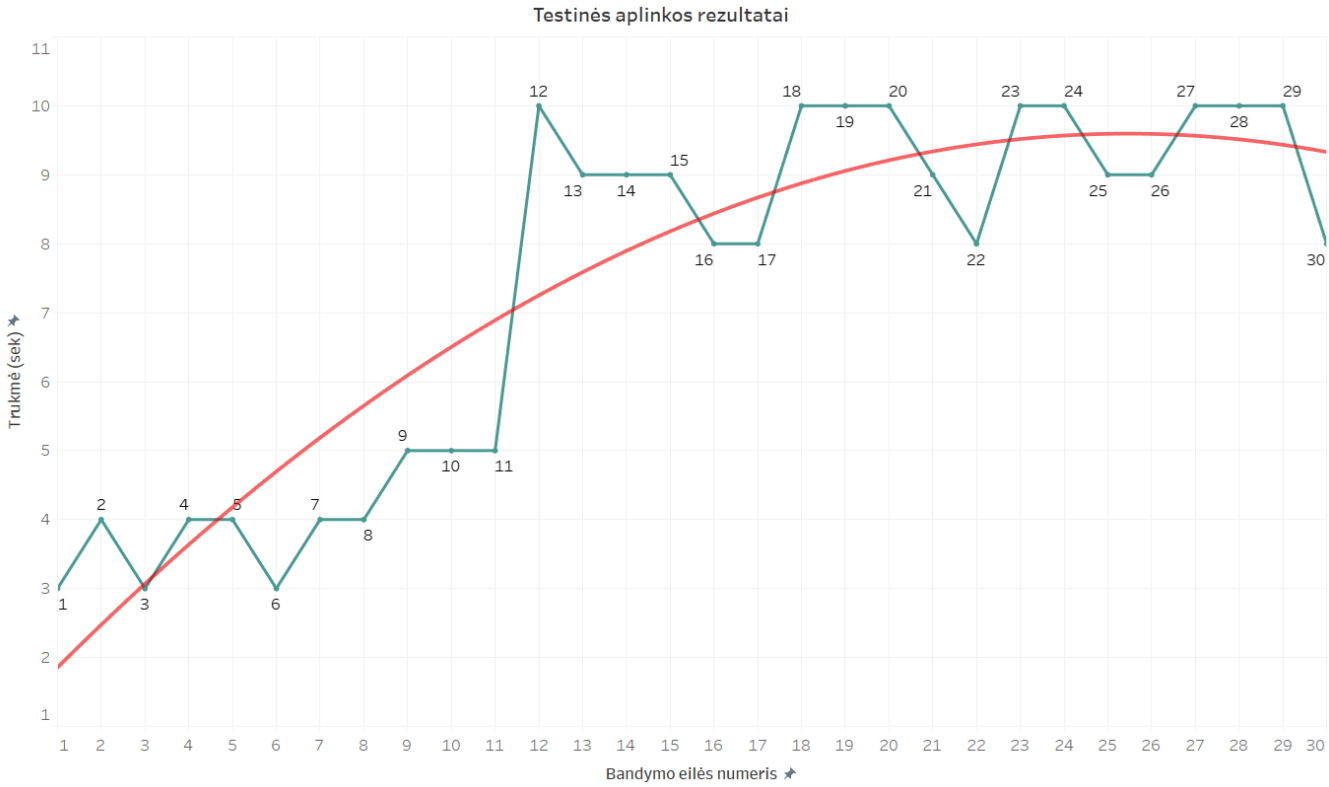
Toliau eksperimente atvaizduojami tyrimo rezultatai aiškiai parodė, kad Europos Sąjungos STD gali žymiai sumažinti įvedimo proceso laiką, kadangi nereikia atlikti net 6 tapatybės patvirtinimo, duomenų surinkimo ir (arba) pateikimo veiksmų etapų (žr. 8 pav. „Su ES STD klientų įvedimo (onboarding) veiksmai"). Bendra kliento įvedimo į finansų įstaigą trukmė naudojant STD gali būti vykdoma trumpiau net iki 10 arba 15 sekundžių, t. y., net 85 - 90 proc. greičiau nei šiuo metu atliekami klientų įvedimo į finansų įstaigą etapai.



