

Valstybės skaitmeninių sprendimų agentūra

Analitinė galimybių studija „Europinės skaitmeninės tapatybės dėklės įgyvendinimo galimybių analizė ir planas“

Etapas 2. Techninio parengtumo vertinimas

Rezultatai R.3.1, R.3.2 ir R.3.3 dėl analitinės studijos dokumento dalies „Techninės ekosistemos vertinimas ir integracijos funkcijų identifikavimas“

2026 m. vasaris

Valstybės skaitmeninių sprendimų agentūra	Analitinė galimybių studija „Europinės skaitmeninės tapatybės dėklės įgyvendinimo galimybių analizė ir planas“	Lapas 1 iš 53
---	--	---------------

Turinys

Turinys	1
Nuorodos į techninę specifikaciją	2
Sąvokos ir sutrumpinimai	3
Anglų – lietuvių kalbos terminų žodynas.....	4
Paveikslų sąrašas.....	6
Lentelių sąrašas.....	7
Studijos santrauka	8
1. Analitinės studijos techninio parengtumo vertinimo (Etapas 2, Uždavinys 3) santrauka.....	11
2. Techninė analizė.....	13
2.1. Dabartinės situacijos analizė dėl Lietuvoje veikiančių informacinių sistemų, registrų ir kitų IT sprendimų analizė.....	13
2.1.1. Aktualių EUDIW kontekstui informacinių sistemų sąrašo sudarymas	13
2.1.2. Informacinių sistemų klausimyno vertinimo kriterijų nustatymas	14
2.1.3. Informacinių sistemų, registrų ir kitų IT sprendimų analizė	14
2.2. Techninės ekosistemos vertinimas ir kritinių funkcijų identifikavimas	22
2.2.1. ES standartų ir reikalavimų palyginimas	22
2.2.2. Informacinių sistemų ir registrų vaidmens svarbiausių EUDIW funkcijų ekosistemoje analizė.....	25
2.3. Siūlomos techninės architektūros ir alternatyvų parengimas.....	28
2.3.1. Vertinimo kriterijų nustatymas alternatyvų vertinimui.....	28
2.3.2. Techninės architektūros alternatyvų analizė	28
2.3.3. Rekomenduojamas architektūros modelis Lietuvos kontekstui.....	33
Išvados ir rekomendacijos.....	50
Priedai	Error! Bookmark not defined.
Priedas 1: Sistemų analizės klausimynas	Error! Bookmark not defined.
Priedas 2: Techninės architektūros vertinimo kriterijai.....	Error! Bookmark not defined.

Valstybės skaitmeninių sprendimų agentūra	Analitinė galimybių studija „Europinės skaitmeninės tapatybės dėklės įgyvendinimo galimybių analizė ir planas“	Lapas 2 iš 53
---	--	---------------

Nuorodos į techninę specifikaciją

Studijos uždaviniai pagal techninę specifikaciją	Nuoroda į atitinkamą informaciją 2-ojo etapo studijos dokumente
3. Techninė analizė	
3.1. Išnagrinėti esamas informacines sistemas, registrus bei kitus IT sprendimus (iki 10 objektų, tarp jų turi būti VIISP, MIGRIS, LR gyventojų, juridinių asmenų, užsieniečių registrai ir kt. su Perkančiąją organizacija suderinti objektai), kurie galėtų būti susiję su EUDIW įgyvendinimu ir sistemų parengtumu, pateikiant duomenis į EUDIW, įskaitant procesus, protokolus, formatus ir technines priemones.	Skyrius 3.1
3.2. Įvertinti esamą techninę ekosistemą ir identifikuoti svarbiausias funkcijas, reikalingas sėkmingai sistemos integracijai.	Skyrius 3.2
3.3. Pasiūlyti EUDIW įgyvendinimo techninę architektūrą ir jos alternatyvas, įskaitant siūlomus integracijos modelius, duomenų mainų mechanizmus, saugumo ir sąveikumo reikalavimus, elektroninės atpažinties ir patikimumo užtikrinimo paslaugų prijungimą prie EUDIW, paslaugų teikimo kanalus bei organizacinę techninės architektūros įgyvendinimą.	Skyrius 3.3

Valstybės skaitmeninių sprendimų agentūra	Analitinė galimybių studija „Europinės skaitmeninės tapatybės dėklės įgyvendinimo galimybių analizė ir planas“	Lapas 3 iš 53
---	--	---------------

Sąvokos ir sutrumpinimai

Sutrumpinimas	Sąvoka
BDAR	2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas)
EY	Ernst & Young Baltic, UAB
eID	Elektroninė tapatybė
eIDAS 2.0 arba EUDI reglamentas	2024 m. balandžio 11 d. Europos Parlamento ir Tarybos reglamentas (ES) 2024/1183, kuriuo iš dalies keičiamas Reglamentas (ES) Nr. 910/2014, kiek tai susiję su Europos skaitmeninės tapatybės sistemos nustatymu
eIDAS arba eIDAS 1.0 reglamentas	2014 m. liepos 23 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB
EK	Europos Komisija
ES	Europos Sąjunga
EUDIW	Europinė skaitmeninė tapatybės dėklė
IRD	Informatikos ir ryšių departamentas prie Lietuvos Respublikos Vidaus reikalų ministerijos
IS	Informacinė sistema (kaip apibrėžiama Valstybės informacinių išteklių valdymo įstatymu)
MD	Migracijos departamentas
RC	Registrų centras
RRT	Ryšių reguliavimo tarnyba
TIS 2 arba NIS 2 direktyva	Europos Parlamento ir Tarybos direktyva (ES) 2022/2555 2022 m. gruodžio 14 d. dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria iš dalies keičiamas Reglamentas (ES) Nr. 910/2014 ir Direktyva (ES) 2018/1972 ir panaikinama Direktyva (ES) 2016/1148 (TIS 2 direktyva)
VIISP	Valstybės informacinių išteklių sąveikumo platforma
VIIVĮ	Valstybės informacinių išteklių valdymo įstatymas
VSSA	Valstybės skaitmeninių sprendimų agentūra

Valstybės skaitmeninių sprendimų agentūra	Analitinė galimybių studija „Europinės skaitmeninės tapatybės dėklės įgyvendinimo galimybių analizė ir planas“	Lapas 4 iš 53
---	--	---------------

Anglų – lietuvių kalbos terminų žodynas

Terminas anglų kalba	Terminas lietuvių kalba
Access Certificate Authority	Prieigos sertifikatų teikėjas
Attribute	Požymis
Attribute Scheme Provider	Požymių liudijimo schemos teikėjas
Attribute Source	Požymio šaltinis
Authentic Source	Autentiškas šaltinis
Conformity Assessment Body (CAB)	Atitikties vertinimo įstaiga ¹
Credential	Įgaliojimas (dėklėje saugomas įrašas)
Credential Issuer	Įgaliojimų teikėjas
Credential Verifier	Įgaliojimų tikrintojas
Data Subject	Duomenų subjektas
Device Manufacturers and Related Subsystems Provider	Įrenginių gamintojas ir susijusių sistemų teikėjas
Electronic Attestation of Attributes (EAA)	Elektroninių požymių liudijimas
EAA Provider	Elektroninio požymių liudijimo (EAA) teikėjas (nekvalifikuotas)
Electronic identification (eID)	Elektroninė atpažintis
EUDI Ecosystem	EUDI ekosistema
EUDI Framework	EUDI sistema / struktūra
High, Substantial and Low LoA	Aukštas, pakankamas ir žemas saugumo užtikrinimo lygiai
Key Store	Raktų saugykla (IT kontekste dėl kriptografinių raktų)
Level of Assurance (LoA)	Saugumo užtikrinimo lygis
LEI	Juridinio asmens identifikatorius (Legal Entity Identifier)
National Accreditation Body (NAB)	Nacionalinė akreditacijos įstaiga
PID Dataset	Asmens identifikavimo duomenų rinkinys
PID Provider	PID teikėjas
Provider of Registration Certificates	Dėklės registracijos sertifikatų teikėjas
PuB-EAA Provider	Viešo elektroninių požymių liudijimo (PuB-EAA) teikėjas
Process Excellence (PEX)	Procesų tobulinimo praktika, siekianti efektyvesnių, nuoseklesnių ir aukštos kokybės veiklos procesų.
QEAA Provider	Kvalifikuotų požymių liudijimų (QEAA) teikėjas
QES (QESRC) Provider	Kvalifikuoto elektroninio parašo teikėjas

¹ Reglamento (EB) Nr. 765/2008 2 straipsnio 13 punkte apibrėžta atitikties vertinimo įstaiga, pagal tą reglamentą akredituota kaip kompetentinga įstaiga atlikti kvalifikuoto patikimumo užtikrinimo paslaugų teikėjo ir jo teikiamų kvalifikuotų patikimumo užtikrinimo paslaugų atitikties vertinimą arba kaip kompetentinga atlikti europinių skaitmeninės tapatybės dėklių ar elektroninės atpažinties priemonių sertifikavimą

Valstybės skaitmeninių sprendimų agentūra	Analitinė galimybių studija „Europinės skaitmeninės tapatybės dėklės įgyvendinimo galimybių analizė ir planas“	Lapas 5 iš 53
---	--	---------------

Registrar	Registrorius (EUDIW apimtyje – kaip pasikliaujančiųjų šalių ir visų EUDIW dalyvių registro valdytojas / tvarkytojas)
Relying Party (RP)	Pasikliaujančioji šalis
Relying Party Service	Pasikliaujančiosios šalies paslauga
Secure Cryptographic Interface (SCI)	Saugi kriptografinė sąsaja
Supervisory Body	Priežiūros įstaiga
OpenID for Verifiable Credential Issuance (OID4VCI)	Standartas, apibrėžiantis, kaip saugiai ir standartizuotai išduodami tikrinami įgaliojimai (VC) skaitmeninėms dėklėms, naudojant OAuth2.0 ir OpenID Connect mechanizmus.
OpenID for Verifiable Presentations (OID4VP)	Standartas, apibrėžiantis, kaip skaitmeninė dėklė saugiai pateikia tikrinamus įgaliojimus pasikliaujančiajai šaliai, užtikrinant duomenų minimizavimą ir sąveikumą.
Trust Framework	Patikimumo užtikrinimo modelis
Trust Service Provider (TSP)	Patikimumo užtikrinimo paslaugų tiekėjas
Trusted List Provider (TLP)	Patikimų QTSP sąrašų teikėjas / Patikimų dėklės ekosistemos sąrašų teikėjas
Verifiable Credential (VC)	Kriptografiškai patikrinamas skaitmeninis kredencialas, kuriuo gali būti įgyvendinamas elektroninių požymių liudijimas (EAA)
Verifiable Presentation (VP)	Kriptografiškai patikrinama verifikuojamų kredencialų pateiktis, skirta VC pateikimui trečiosioms šalims
Wallet Instance (WI)	Dėklės egzempliorius
Wallet Secure Cryptographic Application (WSCA)	Dėklės saugi kriptografinė programa
Wallet Secure Cryptographic Device (WSCD)	Dėklės saugus kriptografinis įrenginys
Wallet Provider	Dėklės teikėjas
Wallet Unit	Dėklės vienetas
Wallet Unit Attestation (WUA)	Dėklės vieneto patvirtinimas
Wallet User	Dėklės naudotojas
Notified eID scheme	Elektroninės atpažinties schemos, apie kurias pranešta

Valstybės skaitmeninių sprendimų agentūra	Analitinė galimybių studija „Europinės skaitmeninės tapatybės dėklės įgyvendinimo galimybių analizė ir planas“	Lapas 6 iš 53
---	--	---------------

Paveikslų sąrašas

Paveikslėlis 1: ARF siūlomas architektūros modelis	46
--	----

Valstybės skaitmeninių sprendimų agentūra	Analitinė galimybių studija „Europinės skaitmeninės tapatybės dėklės įgyvendinimo galimybių analizė ir planas“	Lapas 7 iš 53
---	--	---------------

Lentelių sąrašas

Lentelė 1: Pagrindinės techninio parengtumo vertinimo įžvalgos	8
Lentelė 4: Aktualių informacinių sistemų ir registrų sąrašas	13
Lentelė 5: Esamų informacinių sistemų veiklos architektūros modelis EUDIW vaidmenų įgyvendinimui	15
Lentelė 6: Duomenų valdymas sistemose	16
Lentelė 7: Techniniai sprendimai sistemose.....	18
Lentelė 8: Integracijos galimybės	20
Lentelė 9: Infrastruktūros architektūra	21
Lentelė 10: Lietuvos informacinių sistemų vertinimas pagal eIDAS 2.0 reglamente minimas vertinimo sritis	23
Lentelė 11: Lietuvos informacinių sistemų ir registrų vertinimas svarbiausių EUDIW funkcijų kontekste	25
Lentelė 12: Alternatyvų analizė: Sąveikumo ir ARF reikalavimų įgyvendinamumas.....	29
Lentelė 13: Alternatyvų analizė: Elektroninės atpažinties ir patikimumo užtikrinimo paslaugų pakartotinio panaudojimo galimybės EUDIW aplinkoje	30
Lentelė 14: Alternatyvų analizė: Informacijos saugos (NIS 2 direktyva) ir konfidencialumo reikalavimų įgyvendinamumas (BDAR).....	30
Lentelė 15: Alternatyvų analizė: Pradinis paslaugų teikimo kanalų suteikimas ir plečiamumo galimybės	31
Lentelė 16: Alternatyvų analizė: Naudotojo patirtis ir prieinamumas	32
Lentelė 17: Europinės skaitmeninės tapatybės dėklės ekosistemos vaidmenys ir jų atitikmenys Lietuvoje	34
Lentelė 18: Siūloma EUDIW įgyvendinimo techninė architektūra ir jos alternatyvos	48
Lentelė 19: Studijos 2 Etapo pagrindinės techninio parengtumo vertinimo įžvalgos	50

Valstybės skaitmeninių sprendimų agentūra	Analitinė galimybių studija „Europinės skaitmeninės tapatybės dėklės įgyvendinimo galimybių analizė ir planas“	Lapas 8 iš 53
---	--	---------------

Studijos santrauka

Studijos kontekstas

Europos Sąjungoje, siekiant užtikrinti patikimą elektroninę atpažintį ir patikimumo užtikrinimo paslaugas, 2014 metais buvo priimtas eIDAS reglamentas, o 2024 m. jis buvo iš dalies pakeistas eIDAS 2.0 reglamentu, kuris išplėtė elektroninės atpažinties ir patikimumo užtikrinimo paslaugų ekosistemą. Nors reglamentai yra tiesiogiai taikomi visoms ES valstybėms narėms, jų įgyvendinimas ir poveikis skiriasi, ypač valdymo ir organizacinės struktūros srityse, todėl nacionalinės sistemos ir paslaugų brandos lygis įvairiose šalyse yra nevienodas ir reikalauja atskiros analizės. Pagal atnaujintą eIDAS 2.0 reglamentą valstybės narės, įskaitant Lietuvą, privalo iki 2026 m. pabaigos įgyvendinti ir užtikrinti gyventojams prieinamą bent vieną Europinę skaitmeninės tapatybės dėklę (angl. – European Digital Identity Wallet) (toliau – EUDIW arba dėklė).

Studija apima Lietuvos institucijų teisinio, organizacinio ir techninio pasirengimo vertinimą, siekiant užtikrinti sklandų šalies išitraukimą į EUDIW ekosistemą. Vertinimas orientuotas į praktinį įgyvendinamumą – analizuojami galiojantys teisės aktai bei Lietuvoje esamos informacinės sistemos ir registrai, jų sąveikumo galimybės bei atitiktis EUDI reglamento ir ARF gairėms, identifikuojant spragas, rizikas ir būtinus tolimesnius veiksmus integracijos užtikrinimui.

Studijos turinys

Studija susideda iš trijų pagrindinių etapų:

- 1) Teisinis pasirengimas ir ekosistemos funkcijos;
- 2) Techninio pasirengimo vertinimas;
- 3) Įgyvendinimo plano parengimas.

Ši ataskaita yra priskiriama prie 2 etapo, 3 uždavinio „Techninė analizė“ rezultatų.

Studijos tikslas – įvertinti esminius teisinius, organizacinius ir techninius EUDIW įgyvendinimo Lietuvoje aspektus, užtikrinant jo atitiktį EUDI reglamentui, BDAR, TIS 2 bei ES technologiniams sąveikumo standartams, įskaitant EUDIW architektūrą (pagal ARF v2.6), technines specifikacijas ir Europos sąveikumo sistemos principus.

Skaitmeninės dėklės įgyvendinimui keliami pagrindiniai uždaviniai

- Atlikti teisinės aplinkos analizę ir parengti rekomendacijas dėl teisės aktų pakeitimų, reikalingų EUDIW įgyvendinimui Lietuvoje.
- Nustatyti nacionalinės ekosistemos funkcijų ir vaidmenų alternatyvas bei pateikti preliminarią rekomenduojamą parinktį,
- Įvertinti informacinių sistemų ir registrų techninį parengtumą, siekiant nustatyti jų integracijos galimybes į EUDIW ekosistemą.
- Išanalizuoti Europos valstybių gerąsias praktikas, siekiant identifikuoti efektyvius techninius, teisinius ir organizacinius sprendimus.
- Parengti įgyvendinimo architektūros alternatyvas, įvertinant jų techninį, organizacinį ir ekonominį įgyvendinamumą.
- Sukurti išsamų įgyvendinimo planą ir biudžetą, apibrėžiant veiksmus, terminus ir atsakingas institucijas.

Lentelė 1: Pagrindinės techninio parengtumo vertinimo išvalgos

Nr.	Išvalga dėl praktinio įgyvendinimo	Rekomendacija
1.	Esamos Lietuvos informacinės sistemos didžiąja dalimi dengia EUDIW techninės ekosistemos palaikymui būtinas funkcijų įgyvendinimui bus reikalingas informacinių sistemų modernizavimas, ypatingai sąsajų realizavimo ir pritaikymo pagal EUDIW ES lygmens techninius reikalavimus, specifikacijas ir protokolus.	Dabartinių informacinių sistemų ir registrų modernizavimas siekiant užtikrinanti EUDIW techninės ekosistemos palaikymą yra būtinas, kadangi dauguma sistemų veikia pagal senesnius standartus, nėra vieningos architektūros ir realaus laiko integracijų, o duomenų mainai dažnai vyksta asinchroniškai.

