Kauno technologijos universitetas

Informatikos fakultetas

Modulis „Tiriamasis projektas 1“

Projektas: „Savarankiškos pseudonimizuotos tapatybės valdymo sistema“

Projektavimo metodologijos ir technologijų analizė

IFM 4/2 gr. Danielė Stasiūnaitė
Studentė

Doc. Mindaugas Vasiljevas
Projekto vadovas

Doc. dr. Eglė Butkevičiūtė
Dėstytoja

Kaunas, 2024

Turinys

Iliustracijų sąrašas

Įvadas

Dokumentas yra Programų sistemų inžinerijos magistrantūros disciplinos „Tiriamasis projektas 1“ ataskaita. Dokumento paskirtis apibūdinti tyrimo tikslus, apibendrinti atliktą literatūros analizę, pasirengti projekto reikalavimų specifikavimui, projektavimui, susipažinti su egzistuojančiais tapatybės valdymo sprendimais.

Raktiniai žodžiai: Savarankiška suvereni tapatybė, tapatybės valdymas.

1 Tikslas

Šio darbo tikslas yra sukurti sistemos, leidžiančios neatskleisti privačios asmens informacijos, prototipą, kuris leistų naudotojams išsaugoti savo privatumą internete.

2 Literatūros apžvalga

2.1 Asmens tapatybės valdymas

Gebėjimas įrodyti, kad asmenys yra tie, kuo teigia esą, yra itin svarbus žmonių tarpusavio sąveikai ne tik fiziniame pasaulyje, bet ir internete. Šis įrodymas dabar yra geriau žinomas kaip pažymėjimas - kredencialas, kuris leidžia identifikuoti ir autentifikuoti asmenį. Šis pažymėjimas, sudarytas iš atributų rinkinio, vadinamas asmens tapatybės dokumentu arba tiesiog asmens tapatybe [1].

Dėl nuolat augančio naudotojų ir jų duomenų kiekio asmens tapatybės valdymo modelių ir sistemų vystymas tampa itin aktualia šių laikų sritimi. Asmens tapatybės valdymo sritis apima skirtingus procesus ir technologijas, kurios naudojamos, siekiant užtikrinti, kad prieigą prie įvairių duomenų ar paslaugų turėtų tik identifikuoti ir autorizuoti asmenys [2].

2.1.1 Architektūra

Asmens tapatybės ir prieigos valdymo sistema yra įrankių, procesų ir teisinių nurodymų rinkinys, naudojamas individualioms asmenų tapatybėms, jų autentifikavimui, autorizavimui, vaidmenims ir privilegijoms valdyti organizacijoje arba už jos ribų.

Asmens tapatybės valdymo sistema palengvina organizacijai priklausančių tapatybių administravimą. Ši sistema reikalinga tam, jog būtų galima stebėti roles ir teises, kurios priklauso individualioms asmenų tapatybėms. Taip pat šios sistemos naudojimas padeda sprendimus priimatiems asmenims kontroliuoti prieigą prie jautrios informacijos [2].

Norint tiksliai apibrėžti tapatybę ir egzistuojančius jos valdymo mechanizmus, yra svarbu suprasti pagrindinius su tapatybe susijusius terminus:

- **Subjektas:** tai nagrinėjamos esybės. Pavyzdžiui, žmonės ar daiktai. Subjektas gali pasiekti objektą.
- **Objektas**: tai yra pasyvus subjektas, prie kurio gali prisijungti subjektas. Objektu gali būti laikoma konkreti internetinė paslauga (pavyzdžiui, banko sąskaita) ir panašiai.
- **Identifikatorius:** tai yra subjektams priskirtos etiketės, kurios reikalingos tam, jog būtų galima sekti informaciją apie tam tikrą subjektą. Pavyzdžiui, tai gal būti slapyvardžiai, priskirti identifikaciniai numeriai ir panašiai.

- **Atributas:** tai yra savybių rinkinys, kuris apibūdina subjektą. Atributas yra sudarytas iš dviejų dalių - savybės pavadinimo ir savybės reikšmės. Atributai gali būti naudojami, siekiant identifikuoti subjektą, tačiau šis identifikavimas nėra unikalus subjekto identifikavimas - tam tikros savybės gali būti priskirtos ir kitiems subjektams.

  Atributai gali būti priskirti to paties arba kitų subjektų. Pavyzdžiui, religinės pažiūros ir lytis yra atributai, kurie yra priskiriami to paties subjekto (žmogaus). Egzistuoja ir kiti labai svarbūs atributai - asmenį identifikuojantys duomenys (angl. *Personal Identifiable Information, PII*). Šie duomenys gali padėti identifikuoti asmens tapatybę. Asmenį identifikuojantiems duomenims priklauso ne tik asmens vardas, elektroninio pašto adresas, bet taip pat ir finansiniai, medicininiai įrašai ir net kriminalinė informacija [4].

- **Teiginys:** tai yra tam tikras subjektą apibūdinantis ir asmenį identifikuojančių duomenų informaciją laikantis teisinga tvirtinimas. Kiekvienam subjektui yra priskirtas tokių teiginių rinkinys [5].

- **Pažymėjimas (kredencialas):** teiginių rinkinys, kuris sudarytas iš vieno arba kelių atributų. Finansų įstaigos, vyriausybinės agentūros ir telekomunikacijų bendrovės yra potencialiai patikimos šalys, kurios gali pateikti teiginius apie subjektą. Pačiu paprasčiausiu ir silpniausiu kredencialu yra laikomas slaptažodis. Saugesnių kredencialų kategorijai priskiriami skaitmeniniai sertifikatai, biometriniai duomenys (pavyzdžiui, piršto antspaudas), balso atpažinimas ar akies vyzdžio skenavimas [6].

- **Patikrinamas kredencialas (angl. *verifiable credential*):** tai yra nepakeičiamų teiginių ir metaduomenų rinkinys, kuris kriptografiškai įrodo, kas šiuos teiginius pateikė.

2.1.2 Asmens tapatybės valdyme dalyvaujančios šalys

Pagrindinės asmens tapatybės valdyme dalyvaujančios šalys yra subjektas (naudotojas), tapatybės teikėjas (angl. *Identity Provider, IdP*) ir paslaugų teikėjas (angl. *Service Provider, SP*), kur [2]:

- **Tapatybės teikėjas**: tai yra specialaus tipo paslaugos teikėjas, kuris yra atsakingas už asmens tapatybės valdymą, kuriant, palaikant ir trinant informaciją apie asmenį. Tapatybės teikėjas autentifikuoja naudotoją paslaugų teikėjo vardu.
- **Paslaugos teikėjas**: tai yra sistema arba taikomoji programa, kuri naudoja teiginius, gautus iš tapatybės teikėjo, kad suteiktų subjektui (naudotojui) prieigą prie tam tikrų išteklių ar paslaugų.