Šaltinis: sukurta darbo autoriaus atliekant eksperimentinį tyrimą specializuotoje programoje "Tableau".

8 pav. Asmens tapatybės patvirtinimo proceso veiksmų trukmės palyginimas, kaip yra šiuo metu ir kaip galėtų būti naudojantis ES STD

Papildomai eksperimentinio tyrimo metu įmonės "Soverio" testinėje ("sandbox") aplinkoje buvo imituota 30 autentifikavimo veiksmų simuliacija, kuomet asmenys (vartotojai) yra identifikuojami naudojant ES STD. Taikant šį būdą buvo siekiama papildomai pagrįsti ir įrodyti autentifikavimo proceso greitį bei pritaikomumą realiomis sąlygomis. Tyrimo rezultatai susisteminti ir apibendrinti 9 paveiksle. Tyrimo rezultatai parodė, kad vidutinė asmenų autentifikavimo veiksmų testinėje aplinkoje trukmė – 10 sekundžių. Tai aiškiai parodo, kad asmens tapatybės duomenų autentifikavimas naudojant Europos Sąjungos STD yra atliekamas greičiau ir tiksliau nei taikant dabartinius klientų įvedimo finansinėse įstaigose metodus. Remiantis gautais duomenimis, autentifikavimo procesai su STD gali būti net iki 85 - 90 proc. spartesni, net ir neatsižvelgiant į tai kad, testinė „sandbox" įmonės „Soverio" aplinka paprastai neatspindi maksimalios produkcinės sistemos našumo. Kartu šie rezultatai atskleidė autentifikavimo trukmės skirtumus tarp 30 bandymų (žr. 9 pav.)



Saltinis: sukurta darbo autoriaus atliekant testinį („sandbox“) bandymą „Soverio“ aplinkoje, rezultatai.

9 pav. Asmens tapatybės nustatymo trukmės bandymų rezultatai

Mažiausia trukmė siekia 3-4 sekundes, buvo užfiksuota 8 kartus, t. y., 26 proc. visų bandymų. 5 sekundžių trukmės intervalas buvo užfiksuotas 3 kartus ir sudarė 10 proc. Likusių 19 bandymų kartų trukmė svyravo nuo 8 iki 10 sekundžių, šie bandymai sudarė 63 proc. Gauti rezultatai rodo, kad ES STD ne tik užtikrina greitą ir sėkmingą asmens duomenų autentifikavimą, bet ir pasižymi stabilumu, kuris yra esminis veiksnys efektyviam ir patikimam finansinių operacijų valdymui. Apibendrinus atliktų bandymų rezultatus, galima daryti išvadą, kad asmens tapatybės duomenų autentifikavimo trukmė, kuomet yra naudojama ES STD, vidutiniškai trunka apie 10 sekundžių. Tai reiškia, kad ES STD taikymas asmens tapatybės nustatymui gali būti finansiškai naudingas, nes mažėja operacijų kaštai, reikalingi tradicinėms asmens tapatybės nustatymo procedūroms. Greitesnis vartotojų (asmenų) autentifikavimas tiesiogiai prisideda prie viso proceso efektyvumo didinimo, o tai yra svarbu siekiant gerinti klientų aptarnavimo kokybę ir paslaugų prieinamumą.

Apibendrinant galima teigti, kad atlikti eksperimentinių tyrimo rezultatai aiškiai parodo, jog Europos Sąjungos STD taikymas finansų įstaigoje klientų įvedimo (angl. *onboarding*) procese gali sutrumpinti atliekamų veiksmų laiką net iki 90 proc., palyginant su šiuo metu taikomu įvedimu. Taikant STD yra eliminuojami pakartotini arba papildomi tapatybės nustatymo veiksmai, tokie kaip veido ir asmens dokumento fotografavimas ar vaizdo skambučiu, tapatybės identifikavimas bei klausimų, atsakymų pateikimas. Greitesnis klientų įvedimo procesas reiškia, kad finansinės įstaigos