Valstybės skaitmeninių sprendimų agentūra	Analitinė galimybių studija „Europinės skaitmeninės tapatybės dėklės įgyvendinimo galimybių analizė ir planas“	Lapas 9 iš 53
---	--	---------------

2.	<p>Centralizuotas elektroninių paslaugų teikimas per Valstybės informacinių sistemų sąveikumo platformą (toliau - VIISP) bus svarbi dalis įgyvendinant privalomus EUDIW reikalavimus Lietuvai.</p> <p>VIISP gali būti pritaikytas šioms funkcijom atlikti:</p> <p>(A) VIISP paslaugų katalogas RP (pasikliaujančių šalių) įjungimui/registravimui, (B) Duomenų platforma ir tapatybės patvirtinimas EUDIW kontekste kaip Pub-EAA ir Tarpinė pasikliaujančioji šalis.</p>	<p>Analitinės studijos kontekste tik iš dalies buvo galima įvertinti šiuo metu vystomo projekto dėl Skaitmeninių paslaugų platformos (toliau – SPP) panaudojimo galimybes, turint omenyje, jog techninis šios platformos rengimas nėra pabaigtas ir galimi pokyčiai.</p> <p>Techninio projektavimo etape reikalinga įvertinti, kaip ši platforma ir nauji jos funkcionalumai, integruoti į jau egzistuojančią ir plačiai naudojamą VIISP sistemą, bus susieti su EUDIW įgyvendinimu. Taip pat, siūloma peržvelgti galimybes ir įvertinti, kad VIISP / SPP sistemos iš dalies galėtų patenkinti ir dalį EUDIW keliamų reikalavimų.</p>
3.	<p>Lietuvos EUDIW techninės architektūros modelis priklauso nuo ekosistemos rolių ir jų atsakomybių priskyrimo.</p>	<p>Sprendimai dėl ekosistemos rolių priskyrimo atitinkamoms institucijoms ir jų atsakomybių turi būti pasiekti politikos lygmeniu. Techninio projektavimo etape, siūloma peržiūrėti techninės architektūros modelį pagal preliminariai patvirtintą ekosistemos dalyvių ir jų atsakomybių reglamentavimą (pagal techninio projekto rengimo apimtį).</p>
4.	<p>EUDIW ekosistemos kūrimas Lietuvoje palies visas valstybės institucijas, verslą ir gyventojus.</p>	<p>Siūloma inicijuoti EUDIW ekosistemos kūrimo projektą Lietuvoje Vyriausybės lygyje, ministrą įtraukiant kaip projekto rėmėją. Programos valdymui pritraukti projektų valdymo profesionalus.</p>
5.	<p>EUDIW aptarnauti bus privaloma visoms valstybės institucijoms ir ženkliai daliai verslo.</p>	<p>Siūloma į dėklės ekosistemos kūrimo programą įtraukti ir kaip galima platesnį ratą suinteresuotų šalių. Tai, ministerijos, savivaldybės, FNNT, NKSC, Lietuvos Bankas ir Pinigų plovimo prevencijos kompetencijų centras. Verslo asociacijas.</p>
6.	<p>Kuriama EUDIW ekosistema ateinančius 15-20 metų bus Lietuvos ir Europos Sąjungos skaitmeninių paslaugų (skaitmenizacijos) pagrindas.</p>	<p>Lietuva turėtų orientotis į lietuviško kapitalo įmonių įtraukimą, kuriant dėklės ekosistemą ir taip kaupti patirtį, kad vėliau galėtų kurti aukštos pridėtinės vertės darbo vietas ir eksportuoti paslaugas įgytos patirties pagrindu.</p>
7.	<p>Kuriama EUDIW ekosistema, tai įvairių informacinių sistemų, valstybės registrų, teikiamų paslaugų ir susijusių procesų, bei teisės aktų visuma, veikianti 24/7 režimu, tad jos sėkmingam funkcionavimui reikalinga sukurti centralizuotą monitoringo sistemą.</p>	<p>Siūloma sukurti visos ekosistemos kritinių dalių centralizuotą monitoringo sistemą ir palaikyti identišką testavimo, prieš gamybinę (angl. pre-prod) aplinkas vadovaujantis geriausiomis sistemų valdymo ir saugumo užtikrinimo praktikomis.</p> <p>Taip pat, platesniam ekosistemos dalyvių įtraukimui, rekomenduojame sukurti eksperimentinę EUDIW aplinką (angl. sand-box).</p>
8.	<p>EUDIW ekosistemos įgyvendinimo programai pasibaigus per 2026 m., EUDIW ekosistema turės veikti nustatytoms institucijoms vykdant nustatytus vaidmenis, jų funkcijas, procesus, funkcionavimo taisykles ir metodikas</p>	<p>Siūlome EUDIW ekosistemos įgyvendinimo paruošiamuosius darbus pradėti nuo 2026 m. pradžios, suformuojant EUDIW įgyvendinimo programą su projekto lyderiu VSSA ir programos partneriais, kurių veiklos ir siekiami</p>

Valstybės skaitmeninių sprendimų agentūra	Analitinė galimybių studija „Europinės skaitmeninės tapatybės dėklės įgyvendinimo galimybių analizė ir planas“	Lapas 10 iš 53
---	--	----------------

	detalizuojant veiklos modelyje, kuris turės būti parengtas EUDIW įgyvendinimo metu.	<p>rezultatai programoje būtų nustatyti pagal EUDIW ekosistemos vaidmenis.</p> <p>EUDIW komponentų kūrimas (skaitmeninės dėklės, registro informacinės sistemos sprendimų kūrimas, patikimumo užtikrinimo infrastruktūros komponentų, sąveikumo mazgo su ES kontekstu (kitų ES šalių skaitmeninės dėklės ekosistemomis, esamų informacinių sistemų modernizavimas pritaikymui pagal EUDIW ekosistemos reikalavimus, turi būti atliekamas inkrementiniu iteraciniu būdu, pagal:</p> <ul style="list-style-type: none"> • Dalimis detalizuojamą ir tvirtinamą veiklos modelį (kuris detalizuoja vaidmenis, pareigas ir atsakomybes, procesus ir paslaugas, naudojamus duomenų rinkinius). • Techninę programą, detalizuojamą analizės ir projektavimo etapais, kurioje tiekimas apibrėžiamas kaip būtina sąlyga (programavimo) vystymo veikloms vykdyti sprintais įgyvendinamus IT sprendimų komponentus.
9.	Centralizuotas e. paslaugų teikimas per epaslaugos.lt (VIISP) portalą, bus svarbi dalis įgyvendinant privalomus reglamento reikalavimus Lietuvai.	Siūlome neatidėliotinai vertinti galimybes koreguoti ar išplėsti šiuo metu vykdomo SPP projekto planus, tam, kad būtų galima VIISP tvarkomą paslaugų katalogą ir SPP komponentą pritaikyti EUDIW įgyvendinimui.
10.	Lietuvoje kuriama EUDIW ekosistema, bus bendros Europos Sąjungos ekosistemos dalimi. Vėliau ir pasaulinės.	Siūlome Ekonomikos ir inovacijų ministerijoje sukurti pareigybę, kuri bus atsakinga už santykių su ES palaikymą, skaitmeninės tapatybės dėklės ekosistemos kontekste. Taip pat, vystant EUDIW ekosistemą, reikalinga vadovautis produkto kūrimo gerosiomis praktikomis. Reguliariai viešinti susijusius ES planus, programos iniciatyvas. Taip pat reguliariai tartis su Lietuvos dėklės ekosistemos dalyviais, verslo asociacijomis.

Valstybės skaitmeninių sprendimų agentūra	Analitinė galimybių studija „Europinės skaitmeninės tapatybės dėklės įgyvendinimo galimybių analizė ir planas“	Lapas 11 iš 53
---	--	----------------

1. Analitinės studijos techninio parengtumo vertinimo (Etapas 2, Uždavinys 3) santrauka

Šioje ataskaitoje pateikiama Lietuvos techninio pasirengimo įgyvendinti Europinę skaitmeninės tapatybės dėklę analizė.

eIDAS 2.0 ir ARF kaip vertinimo pagrindas

Techninio parengtumo vertinimas atliekamas eIDAS 2.0 reglamento (Nr. 2024/1183) kontekste, kuris iš dalies keičia eIDAS reglamentą (Nr. 910/2014) ir iš esmės atnaujina eIDAS sistemą bei įtvirtina EUDIW koncepciją kaip privalomą elektroninės atpažinties priemonę visose ES valstybėse narėse. Taip pat, techninis vertinimas yra grindžiamas principais bei techniniais komponentais, kurie yra įtraukti į Europos skaitmeninės tapatybės bendradarbiavimo grupės parengtą nenormatyvinį dokumentą – EUDIW architektūros sprendimų techninės dokumentacijos 2.6 versiją² (European Digital Identity Wallet Architecture and Reference Framework, toliau – ARF). Šis dokumentas nėra teisiškai įpareigojantis ir yra nuolat besikeičiantis, tačiau pateikia detalias technines ir organizacines gaires, padedančias valstybėms narėms nuosekliai įgyvendinti eIDAS 2.0 reglamentą.

eIDAS 2.0 reglamentas, įsigaliojęs 2024 m. gegužės 20 d., nustato, kad kiekviena valstybė narė, įskaitant Lietuvą, per 24 mėnesius turi užtikrinti bent vieną EUDIW, kuri yra suderinama su ES techniniais, saugumo ir sąveikumo standartais.

Be to, reglamentas numato, kad dėklės infrastruktūra turi būti saugi, atitinkanti BDAR ir TIS 2 direktyvos reikalavimus, o jos veikimas grindžiamas patikimumo užtikrinimo paslaugų teikėjų ir asmens identifikacijos atributų teikėjų (PID) sąveika.

Esama situacija Lietuvos viešojo sektoriaus IT infrastruktūros situacija

Atlikus galimai susijusių informacinių sistemų (IS) ir viešojo sektoriaus infrastruktūros parengtumo vertinimą EUDIW ekosistemos diegimui, pastebima, kad:

- IS pasiekusios pakankamą funkcinę brandą, leidžiančią remtis esamais technologiniais sprendiniais projekto įgyvendinimo pradžiai.
- Veikia pažangus valdysenos ir valdymo modelis, suderintas su Valstybės Informacinių Išteklių Valdymo įstatymo (VIIVĮ) nuostatomis ir nacionaline skaitmeninės valdysenos struktūra.
- Įdiegta VII sąveikumo infrastruktūra, apimanti pagrindinius duomenų mainų, paslaugų katalogo ir tapatybės valdymo elementus.
- Veikia techninės ir organizacinės kibernetinio saugumo priemonės su NKSC įgalinimu ir priežiūra.

Vis dėlto EUDIW diegimas ir platesnė skaitmeninės dėklės ekosistemos plėtra sukuria naujus funkcinius ir techninius reikalavimus, kurių esama infrastruktūra pilnai neužtikrina. Todėl būtinas visiškai naujas EUDIW sprendimas:

1. Suderinamumas su eIDAS 1.0. Suderinamumas su eIDAS 1.0 reiškia, kad naujai kuriamas EUDIW sprendimas turi sklandžiai integruotis su šiuo metu veikiančia eIDAS 1.0 infrastruktūra ir ją papildyti. Tai apima techninių sąsajų su nacionaline tapatybės, viešųjų paslaugų ir organizacine aplinka palaikymą, užtikrinant, kad dėklė galėtų veikti kartu su esamais procesais ir sistemomis. Be to, sprendimas turi numatyti aiškius prijungimo taškus ir plėtros kryptis verslo subjektams, kurie ekosistemoje veikia tiek kaip dėklės naudotojai, tiek kaip pasikliaujančiosios šalys.
2. IS sąveikumo modernizavimas. Būtina maksimaliai panaudoti esamas IS, jas modernizuojant pagal EUDIW reikalavimus. Tai apima:
 - Sąveikos specifikacijų (REST API, JSON ir kt.) taikymą.
 - Skaitmeninio patikimumo užtikrinimo modelio principų pritaikymą tarp sistemų, net jei nėra reikalaujamas „Qualified“ statusas.

² <https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/releases/tag/v2.6.0>

Valstybės skaitmeninių sprendimų agentūra	Analitinė galimybių studija „Europinės skaitmeninės tapatybės dėklės įgyvendinimo galimybių analizė ir planas“	Lapas 12 iš 53
---	--	----------------

- Sistemų sąveikos sekų ir procesų įgyvendinimą pagal ARF nustatytus reikalavimus.
3. Bendrųjų VII išteklių ir komponentų įdarbinimas. Efektyviam diegimui būtina koordinuotai panaudoti:
 - Naują EUDIW sprendimą.
 - Esamus VIISP techninius ir funkcinius komponentus (duomenų mainų platformą, paslaugų katalogą, tapatybės paslaugų teikimą).
 - Nacionalinius sąveikumo standartus – Valstybės metaduomenų katalogą, UDTS taikymą tarpinių sąsajų kūrimui ir vieningam duomenų modelių taikymui.
 4. Naujo EUDIW registro ir atitinkamos IS sukūrimas. Pagal EUDI teisės aktus būtina įsteigti naują registrą, užtikrinantį EUDIW pasikliaujančiųjų šalių ir ekosistemos funkcinių dalyvių identifikavimą. Registras turi užtikrinti aiškų, patikimą ir teisiškai pagrįstą dalyvių statuso nustatymą, sudarant prielaidas saugiam naudojimuisi skaitmeninėje erdvėje.

EUDIW įgyvendinimo techninės architektūros alternatyvos

Taip pat, ši ataskaita pasiūlo galimas EUDIW įgyvendinimo techninės architektūros alternatyvas, įskaitant siūlomus integracijos modelius, duomenų mainų mechanizmus, saugumo ir sąveikumo reikalavimus, elektroninės atpažinties ir patikimumo užtikrinimo paslaugų prijungimą prie EUDIW, paslaugų teikimo kanalus bei organizacinę techninės architektūros įgyvendinimą (organizacinis komponentas iš dalies yra padengtas 1 etapo, 2 uždavinio dėl ekosistemos ir funkcijų nustatymo vertinimo rezultate)

Šios ataskaitos apimtyje yra:

- Išnagrinėtos esamos ir šiuo metu veikiančios Lietuvos informacinės sistemos (toliau – IS), registrai bei kiti IT sprendimai (iš viso 11 objektų), susijusių su E UDIW įgyvendinimu ir sistemų parengtumu.
- Atliktas pirminis vertinimas dėl nagrinėtų IS panaudojimo EUDIW architektūros kontekste.
- Pasiūlytos galimos EUDIW techninės architektūros įgyvendinimo alternatyvos, remiantis esamų IS analize bei kitų ES valstybių narių praktikomis.

Valstybės skaitmeninių sprendimų agentūra	Analitinė galimybių studija „Europinės skaitmeninės tapatybės dėklės įgyvendinimo galimybių analizė ir planas“	Lapas 13 iš 53
---	--	----------------

2. Techninė analizė

2.1. Dabartinės situacijos analizė dėl Lietuvoje veikiančių informacinių sistemų, registrų ir kitų IT sprendimų analizė

2.1.1. Aktualių EUDIW kontekstui informacinių sistemų sąrašo sudarymas

Atliekant techninio parengtumo vertinimą, kartu su Valstybės skaitmeninių sprendimų agentūra (VSSA) buvo identifikuotos pagrindinės informacinės sistemos ir registrai, turintys potencialią sąsają su EUDIW įgyvendinimu Lietuvoje. Siekiant užtikrinti išsamų esamos techninės ekosistemos supratimą, buvo parengtas ir su visų identifikuotų informacinių sistemų tvarkytojais pasidalintas sistemų analizės klausimynas (Priedas 1), skirtas įvertinti techninį pasirengimą, duomenų mainų mechanizmus ir integracijos galimybes. Toliau pateikiamas analizei atrinktų informacinių sistemų ir registrų sąrašas.

Lentelė Nr. 2 skirta nustatyti susijusias informacines sistemas ir registrus bei už jų funkcionavimą (įtraukiant papildomą adaptaciją EUDIW poreikiams pagal ARF nustatytas EUDIW roles, detalizuotas Analitinės studijos 1 etapo, 2 uždavinio rezultate) atsakingas institucijas.

Verta paminėti, kad juridinių asmenų PID į analizę nėra įtrauktas, kadangi tai yra Verslo skaitmeninės dėklės analizės apimtis ir verslo EUDIW referencinė architektūra ir reikalavimai analitinės studijos rengimo metu nėra neapibrėžti.

Lentelė 2: Aktualių informacinių sistemų ir registrų sąrašas

Nr.	IS tvarkytojas (pagrindinis administratorius)	Sistema / Registras	Nagrinėti gali informacinių sistemų vaidmenys/ paskirtis Nr. pagal ARF rolių žemėlapi
1.	Valstybės skaitmeninių sprendimų agentūra	VIISP (Valstybės informacinių išteklių sąveikumo platforma)	Pasikliaujančioji šalis viešojo sektoriaus paslaugų teikėjams (10)
		Registrų ir valstybės informacinių sistemų registras	Autentiškas šaltinis (9)
		eIDAS Node (Nacionalinė elektroninės atpažinties informacinė Sistema, NETAIS)	eIDAS reglamento 1.0 reikalaujamų funkcijų palaikymas, EUDIW kontekste esama infrastruktūra dėl eIDAS Node palaikymo negali būti pernaudota
		VIISP/ Skaitmeninių paslaugų platforma (SPP)	Pasikliaujančiosios šalys (tarpininkai) (10)
		VIISP/ Once-Only Technical System (OOTS)	Viešo elektroninių požymių liudijimo (PuB-EAA) teikėjas (6)
2.	Informatikos ir ryšių departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos/ + Migracijos departamentas prie Lietuvos Respublikos Vidaus reikalų ministerijos	Asmens dokumentų išdavimo informacinė sistema (ADIS)	PID tiekėjas (3) ADIS gali suteikti informaciją / duomenis, kokie asmens tapatybės dokumentai (ATK, pasas) asmeniui yra išduoti.
		Užsieniečių registras, MIGRIS	Galimai autentiškas šaltinis – dėl ILTU kodo išdavimo (9) Dėl PID išdavimo – neaktualus.

Valstybės skaitmeninių sprendimų agentūra	Analitinė galimybių studija „Europinės skaitmeninės tapatybės dėklės įgyvendinimo galimybių analizė ir planas“	Lapas 14 iš 53
---	--	----------------

Nr.	IS tvarkytojas (pagrindinis administratorius)	Sistema / Registas	Nagrinėti galimi informacinių sistemų vaidmenys/ paskirtis Nr. pagal ARF rolių žemėlapi
3.	Valstybės įmonė Registrų centras	Lietuvos Respublikos gyventojų registras	PID šaltinis ir teikėjas Autentiškas šaltinis (9)
		Juridinių asmenų registras	Autentiškas šaltinis (9)
		Nacionalinė elektroninių siuntų pristatymo, naudojant pašto tinklą, informacinė sistema	N Autentiškas šaltinis (9)
4.	Ryšių reguliavimo tarnyba	ES IT sprendimas dėl patikimumo užtikrinimo paslaugų ekosistemos dalyvių	Dėklės teikėjas (2) Patikimų sąrašų tiekėjas (4) Kvalifikuotų požymių liudijimų (QEAA) teikėjas (5) Viešo elektroninių požymių liudijimo (PuB-EAA) teikėjas (6) Kvalifikuoto elektroninio parašo teikėjas (8)

2.1.2. Informacinių sistemų klausimyno vertinimo kriterijų nustatymas

Siekiant užtikrinti nuoseklų informacinių sistemų analizės procesą, buvo parengtas standartizuotas klausimynas, skirtas visoms identifikuotoms informacinėms sistemoms ir registrams, turintiems potencialią sąsają su EUDIW įgyvendinimu Lietuvoje. Klausimyno struktūrą sudarė šeši pagrindiniai skyriai, atspindintys esminius techninio parengtumo aspektus:

- Veiklos architektūra – vertinamos sistemos funkcijos skaitmeninio patikimumo užtikrinimui ekosistemoje, naudotojų tipai, palaikomi procesai ir institucinis kontekstas.
- Duomenų architektūra – analizuojami tvarkomi duomenų tipai, duomenų mainų formatai, duomenų kokybės ir validacijos mechanizmai, dokumentacijos prieinamumas.
- Taikomųjų sprendimų architektūra – nustatomas sistemos vaidmuo EUDI ekosistemoje, naudojamos technologijos, prieigos ir sąsajų tipai.
- Technologijų architektūra – vertinama infrastruktūros talpinimo aplinka, saugumo priemonės ir atitiktis BDAR, eIDAS reglamentui.
- Sistemos iššūkiai ir dokumentacija – identifikuojami techniniai iššūkiai, turima dokumentacija ir atsakingi kontaktiniai asmenys.
- Pasirengimas integracijai su EUDIW – įvertinamas esamas integracijos lygis su VIISP, naudojami protokolai, duomenų perdavimo būdai, saugumo mechanizmai ir pasirengimo skalė.

Klausimynas buvo pateiktas užpildyti institucijų atstovams, atsakingiems už konkrečių sistemų techninį palaikymą. Atsakymai leidžia nustatyti esamus sprendimus, spragas ir galimybes, sėkmingai integracijai į EUDIW ekosistemą. Klausimyno rezultatai naudojami kaip pagrindas techninės analizės dalims ir rekomendacijoms, pateikiamoms tolimesnėse studijos dalyse.

2.1.3. Informacinių sistemų, registrų ir kitų IT sprendimų analizė

Atliekant informacinių sistemų techninės architektūros, protokolų ir sąsajų analizę, buvo organizuoti interviu su nustatytų sistemų ir registrų tvarkytojais, siekiant detalai išnagrinėti jų esamą infrastruktūrą, duomenų mainų procesus bei integracijos galimybes su EUDIW.

Pagal atliktą analizę, buvo nustatytas preliminarus sistemos veiklos architektūros modelis, nustatant galimą susijusių registrų, bei informacinių sistemų ir jų vykdomas funkcijų susiejimą. Šis modelis nustatytas

Valstybės skaitmeninių sprendimų agentūra	Analitinė galimybių studija „Europinės skaitmeninės tapatybės dėklės įgyvendinimo galimybių analizė ir planas“	Lapas 15 iš 53
---	--	----------------

atsižvelgiant į šiuo metu esamų informacinių sistemų, įskaitant valstybės ir registrų informacines sistemas, įgyvendinta funkcijas ir informacinę struktūrą (tvarkomus duomenis) ir galimybę panaudoti juos įgyvendinant EUDIW ekosistemos funkcinis vaidmenis.

Toliau pateikiama esamų informacinių sistemų veiklos architektūros analizė, susiejanti jų atliekamas funkcijas su numatomais EUDIW ekosistemos vaidmenimis.