2.1.3 Operacijos

Asmens tapatybės valdymo sistemos apima skirtingas operacijas: identifikavimą, verifikavimą, autentifikavimą ir autorizavimą [2].

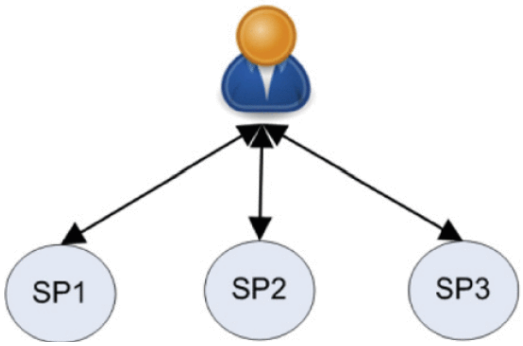
- **Identifikavimas.** Tai yra pirmasis etapas, atpažįstant subjekto, kuris sąveikauja su kitu subjektu (pavyzdžiui, paslaugų teikėju), tapatybę. Identifikavimas įvyksta, kai subjektas teigia turįs tapatybę. Šis procesas paprastai atliekamas, naudojant subjekto vardą, unikalų identifikacinį numerį arba kitus atributus, kurie gali unikaliai identifikuoti subjektą.
- **Verifikavimas.** Šis procesas atliekamas po to, kai įvykdomas atributų identifikavimas. Šio etapo metu subjektui priskiriami atributai, apibūdinantys tam tikrą subjektą.
- **Autentifikavimas.** Įvykdžius šį procesą sistemos naudotojas, procesas arba įrenginys gali prieiti prie sistemos išteklių [8]. Įprastai autentifikavimas atliekamas naudotojui įvedant slaptažodį, naudojant išmanųjį telefoną ar saugų USB raktą arba naudojant piršto antspaudą ar veido atpažinimo funkciją. Operacijai atlikti gali būti naudojamas kelių dalių autentifikavimas (angl. *multifactor authentication, MFA*), kur iš pradžių naudotojas autentifikuojasi, naudodamas slaptažodį arba PIN kodą. Po šio veiksmo naudotojas autentifikuojasi su išmaniuoju telefonu ir galiausiai autentifikavimo procesas užbaigiamas piršto antspaudo nuskaitymu arba veido atpažinimu.
- **Autorizavimas.** Šio procesu metu yra nustatomos naudotojo teisės prie tam tikrų sistemos išteklių.

2.2 Sistemų modelių evoliucija

Siekiant prisitaikyti prie nuolat kintančių asmens tapatybės valdymo reikalavimų buvo sukurtas ne vienas asmens tapatybės valdymo modelis. Šių modelių pritaikymas bei jų konfigūravimas labai priklauso nuo įmonės kultūrinių, istorinių, teisinių ir techninių aspektų. Šie modeliai aprašyti žemiau.

Izoliuota tapatybė

Izoliuotos tapatybės (angl. *Isolated identity*) modelis yra primityviausias iš visų egzistuojančių modelių. Šį modelį sudaro tik dvi šalys: paslaugos teikėjas ir naudotojas (1 pav.). Taikant šį modelį paslaugų teikėjas naudotojui suteikia tam tikrą identifikatorių (pavyzdžiui, slapyvardį) ir atitinkamą kredencialą (pavyzdžiui, slaptažodį). Jeigu naudotojas nori pasinaudoti kito paslaugos teikėjo paslaugomis, naudotojas turi autentifikuotis dar kartą (gauti naują identifikatorių ir kredencialą) [13].



1 pav.: Izoliuotos tapatybės modelis, kur norint pasinaudoti skirtingomis paslaugomis, turi būti atliekamas atskiras autentifikavimo veiksmas.

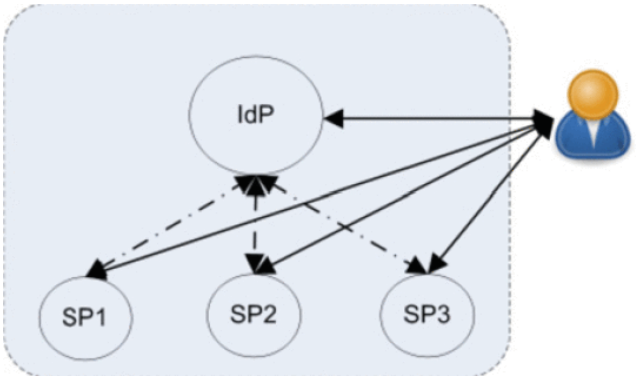
Centralizuota tapatybė

Centralizuotos tapatybės (angl. *Centralized identity*) sistemos modelyje tapatybės ir paslaugos teikėjai yra atskirti (skirtingi), tačiau juos valdo ta pati organizacija. Kiekviena naudotojo sąveika su paslaugų teikėjais turi būti autentifikuojama per centrinį tapatybės teikėją. Šis modelis yra jautrus įvairioms saugumo atakoms [3].

Federacinė tapatybė

Federacinės tapatybės (angl. *Federated identity*) modelyje paslaugų ir tapatybės teikėjų grupės sudaro patikimą federaciją - federacinės tapatybės domeną, kuriame gali būti vienas tapatybės teikėjas ir vienas arba daugiau paslaugos teikėjų (2 pav.). Domenas yra sukuriamas tada, kai sukuriamas patikimas ryšys tarp tapatybės ir paslaugos teikėjų.

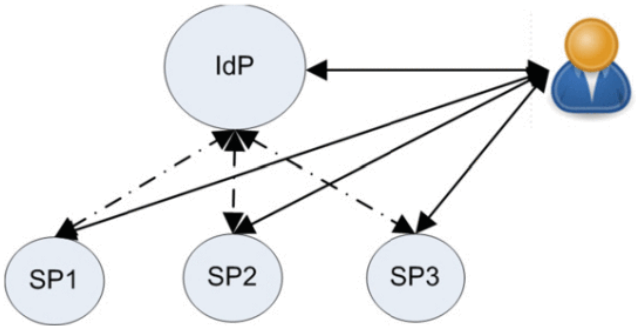
Tapatybės teikėjas išduoda identifikatorių ir kredencialą naudotojui. Tam, jog galėtų pasinaudoti norimomis paslaugomis, naudotojas autentifikuojasi tapatybės teikėjui. Po to, kai pavyksta sėkmingai autentifikuotis, naudotojas gali būti nukreipiamas pas visus paslaugos teikėjus, kurie yra susiję su tuo pačiu tapatybės teikėju [13].



2 pav.: Federacinės tapatybės modelis, kur naudotojas gali pasinaudoti paslaugomis tik tada, kai sėkmingai autentifikuojasi tapatybės teikėjui.