gali sumažinti operacijoms reikalingas laiko sąnaudas, kartu pagerinti klientų patirtį užtikrinant operacijų tikslumą ir sklandumą, sumažinant galimų papildomų veiksmų poreikį bei minimalizuojant galimą žmogaus įsikišimą į procesą poreikį. Taip pat skaitmeninės tapatybės įdiegimas gali prisidėti ir prie platesnių paslaugų spektro, užtikrinant, kad institucijos, įstaigos ar verslai galėtų greitai ir efektingai prisitaikyti prie kintančių reguliavimo reikalavimų. ES STD kuria pridėtinę vertę ne tik finansų įstaigoms, bet ir verslui, jų klientams, sudarydama unikalią galimybę saugiau ir patikimiau naudotis elektroninėje erdvėje prieinamomis viešomis ir privačiomis paslaugomis.

IŠVADOS

- Išnagrinėjus tyrimo rezultatus nustatyta, kad Europos Sąjungos Skaitmeninės Tapatybės Dėklė gali ne tik žymiai pagreitinti klientų įvedimo procesą, bet ir tuo pačiu užtikrinti pinigų plovimo prevenciją dar pradiniame tapatybės nustatymo etape į finansų įstaigas. Taikant STD galima palengvinti finansų įstaigų darbą ir reikšmingai gerinti klientų patirtį, nes aptarnavimas vyksta greičiau ir be perteklinių procedūrų.
- Eksperimentinis tyrimas atskleidė, kad ES STD ekosistema yra naudinga, siekiant optimizuoti kliento įvedimo į finansų įstaigą procesus. STD taikymas klientų įvedimo procese padeda mažinti duomenų pateikimo laiko trukmę ir gerina finansinių institucijų atsparumą įvairiems sukčiavimo modeliams bei kitoms galimoms rizikoms.
- Su ES STD yra sukuriamas vieno langelio principas, naudojantis viešomis ir privačiomis paslaugomis.
- Dėl galimybės minimalizuoti rankinį darbą, STD taikymas gali sumažinti administracines išlaidas ir didinti darbuotojų efektyvumą.
- Naudojantis ES STD, užtikrinama asmens duomenų apsauga, kadangi asmenims leidžiama patiems kontroliuoti savo asmens duomenis, neteikiant perteklinių duomenų.
- STD taikymas padeda sukurti daugiau į vartotoją orientuotą paslaugų modelį. Tikėtinas didesnis klientų pasitenkinimas naudojantis viešomis bei privačiomis paslaugomis, kadangi didėja paslaugų suteikimo sparta ir saugumas. Tai reiškia, kad taikant STD finansų institucijos gali užtikrinti konkurencinį pranašumą ir kartu išlaikyti aukštą asmens tapatybės nustatymo tikslumą bei patikimumą, o tai yra ypač svarbu vykdant pinigų plovimo prevenciją.

PASIŪLYMAI

- Siekiant optimizuoti klientų įvedimo į finansų įstaigas naudojant ES STD, rekomenduojama standartizuoti asmens tapatybės nustatymo etapus, nes dėklė leidžia sumažinti perteklinių asmens duomenų nustatymo veiksmų skaičių ir pasitaikančio rankinio darbo poreikį.
- Galutinai įgyvendinus ES Skaitmeninės Tapatybės Dėklės sprendimus, finansinėse įstaigose būtų galima užtikrinti vienkartinio duomenų pateikimo principo taikymą asmenims ir turėti visus reikiamus asmens tapatybės duomenis vienoje aplinkoje, taip supaprastinant jų valdymą ir mažinant administracinę naštą, tuo pačiu užtikrinant duomenų apsaugą.
- Ne tik priežiūros institucijos, bet ir verslo subjektai turėtų vertinti šį įrankį (ES STD) kaip į strateginį konkurencinį pranašumą, užtikrinant veiklos skaidrumą ir didinant pasitikėjimą tiek klientų, tiek rinkos dalyvių tarpe.