Lentelė 3: Esamų informacinių sistemų veiklos architektūros modelis EUDIW vaidmenų įgyvendinimui

Nr.	Funkcijos / Vaidmenys	Aktuali sistema (detalus aprašymas lentelėje Nr. 9)	Įžvalgos dėl numatomų rolių EUDIW kontekste (vaidmens Nr. pagal ARF rolių žemėlapi)	Paiškinimas
1.	eID atributų / požymių teikimas	<p>Gauna:</p> <ul style="list-style-type: none"> • VIISP (Valstybės IS sąveikumo platforma) • NETAIS (eIDAS Node) • VIISP/ Skaitmeninių paslaugų platforma (SPP) • VIISP/ Once-Only Technical System (OOTS) <p>Teikia:</p> <ul style="list-style-type: none"> • Asmens dokumentų išdavimo IS <p>Valdo:</p> <ul style="list-style-type: none"> • Gyventojų registras • Juridinių asmenų registras 	<p>Pasikliaujančiosios šalys (10)</p> <p>Autentiški šaltiniai (9)</p> <p>PID teikėjai (3)</p> <p>Autentifikacijos modulius papildyti EUDIW funkcionalumu.</p>	<p>Priklausomai nuo rolės - atributų naudojimas, patikimas šaltinis, PID išdavimas.</p>
2.	Autentikavimo (tapatybės patvirtinimo) paslaugų teikimas	<p>VIISP (Valstybės IS sąveikumo platforma), NETAIS (eIDAS Node), VIISP/ Skaitmeninių paslaugų platforma (SPP), VIISP/ Once-Only Technical System (OOTS).</p>	<p>Tarpinė pasikliaujančioji šalis (10)</p> <p>Autentifikacijos modulius papildyti EUDIW funkcionalumu.</p>	<p>Vartotojo identifikacija naudojant PID.</p>
3.	Sąveikumo platformos paslaugų / kitų paslaugų agregavimas	<p>VIISP (Valstybės IS sąveikumo platforma), VIISP/ Skaitmeninių paslaugų platforma (SPP)</p>	<p>Viešo elektroninių požymių liudijimo (PuB-EAA) teikėjai (6)</p> <p>Tarpinė pasikliaujančioji šalis (10).</p>	<p>Siejama su VIISP kaip esminiu centralizuotu agreguojančiu komponentu, naudojamu įgyvendinant EUDIW,</p>

Valstybės skaitmeninių sprendimų agentūra	Analitinė galimybių studija „Europinės skaitmeninės tapatybės dėklės įgyvendinimo galimybių analizė ir planas“	Lapas 16 iš 53
---	--	----------------

Nr.	Funkcijos / Vaidmenys	Aktuali sistema (detalus aprašymas lentelėje Nr. 9)	Išvalgos dėl numatomų rolių EUDIW kontekste (vaidmens Nr. pagal ARF rolių žemėlapi)	Paaškinimas
		, VIISP/ Once-Only Technical System (OOTS).		spartinant jos diegimą ir nedidinant naštos institucijoms pirmajame EUDIW įgyvendinimo etape per 2026 m., pasinaudojant jau turima patirtimi, lengviau įgyvendinti centralizuotai.
4.	Paslaugų teikimas naudojant skaitmeninio patikimumo užtikrinimo paslaugas	Asmens dokumentų išdavimo IS.	PID teikėjai (3) Viešo elektroninių požymių liudijimo (PuB-EAA) teikėjai (6) Kvalifikuoto elektroninio parašo teikėjai (8).	Priklausomai nuo rolės bus reikalingi papildomi veiksmai registruojant patikimų dėklės ekosistemos sąrašuose.

Duomenų architektūra - skirta identifikuoti galimai susijusius registrus, bei informacines sistemas ir jų valdomų duomenų rinkinių galimą panaudojimą EUDIW kontekste.

Lentelė 4: Duomenų valdymas sistemose

Nr.	Tema	Sistemos	Sąsaja su EUDIW (vaidmens Nr. pagal ARF rolių žemėlapi)
Tvarkomi duomenų tipai			
1.	Asmens tapatybės duomenys	1) Lietuvos Respublikos gyventojų registras – pirminis šaltinis. 2) Asmens dokumentų išdavimo informacinė sistema - išduoda eID. Verta paminėti, kad sertifikatų valdymo informacinė sistema išduota sertifikatus.	Priklausomai nuo rolės: Pasikliaujančiosios šalys (10) - atributų naudojimas Autentiški šaltiniai (9) - patikimas šaltinis PID teikėjai (3) - PID išdavimas.
2.	Biometriniai duomenys	Lietuvos Respublikos gyventojų registras – pirminis šaltinis.	Svarstyтина panaudoti priklausomai nuo to, ar bus nustatyti atvejai, kai išduodant PID, siekiant užtikrinti „LoA High“, būtų naudojami biometriniai duomenys, pavyzdžiui,

Valstybės skaitmeninių sprendimų agentūra	Analitinė galimybių studija „Europinės skaitmeninės tapatybės dėklės įgyvendinimo galimybių analizė ir planas“	Lapas 17 iš 53
---	--	----------------

Nr.	Tema	Sistemos	Sąsaja su EUDIW (vaidmens Nr. pagal ARF rolių žemėlapi)
			panaudojant EUDIW naudotojo tapatybės papildomam patvirtinimui papildomą tapatybės patvirtinimui reikalingą informaciją, kaip nuotrauką arba trumpą vaizdo įrašą patikrinant biometrinių atitikimą pagal biometrinius duomenis, užregistruotus gyventojų registre.
3.	Kontaktiniai duomenys	Vidinėms reikmėms arba nenaudoja.	Priklausomai nuo Lietuvos PID specifikacijos gali būti privalomas/ pageidautinas elektroninis adresas, gyvenamoji vieta.
4.	Juridinių asmenų duomenys	Juridinių asmenų registras - sąsaja su fiziniiais asmenimis.	Registratoriaus vaidmeniui įgyvendinti, siūloma naudoti RC tvarkomą Juridinių asmenų registrą, pasikliaujančiųjų šalių registravimui
5.	Dokumentai / įrašai	Daugelis sistemų valdo kaip apibrėžta jų specifikacijoje.	Priklausomai nuo rolės: pirminis šaltinis/atributų tiekėjas.
Duomenų mainų formatai			
1.	JSON	SPP, dėl kitų sistemų JSON duomenų mainų formato naudojimas nėra žinomas.	Reikės adaptuoti EUDIW specifikacijai naudojančiai JSON ir ISO/IEC 18013-5 (mDL / mID).
2.	XML	Pagrinde palaikoma XML specifikacija.	Palaikoma anksčiau populiari XML/SOA specifikacija. Reikės adaptuoti EUDIW specifikacijai naudojančiai JSON ir ISO/IEC 18013-5 (mDL / mID).
3.	RDF / Linked Data	Nagrinėtose sistemose nėra naudojama.	Nėra nustatyta sąsajų.
4.	Duomenų bazės lygmens integracija	Dažnas realizacijos modelis tarp registrų. Dažnai naudojama Oracle.	Griežtai nenaudotinas tarp institucijų, nebent vienos institucijos ribose, kai ji pati yra išdavėjas. Ši sąsaja nėra specifiukuota ARF.

Aplikacijų architektūra - Skirta identifikuoti galimai susijusius registrus, bei informacines sistemas ir naudojamų technologijų galimą panaudojimą EUDIW kontekste.

Valstybės skaitmeninių sprendimų agentūra	Analitinė galimybių studija „Europinės skaitmeninės tapatybės deklės įgyvendinimo galimybių analizė ir planas“	Lapas 18 iš 53
---	--	----------------

Lentelė 5: Techniniai sprendimai sistemose

Nr.	Tema	Sistemos	Sąsaja su EUDIW (vaidmens Nr. pagal ARF rolių žemėlapi)
Potencialus sistemos vaidmuo / architektūros tipas EUDIW ekosistemoje			
1.	Agreguojanti (interoperability) sistema - sujungia kelias šalis ar sistemas	Viešosios ir administracinės paslaugos, teikiamos ar prieinamos VIISP priemonėmis.	Naudotojų autentifikavimo (tapatybės patvirtinimo), rolių ir kitų savybių nustatymų duomenys.
2.	Vartotojų (consumer) sistema naudoja EUDI paslaugas	Savarankiškos sistemos teikiančios paslaugas ne per VIISP.	Naudotojų autentifikavimo, rolių ir kitų savybių nustatymų duomenys.
Naudotojo prieiga ir sąsaja su sistema			
1.	Žiniatinklio aplikacija	Dažniausias naudojamas atvejis.	Aktualu vartotojams turintiems EUDIW pritaikyti nuotoliniam tapatybės patvirtinimui.
2.	Mobilioji aplikacija	Retas naudojimo atvejis (1) (pagal užpildytus IS klausimynus).	Aktualu vartotojams turintiems EUDIW pritaikyti nuotoliniam tapatybės patvirtinimui.
3.	Darbalaukio aplikacija	Šis būdas EUDIW egzemplioriaus (Instance) ir EUDIW vieneto (unit) įgyvendinimo būdas nenustatytas eIDAS 2.0 reglamente, eIDAS 2.0 reglamento įgyvendinimo teisės aktuose ir ARF.	Šis būdas EUDIW egzemplioriaus (Instance) ir EUDIW vieneto (unit) įgyvendinimo būdas nenustatytas EUDI, EUDI įgyvendinamuosiuose teisės aktuose ir ARF.
4.	Tik API/paslauga³	Nebuvo paminėta.	Sąsajų su įgyvendinimo reikalavimais nenustatyta.
5.	Kombinuotai (EUDIW Mobilioji aplikacija ir žiniatinklio aplikacija tame pačiame arba kitame įrenginyje (asmeniniame kompiuteryje, paslaugų terminale ir kitame nešiojamame įrenginyje)	Dažniausiai kombinuotas žiniatinklis ir API.	Aktualu vartotojams turintiems EUDIW.
Informacinių sistemų išorinių sąsajų (API) įgyvendinimas			
1.	REST	VIISP, eSiunta	Sistema jau arti reikalaujamos krypties. Reikia patvirtinti vienodas pateikimų iš EUDI piniginių taisyklių (ką priimame ir kaip tikriname), bei užtikrinti priėjimą prie patikimumo sąrašų ir sertifikuotų piniginių sąrašų.

³ Dažniausiai sistemos kombinuotos - API (sistemoms)+žiniatinklio paslauga (vartotojams)

Valstybės skaitmeninių sprendimų agentūra	Analitinė galimybių studija „Europinės skaitmeninės tapatybės dėklės įgyvendinimo galimybių analizė ir planas“	Lapas 19 iš 53
---	--	----------------

Nr.	Tema	Sistemos	Sąsaja su EUDIW (vaidmens Nr. pagal ARF rolių žemėlapi)
			Teisinė atrama: EUDIW įgyv. aktai 2024/2977 (PID/EAA formatai) ir 2024/2982 (pateikimo/išdavimo sąveika), taip pat 2025/848 (RP registracija) ir 2025/849 (sertifikuotų piniginių sąrašas). ARF griežtai reikalauja JSON/REST + VC-LD/VC-JWT.
2.	SOAP	JAR, GR, eIDAS Node, ADIS	Dabartinis bendravimo būdas nebeatitinka ES krypties. Reikia suteikti vienodą, paprastą įėjimą pagal naujus reikalavimus (pradžioje galima „apkloti“ seną sprendimą, vėliau atnaujinti iš esmės), kad paslaugos ir piniginė galėtų gauti naujo formato įrodymus ir patikrinti jų galiojimą. Teisinė atrama: EUDIW įgyv. aktai 2024/2977 (nustato, kokio formato įrodymai turi būti), 2024/2982 (nustato, kaip jie turi būti priimami/pateikiami), o paslaugų pusės prievolės ir registracijos tvarka - 2025/848 (RP) ir 2025/849 (piniginės sąrašai). ARF griežtai reikalauja JSON/REST + VC-LD/VC-JWT.
3.	GraphQL	Nebuvo paminėta.	Nėra nustatyta sąsajų.
Informacinių sistemų palaikomi autentifikacijos modeliai			
1.	OAuth2.0	VIISP eSiunta	OAuth2 (autorizacijos protokolas) yra suderinamas su ARF, tačiau tiesiogiai nepalaiko patikrinamų prisijungimo duomenų (verifiable credentials). Pereiti prie OIDC (OpenID Connect) + SIOP (Self-Issued OpenID Provider) kad gauti standartizuotą įrodymų formatą (VC-JWT/VC-LD), pateikimo mechanizmą ir kriptografinį patikrinimą pagal ARF/EUDIW.
2.	eIDAS 1.0 modelis	VIISP NETAIS (eIDAS Node) ADIS	Numatyti eID tikrinimo paslaugos komponento įdiegimą, kuris užtikrintų galimybę išduoti PID nuotoliniu būdu.
3.	Elektroninis parašas	ADIS (Migracijos departamentas) LTID (Registru centras)	Gali būti naudojama kvalifikuoto elektroninio parašo funkcijai įgyvendinti dėklės vienetė.
4.	API raktai	Nebuvo paminėta.	API raktus naudoti tik tarp vidinių sistemų.

Valstybės skaitmeninių sprendimų agentūra	Analitinė galimybių studija „Europinės skaitmeninės tapatybės dėklės įgyvendinimo galimybių analizė ir planas“	Lapas 20 iš 53
---	--	----------------

Nr.	Tema	Sistemos	Sąsaja su EUDIW (vaidmens Nr. pagal ARF rolių žemėlapi)
5.	Sertifikatai	JAR, GR	ARF stipriai remiasi PKI. Lengvesnė adaptacija reikalaujamiems standartams.
Naudojami integracijos modeliai			
1.	Real-time API	Dažnas naudojimo atvejis.	Naudoti kaip pagrindinį kanalą.
2.	Integracinė terpė (ESB)	Nėra naudojama.	Naudoti kaip orchestratorių, ne kaip dėklės komponentą.
3.	Įvykių valdymas (event-driven)	Nėra naudojama.	Tik auditui / asinchroninėms užduotims.
4.	Pranešimų eilės (MQ)	Nėra naudojama.	Tik įvykiams.
5.	Duomenų bazės lygmens integracija	Dažnas naudojimo atvejis.	Nenaudoti įgaliojimų tikrinimui.

Integracijos galimybės - Skirta nustatyti galimai susijusius registrus, bei informacines sistemas ir naudojamų integracinių technologijų galimą panaudojimą EUDIW kontekste.

Lentelė 6: Integracijos galimybės

Nr.	Tema	Sistemos	Sąsaja su EUDIW (vaidmens Nr. pagal ARF rolių žemėlapi)
Potencialus sistemos vaidmuo / architektūros tipas EUDIW ekosistemoje			
1.	PID sistema	LR gyventojų registras ir Juridinių asmenų registras - kaip duomenų teikėjas.	Autentiški šaltiniai (9) - patikimas šaltinis.
2.	Agreguojanti (interoperability) sistema - sujungia kelias šalis ar sistemas	Nacionalinė elektroninių siuntų pristatymo IS - kaip kitų IS metaduomenų teikėjas, VIISP API Gateway - Sujungia kelias šalis ar sistemas.	Viešo elektroninių požymių liudijimo (Pub-EAA) teikėjai (6) pirminis šaltinis/atributų tiekėjas.
3.	Vartotojų (consumer) sistema - naudoja EUDI paslaugas	VIISP	Pasikliaujančiosios šalys (10) - atributų naudojimas.
Kita aktuali informacija			
1.	Duomenų mainų formatai	NETAIS - XML (SAML 2.0), VIISP V2 VIISP - SOAP/XML	Inventorizuoti kur REST/JSON reikalingas pereinant prie Wallet ekosistemos, o kur lieka XML/SAML pereinamajam laikotarpiui.
2.	Duomenų kokybės ir validacijos mechanizmai	Yra aprašyta sistemos specifikacijoje registrai.lt kaip duomenų lentelių laukų tipai.	„Schema-first“ nusako, ką tikriname (JSON/JSON-LD schemas ir privalomumo taisyklės), VP (Verifiable Presentation) priėmimo „ketvertas“ — kaip tikriname (parašas, patikimų sąrašai, statusas/atšaukimas, PEX/politikos), o minimalūs

Valstybės skaitmeninių sprendimų agentūra	Analitinė galimybių studija „Europinės skaitmeninės tapatybės dėklės įgyvendinimo galimybių analizė ir planas“	Lapas 21 iš 53
---	--	----------------

Nr.	Tema	Sistemos	Sąsaja su EUDIW (vaidmens Nr. pagal ARF rolių žemėlapi)
			auditai ir duomenų saugojimo (retencijos) taisyklės užtikrina įrodomumą ir ARF/eIDAS 2.0 atitikimą.
3.	Duomenų žodynas arba duomenų ar informacijos modelių (schemų) dokumentacija	Planuojamas duomenų katalogas data.gov.lt ir suteiks priemonės nurodyti ir tvarkyti formalizuotus žodynus; ši funkcija bus įgyvendinta pertvarkyto RISR į ISR kontekste.	Naudoti valstybės duomenų katalogą (data.gov.lt, kaip nustatyta VIIVĮ, kad metaduomenys rengiami ir tvarkomi pagal ekonomikos ir inovacijų ministro tvirtinamą valstybės informacinių išteklių valdymo ir tvarkymo metodiką, taikant bendrą duomenų architektūros valdymo modelį.

Technologijų architektūra - skirta nustatyti esamos susijusių informacinių sistemų infrastruktūros panaudojimo galimybes ir atitikimus ES reikalavimams galimą panaudojimą EUDIW kontekste.

Lentelė 7: Infrastruktūros architektūra

Nr.	Tema	Sistemos	Sąsaja su EUDIW (vaidmens Nr. pagal ARF rolių žemėlapi)
Reikalavimai naudojamų informacinių infrastruktūros talpinimui			
1.	Organizacijos vidinė infrastruktūra	Pagrindinis naudojimo atvejis.	Sąsaja yra neapibrėžta.
2.	Valstybės debesija	Naudojimo atvejis.	Sąsaja yra neapibrėžta.
3.	Viešoji debesija (AWS, Azure, GCP)	Su šiuo atveju nesusidurta.	Sąsaja yra neapibrėžta. Ribota galimybė kritinėms IS, su LRV pritarimu, naudoti IS viešajame debesyje.
4.	Hibridinis sprendimas	Su šiuo atveju nesusidurta.	Sąsaja yra neapibrėžta.
Atitikties reikalavimai			
1.	BDAR	Yra minima viešose techninėse specifikacijose, kaip nuoroda į teisės aktus.	Teisinis pagrindas (dažn. viešasis interesas / teisinė prievolė), DPIA, „privacy by design/default“, duomenų minimizavimas (selektyvus atskleidimas), retencija, 72 h incidentų pranešimas, subjektų teisės, tvarkytojų sutartys (DPA), Art. 32 saugumas.
2.	eIDAS / EUDI reglamentas	eIDAS 1.0 atitinka (sistemoms veikiančioms per VIISP).	Aukštas patikimumo ir teisinio atitikimo lygis pagal eIDAS 2.0, apimantis EUDI

Valstybės skaitmeninių sprendimų agentūra	Analitinė galimybių studija „Europinės skaitmeninės tapatybės dėklės įgyvendinimo galimybių analizė ir planas“	Lapas 22 iš 53
---	--	----------------

Nr.	Tema	Sistemos	Sąsaja su EUDIW (vaidmens Nr. pagal ARF rolių žemėlapi)
			dėklės sertifikavimą ir įtraukimą į ES lygmens sąrašus, kvalifikuotų elektroninių paslaugų prieinamumą fiziniams asmenims bei atitiktį EUDI ARF reikalavimams, įskaitant aiškiai apibrėžtus vaidmenis ir atitikties patikrą.

Įvertinus visas numatomas susijusias informacines sistemas ir registrus, atliktos analizės rezultatai iliustruoja vertintų sistemų techninės architektūros, duomenų valdymo, saugumo, integracijų ir pasirengimo EUDIW diegimui būklę.

Toliau šie analizės rezultatai sudaro pagrindą bendram rezultatų vaizdai, kuris išsamiai atskleidžiamas Lentelė 9 žemiau. Ši lentelė pristato svarbiausias ekosistemos funkcijas, nustatytas Lietuvos informacinių sistemų ir registrų stiprybes, trūkumus ir prioritetines sritis, būtinas sėkmingam Lietuvos integravimuisi į Europinės skaitmeninės tapatybės dėklės ekosistemą.

