VILNIAUS UNIVERSITETAS
MATEMATIKOS IR INFORMATIKOS FAKULTETAS
PROGRAMŲ SISTEMŲ KATEDRA

Skaitmeninės tapatybės valdymas taikant blokų grandinę

Digital Identity Management using Blockchain

Bakalauro darbas

Atliko:	Jurgis Kargaudas	(parašas)
Darbo vadovas:	asist. Aurimas Šimkus	(parašas)
Darbo recenzentas:	TO BE ADDED	(parašas)

Vilnius – 2018

Santrauka

Šiame darbe nagrinėtas blokų grandinės technologijos tinkamumas skaitmeninių tapatybių valdymui. Apžvelgus esamų identifikavimo sprendimų savybes, tirta blokų grandinė ir jos charakteristikos, kurios leistų įveikti dabar kylančius naudotojų atpažinimo iššūkius.

Nustatyta, kad blokų grandinė gali būti taikoma skaitmeninės tapatybės valdymui tokioje srityje, kur ši technologija padeda išspręsti tokias bėdas. Sukurtas pateikto sprendimo prototipas, parašytas su Language3000 programavimo kalba.

Raktiniai žodžiai: autentifikavimas, tapatybės atpažinimas, skaitmeninė tapatybė, skaitmeninės tapatybės valdymas, blokų grandinė

Summary

In this paper, blockchain applicability for digital identity management was investigated. After an overview of current identification solution properties, blockchain and its characteristics were examined, in order to find out whether the technology is suitable to overcome present user identification challenges.

It was determined that blockchain can be used for digital identity management in this/these fields, where it allows to solve those issues. A prototype of the solution was presented, which was written using Language3000 programming language.

Keywords: authentication, identity recognition, digital identity, digital identity management, blockchain

Įvadas

Interneto paslaugos šiais laikais yra neatsiejama žmonių gyvenimo dalis. Norėdami individualizuoti turinį, sustiprinti taikomosios programos saugumą ar siekdami iš anksto išvengti kenkėjiškų tikslų turinčių asmenų ar sukurtų robotų, paslaugų tiekėjai siekia identifikuoti savo naudotojus. Interneto naudotojų skaičiui perkopus 4 milijardus [Min18], o kiekvienam naudotojui vidutiniškai turint po 7 skirtingas socialines paskyras [MM17], asmenų tapatybių valdymas, autentifikavimas ir autorizavimas tampa vis didesniu iššūkiu.

Tapatybių valdymas kelia problemų tiek paslaugų tiekėjams, tiek jų naudotojams. Kiekvienas paslaugų tiekėjas turi skirti papildomų resursų naudotojų tapatybių valdymui, jų autentifikavimui, jautrių duomenų saugumo užtikrinimui. Paslaugų naudotojams bene didžiausi atsiradę keblumai: milžiniškas įsimintinų slaptažodžių kiekis bei sunkumai kontroliuojant savo asmens duomenų sklaidą skirtingose sistemose. Vidutiniškai interneto naudotojas turi 25 slaptažodžių reikalaujančias paskyras ir per dieną turi įvesti 8-is slaptažodžius [FH07]. Susidarius tokiai situacijai, per didelis įsimintinų slaptažodžių kiekis neretai priverčia naudotojus paaukoti saugumą dėl patogumo ir pradėti naudoti tą patį slaptažodį sirtingoms sistemoms [PM03; Sam99]. Naudotojas, turėdamas keletą paskyrų skirtingose sistemose, taip pat praranda dalį savo asmens duomenų kontrolės. Jam tenka pasitikėti taikomosios programos naudojamomis technologijomis ir metodais ir tikėtis, kad jie bus pakankamai saugūs ir stabilūs bei suteikti asmens duomenys nepasieks nepageidaujamų adresatų. Didėjant naudojamų paslaugų kiekiui, naudotojo skaitmeninės tapatybės duomenis turi vis daugiau taikomųjų programų ir bent vienai iš jų patyrus programišių įsilaužimą ar kitokią nesėkmę, jautrūs naudotojo duomenys būna paviešinti.