Į naudotoją orientuota tapatybė

Į naudotoją orientuotos tapatybės (angl. *User-Centric identity*) modelis yra panašus į federacinės tapatybės modelį, tačiau šie modeliai skiriasi tuo, jog taikant į naudotoją orientuotos tapatybės modelį nėra būtina sukurti patikimo ryšio tarp tapatybės ir paslaugos teikėjų (3 pav.). Kiekvieną kartą, kai naudotojas bando pasinaudoti tam tikromis paslaugomis, naudotojas yra nukreipiamas pas tapatybės teikėją, kur naudotojas turi autentifikuotis. Po autentifikacijos tapatybės teikėjas perduoda naudotojo tapatybės duomenis paslaugos teikėjui, kuris atitinkamai leidžia arba draudžia konkrečiam naudotojui naudotis paslaugomis. Šis modelis yra plačiai taikomas, naudojantis Facebook arba Google, kai bandoma pasiekti kitas internetines paslaugas [13].



3 pav.: Į naudotoją orientuotos tapatybės modelis, kur patikimas ryšys tarp tapatybės ir paslaugos teikėjų nėra sukuriamas.

Savarankiška suvereni tapatybė (SST)

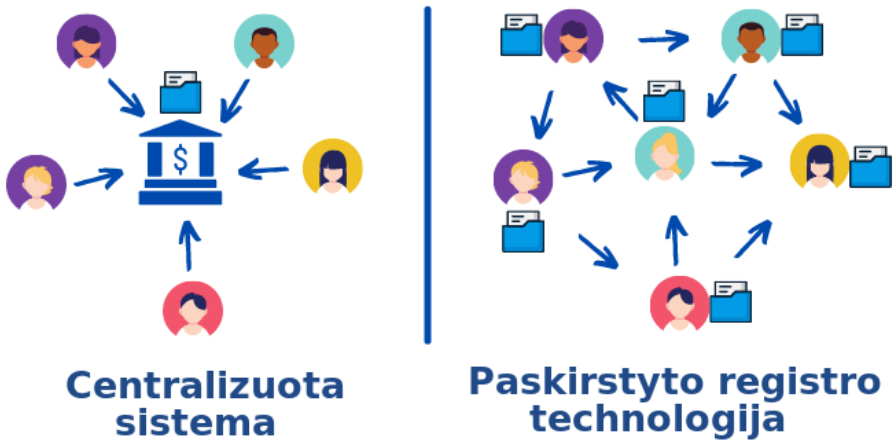
Savarankiškos suverenios tapatybės modelis (angl. *Self-Sovereign identity*) pastaraisiais metais sulaukia didžiausio susidomėjimo, nes jis pasižymi tuo, jog tapatybę turintis naudotojas turi daugiau galimybių kontroliuoti ne tik savo tapatybę, bet ir su ja susijusią informaciją bei atliekamų veiksmų ar operacijų rinkinį - transakcijas [9]. Šiuo modeliu siekiama išsaugoti selektyvų informacijos atskleidimą.

2.3 Blokų grandinės technologija

2.3.1 Paskirstyto registro technologija

Paskirstyto registro technologija (angl. *distributed ledger*) yra bendras protokolas ir struktūra paskirstytam ir saugiam duomenų saugojimui. Ši technologija naudojama sistemose, kai nėra vykdoma centrinė kontrolė ir kriptografiškai apsaugota informacija yra išskirstyta tinkle. Taikant šią technologiją tos pačios informacijos įrašai tinkle yra susieti vieni su kitais kriptografiniais algoritmais [16].

Egzistuoja ne viena paskirstyto registro technologijos forma (pavyzdžiui, maišos grafai, kryptiniai acikliniai grafai (DAG), *Tangle*, *Holochain* ir *Radix*), kur formos skiriasi funkcionalumu, apdorojimo mechanizmais, duomenų struktūromis ir konsensuso algoritmais, tačiau šiuo metu dažniausia paskirstyto registro technologijos forma yra blokų grandinė [15].



4 pav.: Centralizuotos sistemos palyginimas su paskirstyto registro technologija.

2.3.2 Blokų grandinės architektūra

Blokų grandinės technologija pačioje jos sukūrimo pradžioje buvo naudojama finansiniais tikslais - siekiant sukurti sistemą, kuri padėtų spręsti dvigubo pinigų išleidimo problemą. Taip pat ši technolgija geriausiai žinoma dėl jos taikymo bitkoinų kriptovaliutose. Laikui bėgant technologija pradėta taikyti ne tik finansų sektoriuje, bet ir daiktų interneto, išmaniųjų namų, sveikatos priežiūros, tiekimo grandinių valdymo, energetikos srityse ir net užtikrinant sklandesnį rinkimų procesą. Blokų grandinė turi daug skirtingų charakteristikų, kurios lemia spartų šios technologijos taikymą, tačiau svarbiausia charakteristika yra decentralizavimas. Tinkamai realizavus decentralizavimą blokų grandinės technologija ypač naudinga užtikrinant duomenų apsaugą, kadangi blokų grandinės duomenų struktūroje duomenys negali būti pakeisti arba panaikinti [9].

Blokų grandinę sudaro šie pagrindiniai komponentai [9]:

- **Blokas**. Tai yra pagrindiniai blokų grandinės duomenų vienetai. Kiekvienas blokas yra atskira duomenų struktūra, kuri yra naudojama maišos funkcijų reikšmėms saugoti. Pirmasis blokų grandinės vienetas (Genezės blokas) maišos funkcijos reikšmės nesaugo.

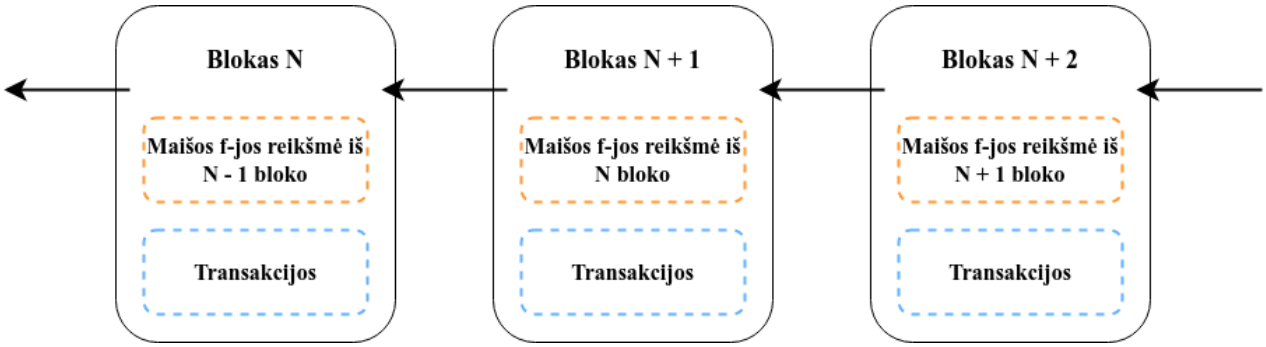
- **Kasėjai**. Tai yra specialūs mazgai, vykdantys bloko tikrinimą - autentifikavimą - prieš įtraukdami jį į blokų grandinės struktūrą [12].