LITERATŪRA

1. Akhtar, N., Khan, A., ir Raza, M. (2023). Technological Advancements and Legal Challenges to Combat Money Laundering: Evidence from Pakistan. *Pakistan Journal of Humanities and Social Sciences*, *11*(1), 473–483. https://doi.org/10.52131/pjhss.2023.1101.0365
2. Akinteye, S. A., Mokube, M., Ochei, D., ir Vutumu, A. (2023). The Impact of Internal Audit on Improving Anti-Money Laundering (Aml) and Counter Terrorist Financing (Ctf) Controls in Nigeria. *UMYU Journal of Accounting and Finance Research*, *5*(1), 11–27. https://doi.org/10.61143/umyu-jafr.5(1)2023.002
3. Aminat, A. B., Ezekiel, A. I., ir Obafemi, D. S. (2023). The Impact of Internal Control Mechanisms on Fraud Detection and Prevention in Nigeria Deposit Money Banks. *International Journal of Social Science And Human Research*, *06*(10), 5990–5996. https://doi.org/10.47191/ijsshr/v6-i10-28
4. Abei, Y. A. (2021). Impact of Internal Control on Fraud Detection and Prevention in Microfinance Institutions. Prieiga per https://www.diva-portal.org/smash/get/diva2:1578691/fulltext01.pdf
5. Achim, M. V., Borlea, S. N., ir Văidean, V. L. (2021). Does technology matter for combating economic and financial crime? A panel data study. *Technological and economic development of economy*, *27*(1), 223–261. https://doi.org/10.3846/tede.2021.13977
6. Bodescu, C. N., Achimb, M. V., ir Rus, A. I. D. (2022). The influence of digital technology in combating money laundering. 24th RSEP International Conference on Economics, Finance ir Business. https://doi.org/10.19275/RSEPCONFERENCES160
7. Durguti, E., Arifi, E., Gashi, E., ir Spahiu, M. (2023). Anti-money laundering regulations' effectiveness in ensuring banking sector stability: Evidence of Western Balkan. *Cogent Economics ir Finance*, *11*(1). https://doi.org/10.1080/23322039.2023.2167356
8. European Comission (2023). Commission welcomes final agreement on EU Digital Identity Wallet. Prieiga per https://ec.europa.eu/commission/presscorner/detail/en/ip_23_5651
9. Finansinių nusikaltimų tyrimo tarnyba (2023). Pinigų plovimo prevencijos valdyba: veiklos rezultatai 2023 m. Prieiga per https://fntt.lrv.lt/media/viesa/saugykla/2024/5/C6ZPhfeeU4g.pdf
10. Finansinių nusikaltimų tyrimo tarnyba (2020). Nacionalinis pinigų plovimo ir teroristų finansavimo rizikos vertinimas. Prieiga per https://fntt.lrv.lt/media/viesa/saugykla/2023/11/wQ_ZHgz7WDg.pdf
11. FATF. (2021). Opportunities and Challenges of New Technologies for AML/CFT. Prieiga per https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf.coredownload.pdf

12. FATF. (2019). Guidance for a risk-based approach: The banking sector. Prieiga per https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Risk-Based-Approach-Legal-Professionals.pdf.coredownload.inline.pdf
13. FATF. (2023). International standards on combating money laundering and the financing of terrorism & proliferation. Prieiga per https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf
14. Gerbrands, P., Unger, B., Getzner, M., ir Ferwerda, J. (2022). The effect of anti-money laundering policies: an empirical network analysis. *EPJ Data Science*, *11*(1), 15. https://doi.org/10.1140/epjds/s13688-022-00328-8
15. Grigaitė, K., Dias, C., ir Magnus, M. (2021). Preventing money laundering in the banking sector-reinforcing the supervisory and regulatory framework. Prieiga per https://www.europarl.europa.eu/thinktank/en/document/IPOL_IDA(2021)659654
16. Gumus, C., ir Cekerekli, S. (2024). Fraud prevention and detection systems running with digital onboarding. https://www.researchgate.net/publication/381925812_FRAUD_PREVENTION_AND_DETECTION_SYSTEMS_RUNNING_WITH_DIGITAL_ONBOARDING
17. Handa, R. K., ir Ansari, R. (2022). Cyber-laundering: an emerging challenge for law enforcement. *Journal of Victimology and Victim Justice*, *5*(1), 80–99. https://doi.org/10.5772/intechopen.1004006
18. Isolauri, E. A., ir Ameer, I. (2022). Money laundering as a transnational business phenomenon: a systematic review and future agenda. *Critical Perspectives on International Business*, *19*(3), 426–468. https://doi.org/10.1108/cpoib-10-2021-0088
19. Iftikhar, N. F., ir Iqbal, S. (2021). The International Cooperation Challenge: Mapping Pakistan's Response to Terrorist Financing and Money Laundering. *RSIL L. Rev.*, 54. Prieiga per https://rsilpak.org/wp-content/uploads/2023/03/THE-INTERNATIONAL-COOPERATION-CHALLENGE-MAPPING-PAKISTANS-RESPONSE-TO-TERRORIST-FINANCING-AND-MONEY-LAUNDERING.pdf
20. Javor, N. (2020). *Combating Money Laundering with Digital Technologies (Daktaro disertacija).* Prieiga per https://repozitorij.efzg.unizg.hr/islandora/object/efzg%3A6500/datastream/PDF/view
21. Kot, M. (2021). Money laundering as a major risk to the stability of the banking industry. *Prace Naukowe Uniwersytetu Ekonomicznego We Wrocławiu*, *65*(4). https://doi.org/10.15611/pn.2021.4.05
22. Kao, K., Laborde, J. P., Riordan, P., Brauders, D., Yoon, H. K., Garcia, M. A., ir Krumov, N. (2023). International Cooperation in Combating the Financing of Terrorism. *The financing of terrorism*, 153. Prieiga per https://m.elibrary.imf.org/display/book/9798400204654/CH006.xml