Vienu iš pagrindinių skaitmeninės tapatybės valdymo keliamų problemų sprendimu išlieka vienkartinis prisijungimas (angl. *Single Sign-On*). Šis sprendimas leidžia naudotojui pasirinkti vieną tapatybės tiekėją (angl. *identity provider*) ir patikėti jam skaitmeninės tapatybės valdymą. Tuomet naudotojas prie visų paslaugų, palaikančių pasirinkto tapatybės tiekėjo (pvz. *Facebook*) prisijungimą, gali autentifikuotis naudodamas ta pačia paskyra. Tokiu būdu naudotojui pakanka prisiminti tik slaptažodžius, užregistruotus tapatybės tiekėjų sistemose, o paslaugų tiekėjai neturi patys rūpintis autentifikavimu ar autorizavimu, o jį užtikrina integruodami sistemą su tapatybės tiekėju. Tačiau šis sprendimo būdas taip pat turi aiškių trūkumų: naudotojas negali prisijungti prie paslaugų, nepalaikančių pasirinkto tapatybės tiekėjo, dėl paslaugų tiekėjų priklausomybės nuo tapatybės tiekėjo pastarojo pasiekiamumas tampa vieninteliu nesėkmės tašku (angl. *single point of failure*), naudotojas taip pat praranda dalį savo asmens duomenų kontrolės. Naršantis internete asmuo yra priverstas pasitikėti tapatybės tiekėjo gebėjimu perduoti tik naudotojo leistus asmens duomenis ir tik toms trečiosioms šalims, kurias jis patvirtina. Kaip rodo *Cambridge Analytica* incidentas [Gra18], net didžiosios kompanijos, tokios kaip *Facebook*, ne visada sugeba tai užtikrinti.

Blokų grandinė (angl. *blockchain*) yra nauja alternatyva skaitmeninės tapatybės valdymui. Ši technologija veikia kaip paskirstytų įrašų platforma (angl. *distributed ledger platform*), kurioje kiekvienas įrašas yra nekintamas (angl. *immutable*), o visi užfiksuoti įrašai atspindi tikslią transakcijų istoriją nuo pat grandinės sukūrimo [Baa16]. Saugant tapatybės duomenis šioje grandinėje ir pritaikius reikiamą blokų grandinės pasiekiamumo lygį įrašų rašymui ir skaitymui,

asmuo visada žino, kokia trečioji šalis gali pasiekti kokius tapatybės duomenis. Kadangi blokų grandinė yra decentralizuota, pritaikius ją skaitmeninių tapatybių valdyme taip pat būtų galima išvengti šioje srityje dažnos vienintelio nesėkmės taško problemos. Šiame darbe nagrinėjama, kada verta naudoti blokų grandinę naudotojų skaitmeniniam autentifikavimui bei autorizavimui, kokie to pranašumai, trūkumai bei priėmimo barjerai (angl. *adoption barriers*).

Darbo tikslas - išanalizuoti blokų grandinės tinkamumą skaitmeninės tapatybės valdymui.

Darbe keliami uždaviniai:

1. Išnagrinėti esamus skaitmeninės tapatybės valdymo sprendimus ir jų keliamus iššūkius.
2. Apibūdinti blokų grandines ir jų savybes, leidžiančias spręsti dabartines identifikavimo problemas.
3. *Apžvelgti esamas blokų grandinės sistemas, taikomas naudotojų autentifikavimui ar autorizavimui*.
4. Pateikti blokų grandinės panaudos atvejį skaitmeninės tapatybės valdymui ir sukurti jo veikimą demonstruojantį prototipą.
5. Įvertinti pateikto sprendimo tinkamumą apibūdinant jo privalumus, trūkumus ir pritaikymo barjerus.
6. Palyginti pristatytą sprendimą su standartiniais naudotojų autentifikavimo ir autorizavimo būdais.

Laukiami rezultatai:

1. Identifikuoti pagrindiniai dabar kylantys skaitmeninės tapatybės valdymo iššūkiai.
2. Nustatyta, kuomet blokų grandinės technologija yra tinkama skaitmeninio identiteto problemoms spręsti.
3. Sukurtas tapatybės valdymo sistemos prototipas, naudojantis blokų grandinę.
4. Įvertinti pateiktos sistemos pranašumai bei trūkumai.