2.2. Techninės ekosistemos vertinimas ir kritinių funkcijų identifikavimas

2.2.1. ES standartų ir reikalavimų palyginimas

Vertinant EUDIW įgyvendinimo galimybes, svarbu įvertinti bei palyginti, kiek esamos Lietuvos informacinės sistemos ir registrai atitinka EUDIW architektūros ir ARF gairių techninius bei funkcinis principus. Toks palyginimas leidžia nustatyti, kurios nacionalinės sistemos gali būti tiesiogiai integruojamos į EUDIW ekosistemą, o kuriose srityse reikės papildomų sprendimų, architektūrinių pakeitimų ar naujų funkcijų sukūrimo.

Verta paminėti, kad EUDIW turi atitikti visus reikalavimus, taikomus aukštam saugumo užtikrinimo lygiui („LoA High“), kaip apibrėžta eIDAS 2.0 reglamento 8 straipsnyje (toliau detalizuota EK įgyvendinimo reglamente 2015/1502). Tačiau sertifikuota EUDIW netaikomas toks pat pranešimo (notification) procesas, kuris yra taikomas elektroninės atpažinties schemoms.

Pagal eIDAS 2.0 reglamento 5d straipsnį, EUDIW turi būti įtraukta į sertifikuotų europinių skaitmeninės tapatybės dėklių sąrašą ir dėl to bus laikoma patikimu dėklės sprendimų visose valstybėse narėse. Be to, EUDIW turi nemokamai teikti kvalifikuoto elektroninio parašo galimybes fiziniams asmenims.

Analizė grindžiama prielaida, kad dalis ARF dokumente apibrėžtų funkcijų ir vaidmenų šiuo metu Lietuvoje gali būti neišvystytos arba neturėti tiesioginio institucinio atitiktens. Siekiant tai įvertinti, analizė atliekama remiantis EUDIW architektūros gairėse (ARF) apibrėžtais pagrindiniais ekosistemos komponentais ir jų sąveikos principais. Tokiu būdu vertinimas leidžia nustatyti tiek technologinius, tiek organizacinius trūkumus bei sąlygas, kurias būtina įgyvendinti siekiant atitikties EUDI reglamento reikalavimams.

Vertinimas atliekamas pagal šias pagrindines sritis:

- Tapatybės išdavimas ir susiejimas (PID Issuance & Binding).
- Požymių liudijimas (EAA / QEAA).
- Autentifikacija ir prieiga (Authentication & Access).
- Sąveikumas (Interoperability).
- Saugumas ir patikimumas (Security & Assurance).
- Sertifikavimas ir priežiūra (Conformity & Governance).

Valstybės skaitmeninių sprendimų agentūra	Analitinė galimybių studija „Europinės skaitmeninės tapatybės dėklės įgyvendinimo galimybių analizė ir planas“	Lapas 23 iš 53
---	--	----------------

Vertinant šias sritis, analizuojama, kurios informacinės sistemos atlieka arba galėtų atlikti atitinkamas funkcijas, kokie sąveikos modeliai šiuo metu taikomi, bei ar egzistuoja technologiniai ar teisiniai apribojimai, galintys trukdyti pilnam integravimui į EUDIW ekosistemą. Kai kurioms sritims šiuo metu Lietuvoje gali nebūti priskirtų institucijų ar veikiančių funkcijų – tokiu atveju jos bus pažymimos kaip neapibrėžtos ir papildomai įvertinamos vėlesniuose studijos etapuose.

Lentelė 8: Lietuvos informacinių sistemų vertinimas pagal eIDAS 2.0 reglamente minimas vertinimo sritis

Nr.	Vertinimo sritis	Susijusios sistemos/ registrai	Atitiktis reikalavimams	Pastabos
1.	PID išdavimas ir susiejimas	Gyventojų registras	Dalinė (kaip autentiški šaltiniai) Reikia realizuoti (jei bus pasirinktas, kaip PID tiekėjas).	Autentiško šaltinio (9) funkcija yra. Galimai PID tiekėjas jei bus nutarta.
		Asmens dokumentų išdavimo IS	Reikia realizuoti (jei bus pasirinktas, kaip PID tiekėjas).	Galimai PID tiekėjas. Šiuo metu saugo įvairių asmeniui išduotų dokumentų registrą. Jei PID interpretuoti kaip asmeniui išduodamą dokumentą su jo gyvavimo ciklo kontrole.
		NETAIS (eIDAS Node)	eIDAS reglamento 1.0 reikalaujamų funkcijų palaikymas.	EUDIW kontekste esama infrastruktūra dėl eIDAS Node palaikymo negali būti pernaudota eIDAS 2.0 reikalavimų išplėtimui
2.	Požymių liudijimas	Valstybė informacinės sistemos ir registrų informacinės sistemos, kuriuose tvarkomi teisės aktų numatyta tvarka priminiai duomenys (Gyventojų, Juridinių asmenų, Užsieniečių ir kt.)	Dalinė (duomenų šaltiniai).	OOTS Veikia kaip tarpvalstybinė duomenų sąveika. Tikėtų EAA ir Viešo elektroninių požymių liudijimo (PuB-EAA) teikėjo (6) duomenų gavimui.
3.	Autentifikacija ir prieiga	Tapatybės patvirtinimas VIISP NETAIS (eIDAS Node)	VIISP kaip tarpinė pasikliaujančioji šalis (10).	VIISP – kaip tarpininkaujanti pasikliaunančioji šalis (Intermediating Relying Party). Reikalinga užtikrinti atitiktį OID4VP (VP priėmimas), būtina įgyvendinti asmens sutikimo ir pasirinkimo, kam ir kokius požymių liudijimus asmuo sutinka teikti modelį

Valstybės skaitmeninių sprendimų agentūra	Analitinė galimybių studija „Europinės skaitmeninės tapatybės dėklės įgyvendinimo galimybių analizė ir planas“	Lapas 24 iš 53
---	--	----------------

Nr.	Vertinimo sritis	Susijusios sistemos/ registrai	Atitiktis reikalavimams	Pastabos
				(consent/selective disclosure model).
4.	Sąveikumas	VIISP, OOTS, EU patikimumo/registru sąrašai	Šiuo metu atitikties nėra.	Yra nacionalinis centras ir ES sąveikos kanalai, bet EUDIW ARF protokolai (OID4VCI/OID4VP/PEX, status) dar netaikomi Reikalingas pritaikymas EUDIW ekosistemai, reikalingas EUDIW dalyvių registras.
5.	Saugumas ir patikimumas	QTSP ekosistema, RRT (TSL),	Dalinai (eIDAS 1.0 ribose).	ARF įtvirtina visos grandinės saugą – nuo patikimų sąrašų ir sertifikatų iki dėklės kripto modulių, nuo VP parašo ir galiojimo patikros iki privatumo užtikrinimo, o visa tai pagrindžiama auditais, žurnalais ir privalomais suderinamumo testais.
6.	Sertifikavimas ir priežiūra	RRT (EU portalas)	Registratorius.	Registruoja patikimus sąrašus.

Atlikta analizė leidžia aiškiai įvertinti Lietuvos informacinių sistemų atitiktį pagrindiniams EUDIW architektūros principams, identifikuojant stipriąsias ir tobulintinas sritis. Šie rezultatai sudarys pagrindą sekančiam daliai, kurioje bus detalai įvertinta techninė ekosistema, jos sąveikos procesai ir integracijos galimybės su būsima EUDIW infrastruktūra.

Valstybės skaitmeninių sprendimų agentūra	Analitinė galimybių studija „Europinės skaitmeninės tapatybės dėklės įgyvendinimo galimybių analizė ir planas“	Lapas 25 iš 53
---	--	----------------

2.2.2 Informacinių sistemų ir registrų vaidmens svarbiausių EUDIW funkcijų ekosistemoje analizė

Lentelė 9: Lietuvos informacinių sistemų ir registrų vertinimas svarbiausių EUDIW funkcijų kontekste

Nr.	Sistema / Registras	Atsakinga institucija	Numatoma rolė EUDIW ekosistemoje pagal ARF	Dabartinis parengtumas integracijai	Pagrindinės kliūtys ar ribojimai	Siūlomas veiksmas / rekomendacija
1.	<u>VIISP (Valstybės IS sąveikumo platforma)</u>	VSSA	Tarpinė pasikliaujančioji šalis	Brandi sąveika, SAML; EUDIW VP dar nėra	Nėra vieningo sprendimo dėl perėjimo nuo esamos tapatybės liudijimo prie VP;	Patvirtinti pereinamojo laikotarpio modelį, aiškiai apibrėžiant momentą, kada paslaugų teikėjai pradeda priimti skaitmeninės tapatybės dėklę. Suderinti vartojamą terminiją su didžiausios apimties paslaugų teikėjais ir pradėti pilotinį skaitmeninės tapatybės dėklės įgyvendinimą su ribotu paslaugų skaičiumi.
2.	<u>Registru ir valstybės informacinių sistemų registras (RISR)</u>	VSSA	Numatoma TLP	Dabartinis parengtumas integracijai nėra žinomas.	Nevienodas įrašų detalumas; trūksta žymėjimo pagal EUDIW vaidmenis.	Gali būti kaip pagrindas EUDIW dalyvių registro ir įgyvendinti EUDIW registro tvarkymui reikalingą registro informacinę sistemą - plėsti funkcionalumą.
	NETAIS (eIDAS Node)	VSSA	Nėra sąsajų su EUDIW	Veikiantis eIDAS 1.0 mazgas.	Strateginis sprendimas dėl tolesnio vaidmens; dubliavimo su kitomis grandimis rizika.	Išplėsti NETAIS funkcijų apimtį ir atlikti plėtrą gretutinių techninio sąveikumo su EUDIW ES ekosistema įgyvendinimui.

Nr.	Sistema / Registras	Atsakinga institucija	Numatoma rolė EUDIW ekosistemoje pagal ARF	Dabartinis parengtumas integracijai	Pagrindinės kliūtys ar ribojimai	Siūlomas veiksmas / rekomendacija
3.	<u>Skaitmeninių paslaugų platforma (SPP)</u>	VSSA	Tarpinė pasikliaujančioji šalis	Sistema kūrimo stadijoje.	Nėra vieningo sprendimo dėl perėjimo nuo esamos tapatybės liudijimo prie VP. Nepatvirtintas bendras naudotojų sutikimų ir selektyvumo modelis paslaugose.	Patvirtinti vieningas taisyklės dėl sutikimų ir selektyvaus atskleidimo.
4.	<u>Once-Only Technical System (OOTS)</u>	VSSA	Viešo elektroninių požymių liudijimo (Pub-EAA) teikėjas	Sistema kūrimo stadijoje.	Teisinio pagrindo ir duomenų apimties derinimas tarp institucijų.	Suderinti atributų rinkinį su nacionaliniais registrais; parengti tarpinstitucinius susitarimus.
5.	<u>Asmens dokumentų išdavimo IS (ADIS)</u>	Migracijos departamentas	PID teikėjas	Informacinė sistema yra pritaikoma integracijai.	Pritaikymas EUDIW standartams.	Priimti politinius/teisinius sprendimus dėl teikiamų įrodymų apimties; atlikti DPIA;
6.	<u>Užsieniečių registras</u>	Migracijos departamentas	Viešo elektroninių požymių liudijimo (Pub-EAA) teikėjas	Dabartinis parengtumas integracijai nėra žinomas.	Pritaikymas EUDIW standartams.	Apibrėžti prioritetinius atvejus (pvz., teisė gyventi/dirbti); įtvirtinti informacijos teikimo taisyklės.
7.	<u>Gyventojų registras</u>	Registru centras	PID tiekėjas	Registras yra pritaikomas integracijai.	Suderinimas tarp institucijų dėl mažiausio reikalingo rinkinio; sutikimų modelio įgyvendinimas, remiantis eIDAS 2.0 reglamento įgyvendinimo aktais (specifiškai – Komisijos	Patvirtinti minimalų PID ir jo naudojimo sąlygas; susitarti dėl institucinių vaidmenų.

Valstybės skaitmeninių sprendimų agentūra	Analitinė galimybių studija „Europinės skaitmeninės tapatybės dėklės įgyvendinimo galimybių analizė ir planas“	Lapas 27 iš 53
---	--	----------------

Nr.	Sistema / Registas	Atsakinga institucija	Numatoma rolė EUDIW ekosistemoje pagal ARF	Dabartinis parengtumas integracijai	Pagrindinės kliūtys ar ribojimai	Siūlomas veiksmas / rekomendacija
					įgyvendinimo reglamentas (2024/2977).	
8.	<u>Juridinių asmenų registras</u>	Registrų centras	Viešo elektroninių požymių liudijimo (Pub-EAA) teikėjas	Registras yra pritaikomas integracijai.	Suderinimas tarp institucijų dėl mažiausio reikalingo rinkinio; sutikimų modelis.	Patvirtinti minimalų PID (LEI) ir jo naudojimo sąlygas; susitarti dėl institucinių vaidmenų.
9.	<u>Nacionalinė elektroninių siuntų pristatymo IS</u>	Registrų centras	Nėra sąsajų su EUDIW	Dabartinis parengtumas integracijai nėra žinomas.	Teisinio poreikio tikslinimas.	Nuspręsti reikalingumą/suderinamumą ES kontekste.
10.	<u>RRT IT sprendimas (ES mastu) dėl patikimumo užtikrinimo paslaugų ekosistemos dalyvių</u>	RRT	Patikimų dėklės sąrašų teikėjas	Šiuo metu Registrui reikalingų priemonių nėra (naudojama bendra ES sistema, su galimybe įkelti/atnaujinti duomenis), reikalinga nauja registro informacinė sistema.	Šiuo metu naudojamas EK suteiktas sprendimas, o sukurtas TSP sąrašas mašininio apdorojimo failo pavidalu (XML) eksportuojamas iš tos priemonės ir skelbiamas RRT svetainėje. Šios priemonės yra skirtos mažam kiekiui (iki 10) dalyvių, esančių šiuo metu Lietuvos kontekste.	Įsteigti EUDIW dalyvių registrą ir įgyvendinti EUDIW registro tvarkymui reikalingą registro informacinę sistemą, kaip: Alt. 1: išplečiant VSSA tvarkomą RISR IS; Alt. 2: sukuriant naują EUDIW registro informacinę sistemą.

Valstybės skaitmeninių sprendimų agentūra	Analitinė galimybių studija „Europinės skaitmeninės tapatybės dėklės įgyvendinimo galimybių analizė ir planas“	Lapas 28 iš 53
---	--	----------------

2.3. Siūlomos techninės architektūros ir alternatyvų parengimas

2.3.1. Vertinimo kriterijų nustatymas alternatyvų vertinimui

Atsižvelgiant į ankstesnėse dalyse atliktą techninės ekosistemos ir informacinių sistemų analizę, šiame skyriuje pateiktas skirtingų EUDIW įgyvendinimo architektūros alternatyvų vertinimas, apimančios galimus integracijos modelius tarp nacionalinių informacinių sistemų, paslaugų teikėjų ir autentifikacijos sprendimų.

Siekiant įvertinti kiekvienos alternatyvos tinkamumą Lietuvos kontekste, buvo panaudoti vertinimo kriterijai, leidžiantys objektyviai palyginti architektūros variantus pagal techninius, organizacinius ir saugumo aspektus. Šie kriterijai pateikti – Priede 2.

2.3.2. Techninės architektūros alternatyvų analizė

Šiai analizei atlikti pasirinkome dvi Europos Sąjungos šalis, kurios jau turi pakankamai brandžią ir analizės apimtyje viešai prieinamą aktualią informaciją susijusią su planuojamu Europinės skaitmeninės tapatybės dėklės diegimu. Analizei naudojome šiuos viešai prieinamus informacijos šaltinius:

- Italijos IT-Wallet techninė dokumentacija⁴
- Vokietijos nacionalinė EUDIW architektūros dokumentacija⁵
- Vokietijos EUDIW ekosistemos koncepcijos dokumentas⁶
- Europinės skaitmeninės tapatybės dėklės architektūros ir gairių dokumentas (ARF, versija 2.6.0)⁷

Šių šalių minėti dokumentai buvo vertinami ir ES „*Architecture and reference framework*“⁸ (ARF; versija 2.6.0) atžvilgiu. Atlikta analizė patvirtina, kad abiejų šalių požiūriai tvirtai pagrįsti pagrindiniais ARF architektūros principais ir saugumo reikalavimais. Nei Italijos, nei Vokietijos pasirinkti metodai tokiose svarbiose srityse kaip tapatybės valdymo integracija, autentiškų šaltinių ryšys, dėklės vieneto liudijimas, WSCD architektūros tipai, asmens identifikavimo duomenų rinkinio arba liudijimo gyvavimo ciklo valdymas arba kvalifikuoti elektroniniai parašai (QES) neprieštarauja ARF specifikacijoms, todėl tolimesniame analizės aprašyme susijusių detalių nepateiksime.

Verta paminėti, kad analizės metu vertinome ir susijusius ES įgyvendinamuosius aktus, tačiau dėl jų siauresnės apimties ir ES komisijos nuostatos, kad įgyvendinamieji aktai bus papildomi specifikacijomis ir standartais kurie dar tik ruošiami, manome, kad vertinimas ARF platesnės apimties specifikacijos pagrindu, yra tinkamas.

Atitiktis eIDAS reglamentui: Abi šalys yra įsipareigojusios pasiekti visišką tarpvalstybinį sąveikumą, įgyvendindamos eIDAS 2.0 reglamento reikalavimus.

Toliau esančioje lentelėje pateikiame apibendrintas išvadas apie Italijos ir Vokietijos identifikuotus skirtumus ruošiantis įgyvendinti eIDAS reglamento reikalavimus. Taip pat atkreipiame dėmesį ir į vienos ar kitos įgyvendinimo alternatyvos panaudojimo galimybes Lietuvai įgyvendinant ES eIDAS reglamento reikalavimus.

⁴ <https://italia.github.io/eid-wallet-it-docs/versione-corrente/en/>

⁵ <https://bmi.usercontent.opencode.de/eudi-wallet/wallet-development-documentation-public/>

⁶ <https://bmi.usercontent.opencode.de/eudi-wallet/eidas-2.0-architekturkonzept/>

⁷ <https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/2.6.0/>

Valstybės skaitmeninių sprendimų agentūra	Analitinė galimybių studija „Europinės skaitmeninės tapatybės dėklės įgyvendinimo galimybių analizė ir planas“	Lapas 29 iš 53
---	--	----------------

Lentelė 10: Alternatyvų analizė: Sąveikumo ir ARF reikalavimų įgyvendinamumas

1. Sąveikumo ir ARF reikalavimų įgyvendinamumas	
Vokietijos strateginis požiūris	Italijos strateginis požiūris
Vokietija planuoja decentralizuotą, daugelio tiekėjų ekosistemą. Tokiam siekiui įgyvendinti reikalinga ir sudėtingesnė valdymo sistema.	Italija planuoja įgyvendinti labiau centralizuotą valdymo sistemą, kurios prižiūra patikėta „The Agency for Digital Italy“ (AgID), ko pasėkoje Europinės skaitmeninės tapatybės dėklės ekosistemos valdymas tampa kiek paprastesnis.
Vokietija planuoja, atskirą susijusių šalių (RP) ekosistemą, tikslingai skirtą Europinei skaitmeninės tapatybės dėklei. Kaip turėtų atrodyti tokia sistema galutiniame variante dar nenuspręsta. Svarbus dėmesys skiriamas aukštiems privatumo ir saugumo standartams.	Italija planuoja pasitelkti esamą susijusių šalių (RP) tinklą, kuris jau yra integruotas su „Public Digital Identity System“ (SPID) ir „The Electronic Identity Card“ (CIE). Pasirinktas principas suteikia lankstumo ir sukuria galimybes greitai plėtrai.
Vokietijos vienareikšmis pasirinkimas – remtis nacionaline asmens tapatybės kortele „eID“ kortelę.	Italija suteikia daugiau lankstumo, leisdama vartotojams rinktis iš dviejų nusistovėjusių nacionalinių elektroninės atpažinties schemų: SPID arba CIE.
Vokietijos pasirinktas modelis yra labiau paskirstytas, jame apibrėžiama sistema, kurioje įvairūs įgalioti emitentai jungiasi prie daugybės autentiškų šaltinių tiek federaliniu, tiek žemių lygmenimis.	Italijos modelis, ypač asmens identifikavimo duomenų (PID) atveju, yra centralizuotas, o numatomas pagrindinis PID teikėjas yra siejamas su nacionalinio gyventojų registru „National Registry of Resident Population“ (ANPR).
Vokietijos planuojama dėklės architektūra yra pabrėžtinai lanksti, aiškiai palaikanti tiek vietini (įrenginyje) WSCD, tiek nuotolinį WSCD modelį.	Italija, akivaizdžiai teikia pirmenybę nuotolinio „Wallet Secure Cryptographic Device“ (WSCD) modeliui, kai susijusi kriptografinė medžiaga laikoma saugioje, nuotolinėje tiekėjo sistemoje.
Vokietijos pasirinktas decentralizuotas, daugelio tiekėjų modelis pilnai atitinka ARF reikalavimus ir nesukelia ypatingų reikalavimų įgyvendinimui, tačiau jo sėkmė didele dalimi priklausys nuo pasirinktos valdymo sistemos ir aiškių techninių taisyklių. Be viso kito, pasirinktas modelis skatina inovacijas, gerina vartotojų pasirinkimą ir konkurenciją.	Italijos pasirinktas labiau centralizuotas valdymo modelis. Planuojama panaudoti esamas ir sėkmingai veikiančias patikimumo užtikrinimo sistemas naudojamas SPID ir CIE, ko pasėkoje sąlyginai mažėja sudėtingumas ir lengvinamas dėklės ekosistemos diegimas.
<p>Alternatyva 1: Atsižvelgiant į Vokietijos svarbią federalinių žemių rolę valstybės valdyme ir su tuo susijusį savarankiškumą, manome, kad Lietuvoje pilnai kartoti Vokietijos pasirinktą labiau decentralizuotą modelį nėra tikslinga.</p> <p>Alternatyva 2: Remiantis Italijos pavydžiu, tikslinga būtų rekomenduoti centralizuotą ES Tapatybės dėklės ekosistemos diegimo modelį, kai naujoms ES dėklės ekosistemos rolėms vykdyti, Lietuvoje parenkamos valstybės institucijos kurios jau dabar teikia panašaus pobūdžio paslaugas.</p> <p>Alternatyva 3: Įvertinus abiejų šalių planus naudojant įrenginio WSCD, ar nutolusio tiekėjo sistemą, bei ARF aprašomus atvejus, tikslinga numatyti, kad kuriama dėklė galėtų palaikyti visus ARF specifikacijoje numatytus atvejus.</p>	

Abi vertinamos šalys, Europinės skaitmeninės tapatybės dėklės ekosistemas planuoja kurti taip, kad panaudotų esamas, eIDAS nacionalines elektroninės identifikacijos (eID) schemas. Toks pasirinktas principas tiesiogiai atitinka ARF ir eIDAS reglamento nuostatas, kad ES dėklės ekosistema būtų paremta jau egzistuojančiomis šalių narių sistemomis.