23. Krsteski, N. G. H. (2020). Concept, definition and characteristics of the money laundering phenomenon. *Journal of process management and new technologies*, *8*(2), 23–37. https://doi.org/10.5937/jouproman8-26220
24. Kolachala, K., Simsek, E., Ababneh, M., ir Vishwanathan, R. (2021, August). SoK: Money laundering in cryptocurrencies. Iš *Proceedings of the 16th International Conference on Availability, Reliability and Security* (p. 1-10). https://doi.org/10.1145/3465481.3465774
25. Kurniawan, V. (2023). The Role of Regulatory Technology ir Bankers to Prevent Money Laundering in Bank. *Jurnal Bisnis, Manajemen dan Perbankan*, *9*(1), 43–52. https://doi.org/10.21070/jbmp.v9i1.1660
26. Kenneth, S. (2022) The Satoshi Laundromat: A Review on the Money Laundering Open Door of Bitcoin Mixers. *Journal of Financial Crime*. https://doi.org/10.13140/RG.2.2.21666.50884
27. Lietuvos Respublikos vidaus reikalų ministerija (2024). *ES įteisino skaitmeninę tapatybę – bandomajame projekte dalyvauja ir Lietuva bei Ukraina.* Prieiga per https://vrm.lrv.lt/lt/naujienos/es-iteisino-skaitmenine-tapatybe-bandomajame-projekte-dalyvauja-ir-lietuva-bei-ukraina/
28. Lienov, S., Vasilyeva, T., Mynenko, S., ir Dotsenko, T. (2021) *Banking in Digital Age: Efficiency of Anti-Money Laundering System, 2*(37), 4–13. https://doi.org/10.18371/fcaptp.v2i37.229678
29. Lannoo, K., ir Parlour, R. (2021). *Anti-Money Laundering in the EU: Time to get serious* (No. 31980). Centre for European Policy Studies. Prieiga per https://www.ecri.eu/sites/default/files/tfr_anti-money_laundering_in_the_eu.pdf
30. Marcinkevičiūtė, E. (2023). Kriptovaliutų naudojimo įtaka tarptautinei valiutų rinkai. Iš *Young Scientist, Conference/Jaunasis mokslininkas, konferencija* (p. 13-18). Prieiga per https://ejournals.vdu.lt/index.php/jm2022/article/download/3985/2745/19010
31. Malahim, S. S., Alrawashdeh, S. T., Saraireh, S. A. M., Salameh, R. S., Yaseen, A. A., ir Khalil, H. M. (2023). The Relevance of Internal Control System on Money Laundering in Jordanian Islamic and Commercial Banks. *International Journal of Professional Business Review: Int. J. Prof. Bus. Rev.*, *8*(6), 15. https://doi.org/10.26668/businessreview/2023.v8i6.2363
32. Musyoki, K. M. (2023). Internal Control Systems and their role in Financial Fraud Prevention in Kenya. *African Journal of Commercial Studies*, *3*(3), 173–180. https://doi.org/10.59413/ajocs/v3.i3.4
33. Omar, Z. M., ir Ibrahim, J. (2020). An overview of Darknet, rise and challenges and its assumptions. *Int. J. Comput. Sci. Inf. Technol*, *8*, 110-116. Prieiga per https://www.researchgate.net/publication/343282387_An_Overview_of_Darknet_Rise_and_Challenges_and_Its_Assumptions