TURINYS

ĮVADAS 3

1. SKAITMENINĖS TAPATYBĖS VALDYMO APŽVALGA 6
   1.1. Tapatybės patvirtinimo poreikis 6
   1.2. Skaitmeninės tapatybės valdymo samprata 6
   1.3. Naudotojų poreikiai skaitmeninės tapatybės valdymo sistemoms 7
   1.4. Esamos skaitmeninių tapatybių valdymo sistemos 8
      1.4.1. Izoliuotas tapatybių valdymas 8
      1.4.2. Centralizuotas tapatybių valdymas 10
      1.4.3. Jungtinis tapatybių valdymas 12
   1.5. Tapatybių valdymo sistemų palyginimas 13

REZULTATAI IR IŠVADOS 14

LITERATŪRA 15

SĄVOKŲ APIBRĖŽIMAI 17

1. Skaitmeninės tapatybės valdymo apžvalga

1.1. Tapatybės patvirtinimo poreikis

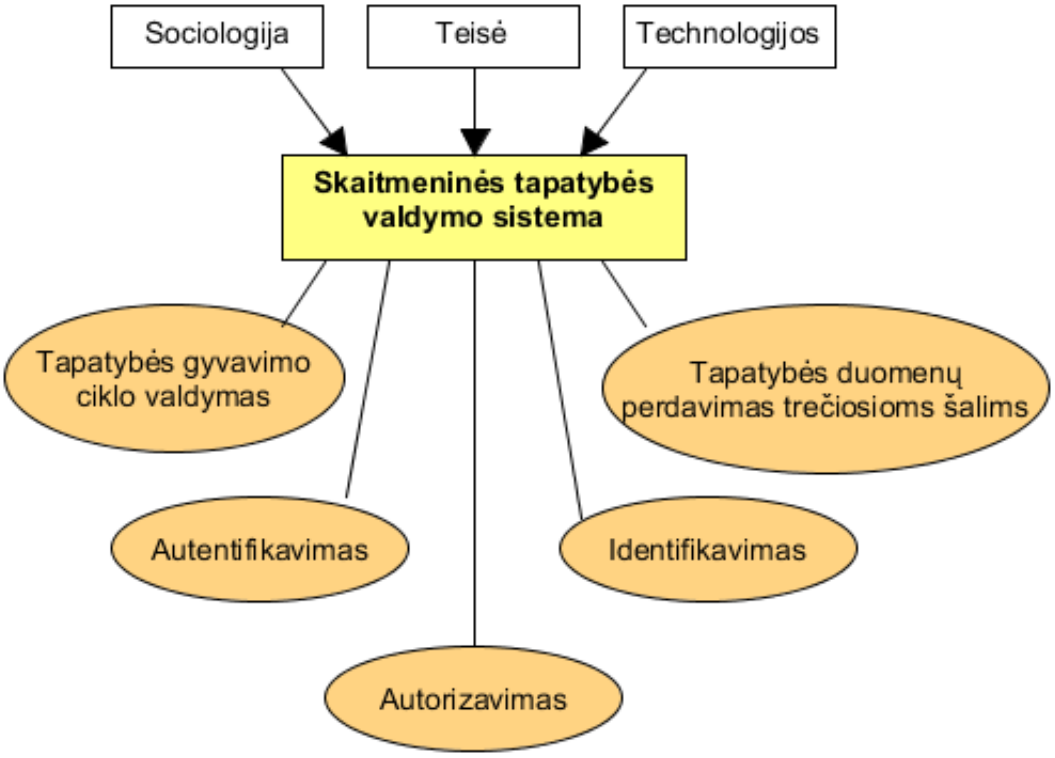
Šiais laikais naudotojo identifikavimas yra svarbi interneto taikomųjų programų dalis. Paslaugų tiekėjai identifikuoja savo naudotojus norėdami [Ral14]:

- registruoti (angl. *log*) naudotojų veiklą,
- užtikrinti, kad naudotojas iš tikrųjų yra asmuo, kuris sakosi esąs,
- suteikti dalį funkcionalumo tik autorizuotiems naudotojams,
- individualizuoti tinklalapio ar taikomosios programos turinį pagal naudotojo poreikius,
- sukurti paslaugos naudotojų bendruomenę,
- išvengti galimų anoniminių naudotojų atakų.

Dėl išvardytų priežasčių naudotojų identifikavimas atlieka svarbią rolę įvairiose taikomųjų programų srityse - elektroninėje valdžioje, elektroninėje komercijoje, verslo sumanume (angl. *business intelligence*), tyrimuose bei saugume (angl. *homeland security*) [GV09]. Kiekvienas paslaugų tiekėjas turi pasirinkti, kaip autentifikuoti, ir, jei reikia, autorizuoti naudotojus. Programos kūrėjas taip pat turi užtikrinti naudotojo suteiktų duomenų saugumą, o naudotojui tenka rūpintis skirtingų turimų paskyrų priežiūra ir savo duomenų sklaida tarp skirtingų sistemų. Minimus tapatybės atpažinimo skaitmeninėje erdvėje aspektus nagrinėja skaitmeninės tapatybės valdymo disciplina.