Valstybės skaitmeninių sprendimų agentūra	Analitinė galimybių studija „Europinės skaitmeninės tapatybės dėklės įgyvendinimo galimybių analizė ir planas“	Lapas 30 iš 53
---	--	----------------

Lentelė 11: Alternatyvų analizė: Elektroninės atpažinties ir patikimumo užtikrinimo paslaugų pakartotinio panaudojimo galimybės EUDIW aplinkoje

2. Elektroninės atpažinties ir patikimumo užtikrinimo paslaugų pakartotinio panaudojimo galimybės EUDIW aplinkoje	
Vokietijos strateginis požiūris	Italijos strateginis požiūris
Vokietijoje Europinės skaitmeninės tapatybės dėklės aktyvavimas planuojamas naudojant nacionalinės asmens tapatybės kortelės nuotolinės identifikacijos funkciją „eID-Funktion“. Tai eIDAS reglamento reikalavimus atitinkanti notifikuota schema, atitinkanti ir aukštą patikimumo lygio (LoA High) reikalavimus.	Italijoje Europinės skaitmeninės tapatybės dėklės aktyvavimas turėtų būti atliekamas naudojant vieną iš dviejų nacionalinių elektroninės tapatybės schemų: SPID arba CIE, kurios tenkintų eIDAS reglamento reikalaujamą aukštą patikimumo lygį (LoA High).
Tiek Italija, tiek Vokietija planuoja sukurti galimybes panaudoti jau esamas kvalifikuoto elektroninio parašo (QES) paslaugas teikiamas kvalifikuotų patikimumo užtikrinimo paslaugų teikėjų (QTSP).	
Abiejų šalių pasirinktos strategijos užtikrina Europinės skaitmeninės tapatybės dėklės ekosistemų vientisumą pakartotinai panaudojant sukurtas patikimumo užtikrinimo paslaugas, pirmiausia tas, kurios susijusios su viešojo rakto infrastruktūra (PKI), siekiant saugiai identifikuoti dalyvius.	
Vokietijos atveju, dokumentuose aiškiai reikalaujama, kad pasikliaujančioji šalis identifikuojama dėklėje, naudojant didelio patikimumo paslaugą.	Italijos atveju reikalaujama saugių ryšio protokolų, kur pasikliaujančiosios šalys turi identifikuoti save galiojančiais skaitmeniniais sertifikatais.
<p>Alternatyva 1: remiantis Vokietijos ir Italijos atvejais akivaizdu, kad yra tikslinga sukurti galimybes Europinės skaitmeninės tapatybės dėklės ekosistemoje panaudoti jau dabar Lietuvoje teikiamas QES paslaugas, juolab, kad tai įpareigoja EUDI ir EUDI įgyvendinamieji teisės aktai.</p> <p>Alternatyva 2: Lietuvos atveju Europinės skaitmeninės tapatybės dėklės aktyvavimas (PID patvirtinimo ir išdavimo į dėklę) galėtų būti paremtas dviem būdais:</p> <p>I) naudojant notifikuotas eID schemas</p> <p>Pastaba: Svarstyta panaudoti mCard LTU kaip priemonę tuo atveju, jei tai nesukurs papildomų veiksmų galutiniam naudotojams, kaip papildomai reikalinga programėlė. Kitu atveju, pasinaudoti mCard LTU kūrimo patirtimi, o jei valstybė yra išlaikiusi teises, programinės įrangos išėties tekstais tam, kad galima būtų efektyviai gyvendinti EUDIW vienetui veikti reikalingas sąsajas.</p> <p>II) Galimai panaudojant nacionalines eID schemas vadovaujantis įgyvendinamojo akto nuostatomis. .</p>	

Lentelė 12: Alternatyvų analizė: Informacijos saugos (NIS 2 direktyva) ir konfidencialumo reikalavimų įgyvendinamumas (BDAR)

3. Informacijos saugos (NIS 2 direktyva) ir konfidencialumo reikalavimų įgyvendinamumas (BDAR)	
Vokietijos strateginis požiūris	Italijos strateginis požiūris
Decentralizuota, daugelio tiekėjų ekosistema. Šis modelis remiasi tvarios patikimumo užtikrinimo sistemos sukūrimu, vadovaujantis sutartais naudoti standartais ir privalomu sertifikavimu.	Centralizuotas modelis remiasi Europinės skaitmeninės tapatybės dėklės sistema kaip pagrindiniu saugumo politikos įgyvendinimo tašku, suteikiančiu vieną kontrolės ir stebėjimo tašką visai dėklės ekosistamai.
Nepriklausomai nuo to, ar sistema yra decentralizuota, ar centralizuota, reikalaujama aukščiausio lygio saugumo, įskaitant didelio patikimumo elektroninės atpažinties priemonių naudojimą pradiniam dėklės	

Valstybės skaitmeninių sprendimų agentūra	Analitinė galimybių studija „Europinės skaitmeninės tapatybės dėklės įgyvendinimo galimybių analizė ir planas“	Lapas 31 iš 53
---	--	----------------

3. Informacijos saugos (NIS 2 direktyva) ir konfidencialumo reikalavimų įgyvendinamumas (BDAR)

Vokietijos strateginis požiūris	Italijos strateginis požiūris
susiejimui ir reikalavimą atlikti dėklės instancijos atestavimą ⁹ (Wallet Instance Attestation, WIA) siekiant užtikrinti dėklės ir naudojamo įrenginio vientisumą.	
Vertinant eIDAS reglamento ir ARF dokumento nuostatas, skirtumo tarp decentralizuoto ir centralizuoto modelių BDAR atitikties požiūriu nėra. Abiem atvejais privaloma užtikrinti su BDAR susijusių eIDAS reglamento reikalavimų įgyvendinimą.	
Nė vienos vertintos šalies dokumentuose nepateiktas incidentų valdymo planas, tačiau tai nereiškia architektūrų neatitikimo eIDAS reglamento ar ARF dokumento reikalavimams. Abi nagrinėtos architektūros sukuria pakankamą techninį pagrindą reikalavimus atitinkančiam įgyvendinimo planui parengti.	
Šiuo atveju, Europinės skaitmeninės tapatybės dėklės ekosistemos įgyvendinimo alternatyvų, remiantis vertintų šalių prieinamais dokumentais, nenustatyta. Abi šalys vienaip ar kitaip planus sieja su eIDAS reglamento reikalavimais.	

Vokietijos ir Italijos vertinti dokumentai pagrindinį dėmesį skiria Europinės skaitmeninės tapatybės dėklės architektūrai, žemiau esantys palyginimai pirmiausiai yra susiję su centralizuotos ir decentralizuotos architektūros palyginimu trijose pagrindinėse srityse: naudotojų mastelio keitimas, funkcinis išplėtimas ir ekosistemos augimas.

Lentelė 13: Alternatyvų analizė: Pradinis paslaugų teikimo kanalų suteikimas ir plečiamumo galimybės

4. Pradinis paslaugų teikimo kanalų suteikimas ir plečiamumo galimybės

Vokietijos strateginis požiūris	Italijos strateginis požiūris
<p>Naudotojų mastelio keitimas</p> <p>Vokietija pasirinko decentralizuotą ir rinkos valdomą „mastelio keitimo“ principą. Architektūra palaiko kelis nepriklausomus dėklių teikėjus, paskirstant galimą apkrovą įvairiems teikėjams, o ne sutelkiant ją vienoje vietoje. Planuojama panaudoti esamą ir patikrintą nacionalinės asmens tapatybės kortelės „eID-Funktion“ infrastruktūrą. Tokia decentralizacija neleidžia susidaryti vienai techninei „butelio kaklelio“ tipo, kliūčiai. Vieno dėklės tiekėjo sutrikimo atveju nukentėtų tik to tiekėjo vartotojai, todėl visa sistema būtų atsparesnė pavieniams gedimams. Pasirinktas rinkos modelis užtikrina, kad ekosistema galėtų augti taip, kad būtų aptarnaujami visi gyventojai ir būtų skatinama konkurencija bei inovacijos.</p>	<p>Naudotojų mastelio keitimas</p> <p>Italija planuoja naudoti centralizuotą „mastelio didinimo“ principą. Planuojama, kad sistema naudos esamas didelio masto nacionalines elektroninės tapatybės infrastruktūras (SPID ir CIE) vartotojų įtraukimui. Iššūkis yra sukurti pakankamai galingą ekosistemą. Tokio principo pasirinkimas sukuria rizikas, susijusias ekosistemos našumo užtikrinimu. Nepaisant to, toks modelis leidžia griežčiau ir nuosekliau kontroliuoti vartotojo patirtį ir saugumą.</p>

⁹ Pastaba: „dėklės instancijos atestavimas“ – siūlomas lietuviškas termino „Wallet Instance Attestation (WIA)“ vertimas, nes oficialus lietuviškas atitikmuo šiuo metu nėra nustatytas.

Valstybės skaitmeninių sprendimų agentūra	Analitinė galimybių studija „Europinės skaitmeninės tapatybės dėklės įgyvendinimo galimybių analizė ir planas“	Lapas 32 iš 53
---	--	----------------

4. Pradinis paslaugų teikimo kanalų suteikimas ir plečiamumo galimybės

Vokietijos strateginis požiūris	Italijos strateginis požiūris
<p>Funkcinis išplėtimas</p> <p>Vokietijos pasirinktas modelis iš esmės yra sukurtas funkciniam išplėtimui, skatinant inovacijų aplinką. Bet kuri organizacija, atitinkanti nacionalinės patikimumo užtikrinimo sistemos reikalavimus, gali tapti naujų įgaliojimų išdavėja. Šis „iš apačios į viršų“ metodas leidžia sparčiau diegti inovacijas ir siūlyti įvairesnį paslaugų asortimentą, nes patekimo į rinką kliūtys pirmiausia susijusios su atitiktimi, o ne centrine integracija. Tai atspindi filosofiją, kuri teikia pirmenybę rinkos valdomoms ir decentralizuotoms inovacijoms.</p>	<p>Funkcinis išplėtimas</p> <p>Italija taiko struktūrizuotą „iš viršaus į apačią“ principą, pirmenybę teikdama kontroliuojamam augimui. Išplėtimo galimybės valdomos aiškiai atskiriant PID tiekėją nuo platesnės Elektroninių požymių liudijimų (EAA) išdavėjų ekosistemos. Dėklės sistema veikia kaip centrinis taškas, skirtas naujų išdavėjų (pvz., mobiliųjų vairuotojo pažymėjimų ar diplomų) integracijai ir atitikties užtikrinimui. Nauji Elektroninių požymių liudijimai (EAA) greičiausiai būtų diegiami vykdant oficialų integracijos ir patvirtinimo procesą su centrine institucija. Nors toks modelis užtikrina aukštą nuoseklumo ir kontrolės lygį, inovacijų diegimas gali būti lėtesnis.</p>
<p>Ekosistemos augimas</p> <p>Vokietija daugiausia dėmesio skiria rinkos kūrimo strategijai, kuria siekiama paskatinti įvairius veikėjus dalyvauti, apibrėžiant aiškius, atvirus standartus ir skaidrią patikimumo užtikrinimo sistemą. Tikėtina, kad tokio modelio pagrindu kuriamos ekosistemos augimas pradinėje stadijoje bus lėtesnis, tačiau ilguoju laikotarpiu bus naudingesnis, palaikantis inovacijas ir konkurenciją.</p>	<p>Ekosistemos augimas</p> <p>Galima teigti, kad Italija pasirinko pragmatišką dėklės ekosistemos kūrimo strategiją, kurios centre – platus, SPID ir CIE nacionalinių elektroninės atpažinties schemų, tinklo panaudojimas. Šios strategijos tikslas – nuo pat pradžių suteikti apčiuopiamą naudą dėklės naudotojams.</p>
<p>Alternatyva 1: remiantis Vokietijos pavyzdžiu kurti dėklės ekosistemą skatinančią konkurenciją ir inovacijų diegimą, mažiau centralizuojant ekosistemos valdymą ar paslaugų tiekėjų pasirinkimą.</p> <p>Alternatyva 2: remiantis Italijos pavyzdžiu, kurti stipriai centralizuotą ekosistemą, kur su Europine skaitmeninės tapatybės dėkle susijęs paslaugų tiekimas yra centralizuotas, ypač jei tai susiję su valstybės institucijomis.</p>	

Šios analizės metu mums nebuvo prieinami dokumentai kur Vokietijos ar Italijos institucijos atsakingos už Europinės skaitmeninės tapatybės dėklės ekosistemos sukūrimą, skelbtų būsimos dėklės ar susijusių sistemų, su naudotojo patirtimi ir prieinamumu, susijusių informaciją. Žemiau lentelėje esanti apžvalga yra susijusi su pasirinktų įgyvendinimo architektūrų analize, dėmesį skiriant tam, kaip pasirinkti strateginiai sprendimai daro įtaką naudotojo patirčiai, prieinamumui ir naudotojo palaikymui.

Lentelė 14: Alternatyvų analizė: Naudotojo patirtis ir prieinamumas

5. Naudotojo patirtis ir prieinamumas

Vokietijos strateginis požiūris	Italijos strateginis požiūris
---------------------------------	-------------------------------

Valstybės skaitmeninių sprendimų agentūra	Analitinė galimybių studija „Europinės skaitmeninės tapatybės deklės įgyvendinimo galimybių analizė ir planas“	Lapas 33 iš 53
---	--	----------------

<p>Naudotojo patirtis (decentralizuotas atvejis)</p> <p>Pirmenybė teikiama naudotojo pasirinkimui ir rinkos skatinamoms inovacijoms. Palaikoma konkurencinga nepriklausomų teikėjų rinka.</p> <p>Pagrindinis mechanizmas – konkurencija, skatinanti teikėjus kurti intuityviausias ir patogias naudoti programas. Reguluotojas nustato saugumo ir sertifikavimo reikalavimus.</p> <p>Manoma, kad tai skatina inovatyvesnę dizainą, tačiau gali lemti fragmentišką naudotojo patirtį. Bendri sertifikavimo proceso reikalavimai užtikrina aukštą patikimumą konkuruojančiais produktais.</p>	<p>Naudotojo patirtis (centralizuotas atvejis)</p> <p>Pirmenybė teikiama vienodumui ir pažįstamam naudojimui patirčiai, siekiant užtikrinti nuoseklią ir standartizuotą naudotojo patirtį.</p> <p>Pagrindinis mechanizmas – nusistovėję veikimo principai ir pažįstami autentifikavimo srautai (pvz., naudojami SPID ir CIE).</p> <p>Tokio požiūrio pranašumas – nuspėjamumas, tačiau inovacijų diegimas gali būti lėtesnis. Susijęs iššūkis yra sukurti vieną programėlę, kuri būtų tinkama naudoti ir prieinama įvairioms naudotojų grupėms.</p>
<p>Prieinamumas</p> <p>Decentralizuotas modelis užtikrina prieinamumą reguliavimu ir sertifikavimu. Prieinamumo standartai yra privaloma sertifikavimo proceso dalis, užtikrinanti aukštą ir nuoseklų visų paslaugų teikėjų bazinį lygį. Toks modelis gali skatinti inovacijas prieinamumo srityje, nes konkuruojantys paslaugų teikėjai gali siekti viršyti minimalius reikalavimus.</p>	<p>Prieinamumas</p> <p>Centralizuotas modelis sukuria aiškią produkto kūrimo aplinką, nes vienas subjektas yra atsakingas už standartų (pvz., EN 301 549 arba WCAG) reikalavimų, kuriamame produkte pritaikymą.</p>
<p>Naudotojų palaikymas</p> <p>Decentralizuotas naudotojų palaikymo modelis, kai pagrindinė atsakomybė tenka konkrečiam naudotojo pasirinktam deklės teikėjui. Palaikymo kokybė ir reagavimas gali skirtis priklausomai nuo teikėjo. Centrinė institucija veikia kaip reguliuotojas, apibrėždama ir vykdydama minimalius naudotojų palaikymo standartus kaip sertifikavimo proceso dalį.</p>	<p>Naudotojų palaikymas</p> <p>Centralizuota architektūra reiškia supaprastintą ir centralizuotą naudotojų palaikymo modelį. Pilietis, susidūręs su problema, greičiausiai turėtų vieną aiškų kontaktinį asmenį, pavyzdžiui, nacionalinę pagalbos tarnybą, o tai supaprastina palaikymo organizavimą, nors vienas iš pagrindinių iššūkių susijusių su centralizuotu palaikymu yra išplėsti ir išlaikyti vieną nacionalinį palaikymo centrą, kad būtų patenkinti visų gyventojų poreikiai.</p>
<p>Alternatyva 1: pasirinkti centralizuotą valdymo modelį. Lietuvoje, kur gyventojų populiacija yra sąlyginai nedidelė, toks modelis gali būti tinkamas būdas kurti Europinės skaitmeninės tapatybės deklės ekosistemą, ypač pradinėje jos kūrimo stadijoje.</p> <p>Alternatyva 2: kurti Europinės skaitmeninės tapatybės deklės ekosistemą, remiantis decentralizuotų sistemų kūrimo principais ir sudarant maksimalias sąlygas konkurencijai.</p>	

2.3.3. Rekomenduojamas architektūros modelis Lietuvos kontekstui

Atsižvelgiant į 2.3.2 dalyje išanalizuotus Italijos ir Vokietijos strateginius požiūrius / pritaikymo metodus, siekiant išpildyti eIDAS 2.0 reglamento reikalavimus ir atsižvelgti į techninį EUDIW išpildymą, numatytą pagal ARF, šiame skyriuje pateikiame bendras rekomendacijas dėl architektūros modelio pasirinkimo Lietuvos kontekste.

Rekomenduojame strategiškai orientotis į kaip galimą pilnesnę specifikacijų ir standartų, įvardintų ARF dokumente, palaikymą kuriamoje Lietuvos EUDIW ekosistemoje. Ši rekomendacija yra susijusi su Europos Komisijos nuostata, kad kol standartas ar specifikacija nėra galutinai patvirtinama, ji nėra įtraukiama į susijusius įgyvendinimo aktus. Todėl manome, kad ir per 2026 metus, kol bus kuriama Lietuvos ekosistema, dalis įgyvendinamųjų aktų bus papildyta naujomis specifikacijomis ar standartais.