34. Podgorelec, B., Alber, L., ir Zefferer, T. (2022, June). What is a (digital) identity wallet? a systematic literature review. Iš *2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC)* (p. 809-818). IEEE. https://doi.org/10.1109/COMPSAC54236.2022.00131
35. Pratomo, W. B., Zainal, V. R., ir Hakim, A. (2023). Money Laundering With Financial Technology. *Journal of Economics and Business UBS*, *12*(5), 3132–3141. https://doi.org/10.52644/joeb.v12i5.614
36. Padalkar, N. R. (2023). Unveiling the Digital Shadows: Exploring the Role of Technology in Illicit Financial Flows. Prieiga per https://www.imf.org/-/media/Files/News/Seminars/2023/11th-stats-forum/session-iii-nakul-r-padalkar.ashx
37. Steblianko, A. V., Chernadchuk, T. O., Kravchenko, I. O., Andriichenko, N. S., ir Rudanetska, O. S. (2020). International Law Enforcement Cooperation against Money Laundering. *Cuestiones Políticas*, *37*(65), 217–229. Prieiga per https://produccioncientificaluz.org/index.php/cuestiones/article/view/33314
38. Silvana, L. (2021) *International Cooperation Combating Financial Proceeds of Crime. European Journal of Economics and Business Studies, 7*(1), 37–45. https://doi.org/10.26417/327yrf22i
39. Subbagari, S. (2023). Counter Measures to Combat Money Laundering in the New Digital Age. *Digital Threats: Research and Practice*. https://doi.org/10.1145/3626826
40. Svensson, M. (2021). *Dirty Money Exploits Weakness to Enter: A Narrative Literature Review on the Challenges of Combatting Money Laundering (daktaro disertacija).* Prieiga per https://www.diva-portal.org/smash/get/diva2:1584657/FULLTEXT02.pdf
41. Rocha-Salazar, J. J., ir Segovia-Vargas, M. J. (2024). *Money Laundering in the Age of Cybercrime and Emerging Technologies.* https://doi.org/10.5772/intechopen.1004006
42. Tiwari, M., Gepp, A., ir Kumar, K. (2020). A review of money laundering literature: the state of research in key areas. *Pacific Accounting Review*, *32*(2), 271–303. https://doi.org/10.1108/PAR-06-2019-0065
43. Vijeyan, S. A. N. T. N. I., ir Rahmat, M. (2022). Effects of Internal Control towards Money Laundering Prevention: An Interrelation Perspective. *Asian Journal of Accounting and Governance*, *17*, 13–25. Prieiga per https://journalarticle.ukm.my/19732/1/50268-182850-2-PB.pdf
44. Zavoli, I., ir King, C. (2021). The challenges of implementing anti-money laundering regulation: an empirical analysis. *The Modern Law Review*, *84*(4), 740–771. https://doi.org/10.1111/1468-2230.12628
45. Wang, Y. (2023). The Impact of Financial Technology Development on Money Laundering Risks. Iš *Proceedings of the 2023 International Conference on Finance, Trade and Business Management (FTBM 2023)* (p. 180-192). Springer Nature. Prieiga per https://www.atlantis-press.com/article/125994662.pdf