- **Mazgas**. Tai yra įprasti mazgai - elektroniniai įrenginiai, kurie saugo pilną visos blokų grandinės informacijos kopiją. Šie mazgai taip pat reikalingi kasėjų mazgų autentifikuotų transakcijų verifikavimui, koordinavimui ir validavimui [12].

- **Grandinė**. Tai yra blokų grandinė.

- **Konsensuso protokolas**. Tai yra taisyklių ir susitarimų rinkinys blokų grandinės operacijoms atlikti. Šis protokolas užtikrina, kad į blokų grandinę yra įtraukiamos tik validžios transakcijos.

Penktame paveiksle (5 pav.) pavaizduotas blokų grandinės fragmentas, kur kiekvienas blokas turi antraštę su nuoroda į prieš tai buvusį bloką (išskyrus pirmąjį - Genezės - bloką, kuris šios nuorodos neturi).



5 pav.: Blokų grandinės fragmentas.

2.3.3 Viešos ir privačios blokų grandinės sistemos

Blokų grandinės sistemos gali būti padalintos į dvi kategorijas: viešas ir privačias. Taip pat gali būti išskaidytos pagal tipus: leidimų reikalaujančios ir nereikalaujančios blokų grandinės sistemos.

Viešos blokų grandinės (leidimų nereikalaujančios) yra prieinamos visiems, todėl šios kategorijos sistemos dažniausiai naudojamos kriptovaliutų kasyboje. Kadangi šios sistemos pritaikymui nereikalingas centrinės šalies įsikišimas, ši sistema laikoma pilnai decentralizuota [11, 14].

Privačios blokų grandinės (leidimų reikalaujančios) yra prieinamos ribotam naudotojų ratui ir yra kontroliuojamos konkrečios organizacijos. Tam, jog būtų galima naudotis šia sistema, iš pradžių turi būti gauta šią sistemą prižiūrinčios organizacijos autorizacija. Kadangi privačios blokų grandinės naudojamos organizacijose, kur tapatybės ir jų patikimumas yra gerai žinomi, o blokų grandinę sudaro mažiau mazgų, tapatybės verifikavimas ir konsensuso mechanizmai yra gerokai paprastesni, transakcijos įvykdomos greičiau ir pigiau nei viešų blokų grandinių atveju.

2.4 Savarankiška suvereni tapatybė

Dėl išaugusio duomenų pažeidimo atvejų skaičiaus, lėmusių asmeninių duomenų nutekinimą bei tapatybės vagystes, atsirado poreikis keisti asmens tapatybės valdymo mechanizmus. Tobulėjanti blokų grandinės technologija davė pradžią savarankiškos suverenios tapatybės (SST) modelio atsiradimui - naujai naudotojo valdomai asmens tapatybės valdymo sistemai, kuriai įgyvendinti panaudota paskirstyto registro technologija.

Įprastai, asmens tapatybės valdymo sistemos yra saugomos centralizuotose duomenų bazėse, kurios yra kontroliuojamos paslaugas teikiančių institucijų. W3C konsorciumas siekia sukurti naujus standartus, jog naudotojams būtų prieinamos decentralizuotų tapatybių sistemos. Šios sistemos leistų susieti naudotojus su jiems priklausančia informacija be trečiųjų šalių įsikišimo. Tai padėtų eliminuoti duomenų pažeidžiamumo ir neteisėto panaudojimo problemą [18].

Visi (išskyrus savarankiškos suverenios tapatybės valdymo) modeliai pasižymi tuo, jog jie yra visiškai priklausomi nuo trečiosios šalies (tapatybės teikėjo), kuri valdytų ir kontroliuotų naudotojų tapatybę bei tuo pačiu teiktų kredencialus, būtinus autentifikavimui. Taip pat šiems modeliams yra būdingas paskyrų kūrimas, kuris reikalingas, siekiant pasinaudoti paslaugų teikėjų paslaugomis. Tuo tarpu savarankiškos suverenios tapatybės modelis paremtas tiesioginio ryšio kūrimu tarp naudotojo ir kitos šalies - paskyrų kūrimas nereikalingas. Nei vienai iš šalių šis ryšis nepriklauso. Tai reiškia, jog kol abi šalys sutaria dėl ryšio palaikymo, tol šis, savarankiškos suverenios tapatybės, ryšys egzistuoja [24]. Šiuo modeliu siekiama išlaikyti naudotojo privatumą, laikantis naujų decentralizavimo principų [9].

2.4.1 SST apibūdinantys principai

Savarankiškos suverenios tapatybės modelis yra apibūdinamas pagal 10 Kristoferio Aleno 2016 m. pateiktų principų [3, 10, 7, 25]:

1. **Egzistavimas:** naudotojai turi turėti nepriklausomą egzistavimą. Tai reiškia, kad naudotojai niekada negali būti pilnai skaitmeniniai - savarankiška suvereni tapatybė turi būti sukurta fizinės tapatybės pagrindu [7].

2. **Kontrolė:** naudotojai turi kontroliuoti savo tapatybes. Jie turėtų turėti laisvę valdyti savo atributus bet kokiu norimu būdu, nes jie turi visišką savo tapatybės duomenų kontrolę.

3. **Prieiga:** naudotojai turi turėti prieigą prie savo duomenų. Tai nereiškia, kad naudotojas gali keisti su tapatybe susijusius teiginius. Tai reiškia, kad naudotojas turi visada žinoti, jei yra bandoma šiuos teiginius pakeisti.

4. **Skaidrumas:** sistemos ir algoritmai turi būti skaidrūs. Tai reiškia, jog naudotojams turi būti žinoma, kaip veikia sistemos ir algoritmai, kurie naudojami tapatybių administravimui.

Šie algoritmai turi būti nemokami, gerai žinomi, atviro kodo ir nepriklausantys nuo vienos konkrečios architektūros.

5. **Patvarumas:** naudotojai bėgant laikui turi turėti galimybę išlaikyti savo tapatybę. Tapatybės turi išlikti amžinai arba bent tol, kol tai yra reikalinga. Su tapatybe susiję duomenys gali būti atnaujinami ir keičiami, tačiau tapatybė išlieka.

6. **Perkeliamumas:** naudotojai turi turėti galimybę perkelti savo tapatybę iš vienos sistemos į kitą. Tapatybių perkeliamumas užtikrina, kad naudotojas yra vieninitelis atsakingas už savo tapatybės kontrolę.

7. **Suderinamumas:** tapatybės sistemos turi būti suderinamos su įvairiomis technologijomis ir paslaugų teikėjais. Tai užtikrina, kad naudotojai galės naudoti savo tapatybę įvairiose situacijose ir platformose.