Įvertinus Lietuvos patirtį, gyventojų populiacijos dydį bei ES privalomų reikalavimų įgyvendinimo tvarkaraštį, siūlome Lietuvos skaitmeninės tapatybės deklės ekosistemos kūrimą pradėti vadovaujantis

Valstybės skaitmeninių sprendimų agentūra	Analitinė galimybių studija „Europinės skaitmeninės tapatybės dėklės įgyvendinimo galimybių analizė ir planas“	Lapas 34 iš 53
---	--	----------------

centralizuotos sistemos kūrimo principais. Dėklės ekosistemos roles rekomenduojama priskirti toms organizacijoms, kurios jau yra susijusios su panašių paslaugų teikimu.

Vėlesniais ekosistemos kūrimo ir vystymo etapais, kai su Europine skaitmeninės tapatybės dėkle susiję reikalavimai bus paruošti ir įgyta susijusi patirtis, bus galima atnaujinti Lietuvos dėklės ekosistemos vystymo strategiją.

Toliau pateikiama lentelė, kurioje išvardintos Europinės skaitmeninės tapatybės dėklės ekosistemos rolės (pagal pirmo etapo, antro uždavinio rezultato dėl ekosistemos ir funkcijų nustatymo pagal ARF v2.6) ir jų vykdymui reikalingų informacinių sistemų (IT) sąrašas bei galimi Lietuvoje jau veikiančių IT sistemų atitikmenys.

Lentelė 15: Europinės skaitmeninės tapatybės dėklės ekosistemos vaidmenys ir jų atitikmenys Lietuvoje

Rolė	Technologijų poreikis	LT veikiančios sistemos galimas vaidmuo	Komentaras dėl įgyvendinimo
Naudotojas (1)	Tvarkyti, saugoti ir pateikti PID duomenis / požymių liudijimus (EAA)		
	Naudoja specializuotą ir sertifikuotą mobiliąją programėlę (palaikančią Android ir iOS), kurią teikia autorizuotas Dėklės teikėjas (2).	Atitikmens nėra, nes EUDIW atitikmens nėra, reikalinga sukurti techninį sprendimą.	Kitos, jau veikiančios programėlės (pvz., bankų ar valstybinių paslaugų) gali būti papildytos dėklės funkcionalumu. Tačiau jų naujos versijos su dėklės funkcionalumu privalės būti sertifikuotos ir notifikautos kaip nacionalinės schemos dalis.
Dėklės teikėjas (2)	Teikti naudotojams sertifikuotą dėklės sprendimą		
	Kuria ir teikia specializuotą ir sertifikuotą mobiliąją programėlę (veikiančią Android ir iOS), naudojamą naudotojų (1).	Atitikmens nėra, reikalinga sukurti techninį EUDIW sprendimą.	Rekomenduojama, kad VSSA įgyvendintų kaip atviro kodo sprendimą, kiek įmanomą pasiremiant ES pilotinių projektų rezultatais, įskaitant programinį kodą.
	Privalo turėti Dėklės programėlių valdymo sistemą.	Atitikmens nėra reikalinga sukurti techninį EUDIW sprendimą.	Pagal ARF - Wallet Provider Backend (WPB).
PID teikėjas (3)	Išduoti naudotojams asmens identifikavimo duomenis (PID)		
	IT sistema, turinti API sąsajas, leidžiančias keistis duomenimis su išorinėmis IT sistemomis ir	Galimybės panaudoti: (I) LR GR IS ir (II) ADIS jas modernizuojant ir pritaikant veikimui EUDIW LT ekosistemoje.	PID yra QEAA, EAA ir PuB-EAA analogas, skiriasi tik teisinis statusas. Techniniu požiūriu ta pati programinė įranga gali būti naudojama

Valstybės skaitmeninių sprendimų agentūra	Analitinė galimybių studija „Europinės skaitmeninės tapatybės dėklės įgyvendinimo galimybių analizė ir planas“	Lapas 35 iš 53
---	--	----------------

Rolė	Technologijų poreikis	LT veikiančios sistemos galimas vaidmuo	Komentaras dėl įgyvendinimo
	išduoti PID, naudojant su dėkle suderintus duomenų formatus ir protokolus.		PID, QEAA, PuB-EAA ir EAA išdavimui.
	Išduotų PID atšaukimų sąrašo sistema (Revocation lists).	Atitiktis nėra.	Privaloma viešinti informaciją apie išduoto PID būseną (statusą). PID išdavimui taikomi ISO 18013 ir SD-JWC VC standartai.
	IT sistema, gebanti suformuoti dėklei reikalingų duomenų užklausą ir, naudojant su dėkle suderintus duomenų formatus bei protokolus, pateikti ją dėklei ir priimti dėklės pateiktus duomenis.	VIISP, duomenų mainų platforma, ją pritaikant veikimui EUDIW ekosistemoje.	Patikrinti ar dėklė į kurią planuojama išduoti PID atitinka visus kvalifikacinius reikalavimus PID išdavimui.
Patikimų dėklės ekosistemos sąrašų teikėjas (4)	Priziūrėti, tvarkyti ir skelbti patikimų sąrašų informaciją ¹⁰		
	Tvarkyti sistemą ir publikuoti patikimų sąrašus.	Šiuo metu RRT tvarko ir skelbia Lietuvos patikimumo užtikrinimo paslaugų ir šių paslaugų teikėjų patikimų sąrašą pagal RRT nuostatus. Taigi, RRT nustato patikimumo užtikrinimo paslaugų teikėjų, kvalifikuotos elektroninės atpažinties priemonės išdavimo paslaugos teikėjų priežiūros įstaigos funkcijas.	<ul style="list-style-type: none"> Sąrašų subjektai numatomi šie: Dėklės teikėjai (Wallet Providers) PID teikėjai Kvalifikuotų EAA teikėjai (QEAA Providers) Viešo

¹⁰ Pastaba:

- Pasikliaujančiosioms šalims nesudaromas patikimumo sąrašas (Trusted List). Prognozuojamas pasikliaujančiųjų šalių skaičius visoje Europos Sąjungoje padarytų tokio sąrašo sudarymą neįmanomu. Vietoje to, pasikliaujančioji šalis gauna prieigos sertifikatą iš prieigos sertifikatų teikėjo (Access Certificate Authority), o šis sertifikatas suteikia dėklės vienetai galimybę autentifikuoti pasikliaujančiąją šalį. Pasikliaujančiųjų šalių ir EUDIW ekosistemos dalyvių registravimui, turi būti įsteigtas ir sukurtas Pasikliaujančiųjų šalių ir EUDIW ekosistemos dalyvių registras, kuriame rekomenduojama registruoti visus pasikliaujančias šalis, ir suteikti registravimo sertifikatus, o techninei prieigai realizuoti, numatoma įgyvendinti prieigos sertifikatų išdavimo ir valdymo priemonės.
- Dėklės teikėjai, PID teikėjai, prieigos sertifikatų teikėjai ir registracijos sertifikatų teikėjai nėra patikimumo užtikrinimo paslaugų teikėjai (TSP) pagal Europos skaitmeninės tapatybės reglamentą. Todėl jų sudaromi patikimumo sąrašai teisine prasme nelaikomi patikimumo sąrašais, kaip apibrėžta Reglamento 22 straipsnyje. Tačiau techniniai reikalavimai visiems patikimumo sąrašams ir jų teikėjams yra vienodi, todėl ARF neskiria šių subjektų patikimumo sąrašų nuo patikimumo sąrašų, sudaromų QEAA ir PuB-EAA teikėjams, kurie laikomi patikimumo užtikrinimo paslaugų teikėjais pagal reglamentą. Nekvalifikuoti EAA teikėjai laikomi patikimumo užtikrinimo paslaugų teikėjais pagal Europos skaitmeninės tapatybės reglamentą. Todėl jiems taip pat gali būti sudaromi patikimumo sąrašai ir gali veikti patikimumo sąrašų teikėjai. Tačiau tai nepatenka į ARF taikymo sritį.

Valstybės skaitmeninių sprendimų agentūra	Analitinė galimybių studija „Europinės skaitmeninės tapatybės dėklės įgyvendinimo galimybių analizė ir planas“	Lapas 36 iš 53
---	--	----------------

Rolė	Technologijų poreikis	LT veikiančios sistemos galimas vaidmuo	Komentaras dėl įgyvendinimo
		IS atitiktims nėra, reikalinga sukurti naujas priemones, greta kuriamo Registro informacinės sistemos, arba jos apimtyje.	<p>elektroninių požymių liudijimo teikėjai (PuB-EAA Providers)</p> <ul style="list-style-type: none"> Kvalifikuoto elektroninio parašo nuotolinio sudarymo paslaugų teikėjai (QESRC Providers) Prieigos sertifikatų teikėjai (Access Certificate Authorities) Registracijos sertifikatų teikėjai
Kvalifikuoto elektroninio požymių liudijimo (QEAA) teikėjas (5)	Išduoti kvalifikuotus požymių liudijimus (QEAA)		
	IT sistema su API sąsajomis, leidžiančiomis keistis duomenimis su išorinėmis informacinėmis sistemomis ir išduoti QEAA, naudojant su dėkle suderintus duomenų formatus ir protokolus.	Atitiktims nėra	PID ir QEAA arba EAA yra elektroninių požymių liudijimų tipai, kurie skiriasi tik teisiniu statusu. Vertinant iš techninės pusės, ta pati programinė įranga gali būti naudojama PID, QEAA, PuB-EAA ir EAA išdavimui. Šalys narės turi užtikrinti galimybę QEAA išdavėjams suteikti prieigą prie informacijos pagal eIDAS reglamento VI priedą.
	Išduotų QEAA atšaukimų sąrašo sistema (Revocation Lists).	Atitiktims nėra.	Viešinti informaciją apie išduoto QEAA būseną (statusą). Skirtingi ISO18013, SD-JWC VC ir W3C
	IT sistema, galinti suformuoti reikiamą duomenų užklausą dėklei ir pateikti arba gauti duomenis,	Atitiktims nėra.	-

Valstybės skaitmeninių sprendimų agentūra	Analitinė galimybių studija „Europinės skaitmeninės tapatybės dėklės įgyvendinimo galimybių analizė ir planas“	Lapas 37 iš 53
---	--	----------------

Rolė	Technologijų poreikis	LT veikiančios sistemos galimas vaidmuo	Komentaras dėl įgyvendinimo
	naudojant su dėkle suderintus formatus ir protokolus.		
Viešojo elektroninio požymių liudijimo (PuB-EAA) teikėjas (6)	Išduoti elektroninių požymių liudijimus (EAA) kaip viešojo sektoriaus institucijai pavestą funkciją		
	IT sistema su API sąsajomis, leidžiančiomis keistis duomenimis su išorinėmis IT sistemomis ir išduoti PuB-EAA, naudojant su dėkle suderintus duomenų formatus ir protokolus.	1) VIISP, duomenų mainų platforma, ją pritaikant veikimui EUDIW ekosistemoje kaip Pub-EAA. 2) RC - vykdytų PuB-EAA išdavimą pagal tvarkomus registrus ir IS 3) Kiti viešojo sektoriaus subjektai - Teisiniu reguliavimu neapribojama galimybė PuB-EAA teikti kitoms už atitinkamą šaltinį atsakingoms viešojo sektoriaus įstaigoms. Praktiniu požiūriu, po 2026 metų numatoma galimybė registruoti Pub-EAA tapti norinčius viešojo sektoriaus subjektus savo tvarkomų IS kaip autentiškų šaltinių apimtyje.	PuB-EAA ir QEAA ar EAA yra to paties tipo elektroninių požymių liudijimai, besiskiriantys tik teisiniu statusu. Vertinant iš techninės pusės, ta pati programinė įranga gali būti naudojama PID, QEAA, PuB-EAA ir EAA išdavimui.
	Išduotų PuB-EAA atšaukimų sąrašo sistema (Revocation Lists).	Atitiktims nėra, priemonės rekomenduojama įgyvendinti kartu su VIISP plėtra Pub-EAA vaidmens pritaikymui.	Viešinti informaciją apie išduoto PuB-EAA būseną (statusą). Skirtingi ISO18013, SD-JWC VC ir W3C.
	IT sistema, galinti suformuoti reikiamą duomenų užklausą dėklei ir pateikti arba gauti duomenis, naudojant su dėkle suderintus duomenų formatus ir protokolus.	VIISP, duomenų mainų platforma, ją pritaikant veikimui EUDIW ekosistemoje.	
Elektroninio požymių liudijimo (EAA) teikėjas (7)	Išduoti nekvalifikuotus požymių liudijimus (EAA)		
	IT sistema su API sąsajomis, leidžiančiomis keistis duomenimis su išorinėmis IT sistemomis ir išduoti EAA, naudojant su dėkle suderintus duomenų	Atitiktims nėra.	EAA, QEAA ir PuB-EAA yra to paties tipo elektroninių požymių liudijimai, besiskiriantys tik teisiniu statusu. Vertinant iš techninės pusės, ta pati programinė įranga gali būti naudojama PID, QEAA, PuB-EAA

Valstybės skaitmeninių sprendimų agentūra	Analitinė galimybių studija „Europinės skaitmeninės tapatybės dėklės įgyvendinimo galimybių analizė ir planas“	Lapas 38 iš 53
---	--	----------------

Rolė	Technologijų poreikis	LT veikiančios sistemos galimas vaidmuo	Komentaras dėl įgyvendinimo
	formatus ir protokolus.		ir EAA išdavimui.
	Išduotų EAA atšaukimų sąrašo sistema (Revocation Lists).	Atitiktims nėra.	Viešinti informaciją apie išduoto EAA būseną (statusą). Skirtingi ISO18013, SD-JWC VC ir W3C.
	IT sistema, galinti suformuoti reikiamą duomenų užklausą dėklei ir pateikti arba gauti duomenis, naudojant su dėkle suderintus duomenų formatus ir protokolus.	Atitiktims nėra.	
Nuotolinio kvalifikuoto elektroninio parašo kūrimo įtaiso teikėjas (8)	Teikti kvalifikuoto elektroninio parašo nuotolinio sudarymo paslaugas		
	Kvalifikuoto nuotolinio elektroninio parašo paslauga dėklėje.	Šiuo metu toks paslaugos teikėjas LT patikimų tiekėjų sąrašė nenustatytas. Numatomas šių subjektų ir jų valdomų IS įtraukimas: <ul style="list-style-type: none"> • Registrų centras yra Juridinių asmenų ir Gyventojų registrų valdytojas, turi reikiamą infrastruktūrą bei iš dalies jau teikia nuotolinio kvalifikuoto elektroninio parašo gavimo funkcionalumą. Reikalinga praplėsti funkcionalumus juos pritaikant veikimui EUDIW ekosistemoje. • Migracijos departamentas turi reikiamą infrastruktūrą bei iš dalies jau teikia nuotolinio kvalifikuoto elektroninio parašo gavimo funkcionalumą. Reikalinga papildomai įvertinti techninius ir funkcinius įgyvendinimo parametrus bei kaštų-naudos santykį. Taip pat reikalinga atitinkamai praplėsti funkcionalumus juos pritaikant veikimui EUDIW ekosistemoje • Numatoma, jog ateityje (po 2026 metų) verslo subjektai taip pat galėtų teikti nuotolinio 	Svarbu paminėti, kad be nuotolinio kvalifikuoto elektroninio parašo kūrimo įtaiso teikėjo, ARF įvardija numato galimas kitas tris e.parašo architektūras: <ol style="list-style-type: none"> 1. Local external WSCD 2. Local internal WSCD 3. Local native WSCD

Valstybės skaitmeninių sprendimų agentūra	Analitinė galimybių studija „Europinės skaitmeninės tapatybės dėklės įgyvendinimo galimybių analizė ir planas“	Lapas 39 iš 53
---	--	----------------

Rolė	Technologijų poreikis	LT veikiančios sistemos galimas vaidmuo	Komentaras dėl įgyvendinimo
		elektroninio parašo kūrimo įtaisus pagal turimus IS. Taip pat svarstyтина detaliau nagrinėti galimybes dėl esamų priemonių (pavyzdžiui, LT ID, Mobile ID) pritaikymo.	
	Kvalifikuoto elektroninio parašo paslauga dėklėje.	mCard-LTU patirties arba, jeigu valstybė turi intelektinės nuosavybės teisę, panaudojimas įgyvendinant reikalingas priemones.	Pačioje dėklėje gali būti palaikomi ir kiti trys elektroninio pasirašymo įgyvendinimo scenarijai: 1. Local external WSCD 2. Local internal WSCD 3. Local native WSCD Panaudojant mCard-LTU modelį, kvalifikuoto elektroninio parašo paslaugos gali būti integruotos į dėklę, remiantis pirmu (1. Local external WSCD) scenarijumi.
Autentiškas šaltinis (9)	Veikti kaip autentiškas tam tikrų požymių šaltinis		
	Reglamentas nereikalauja sukurti naujų autentiškų šaltinių, daroma prielaida, kad valstybė narė jau turi reikiamus informacijos autentiškus šaltinius.	Valstybės informacinės sistemos ir registrai, pritaikyti teikti duomenis naudojant VIISP duomenų platformos priemones, ir kiek reikalinga, modernizuoti elektroninio požymių liudijimo teikimui naudojant Pub-EAA vaidmeniui pritaikytą VIISP duomenų mainų platformą, RISR tvarkomą metaduomenų katalogą ir, ateityje, išmaniasią sutartis, kurių veikimas užtikrintas naudojant VIISP ir ISR priemones.	Svarbi dalis - Reglamento VI priedo reikalavimai, pagal kuriuos valstybės narės turi užtikrinti prieigą prie platesnio informacijos sąrašo. Pavyzdžiui, mokslo diplomai ar profesiniai kvalifikacijos pažymėjimai.
Pasikliaujančioji šalis (10)	Pateikti prašymą ir gauti iš dėklės vieneto perduodamus požymius		
	IT sistema su API sąsajomis, leidžiančiomis keistis duomenimis su išorinėmis IT sistemomis, taip pat suformuoti ir pateikti duomenų užklausą dėklei	VIISP, duomenų mainų platforma ir paslaugų katalogas, juos pritaikant veikimui EUDIW ekosistemoje.	Tikėtina, kad reikalingas funkcionalumas galėtų būti išplėstas remiantis jau šiuo metu VIISP egzistuojančiais moduliais, kurie vykdo vartotojų identifikavimą ir

Valstybės skaitmeninių sprendimų agentūra	Analitinė galimybių studija „Europinės skaitmeninės tapatybės dėklės įgyvendinimo galimybių analizė ir planas“	Lapas 40 iš 53
---	--	----------------

Rolė	Technologijų poreikis	LT veikiančios sistemos galimas vaidmuo	Komentaras dėl įgyvendinimo
	pagal suderintus duomenų formatus ir protokolus. Priimti dėklės pateiktus duomenis pagal suderintus duomenų formatus ir protokolus.		autentifikavimą.
Tarpinė pasikliaujančioji šalis	Pateikti prašymą ir gauti iš dėklės vieneto perduodamus požymius kitos organizacijos vardu		
	IT sistema su API sąsajomis, leidžiančiomis keistis duomenimis su išorinėmis IT sistemomis, taip pat suformuoti ir pateikti duomenų užklausą dėklei pagal suderintus duomenų formatus ir protokolus. Priimti dėklės pateiktus duomenis pagal suderintus duomenų formatus ir protokolus.	VIISP, duomenų mainų platforma ir paslaugų katalogas, juos pritaikant veikimui EUDIW ekosistemoje kaip tarpinei (tarpininkaujančiajai) šaliai (Intermediating Relying Party).	Tikėtina, kad reikalingas funkcionalumas galėtų būti išplėstas remiantis jau šiuo metu VIISP egzistuojančiais moduliais, kurie vykdo vartotojų identifikavimą ir autentifikavimą.
Atitikties vertinimo įstaiga (CAB) (11)	Sertifikuoti dėklės sprendimus ir audituoti patikimumo užtikrinimo paslaugų teikėjus (TSP)		
	Susijusi IT sistema neplanuojama.	-	-
Dėklės priežiūros įstaiga (12)	Vertinti, ar ekosistemos dalyviai veikia tinkamai.		
	Rekomenduojama panaudoti naujai steigiamo ir kuriamo EUDIW dalyvių Registro informacinės sistemos priemonės.	Atitiktis nėra.	Reikalingi įgyvendinti stebėsenos ir analitikos priemonės, užtikrinant organizacinį sąveikumą su NKSC dėl kibernetinės saugos incidentų ir su VDAI dėl asmens