46. Hilal, W., Gadsden, S. A., ir Yawney, J. (2022). Financial fraud: a review of anomaly detection techniques and recent advances. *Expert systems With applications*, *193*. https://doi.org/10.1016/j.eswa.2021.116429
47. Dullaert, I.**,** Weitzberg, K., Schoemaker, E., ir Martin, A. (2024 June) *The European Digital Identity Wallet.* Prieiga per https://www.cariboudigital.net/wp-content/uploads/2024/06/European-Digital-Identity-Wallet-Brief.pdf
48. LR Nacionalinis kibernetinio saugumo centro, 2022 ataskaita (2022). *"Nacionalinė kibernetinio saugumo būklės ataskaita".* Prieiga per https://www.nksc.lt/doc/Nacionaline-kibernetinio-saugumo-ataskaita-2022.pdf
49. Europos Parlamento ir Tarybos Reglamentas, 2024 (ES) 2024/1183, kuriuo iš dalies keičiamas Reglamentas (ES) Nr. 910/2014, kiek tai susiję su Europos skaitmeninės tapatybės sistemos nustatymu. Prieiga per https://eur-lex.europa.eu/eli/reg/2024/1183/oj?uri=CELEX:32024R1183
50. Hamele, T., ir Dathan, O (2018). Pwc Study. *Next-Generation Client Onboarding.* Prieiga per https://www.pwc.de/en/digitale-transformation/pwc-study-next-generation-client-onboarding-2018.pdf
51. „*Onfido*" (2022). „*KYC process steps*". Prieiga per https://onfido.com/blog/kyc-process-steps/
52. "Regula" (2023) "*Digital Onboarding: Definition, Benefits & How It Works*". Prieiga per https://regulaforensics.com/blog/digital-onboarding/
53. Wyman, O (2019). "*Time to Start again*". Prieiga per https://www.oliverwyman.com/content/dam/oliverwyman/v2/publications/2019/January/The-State-Of-Financial-Services-2019-Time-to-start-again.pdf
54. "FinTech Global" (2022). "UBS links with Regula to automate onboarding". Prieiga per https://fintech.global/2022/11/29/ubs-links-with-regula-to-automate-onboarding/
55. "Innovatrics" (2020). "Onboardin report". Prieiga per https://innovatrics.com/trustreport/63-of-customers-abandon-digital-bank-onboarding-is-biometrics-the-solution/
56. "Fenergo" (2024). "*KYC compliance for banks: Addressing the cost*". Prieiga per https://resources.fenergo.com/blogs/kyc-compliance-for-banks-addressing-the-cost
57. "Ondato" (2023). "Everything you need to know about KYC". Prieiga per https://ondato.com/blog/know-your-customer/
58. "Keller CPP Ltd" (2016). "User guide to completing the risk KYC Questionnaire". Prieiga per https://english.kelerkszf.hu/Key%20documents/Announcements/Financial%20market/Announcement%20on%20Risk%20Know%20Your%20Customer%20(KYC)%20Questionnaire/2016/2016_09_15_Risk%20KYC%20Questionnaire%20User%20Guide.pdf?download

59. Europos Parlamento ir Tarybos reglamentas (ES) 2023/1114, 2023 m. gegužės 31 d., dėl kripto rinkų, kuriuo iš dalies keičiami reglamentai (ES) Nr. 1095/2010 ir direktyvos 2013/36/ES bei (ES) 2019/1937. Prieiga per https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:32023R1114
60. Naujų tapatybės patvirtinimo priemonių galimybių ir atitikties pinigų plovimo prevencijos tikslams problematika (2019). Galimybių studija. Mokėjimų taryba. ISBN 978-609-8204-33-9
61. Demetis, D. S. (2008). A Systems Theoretical approach for Anti-Money Laundering informed by a Case Study in a Greek Financial Institution. https://etheses.lse.ac.uk/2571/1/U615520.pdf
62. Europos Parlamento ir Tarybos direktyvą 2014/92/ES dėl mokesčių, susijusių su mokėjimo sąskaitomis, palyginamumo, mokėjimo sąskaitų perkėlimo ir galimybės naudotis būtiniausias savybes turinčiomis mokėjimo sąskaitomis (*15 straipsnis*).
63. Darius Štitilis, Pakutinskas, P., Dauparaitė, I., & Laurinaitis, M. (2011). Preconditions for Legal Regulation of Personal Identification in Cyberspace. *Jurisprudence, 18*(2), 703–724
64. Ronald F. Pol (2020): Anti-money laundering: The world's least effective policy experiment? Together, we can fix it, Policy Design and Practice, DOI:10.1080/25741292.2020.1725366