8. **Sutikimas:** naudotojai turi sutikti su savo tapatybės naudojimu. Bet kuri tapatybės valdymo sistema remiasi tuo, jog yra dalinamąsi informacija apie tapatybę ir kadangi yra didinamas tapatybės sistemos suderinamumas su kitais paslaugų teikėjais, tuo pačiu dažnėja ir informacijos dalinimąsis su trečiosiomis šalimis, todėl tapatybės turėtojas turėtų aiškiai suprasti ir duoti sutikimą, kaip yra naudojami jo tapatybės duomenys.

9. **Minimalizavimas:** tapatybę apibūdinančių teiginių atskleidimas turi būti kuo mažesnis. Tai reiškia, kad turi būti atskleista tik tiek informacijos apie tapatybę, jog būtų galima užbaigti kokią nors užduotį. Pavyzdžiui, jeigu yra reikalaujama nurodyti asmens amžių, turi būti nurodytas tik amžius - konkreti gimimo data neturėtų būti nurodoma, siekiant užtikrinti asmens privatumą.

10. **Apsauga:** naudotojų teisės turi būti saugomos. Savarankiškos suverenios tapatybės modelyje tapatybės turėtojas yra architektūros centre, todėl tapatybės turėtojo teisės yra laikomos viršesnėmis. Asmens tapatybės autentifikavimas privalo būti atliekamas, taikant nepriklausomus algoritmus, kuriems būdingas decentralizuotas veikimas.

2.4.2 Architektūra

Savarankiškos suverenios tapatybės modelis yra sudarytas iš skirtingų komponentų, kurie yra aprašyti žemiau pateiktuose skyriuose.

Decentralizuotas identifikatorius

Tai yra esminiai modelio komponentai - kriptografiškai sugeneruoti unikalūs decentralizuoti identifikatoriai (DID), nereikalaujantys centralizuotos registracijos institucijos, kuri valdytų šiuos identifikatorius, tačiau jie gali būti valdomi naudojant decentralizuotą infrastruktūrą (pavyzdžiui, paskirstyto registro technologiją). DID adresai yra sudaryti iš trijų dalių ir yra sugeneruojami, remiantis kriptografinių raktų poromis. Kiekvienam DID adresui būdingas šis formatas [26]:

`<schema>:<metodas>:<metodui specifiškas identifikatorius>`, kur:

- `schema`: visada atitinka „`did`“, kas indikuoja, jog tai yra decentralizuotas identifikatorius.
- `metodas`: apibūdina, kaip perskaityti ir sukurti DID dokumentą blokų grandinėje arba paskirstyto registro architektūroje. Šiuo metu egzistuoja šie DID metodai: *Sovrin*, *Ethereum uPort*, *Blockstack*, *Veres One* ir *IPFS*. Šie metodai aprašo, kaip sudaromi nuo metodo priklausantys identifikatoriai, kaip kuriamas DID dokumentas ir taip pat aprašo CRUD operacijas DID ir jų dokumentams [7].
- `metodui specifiškas identifikatorius`: tai yra unikalus identifikatorius, kurio formatas ir struktūra priklauso nuo naudojamo DID metodo.

Pavyzdžiui, gali būti sugeneruoti tokie decentralizuotų identifikatorių adresai:

- `did:sov:WRfXPg8dantKVubE3HX8pw` (naudojant *Sovrin* DID metodą);
- `did:ethr:0x123456789abcdef` (naudojant *Ethereum* DID metodą).

DID dokumentas

Kiekvienas DID adresas turi su juo susietą DID dokumentą (JSON-LD formato dokumentą), kuriame nurodyta informacija apie DID subjektą: servisų galutiniai taškai (leidžia susisieti su DID subjektu), kriptografiniai viešieji raktai, autentifikavimo parametrai ir kiti meta duomenys. Šio dokumento pavyzdys pateiktas šeštame paveiksle (6 pav.).

```
{
  "@context": "https://www.w3.org/ns/did/v1",
  "id": "did:example:123456789abcdefghi",
  "verificationMethod": [
    {
      "id": "did:example:123456789abcdefghi#keys-1",
      "type": "Ed25519VerificationKey2020",
      "controller": "did:example:123456789abcdefghi",
      "publicKeyMultibase": "z6Mki9z..."
    }
  ],
  "authentication": [
    "did:example:123456789abcdefghi#keys-1"
  ],
  "keyAgreement": [
    {
      "id": "did:example:123456789abcdefghi#keys-2",
      "type": "X25519KeyAgreementKey2020",
      "controller": "did:example:123456789abcdefghi",
      "publicKeyMultibase": "z6LS..."
    }
  ],
  "service": [
    {
      "id": "did:example:123456789abcdefghi#vcs",
      "type": "VerifiableCredentialService",
      "serviceEndpoint": "https://example.com/credentials"
    }
  ]
}
```

6 pav.: DID dokumento pavyzdys.

DID dokumentą sudaro šios dalys:

1. **Kontekstas** (`@context`): tai yra tam tikri trumpiniai, kurie naudojami tam, jog būtų užtikrinta efektyvi sistemų komunikacija.

2. **Identifikatorius** (`id`): tai yra unikali su konkrečiu naudotoju (subjektu) susieta reikšmė.

3. **Verifikavimo metodai** (`verificationMethod`): tai yra kriptografinių viešųjų raktų ar kitos informacijos, kuri naudojama autentifikuoti sąsają su DID subjektu, rinkinys.

4. **Autentifikacija** (`authentication`): elementas apibūdina subjekto autentifikavimo būdą, bandant pasiekti norimas paslaugas.

5. **Tvirtinimo metodai** (`assertionMethod`): elementas nurodo, kaip subjektas pateiks teiginius (angl. *claims*), pavyzdžiui, išduodant patikrinamą kredencialą.

6. **Šifravimo raktų sutartys** (`keyAgreement`): elementas nurodo, kaip gali būti sukurtas užšifruotas asmeninės informacijos turinys, siekiant užtikrinti saugią šalių komunikaciją.

7. **Paslaugų nuorodos** (`service`): elementas nurodo būdus, kaip sąveikauti su subjektu.

Patikrinamas pažymėjimas

Patikrinamas pažymėjimas (angl. *verifiable credential*) yra skaitmeniniai duomenys, patvirtinantys tam tikrus teiginius apie subjektą. Patikrinami duomenys susieja subjektą su identifikatoriumi ir gali apimti įvairius teiginius, tokius kaip vardas, pavardė, gimimo data. Patikrinami kredencialai yra sukuriami išdavėjo ir išsiunčiami gavėjui. Šiame pažymėjime yra pateikiamas tam tikras teiginių apie atributus rinkinys, pvz., vardas, gimimo data, identifikacinis numeris ar kita informacija, kurią išdavėjas nori priskirti gavėjui. Norint perduoti teiginį tikrintojui yra sukuriama prezentacija. Prezentacija leidžia pateikti tik pasirinktą atributų dalį, pavyzdžiui, atskleisti gimimo datą, neatskleidžiant vardo atributo [17].