Valstybės skaitmeninių sprendimų agentūra	Analitinė galimybių studija „Europinės skaitmeninės tapatybės dėklės įgyvendinimo galimybių analizė ir planas“	Lapas 41 iš 53
---	--	----------------

Rolė	Technologijų poreikis	LT veikiančios sistemos galimas vaidmuo	Komentaras dėl įgyvendinimo
			duomenų apsaugos incidentų, susijusių su EUDIW dalyviais stebėsenos ir atsakomųjų priemonių pritaikymo (laikino dalyvių vaidmenų sustabdymo, atšaukimo, atnaujinimo).
Įrenginių gamintojas ir susijusių sistemų teikėjas (13)	Tiekėjai sprendžia savarankiškai.	Atitiktis nėra.	Suteikti EUDIW eksperimentinę aplinką, naujų skaitmeninės dėklės sprendimų vystymo palaikymui, išbandymui, testavimui, prie EUDIW ekosistemos ketinančių prisijungti išbandymui.
	Nustatyti ir paskelbti liudijimų taisyklių rinkinius ir schemas		
Požymių liudijimo schemas teikėjas (14)	IT sistema viešinti sukurtus požymių liudijimo rinkinius ir schemas. Viešinimo tipai – žmogaus ir kompiuterio skaitomu formatu.	Valstybės metaduomenų katalogas, kurio naudojimas planuojamas nuo 2025 m. gruodžio mėn.	Požymių liudijimo duomenų rinkinius ir schemas rekomenduojama tvarkyti ir skelbti valstybės metaduomenų kataloge ir duomenų valdymo infrastruktūroje. VSSA yra atsakinga už valstybinių informacinių sistemų duomenų struktūrų aprašų ir Valstybės informacinių išteklių metaduomenų standarto tvarkymą. Šių schemų tarkymo funkcija inkrementaliai praplėstų ir būtų tiesiogiai susijusios su esamomis VSSA funkcijomis.
Nacionalinė	Akredituoti atitikties vertinimo įstaigas (CAB) pagal ES reglamentus		

Valstybės skaitmeninių sprendimų agentūra	Analitinė galimybių studija „Europinės skaitmeninės tapatybės deklės įgyvendinimo galimybių analizė ir planas“	Lapas 42 iš 53
---	--	----------------

Rolė	Technologijų poreikis	LT veikiančios sistemos galimas vaidmuo	Komentaras dėl įgyvendinimo
akreditacijos įstaiga (15)	Susijusi IT sistema neplanuojama.	-	-
Registratorius (16)	Tvarko teikėjų ir pasikliaujančiųjų šalių registraciją		
	IT sistema registruoti šalies narės PID, QEAA, Pub-EAA, EAA tiekėjus ir susijusias šalis. Registracijos procesą, sąlygas ir reikalavimus nustatys kiekviena valstybė narė.	Atitiktis nėra, reikalinga įsteigti EUDIW dalyvių registrą ir sukurti EUDIW dalyvių registro informacinę sistemą.	Duomenys apie subjektą registruoja registratorius ir jie pateikiami internete žmogaus ir kompiuterio skaitomu formatu bet kuriai suinteresuotai šaliai. Registruoti subjektai gauna prieigos sertifikatą iš prieigos sertifikatų teikėjo (17). Jei registratorius tai palaiko, registruotas subjektas taip pat gauna registracijos sertifikatą iš registracijos sertifikatų teikėjo (18). Tuo atveju jei registratorius nepalaiko registracijos sertifikatų išdavimo, jis privalo viešinti susijusius sąrašus, kad deklė turėtų galimybę patikrinti kokius atributus susijusi šalis turi teisę gauti iš deklės.
Prieigos sertifikatų teikėjas (17)	Išduoti prieigos sertifikatus autentifikavimui		
	IT sistema turi sukurti ir išduoti prieigos sertifikatus šalies narės PID, QEAA, Pub-EAA, EAA tiekėjams ir susijusioms šalims.	Kaip registrų infrastruktūros tvarkytojas ir duomenų teikimą vykdanči institucija, RC numatoma teikti prieigos sertifikatus. RC turi technines ir programines priemones generuoti prieigos sertifikatus pagal reikalavimus, pavyzdžiui, panaudojant RC, el. parašo padalinio turimą infrastruktūrą ir priemones.	RC turi technines ir programines priemones generuoti prieigos sertifikatus pagal reikalavimus, pavyzdžiui, panaudojant RC, el. parašo padalinio turimą infrastruktūrą ir priemones.
	Sistema viešinti	Tiesioginio atitiktis nėra, gali būti	Kadangi esami VIISP

Valstybės skaitmeninių sprendimų agentūra	Analitinė galimybių studija „Europinės skaitmeninės tapatybės dėklės įgyvendinimo galimybių analizė ir planas“	Lapas 43 iš 53
---	--	----------------

Rolė	Technologijų poreikis	LT veikiančios sistemos galimas vaidmuo	Komentaras dėl įgyvendinimo
	išduotų prieigos sertifikatų atšaukimo sąrašus (Certificate Revocation List).	pritaikomos VIISP, duomenų mainų platformos, ir ISR IS metaduomenų katalogo ir duomenų valdymo infrastruktūros priemonės.	ir ISR IS sprendimai numato naudoti x.509 sertifikatus duomenų mainų ir prieigos prie duomenų pagal metaduomenų katalogo, būtų reikalingas sąlyginai nedidelės apimties išplėtimas esamuose sprendimuose.
Registracijos sertifikatų teikėjas (18)	Išduoti registracijos sertifikatus, patvirtinančius registracijos statusą ir veiklos apimtį	<p>IT sistema sukurti ir išduoti registracijos sertifikatus šalies narės PID, QEAA, Pub-EAA, EAA tiekėjams ir susijusioms šalims.</p> <p>Atitikmens nėra.</p> <p>Reikalingos naujos priemonės, kartu su Registratoriaus funkcijoms įgyvendinti reikalingu įsteigti EUDIW dalyvių registru ir sukurti reikalingą informacinę sistemą.</p> <p>Šiomis priemonėmis būtų išduodami ir tvarkomi registracijos sertifikatai, reikalingi naujų dėklės ekosistemos dalyvių įtraukimui, funkcinių vaidmenų įgyvendinimui ir jų veiklos EUDIW ekosistemoje priežiūros priemonėms įgyvendinti.</p> <p>Numatoma, jog RC turi technines ir programines priemones generuoti prieigos sertifikatus pagal reikalavimus, pavyzdžiui, panaudojant RC, el. parašo padalinio turimą infrastruktūrą ir priemones.</p>	<p>Neprivaloma.</p> <p>Gali būti naudojamos modifikuoto formato x.509 sertifikatais pagrįsti technologiniai sprendimai.</p> <p>VSSA, kaip Viešojo sektoriaus/ viešųjų ir administracinių paslaugų teikėjų duomenų tvarkytojas Registre (kaip VIISP esančio viešųjų ir administracinių katalogo tvarkytojas) ir duomenų teikėjas registravimui, bei registracijos sertifikatų išdavėjas viešojo sektoriaus / viešųjų ir administracinių paslaugų teikėjams (patikimumo užtikrinimo inkarai pateikiami valstybės administruojamame paslaugų kataloge).</p> <p>RC, kaip Verslo subjektų duomenų tvarkytojas Registre ir duomenų teikėjas registravimui, ir registracijos sertifikato išdavėjas verslo subjektams (patikimumo</p>

Valstybės skaitmeninių sprendimų agentūra	Analitinė galimybių studija „Europinės skaitmeninės tapatybės dėklės įgyvendinimo galimybių analizė ir planas“	Lapas 44 iš 53
---	--	----------------

Rolė	Technologijų poreikis	LT veikiančios sistemos galimas vaidmuo	Komentaras dėl įgyvendinimo
			<p>užtikrinimo inkarai pateikiami JAR viešojoje prieigoje).</p> <p>RRT, kaip skaitmeninių paslaugų teikėjų duomenų tvarkytojas Registre ir duomenų teikėjas registravimui (patikimumo užtikrinimo inkarai pateikiami SP teikėjų kataloge).</p> <p>Taip pat svarstyta panaudoti QWAC sertifikatus, tačiau jų kvalifikuotų išdavėjų ir registruojančių subjektų Lietuvoje nenustatyta.</p> <p>Jei šalis narė nusprendžia neišdavinti registracijos sertifikatų, tada privalu tą pačią informaciją skelbti Registratoriaus „online“ (16) paslauga.</p>
Dėklės sertifikavimo schemos savininkas (19)	Užtikrinti dėklės schemos priežiūrą, standartų ir procedūrų nustatymą bei sąveiką su nacionalinėmis akreditacijos įstaigomis (NAB) ir atitikties vertinimo įstaigomis (CAB)		
	Susijusi IT sistema neplanuojama.	-	-
Už kibernetinių pažeidimų valdymą atsakinga institucija (20)	Įgyvendinti kibernetinio saugumo politiką		
	Susijusi IT sistema neplanuojama.	-	-
Asmens duomenų apsaugos nuostatas įgyvendinanti institucija	Įgyvendinti privatumo nuostatas		
	Susijusi IT sistema neplanuojama.	-	-

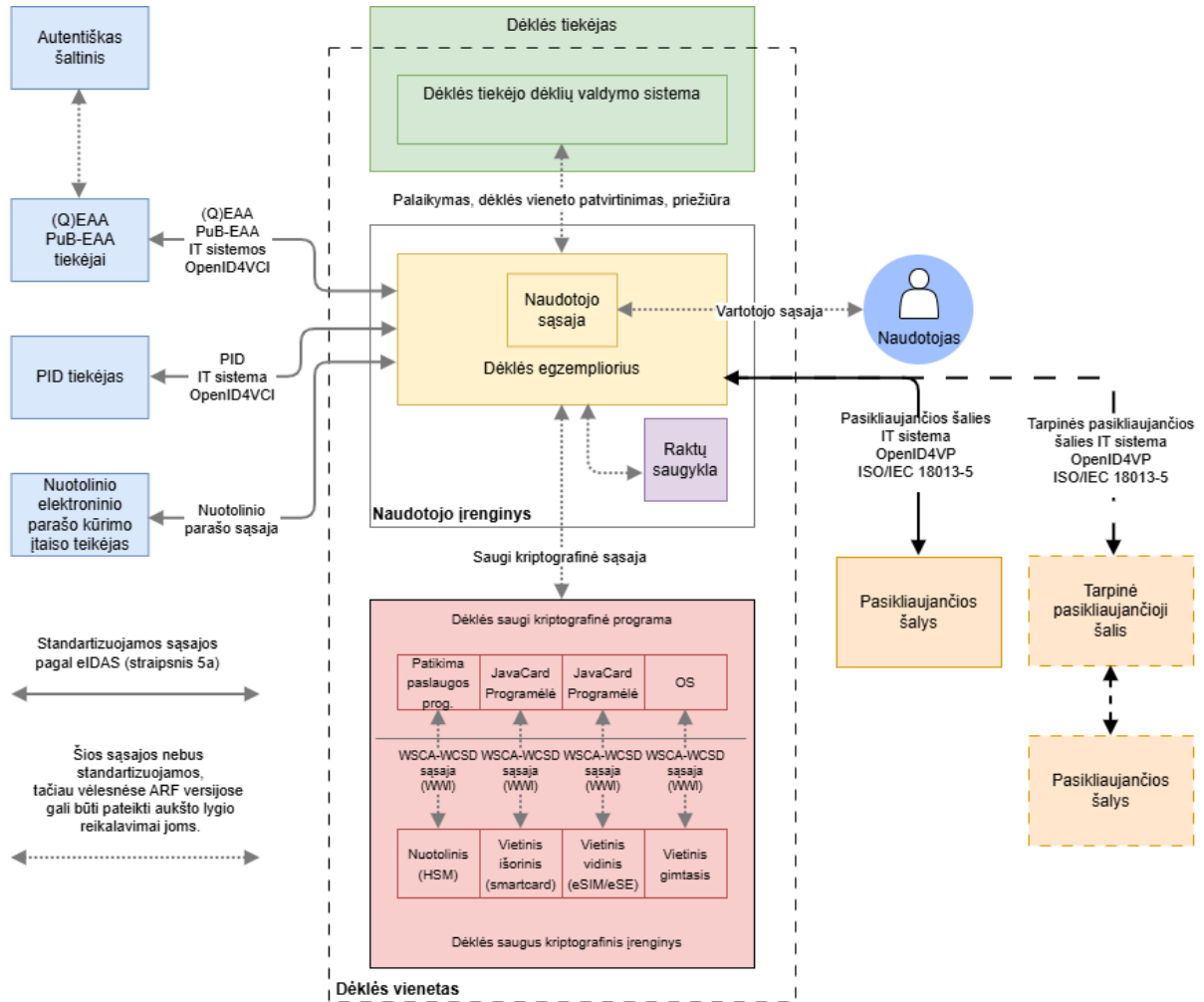
Valstybės skaitmeninių sprendimų agentūra	Analitinė galimybių studija „Europinės skaitmeninės tapatybės dėklės įgyvendinimo galimybių analizė ir planas“	Lapas 45 iš 53
---	--	----------------

Rolė	Technologijų poreikis	LT veikiančios sistemos galimas vaidmuo	Komentaras dėl įgyvendinimo
(21)			
Skaitmeninės veiklos atsparumo nuostatas finansų sektoriuje įgyvendinanti institucija (22)	Užtikrinti skaitmeninės veiklos atsparumą pagal nustatytus saugumo reikalavimus finansų sektoriaus subjektų veiklos procesuose Susijusi IT sistema neplanuojama.	-	-

Kuriant Lietuvos skaitmeninės tapatybės dėklės architektūros modelį reikėtų vadovautis baziniu architektūros modeliu pavišintu ARF dokumente (versija 2.6.0. pastraipa 4.3). Žemiau pateiktas paveikslėlis atvaizduoja ARF pavišintą modelį, papildytą tarpine pasikliaujančia šalimi. Manome, kad Lietuvos kontekste tokia rolė bus reikalinga įgyvendinant vartotojų tapatybės patvirtinimo, dėklės pagalba, epaslaugos.lt (VIISP) portale.

Pastaba: Atsižvelgiant į tai, kad ARF dokumentas yra vis dar atnaujinamas, detalaus ARF pateiktos architektūros modelio aprašymo nekartojame. Aprašome tik tas dalis, kurios galimai skirsis nuo ARF modelio. Visais kitais atvejais rekomenduojame vadovautis aprašymu pateiktu ARF dokumente ir sekti jo pokyčius.

Paveikslėlis 1: ARF siūlomas architektūros modelis



Europinės skaitmeninės tapatybės dėklės panaudojimas sudaro galimybę tiek patvirtinti naudotojo tapatybę ar pasirašyti elektroniniu parašu skaitmeninius dokumentus, tiek gauti su naudotoju susijusią informaciją Elektroninių požymių liudijimų (EAA) formatu, kurie turi tokią pačią juridinę galią kaip ir tokio pat turinio spausdinti dokumentai.

Atsižvelgiant į tai, su naujomis dėklės sukuriomomis galimybėmis rekomenduotume VIISP sistemoje įgyvendinti šias, su dėkle susijusias funkcijas:

A. Vartotojo tapatybės patvirtinimas dėklės pagalba (tapatybės patvirtinimo scenarijai naudojant dėklę).

a. El. paslaugos atvejai

Scenarijus 1 - vartotojas jungiasi į SPP paslaugų portalą, prieina prie savo profilio ir t.t. Tokiu atveju SPP paslaugų portalas kreipiasi į SPP Tapatybės Nustatymo modulį (dabartinį VIISP tapatybės nustatymą), **RP - VSSA VIISP**.

Scenarijus 2 - vartotojas el. paslauga naudojami per epaslaugos.lt (SPP), bet paslauga yra teikiama per įstaigos portalą. Tada SPP paslaugų portalas kreipiasi į SPP Tapatybės Nustatymo modulį (dabartinį VIISP tapatybės nustatymą) (**RP - VSSA VIISP**) ir perduoda tapatybės patvirtinimo faktą institucijai (OpenID Connect, SPP Tapatybės Nustatymo

Valstybės skaitmeninių sprendimų agentūra	Analitinė galimybių studija „Europinės skaitmeninės tapatybės dėklės įgyvendinimo galimybių analizė ir planas“	Lapas 47 iš 53
---	--	----------------

modulis).

Scenarijus 3 - vartotojas bendrauja tiesiogiai su el. paslauga institucijos portale. Autentifikacija vykdoma per SPP Tapatybės nustatymo modulį (**SPP TNM (intermediate RP)**)

Scenarijus 4 - vartotojas bendrauja tiesiogiai su el. paslauga institucijos portale. Autentifikacija vykdoma tiesiogiai pačios institucijos (RP - institucija).

b. Betarpiški (Proximity) atvejai

Scenarijus 5 – vartotojas bendrauja betarpiškai su institucijos atstovu. Vartotojas jo identifikacijai pateikia dėklėje esantį PID. Institucijos atstovas naudodamasis Dėklės skaitytuvo pagalba patikrina vartotojo tapatybę.

Scenarijus 6 – vartotojas bendrauja betarpiškai su institucijos atstovu ir pateikto PID atributai turi būti perduodami ir išsaugomi informacinėje sistemoje kaip paslaugos teikimo proceso dalis.

B. Tarpininkavimo paslauga kuriant elektroninių požymių liudijimų užklausa, gauti iš dėklės duomenis ir perduoti juos kitai valstybės institucijai. VIISP veikia kaip tarpinė susijusi šalis. SVARBU: VIISP šiuo atveju privalo nekaupti su šia paslauga gaunamų duomenų, o juos tik perduoti.

a. El. paslaugos atvejai

Scenarijus 7 - Paslauga teikiama (inicijuojama) per e-paslaugos.lt (sukonfiguruota paslauga). **RP - Institucija, teikianti paslaugą, o Intermediate RP - VSSA VIISP. Tokiu atveju VIISP ir paslaugos teikėja (institucija) privalo užtikrinti reglamento reikalavimą išsaugoti tranzakcijų įrašus.**

Scenarijus 8 - Paslauga teikiama (inicijuojama) per institucijos portalą. **RP - institucija, VIISP - Intermediate RP.**

Scenarijus 9 - Paslauga teikiama (inicijuojama) per institucijos portalą **RP – institucija. VIISP nedalyvauja procese.**

b. Betarpiški (Proximity) atvejai

Scenarijus 10 – Vartotojas bendrauja betarpiškai su institucijos atstovu. Vartotojas, pateikia jo dėklėje esančius elektroninius atestacijos atributus. Institucijos atstovas naudodamasis Dėklės skaitytuvo pagalba patikrina pateiktus elektroninius atestacijos atributus .

Scenarijus 11 – Vartotojas bendrauja betarpiškai su institucijos atstovu, vartotojo pateikti elektroniniai atestacijos atributai turi būti perduodami ir išsaugomi informacinėje sistemoje kaip paslaugos teikimo proceso dalis.

C. Elektroninių Atestacijos Atributų išdavimo tarpininkavimo paslauga kitoms institucijoms. VIISP veikia kaip PuB-EAA tiekėjas:

a. El. paslaugos atvejai

Scenarijus 12 - Paslauga teikiama (inicijuojama) per e-paslaugos.lt. PuB-EAA (išdavėjas) - VIISP, Authentic Source – Institucija.

Scenarijus 13 - Paslauga teikiama (inicijuojama) per e-paslaugos.lt. PuB-EAA (išdavėjas) - Institucija, Authentic Source – Institucija.

Scenarijus 14 - Paslauga teikiama (inicijuojama) per institucijos portalą. PuB-EAA (išdavėjas) - VIISP, Authentic Source – Institucija.

Scenarijus 15 - Paslauga teikiama (inicijuojama) per institucijos portalą. PuB-EAA (išdavėjas) - institucija, Authentic Source – Institucija.

b. Betarpiški (Proximity) atvejai

Scenarijus 16 - Vartotojas bendrauja betarpiškai su institucijos atstovu. Institucijos atstovas naudodamasis Dėklės terminalo pagalba pateikia vartotojui išduodamus

Valstybės skaitmeninių sprendimų agentūra	Analitinė galimybių studija „Europinės skaitmeninės tapatybės dėklės įgyvendinimo galimybių analizė ir planas“	Lapas 48 iš 53
---	--	----------------

elektroninius atestacijos atributus .