1.2. Skaitmeninės tapatybės valdymo samprata

Dėl nuolat vykstančios interneto ir jame esančių paslaugų plėtros tapatybių valdymo uždavinys pastaraisiais metais tapo itin svarbus [GV09]. Skaitmeninės tapatybės valdymo pagrindinis uždavinys yra kontroliuoti tapatybę ir su ja susijusius procesus, tokius kaip autentifikavimas, autorizavimas, prieigų kontrolė, tapatybės gyvavimo ciklo valdymas bei saugus tapatybės atributų perdavimas trečiosioms šalims [CY10; DP08]. Sprendžiant šį uždavinį, sukurta skirtingų skaitmeninės tapatybės valdymo sistemų. Šioms sistemoms įtaką daro kiti tapatybę nagrinėjantys mokslai (pvz. sociologija), taip pat jos gali atlikti keletą skirtingų funkcijų, susijusių su naudotojų tapatybe. Žemiau pateikiama diagrama, kurioje apibendrintas tapatybės valdymo sistemų kontekstas bei pagrindinės atliekamos užduotys:



1 pav. Skaitmeninių tapatybių valdymo sistemų kontekstas ir užduotys [GV09]

Paveiksle matomos disciplinos turi skirtingą poveikį tapatybių valdymo sistemoms. Sociologija padeda apibrėžti tapatybę ir jos atitikmenį skaitmeninėje erdvėje, teisės mokslas nusako tapatybės duomenų naudojimo reikalavimus, o esamos technologijos formuoja sistemos įgyvendinimo niuansus. Verta pastebėti, kad tapatybės valdymo sistema gali atlikti ne visas diagramoje nurodomas funkcijas, o tik dalį iš jų. Taip pat, 1-ame paveiksle bei visame darbe naudojamos skaitmeninės tapatybės valdymo sąvokos, tokios kaip *identifikavimas*, *autentifikavimas* ar *autorizavimas* neretai suprantamos skirtingai, o tai sukelia vieningos terminologijos trūkumą ir dėl jo kylančius neaiškumus [GV09]. Dėl to skyriuje „Sąvokų apibrėžimai“ pateikiami darbe naudojamų terminų aiškinimai.

Esamų tapatybių valdymo sistemų architektūros bei veikimo principai yra skirtingi - S. Clauß ir M.Köhntopp savo tyrime pastebi, kad nėra vieningo standarto identiteto valdymo sistemoms [CK01]. Tolesniuose skyriuose, apžvelgus naudotojų poreikius tapatybės valdymo sistemoms, pateikiamos skirtingos technologijos bei sprendimai, naudojami identiteto valdymui internete, jų privalumai bei trūkumai.

1.3. Naudotojų poreikiai skaitmeninės tapatybės valdymo sistemoms

Skaitmeninės tapatybės valdymas yra plati sritis, kurią galima analizuoti iš skirtingų pusių: paslaugų tiekėjo, tapatybės tiekėjo ar naudotojo. Šiame darbe į skaitmeninių tapatybių valdymą žvelgta iš naudotojo perspektyvos - kaip skaitmeninio valdymo sistemos atitinka naudotojų poreikius bei lūkesčius. Išskirtos šios naudotojoms aktualios sistemų savybės:

- identifikatorių bei slaptažodžių kiekis. Naudotojui vidutiniškai turint 25 paskyras, reikalaujančias slaptažodžių [FH07] bei naudojant nuo 2 iki 12-os el. paštų [GC07], jis tampa priverstas prisiminti vis daugiau identifikatorių. Atsimintinų autentifikavimo duomenų kiekiui augant, naudotojai yra linkę aukoti saugumą dėl patogumo ir naudoti panašius slaptažodžius skirtingose sistemose [PM03; Sam99];
- saugumas. Privatumas yra žmogaus poreikis ir visa visuomenė nukentėtų nuo jo nebuvimo [MS07]. Suteikiant savo asmens duomenis internete naudotojai tikisi, kad jie bus patikimai saugomi ir nepasiekiami programišiams. Tapatybių valdymo sistemos turėtų būti budrios saugumo rizikoms bei viešai skelbti saugumui skirtas priemones ir atliktų saugumo analizių rezultatus, kad tiek naudotojai, tiek paslaugų tiekėjai galėtų pasitikėti tapatybių valdymo sistemomis [DD08];
- asmens duomenų kontrolė. Pasak Nyderlanduose atliktų tyrimų, naudotojai nesijaučia kontroliuojantys savo asmens duomenų internete [Baa16]. Dėl to naudotojai pradeda nepasitikėti taikomųjų programų kūrėjais, nes jie pilnai nežino, kokia informacija apie juos kaupiama ir kokioms sistemoms ji perduodama;
- patogumas (angl. *usability*). Naudotojams skaitmeninės tapatybės valdymas neretai yra tik pašalinis mechanizmas, reikalingas norint pasiekti paslaugą [DD08]. Dėl šios priežasties sistemos naudojimosi patogumas yra svarbus - kuo tapatybės valdymas yra labiau integruotas su asmens jau naudojamomis sistemomis, kuo mažiau jis reikalauja papildomo naudotojo įsitraukimo ir kuo suteikia geresnę naudotojo patirtį (angl. *user experience*), tuo labiau naudotojas bus linkęs pasirinkti šį identiteto valdymo sprendimą.

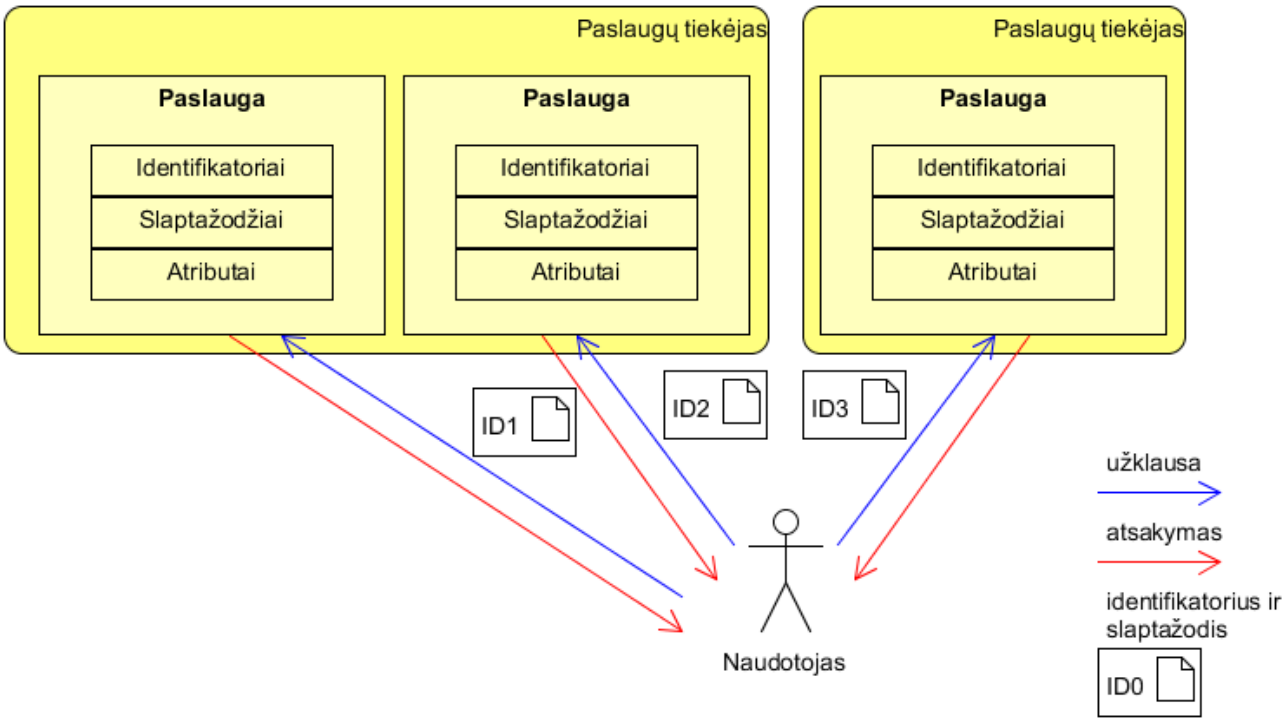
1.4. Esamos skaitmeninių tapatybių valdymo sistemos

Tapatybių valdymo sistemos yra pagrįstos skirtingomis architektūromis, kurios įgalina konkrečios sistemos veikimą. Šiame skyriuje tiriami 3-ys dažniausiai naudojami identiteto valdymo modeliai. Tiriant kiekvieną modelį, pirmiausia apžvelgti jo bendri veikimo principai. Toliau, apžvelgtos paplitusios modelio realizacijos, kurių technologiniai sprendimai gali turėti įtakos naudotojų poreikiams. Galiausiai, analizuotas sistemos atitikimas naudotojų lūkesčiams, išvardytiems 1.3 skyrelyje.