Decentralizuota viešojo rakto infrastruktūra

Viešojo rakto infrastruktūra leidžia atlikti kriptografines operacijas, pagrįstas viešojo rakto kriptografija. Tradicinėje viešojo rakto sistemoje sertifikatus išduoda centralizuotos sertifikavimo institucijos. Decentralizuota viešojo rakto infrastruktūra naudoja protokolus, tokius kaip DID, viešiesiems raktams atrasti ir patikrinti.

Blokų grandinė

Blokų grandinės (2.3.2) technologija yra svarbi suverenios savarankiškos tapatybės modelyje, nes ji suteikia patikimą ir skaidrią duomenų saugojimo ir apdorojimo sistemą, kurioje nereikia nuolat veikiančių centrinių tapatybės teikėjų. Ši technologija leidžia skirtingoms, tačiau bendrų interesų turinčioms šalims vykdyti nuolatinius, nekintančius ir skaidrius duomenų mainus be trečiųjų šalių įsikišimo, užtikrinant saugią autentifikaciją ir anonimiškumą [21].

Patikrinamų duomenų registras

Tai sistema, skirta DID identifikatorių ir kitos informacijos, kuri yra būtina DID dokumentų generavimui, saugojimui. Tam, jog būtų sukurtas ryšys tarp SST aktorių, vieši DID identifikatoriai ir jų DID dokumentai turi būti saugomi šiame duomenų registre, kuriam gali būti būdinga skirtinga struktūra: paskirstyto registro, decentralizuotos failų sistemos, duomenų bazės, *„peer-to-peer“* tinklų ar kitos patikimos duomenų saugojimo struktūros [19].

Agento programinė įranga

Agentai yra programinės įrangos komponentai, veikiantys subjekto vardu. Jie suteikia tinklo adresą, per kurį kiti subjektai gali prisijungti. Šie komponentai įprastai turi prieigą prie skaitmeninės piniginės, kad galėtų saugoti kriptografinius raktus.

Tapatybės centrai

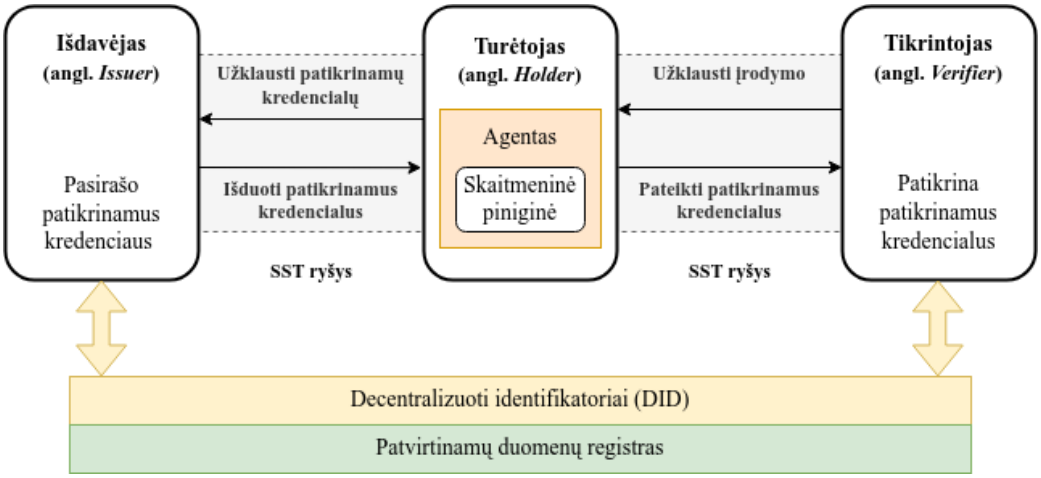
Tai sistemos, leidžiančios naudotojams saugoti savo tapatybės duomenis ir valdyti prieigą prie jų. Naudotojai gali pasirinkti, su kuo ir kokia informacija nori dalytis, o autentifikavimas atliekamas naudojant protokolus, tokius kaip DID.

Skaitmeninės piniginės

Tai saugi programinės įrangos programa, leidžianti naudotojams saugoti ir valdyti savo skaitmeninius identifikatorius, tokius kaip DID ir patikrinamus duomenis bei kriptografinius raktus. Skaitmeninės piniginės paprastai yra prieinamos kaip mobiliosios arba darbalaukio programos ir suteikia naudotojams galimybę saugoti ir tvarkyti savo skaitmeninę tapatybę, įrodyti savo tapatybę trečiosioms šalims bei suteikti sutikimą dėl savo duomenų naudojimo. Agentų programinė įranga paprastai turi prieigą prie skaitmeninės piniginės, kad galėtų saugoti kriptografinius raktus ir vykdyti operacijas naudotojo vardu.

2.4.3 Modelio aprašymas

Septintame paveiksle (7 pav.) pavaizduotas savarankiškos suverenios tapatybės modelis, kur išskirti pagrindiniai dalyviai (išdavėjas, turėtojas ir tikrintojas) ir aprašyti veiksmai, kurie yra susiję su decentralizuotų identifikatorių ir patikrinamųjų pažymėjimų naudojimu. Visas procesas prasideda nuo DID sukūrimo ir baigiasi tapatybių patikrinimu [17].



7 pav.: SST modelis. Adaptuota pagal [19] straipsnio iliustraciją.

Išdavėjo veiksmai:

1. Pirmiausia, išdavėjas turi sukurti DID, pasirinkdamas DID metodą iš galimų variantų sąrašo. Galima naudoti tą patį DID visiems patikrinamiems pažymėjimams arba kurti naują kiekvienam.

2. Sukūrus DID, išdavėjas gali atnaujinti DID dokumentą, kuriame aprašomi su DID susiję kriptografiniai raktai. Svarbu atkreipti dėmesį, kad išdavėjas yra atsakingas už privačiųjų raktų saugojimą, nes praradus juos, nėra numatyto būdo juos atkurti.

3. Prieš generuojant patikrinamuosius pažymėjimus, išdavėjas turi gauti gavėjo DID ir, jei reikia, patikrinti gavėjo tapatybę. Tapatybės patikrinimo detalumas priklauso nuo patikrinamojo pažymėjimo tipo.

4. Gavęs gavėjo DID, išdavėjas sukuria patikrinamą pažymėjimą, kuriame nurodomi išdavėjo ir gavėjo DID. Patikrinamas pažymėjimas yra pasirašomas skaitmeniniu parašu, naudojant išdavėjo DID. Sukurtas pažymėjimas siunčiamas gavėjui.

5. Išdavėjas negali ištrinti jau išduoto pažymėjimo, tačiau kai kurie DID metodai leidžia jį atšaukti (pavyzdžiui, *Sovrin* metodas).