Kuriant Europinės skaitmeninės tapatybės dėklės ekosistemą, verta įvertinti ir galimybes kituose etapuose plėsti ir kurti visiškai naujas skaitmenines paslaugas, kurių įgyvendinimas be dėklės pagalbos būtų sudėtingas ar neįmanomas. Žemiau pateikiame tokių paslaugų pavyzdžius:

- Nuotolinės medicinos paslaugų teikimo atvejui – identifikuoti ne tik pacientą, bet ir suteikti galimybę pacientui patikrinti gydytojo teisę teikti sveikatos priežiūros paslaugas.
- Šalies mastu parengti su „KYC“ susijusių Elektroninių požymių liudijimų (EAA) „Rulebook“, kuris supaprastintų paslaugų institucijoms, privalančioms vykdyti AML reglamento reikalavimus, vartotojams reguliariai teikiamos informacijos pateikimą finansų institucijoms (Su planuojamais, Pinigų Plovimo Terorizmo Finansavimo Prevencijos (PPTFP) teisės aktais susijusių reikalavimų įgyvendinimui).
- Sudaryti galimybę iš e. sveikatos sistemos gauti receptinius vaistus Pub-EAA formatu dėklėje, taip suteikiant teisę pacientui įsigyti receptinius vaistus kitoje ES valstybėje narėje.
- Sudaryti galimybę dėklės pagalba identifikuoti skambinantįjį telefonu, tokiu būdu mažinant rizikas, susijusias su sukčiavimu.

Atsižvelgiant į Italijos ir Vokietijos Europinės skaitmeninės tapatybės dėklės architektūrų analizę, taip pat į ARF dokumente numatytus vaidmenis, techninius reikalavimus ir duomenų apsikeitimo principus, lentelėje žemiau pateikiame rekomendacijas dėl Europinės skaitmeninės tapatybės dėklės ekosistemos kūrimo ir įgyvendinimo Lietuvoje. Rekomendacijos orientuotos į Lietuvos institucijų brandą, jau veikiančias informacines sistemas, duomenų šaltinius bei nacionalinę skaitmeninių paslaugų teikimo praktiką, siekiant užtikrinti sklandų perėjimą prie EUDIW reikalavimų ir maksimaliai pasinaudoti dėklės teikiama naujomis galimybėmis.

Pastaba: Verta pastebėti, jog ARF nėra normatyvinis dokumentas, tad pateiktos rekomendacijos yra numatytos pagal ARF 2.6 versijos komponentus ir yra tikimybė, jog bus reikalinga šias rekomendacijas peržiūrėti ir įvertinti pagal pokyčius, įtrauktus į naujesnes ARF versijas.

Lentelė 16: Siūloma EUDIW įgyvendinimo techninė architektūra ir jos alternatyvos

<p>1. Rekomendacijos dėl duomenų apsikeitimo mechanizmo įgyvendinamumo Lietuvos kontekste</p>
<p>ARF dokumentas ir eIDAS 2.0 reglamento įgyvendinimo aktai griežtai reglamentuoja su PID išdavimu ir pateikimu susijusius duomenų mainus su Europine skaitmeninės tapatybės dėkle.</p> <p>PID atributų rinkinys turi būti išduotas šiais dviem duomenų formatais: SD-JWT VC ir ISO/IEC 18013-5 (apibendrinta ISO/IEC 23220-2). Kai tuo tarpu (Q)EAA ir PuB-EAA atveju atestacijos atributų rinkiniai gali būti išduoti ir trečio tipo duomenų formatu W3C VCDM 2.0.</p> <p>Duomenų apsikeitimo su dėkle protokolai taip pat yra griežtai reglamentuoti, tai OpenID4VCI – išduodant PID ar (Q)EAA/PuB-EAA ir OpenID4VP protokolas pateikti duomenų užklausą dėklei ir juos gauti. Duomenų užklausai ir jų gavimui net esant ribotam ar nepasiekiamam interneto ryšiui, kai naudojama betarpiškam duomenų gavimui skirta programėlė – protokolas specifikuotas standarte ISO/IEC 18013-5. Tokiu atveju naudojamas tarp įrenginių duomenų gavimo funkcija (device-to-device data retrieval) pasitelkiant šiuolaikines ryšio technologijas, pvz. Bluetooth.</p> <p>Tuo pačiu ARF dokumentas ir įgyvendinimo aktai nereglamentuoja vidinių IT sistemų duomenų formatų ar jų tarpusavio apsikeitimo protokolų. Praktikoje IT sistemos, kurios teikia vartotojo identifikavimo, autorizavimo ar duomenų pateikimo funkcijas (PID, (Q)EAA, PuB-EAA), dažniausiai naudoja REST API sąsajas ir JSON duomenų formatą, kad galėtų suformuoti tinkamas užklausas dėklei bei priimti iš jos gautus duomenis. Tokiu būdu užtikrinamas suderinamumas tiek su esamomis valstybės IT sistemomis, tiek su dėklės specifikacijomis ir ARF reikalavimais. Pavyzdžiui tokia sistema iš Gyventojų Registro per API REST sąsają, JSON formatu gauna visą reikiamą informaciją išduoti PID, ar gavus duomenis iš dėklės sistema REST API pagalba ir JSON duomenų formatu atiduoda informaciją apie pateiktą PID.</p>
<p>2. Rekomendacijos dėl sąveikumo ir ARF reikalavimų įgyvendinamumo Lietuvos kontekste</p>
<p>Rekomenduojama laikytis ARF dokumento kaip bendrojo EUDIW ekosistemos įgyvendinimo modelio (angl. blueprint). Nacionalinis EUDIW architektūros modelis turėtų būti rengiamas inkrementiškai,</p>

Valstybės skaitmeninių sprendimų agentūra	Analitinė galimybių studija „Europinės skaitmeninės tapatybės dėklės įgyvendinimo galimybių analizė ir planas“	Lapas 49 iš 53
---	--	----------------

periodiškai atnaujinamas ir derinamas su ARF reikalavimais bei ES lygmens techninėmis specifikacijomis. Atsižvelgiant į tai, kad Lietuva EUDIW ekosistemą įsigys pirkimo būdu, inkrementinis vystymas turėtų būti realizuojamas per paslaugų teikėjo atliekamus darbų etapus, užtikrinant, kad sprendimas atitiktų ARF numatytas funkcines, technines ir sąveikumo gaires.

3. Rekomendacijos dėl Lietuvos turimų elektroninės atpažinties ir patikimumo užtikrinimo paslaugų sistemų pakartotinio panaudojimo galimybės EUDIW aplinkoje

Su Europine skaitmeninės tapatybės dėkle susiję techniniai reikalavimai nereikalauja privalomai pasinaudoti šalyje narėje turima elektroninės atpažinties ir (ar) patikimumo užtikrinimo paslaugų sistemomis, tačiau rekomenduoja dėklės ekosistemą kurti remiantis šalyje narėje jau egzistuojančiomis atpažinties sistemomis. Verta paminėti, jog saugumo lygių nustatymo reikalavimai, įtraukti į Komisijos įgyvendinimo reglamento dokumentą 2015/1502, vis dar galioja ir sudaro pagrindą EUDIW ekosistemos veikimui, kadangi PID išdavimui ir EUDIW aktyvacijai vartotojas privalo naudoti elektroninės atpažinties priemonę, kuri atitinka aukšto saugumo lygmens reikalavimus (LoA High) arba pakankamo saugumo lygmens su papildomu aukšto saugumo lygmens elementu.

Pagal ARF dokumentą, PID teikėjai gali būti tos pačios organizacijos, kurios šiandien išduoda oficialius asmens tapatybės dokumentus, elektroninės tapatybės priemones ir kt. PID teikėjai gali būti tos pačios organizacijos, kaip ir dėklės teikėjai. Jei organizacija veikia ir kaip PID teikėja, ir kaip dėklės teikėja, ji privalo laikytis visų PID teikėjams ir dėklės teikėjams keliamų reikalavimų. Todėl verta paminėti Lietuvoje jau turimą sistemą „mCard LTU“, kuri gali būti panaudota PID išdavimui, ypač jei PID išdavimas vykdomas nuotoliniu būdu.

Svarbu atkreipti dėmesį į tai, kad šiuo metu „mCard LTU“ naudojamas metodas, naudojant išorinę asmens tapatybės kortelę, eIDAS reglamento rekomenduojamas kaip pereinamojo laikotarpio priemonė (EU 2024/1183, preambulė (29)). Taip pat svarbu paminėti, kad naujoji eIDAS reglamento redakcija naudoja esamas elektroninės atpažinties ar patikimumo užtikrinimo paslaugų sistemas kaip pagrindą.

4. Rekomendacijos dėl informacijos saugos (NIS 2 direktyva) ir konfidencialumo reikalavimų įgyvendinamumo (BDAR) Lietuvos kontekste

Naujoji eIDAS reglamento redakcija sukuria naujas galimybes kurti didesnio saugumo paslaugas ir atsisakyti perteklinės informacijos rinkimo. Rekomendacija kuriant Lietuvos dėklės ekosistemą įtraukti ir tokias organizacijas kaip, FNTT, NKSC, Lietuvos Banką ar pavyzdžiui Pinigų plovimo prevencijos kompetencijų centrą. Tinkamas dėklės panaudojimas įgalintų kurti ar modifikuoti jau esamas paslaugas, kurios mažintų rizikas susijusias su sukčiavimu skaitmeninėje erdvėje, leistų atsisakyti perteklinės, su asmeniu susijusios asmens informacijos viešinimo.

Dėklės atsiradimas sukuria technines galimybes realizuoti funkciją, kai naudotojas gali kurti ir naudoti slapyvardžius prieigai prie internetinių paslaugų (EU 2024/1183, preambulė (22)).

5. Rekomendacijos dėl pradinių paslaugų teikimo kanalų suteikimo ir plečiamumo galimybių Lietuvos kontekste

Rekomenduojama pradiniu etapu (iki 2026 m. gruodžio mėnesio) sukurti Europinės skaitmeninės tapatybės dėklės ekosistemą, galinčią išduoti PID į Lietuvoje išleistą ir sertifikuotą dėklę, bei užtikrinti galimybę, naudojant dėklę ir joje esantį PID, prisijungti prie epaslaugos.lt (VIISP) portalo.

Idealiu atveju iki minėtos datos taip pat būtų parinkti ir įgyvendinti keli papildomi atestacijos atributų rinkinio panaudojimo atvejai, kurie leistų pademonstruoti šalies gyventojams geresnes galimybes naudotis skaitmeninėmis paslaugomis pasitelkiant dėklę.

6. Rekomendacijos dėl naudotojo patirties ir prieinamumo EUDIW Lietuvos kontekste

Rekomenduojama vadovautis EUDIW įgyvendinimo aktais, ARF rekomendacijomis ir paplitusiais industrijos, pritaikant ir detalizuojant EUDIW LT įgyvendinimo techniniame dokumente, o įgyvendinimo metu įtraukti galutinių naudotojų grupės, kiek įmanoma iš anksto suteikiant galimybę išbandyti panaudojimo atvejus ir suenkant atsiliepimus ir naudotojų patirties įžvalgas, pritaikant naudotojų sąsajas ir naudojimo režimus pagal naudotojų tipus (persona types). Nuo pat dėklės kūrimo pradžios svarbu užtikrinti daugiakalbystės palaikymą – pirmiausia, lietuviškai ir angliškai - tiek dėklės vartotojo sąsajoje, tiek ir dėklėje išduodamų PID, (Q)EAA bei PuB-EAA atestacijų atributuose.

Valstybės skaitmeninių sprendimų agentūra	Analitinė galimybių studija „Europinės skaitmeninės tapatybės dėklės įgyvendinimo galimybių analizė ir planas“	Lapas 50 iš 53
---	--	----------------

Išvados ir rekomendacijos

Šio analitinės studijos etapo metu buvo detalizuotai įvertintas Lietuvos informacinių sistemų, registrų ir kitų IT sprendimų techninis parengtumas integracijai į Europinės skaitmeninės tapatybės dėklės ekosistemą. Vertinimas atliktas remiantis ARF dokumento techninėmis specifikacijomis, Lietuvos institucijų pateiktais duomenimis ir studijos metu surinkta informacija apie šiuo metu veikiančias technologines infrastruktūras.

Taip pat šiame etape buvo identifikuoti ir įvertinti pagrindiniai Lietuvos ekosistemai aktualūs dėklės vaidmenys, jų funkcijos ir atitiktis ARF reikalavimams. Išanalizuota, kurios valstybės informacinės sistemos galėtų atlikti tam tikras Europinės skaitmeninės tapatybės dėklės ekosistemos funkcijas, kur reikalingi nauji sprendimai, o kur galima remtis jau veikiančiomis platformomis. Atskirai įvertintos duomenų apsikeitimo technologinės galimybės, integracijų poreikiai, būtinų API ar protokolų parengimas bei potencialios techninės rizikos.

Toliau pateikiamos šio etapo pagrindinės išvados ir rekomendacijos.

Lentelė 17: Studijos 2 Etapo pagrindinės techninio parengtumo vertinimo išvalgos

Nr.	Išvalga dėl praktinio įgyvendinimo	Rekomendacija
1.	Esamos Lietuvos informacinės sistemos didžiaja dalimi dengia EUDIW techninės ekosistemos palaikymui būtinas funkcijas. Įgyvendinimui bus reikalingas informacinių sistemų modernizavimas, ypač sąsajų realizavimo ir pritaikymo pagal EUDIW ES lygmens techninius reikalavimus, specifikacijas ir protokolus.	Dabartinių informacinių sistemų ir registrų modernizavimas siekiant užtikrinti EUDIW techninės ekosistemos palaikymą yra būtinas, kadangi dauguma sistemų veikia pagal senesnius standartus, nėra vieningos architektūros ir realaus laiko integracijų.
2.	Centralizuotas elektroninių paslaugų teikimas per Valstybės informacinių sistemų sąveikumo platformą (toliau - VIISP) bus svarbi dalis įgyvendinant privalomus EUDIW reikalavimus Lietuvai. VIISP gali būti pritaikytas šioms funkcijom atlikti: (A) VIISP paslaugų katalogas RP (pasikliaujančių šalių) įjungimui/registravimui, (B) Duomenų platforma ir tapatybės patvirtinimas EUDIW kontekste kaip Pub-EAA ir Tarpinė pasikliaujančioji šalis.	Analitinės studijos kontekste tik iš dalies buvo galima įvertinti šiuo metu vystomo projekto dėl Skaitmeninių paslaugų platformos (toliau – SPP) panaudojimo galimybes, turint omenyje, jog techninis šios platformos rengimas nėra pabaigtas ir galimi pokyčiai. Techninio projektavimo etape reikalinga įvertinti, kaip ši platforma ir nauji jos funkcionalumai, integruoti į jau egzistuojančią ir plačiai naudojamą VIISP sistemą, bus susieti su EUDIW įgyvendinimu. Taip pat, siūloma peržvelgti galimybes ir įvertinti, kad VIISP / SPP sistemos iš dalies galėtų patenkinti ir dalį EUDIW keliamų reikalavimų.
3.	Lietuvos EUDIW techninės architektūros modelis priklauso nuo ekosistemos rolių ir jų atsakomybių priskyrimo.	Sprendimai dėl ekosistemos rolių priskyrimo atitinkamoms institucijoms ir jų atsakomybių turi būti pasiekti politikos lygmeniu. Techninio projektavimo etape, siūloma peržiūrėti techninės architektūros modelį pagal preliminariai patvirtintą ekosistemos dalyvių ir jų atsakomybių reglamentavimą (pagal techninio projekto rengimo apimtį).
4.	EUDIW ekosistemos kūrimas Lietuvoje palies visas valstybės institucijas, verslą ir gyventojus.	Siūloma inicijuoti EUDIW ekosistemos kūrimo projektą Lietuvoje Vyriausybės lygyje, ministrą įtraukiant kaip projekto rėmėją. Programos

Valstybės skaitmeninių sprendimų agentūra	Analitinė galimybių studija „Europinės skaitmeninės tapatybės dėklės įgyvendinimo galimybių analizė ir planas“	Lapas 51 iš 53
---	--	----------------

		valdymui pritraukti projektų valdymo profesionalus.
5.	EUDIW aptarnauti bus privaloma visoms valstybės institucijoms ir ženkliai daliai verslo.	Siūloma į dėklės ekosistemos kūrimo programą įtraukti ir kaip galima platesnį ratą suinteresuotų šalių. Tai, ministerijos, savivaldybės, FNTT, NKSC, Lietuvos Bankas ir Pinigų plovimo prevencijos kompetencijų centras. Verslo asociacijas.
6.	Kuriama EUDIW ekosistema ateinančius 15-20 metų bus Lietuvos ir Europos Sąjungos skaitmeninių paslaugų (skaitmenizacijos) pagrindas.	Lietuva turėtų orientuotis į lietuviško kapitalo įmonių įtraukimą, kuriant dėklės ekosistemą ir taip kaupti patirtį, kad vėliau galėtų kurti aukštos pridėtinės vertės darbo vietas ir eksportuoti paslaugas įgytos patirties pagrindu.
7.	Kuriama EUDIW ekosistema, tai įvairių informacinių sistemų, valstybės registru, teikiamų paslaugų ir susijusių procesų, bei teisės aktų visuma, veikianti 24/7 režimu, tad jos sėkmingam funkcionavimui reikalinga sukurti centralizuotą monitoringo sistemą.	Siūloma sukurti visos ekosistemos kritinių dalių centralizuotą monitoringo sistemą ir palaikyti identišką testavimo, prieš gamybinę (angl. pre-prod) aplinkas vadovaujantis geriausiomis sistemų valdymo ir saugumo užtikrinimo praktikomis. Taip pat, platesniam ekosistemos dalyvių įtraukimui, rekomenduojame sukurti eksperimentinę EUDIW aplinką (angl. sand-box).
8.	EUDIW ekosistemos įgyvendinimo programai pasibaigus per 2026 m., EUDIW ekosistema turės veikti nustatytoms institucijoms vykdant nustatytus vaidmenis, jų funkcijas, procesus, funkcionavimo taisykles ir metodikas detalizuojant veiklos modelyje, kuris turės būti parengtas EUDIW įgyvendinimo metu.	Siūlome EUDIW ekosistemos įgyvendinimo paruošiamuosius darbus pradėti nuo 2026 m. pradžios, suformuojant EUDIW įgyvendinimo programą su projekto lyderiu VSSA ir programos partneriais, kurių veiklos ir siekiami rezultatai programoje būtų nustatyti pagal EUDIW ekosistemos vaidmenis. EUDIW komponentų kūrimas (skaitmeninės dėklės, registro informacinės sistemos sprendimų kūrimas, patikimumo užtikrinimo infrastruktūros komponentų, sąveikumo mazgo su ES kontekstu (kitų ES šalių skaitmeninės dėklės ekosistemomis, esamų informacinių sistemų modernizavimas pritaikymui pagal EUDIW ekosistemos reikalavimus, turi būti atliekamas inkrementiniu iteraciniu būdu, pagal: <ul style="list-style-type: none"> • Dalimis detalizuojamą ir tvirtinamą veiklos modelį (kuris detalizuoja vaidmenis, pareigas ir atsakomybes, procesus ir paslaugas, naudojamus duomenų rinkinius). • Techninę programą, detalizuojamą analizės ir projektavimo etapais, kurioje tiekimas apibrėžiamas kaip būtina sąlyga (programavimo) vystymo veikloms vykdyti sprintais įgyvendinamus IT sprendimų komponentus.
9.	Centralizuotas e. paslaugų teikimas per epaslaugos.lt (VIISP) portalą, bus svarbi	Siūlome neatidėliotinai vertinti galimybes koreguoti ar išplėsti šiuo metu vykdomo SPP projekto planus, tam, kad būtų galima VIISP

Valstybės skaitmeninių sprendimų agentūra	Analitinė galimybių studija „Europinės skaitmeninės tapatybės dėklės įgyvendinimo galimybių analizė ir planas“	Lapas 52 iš 53
---	--	----------------

	dalis įgyvendinant privalomus reglamento reikalavimus Lietuvai.	tvarkomą paslaugų katalogą ir SPP komponentą pritaikyti EUDIW įgyvendinimui.
10.	Lietuvoje kuriama EUDIW ekosistema, bus bendros Europos Sąjungos ekosistemos dalimi. Vėliau ir pasaulinės.	Siūlome Ekonomikos ir inovacijų ministerijoje sukurti pareigybę, kuri bus atsakinga už santykių su ES palaikymą, skaitmeninės tapatybės dėklės ekosistemos kontekste. Taip pat, vystant EUDIW ekosistemą, reikalinga vadovautis produkto kūrimo gerosiomis praktikomis. Reguliariai viešinti susijusius ES planus, programų iniciatyvas. Taip pat reguliariai tartis su Lietuvos dėklės ekosistemos dalyviais, verslo asociacijomis.