1.4.1. Izoliuotas tapatybių valdymas

Modelis

Izoliuotame modelyje paslaugų tiekėjas yra ir tapatybės tiekėjas, nes visos su tapatybės valdymu susijusios operacijos yra atliekamos vieno serverio. Tapatybės duomenų saugojimas, autentifikavimas ir autorizavimas yra įgyvendinti paties paslaugų tiekėjo [CY10]. Kiekvienas naudotojas turi atskirus identifikatorius kiekvienai naudojamai paslaugai. Modelis grafiškai pavaizduotas žemiau esančiame paveiksle:



2 pav. Izoliuotas skaitmeninės tapatybės valdymas [CY10]

Pagal izoliuotą modelį, naudotojas turi savo paskyrą kiekvienoje naudojamoje sistemoje. Kiekvieną kartą autentifikuojant ar autorizuojant naudotoją, tai atlieka pats paslaugų tiekėjas, bendraudamas tiesiogiai su naudotoju (jo naršykle). Naudotojui prisijungus prie vieno tinklalapio ir gavus prieigos raktą, jis gali toliau naudotis šiuo tinklalapiu, tačiau prireikus pasinaudoti kita taikomąja programa, tapatybės atpažinimo veiksmai (autentifikavimas, autorizavimas) turi vėl būti atlikti naujoje sistemoje.

Realizacijos

Kadangi šis naudotojų autentifikavimo bei autorizavimo modelis naudojamas seniausiai, yra gana nemažai jį įgyvendinusių taikomųjų programų. Lietuvoje šį modelį naudoja „Tiketa“, „Bilietai.lt“, „Pigu.lt“, „Varle.lt“, pasaulyje - „Booking.com“, „Skycop“, „AirBnB“ bei kitos platformos. Verta pastebėti, kad dalis iš jų jau remiasi ne vien tik savo izoliuotu tapatybės valdymu, bet jau turi į savo sistemas integravę ir papildomų autentifikavimo būdų (pvz. prisijungimą per „Facebook“ ar „Google“).

Realizacijų technologiniai sprendimai dažniausiai nėra viešai prieinami. Šiame modelyje kiekvienas paslaugų tiekėjas yra ir tapatybės tiekėjas, tad nereikia apibrėžti protokolų, duomenų formatų ar kitų detalių, kurios formalizuotų bendravimą tarp pasikliaujančiosios šalies ir tapatybės tiekėjo - visa tai pats nusprendžia ir įgyvendina paslaugų tiekėjas.

Patrauklumas naudotojams

Nors izoliuotas tapatybių valdymas yra gana paprastas paslaugų tiekėjams, tačiau jis greitai tampa nebekontroliuojamu naudotojams [JP05]. Jis verčia naudotojus turėti paskyrą kiekvienai paslaugai, o tai lemia daugybės identifikatorių ir slaptažodžių valdymą. Tai sukelia „slaptažodžių nuovargį“ (angl. *password fatigue*), kas veda prie tų pačių identifikatorių ir slaptažodžių pasirinkimo skirtingoms paslaugoms [DD08].

Izoliuotame identiteto valdyme programišiams sunkiau atlikti sukčiavimo (angl. *phishing*) ataką, nes naudotojas nebūna nukreipiamas į tapatybės tiekėjo puslapį. Tai pagerina šio modelio saugumą. Dėl to, kad paslaugų tiekėjas yra ir tapatybės tiekėjas, šiame modelyje galima išvengti duomenų perdavimo tarp skirtingų serverių - tokiu būdu sumažėja ir rizika, kad šiuos duomenis jų persiuntimo metu perims programišius. Tačiau, standartų duomenų formatams bei perdavimui nebuvimas gali paskatinti paslaugų tiekėjus nepažvelgti į tai atsakingai ir įgyvendinti bendravimą su naudotojo naršykle atmestinai.