Gavėjo veiksmai:

1. Gavėjas taip pat turi sukurti DID prieš gaudamas patikrinamą pažymėjimą. Galima kurti naują DID kiekvienam patikrinamam pažymėjimui, siekiant apsaugoti privatumą ir apsunkinti pažymėjimo susiejimą su tuo pačiu gavėju. Gavėjas yra atsakingas už savo privačiųjų raktų saugojimą.

2. Norėdamas gauti pažymėjimą gavėjas turi pasidalyti savo DID su išdavėju. Išdavėjas gali reikalauti papildomų identifikavimo mechanizmų.

3. Gavęs pažymėjimą gavėjas gali pasirinkti ir bendrinti tik tam tikrus pažymėjimo duomenis, siekdamas apsaugoti savo privatumą.

4. Sukurtas duomenų pateikimas siunčiamas tikrintojui. Bendrinimo būdas priklauso nuo gavėjo ir tikrintojo naudojamų komunikacijos metodų.

Tikrintojo veiksmai:

1. Tikrintojas, skirtingai nuo išdavėjo ir gavėjo, neprivalo kurti DID prieš patikrindamas pateikiamų duomenų rinkinį.

2. Pirma, tikrintojas turi gauti išdavėjo ir gavėjo DID dokumentus. Gavęs duomenų rinkinį tikrintojas patikrina kiekvieną rinkinyje esantį duomenų elementą.

3. Naudodamas gautuose DID dokumentuose esančius raktus tikrintojas patikrina, ar duomenų elemento parašai sugeneruoti išdavėjo ir gavėjo.

4. Jei DID metodas leidžia atšaukti patikrinamą pažymėjimą, tikrintojas turi patikrinti, ar pažymėjimas vis dar galioja.

5. Paskutinis žingsnis - patikrinti išdavėjo ir gavėjo tapatybes.

2.4.4 SST iššūkiai

Skaitmeninių tapatybių kūrimas ir jų valdymas yra esminiai etapai tam, jog būtų galima pasinaudoti įvairiomis internetinėmis paslaugomis. Tapatybių valdymui sukurta ne viena metodika, tačiau savarankiškos suverenios tapatybės valdymo sistema yra naujausia paradigma, suteikianti naudotojams daugiau tapatybės duomenų kontrolės. Nepaisant to, kad SST technologija turi didelį potencialą pakeisti skaitmeninės tapatybės valdymą, suteikdama naudotojams daugiau kontrolės ir autonomijos, norint sėkmingai įdiegti šią technologiją būtina išspręsti ne vieną iššūkį, susijusį su techniniais, teisiniais, naudotojų sąveikos ir valdymo aspektais [20]. Šių iššūkių sprendimas gali apimti naudojamų mechanizmų stiprinimą (algoritmų keitimą), tinklo stebėseną ir atakų aptikimo sistemų naudojimą. Žemiau aprašomi tokių iššūkių pavyzdžiai:

- **Blokų grandinės pažeidžiamumai.** Nors blokų grandinės pasižymi decentralizacija ir skaidrumu, jos gali būti pažeidžiamos ir tai gali kelti grėsmę SST sistemos saugumui ir privatumui. Blokų grandinių veikla gali būti sutrikdyta įvairiomis atakomis. Pavyzdžiui, „51% ataka“, kai užpuolikas kontroliuoja daugiau nei 50% blokų grandinės mazgų ir tokiu būdu gali išbalansuoti grandinės struktūrą; „*Sibilo* ataka“, kai užpuolikas sukuria daug nelegalių blokų grandinės mazgų, siekdamas įgauti didesnę įtaką tinkle; pakartotinio perdavimo atakos (tai dažniausiai pasitaikantis blokų grandinę galintis paveikti pažeidžiamumas), kai užpuolikas perima ir pakartotinai perduoda teisėtas transakcijas, siekdamas apgauti sistemą [14].

- **SST tinklo plėtra.** Augant SST sistemų naudojimui šios sistemos turi gebėti apdoroti augantį naudotojų ir operacijų skaičių, nepakenkiant sistemos našumui. Viešos blokų grandinės sistemos, tokios kaip *Ethereum* (vienas iš dažniausiai naudojamų blokų grandinės metodų), dėl sudėtingų konsensusų mechanizmų nepalaiko didelio naudotojų ir operacijų skaičiaus. Privačios blokų grandinės technologijos geba apdoroti didesnį naudotojų ir operacijų skaičių, tačiau dėl to gali būti pakenkta saugumui.

- **Suderinamumas su privatumo įstatymais.** Blokų grandinės sistemos ypatybės, tokios kaip duomenų nekintamumas ir viešai prieinami registrai, kelia susirūpinimą dėl atitikimo duomenų apsaugos įstatymams, įskaitant ES Bendrąjį duomenų apsaugos reglamentą (BDAR). Ypač sudėtinga įgyvendinti reikalavimą, nusakantį, kad duomenų subjektas turi teisę reikalauti duomenų valdytojo ištrinti subjekto asmeninius duomenis („teisė būti pamirštam“) [22, 23], nes blokų grandinės duomenų ištrinti neįmanoma.

- **Apribojimai, susiję su paskirstyto registro pagrindu sukurtais DID metodais.** Dauguma DID metodų remiasi paskirstytais registrais, kurie gali būti brangūs ir lėti. Be to, blokų grandinės sistemų saugumas priklauso nuo jų dydžio (mažesnės sistemos yra pažeidžiamesnės atakoms) ir decentralizacijos.

- **Programų ir sistemų patogumas.** Dabartinės SST sistemos dažnai yra sudėtingos naudoti ir suprasti, ypač netechniniams naudotojams. Reikalingas didesnis dėmesys naudotojo sąsajos dizainui ir patogumui.
- **Naudotojo sąveika.** SST sistemų kūrėjai dažnai nepakankamai dėmesio skiria naudotojo sąveikos aspektams, pvz., sąsajų patogumui ir privatumo užtikrinimui. Reikalingas išsamesnis naudotojų poreikių ir privatumo aspektų nagrinėjimas.
- **Technologijų diegimas.** Sėkmingam SST diegimui reikalingi pokyčiai esamose sistemų architektūrose, atitinkami technologiniai sprendimai ir naudotojų palaikymas. Reikia užtikrinti, kad SST technologija būtų prieinama ir suprantama plačiajai visuomenei.
- **Priemonių ir sistemų trūkumas.** Trūksta priemonių, skirtų „blockchain“ duomenų paieškai ir SST sistemų kūrimui. Reikalingos inovatyvios priemonės ir sistemos, palengvinančios SST technologijos naudojimą.

Išvados

Atlikus projektavimo metodologijos ir technologijų analizę gautos šios išvados:

- Apžvelgta asmens tapatybės valdymo sistemų architektūra bei pagrindiniai šių sistemų operacijų principai.
- Apibūdinti asmens tapatybės valdymo sistemose taikomi modeliai.
- Pristatyta blokų grandinės technologija, davusi pradžią perspektyviausiai - savarankiškos suverenios - asmens tapatybės valdymo sistemai.
- Išanalizuota savarankiškos suverenios tapatybės valdymo modelio architektūra bei išskirtos pagrindinės probleminės šios technologijos sritys.

Literatūros sąrašas

[1] Schardong, F.; Custódio, R. Self-Sovereign Identity: A Systematic Review, Mapping and Taxonomy. Sensors 2022, 22, 5641. Pasiekiama: https://doi.org/10.3390/s22155641.

[2] Soltani, Reza, Nguyen, Uyen Trang, An, Aijun, A Survey of Self-Sovereign Identity Ecosystem, Security and Communication Networks, 2021, 8873429, 26 pages, 2021. Pasiekiama: https://doi.org/10.1155/2021/8873429.

[3] Jøsang A. and Pope S., User centric identity management, Proceedings of the AusCERT Asia Pacific Information Technology Security Conference, 2005, Brisbane, Australia.

[4] National Institute of Standards and Technology. (2010). Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) (Special Publication 800-122). Gaithersburg, MD: U.S. Department of Commerce. Pasiekiama: https://doi.org/10.6028/NIST.SP.800-122.

[5] Alrodhan, Waleed & Mitchell, Chris. (2010). Enhancing user authentication in claim-based identity management. 75 - 83. 10.1109/CTS.2010.5478521.

[6] M. S. Ferdous, F. Chowdhury and M. O. Alassafi, "In Search of Self-Sovereign Identity Leveraging Blockchain Technology," in IEEE Access, vol. 7, pp. 103059-103079, 2019, doi: 10.1109/ACCESS.2019.2931173.

[7] Dib, Omar and Toumi, Khalifa, Decentralized Identity Systems: Architecture, Challenges, Solutions and Future Directions (December 20, 2020). Annals of Emerging Technologies in Computing (AETiC), Print ISSN: 2516-0281, Online ISSN: 2516-029X, pp. 19-40, Vol. 4, No. 5 (2020), Published by International Association of Educators and Researchers (IAER), DOI: 10.33166/AETiC.2020.05.002. Pasiekiama: https://ssrn.com/abstract=3785452.

[8] Apthorpe, Noah, et al. "The Authentication Gap: Higher Education's Widespread Noncompliance with NIST Digital Identity Guidelines." arXiv preprint arXiv:2409.00546 (2024).

[9] Alanzi, H., & Alkhatib, M. (2022). Towards Improving Privacy and Security of Identity Management Systems Using Blockchain Technology: A Systematic Review. Applied Sciences, 12(23), 12415. Pasiekiama: https://doi.org/10.3390/app122312415.

[10] Allen C., The Path to Self-Sovereign Identity. Life with Alacrity, 2016.

[11] Baars, D. S. Towards self-sovereign identity using blockchain technology. MS thesis. University of Twente, 2016.

[12] Aggarwal, Shubhani, and Neeraj Kumar. "Core components of blockchain." Advances in Computers. Vol. 121. Elsevier, 2021. 193-209.

[13] M. S. Ferdous, F. Chowdhury and M. O. Alassafi, "In Search of Self-Sovereign Identity Leveraging Blockchain Technology," in IEEE Access, vol. 7, pp. 103059-103079, 2019, doi: 10.1109/ACCESS.2019.2931173.

[14] M. R. Ahmed, A. K. M. M. Islam, S. Shatabda and S. Islam, "Blockchain-Based Identity Management System and Self-Sovereign Identity Ecosystem: A Comprehensive Survey," in IEEE Access, vol. 10, pp. 113436-113481, 2022, doi: 10.1109/ACCESS.2022.3216643.

[15] Sadeghi, M., Mahmoudi, A. & Deng, X. Adopting distributed ledger technology for the sustainable construction industry: evaluating the barriers using Ordinal Priority Approach. Environ Sci Pollut Res 29, 10495-10520 (2022). Pasiekiama: https://doi.org/10.1007/s11356-02116376y.

[16] Soltani, R.; Zaman, M.; Joshi, R.; Sampalli, S. Distributed Ledger Technologies and Their Applications: A Review. Appl. Sci. 2022, 12, 7898. Pasiekiama: https://doi.org/10.3390/app12157898.

[17] Clemens Brunner, Ulrich Gallersdörfer, Fabian Knirsch, Dominik Engel, and Florian Matthes. 2020. DID and VC: Untangling Decentralized Identifiers and Verifiable Credentials for the Web of Trust. In 2020 the 3rd International Conference on Blockchain Technology and Applications (ICBTA 2020), December 14–16, 2020, Xi'an, China. ACM, New York, NY, USA, 6 pages. Pasiekiama: https://doi.org/10.1145/3446983.3446992.

[18] Stockburger, L.; Kokosioulis, G.; Mukkamala, A.; Mukkamala, R.; Avital, M. Blockchain-enabled Decentralized Identity Management: The Case of Self-sovereign Identity in Public Transportation. Blockchain Res. Appl. 2021, 2, 100014.

[19] Satybaldy, Abylay. "Towards Self-Sovereign Identity." (2024).

[20] A. Satybaldy, M. S. Ferdous and M. Nowostawski, "A Taxonomy of Challenges for Self-Sovereign Identity Systems," in IEEE Access, vol. 12, pp. 16151-16177, 2024, doi: 10.1109/ACCESS.2024.3357940.

[21] Aggarwal, Shubhani, and Neeraj Kumar. "Architecture of blockchain." Advances in Computers. Vol. 121. Elsevier, 2021. 171-192.

[22] General Data Protection Regulation (GDPR). (n.d.). *Article 17
- Right to erasure ('right to be forgotten'). Pasiekiama: https://gdpr-info.eu/art-17-gdpr/https://gdpr-info.eu/art-17-gdpr/ [žiūrėta 2025-01-02].

[23] Kondova, Galia and Erbguth, Jörn, Self-Sovereign Identity on Public Blockchains and the GDPR (April 1, 2020). Proceedings of ACM SAC Conference, Brno, Czech Republic,

March 30- April 3, 2020 (SAC'20), 342 - 345. DOI: 10.1145/3341105.3374066. Pasiekiama: https://ssrn.com/abstract=3515213.

[24] Preukschat, Alex, and Drummond Reed. Self-sovereign identity. Manning Publications, 2021.

[25] Allen, C. (2016). Self-sovereing identity principles. Pasiekiama: https://github.com/WebOfTrustInfo/self-sovereign-identity/blob/master/self-sovereign-identity-principles.md [žiūrėta 2025-01-02].

[26] World Wide Web Consortium (W3C). (2022). Decentralized Identifiers (DIDs) v1.0. Pasiekiama: https://www.w3.org/TR/did-core/ [žiūrėta 2025-01-02].