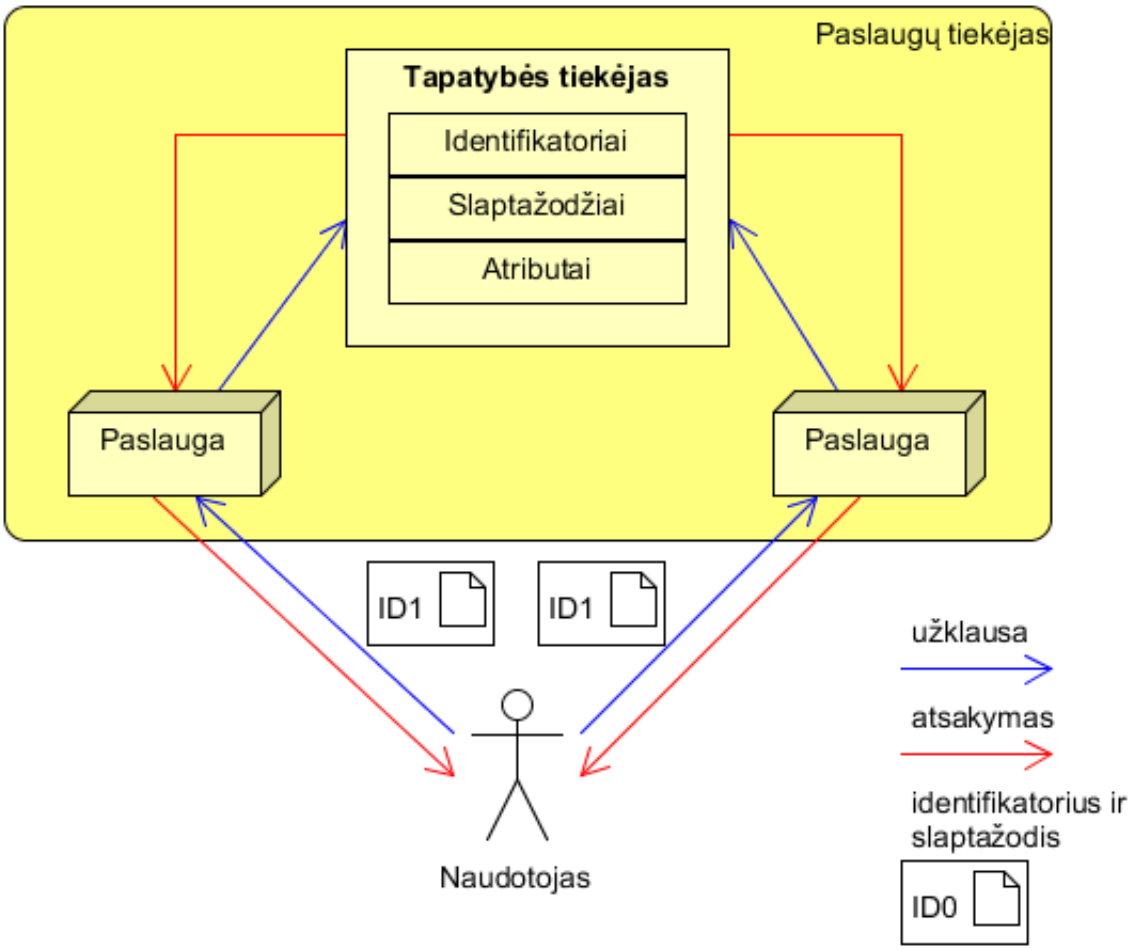
Naudotojų asmens duomenų kontrolė šiame modelyje priklauso nuo kiekvienos paslaugos. Asmenys atskirai suteikia savo duomenis kiekvienai paslaugai, dažniausiai paskyros sukūrimo metu. Jei paslauga informuoja apie duomenų panaudos atvejus (pvz. kam bus naudojamas el. pašto adresas), tuomet asmuo jausis labiau užtikrintas savo duomenų kontrole. Tačiau dėl šiame modelyje neišvengiamo duomenų suteikimo dideliam skirtingų paslaugų kiekiui, asmeniui tampa sunku prisiminti kiekvienos naudojamos platformos duomenų platinimo taisykles.

Izoliuotame tapatybės valdyme naudotojams tenka kartoti identifikavimo procesus (autentifikavimą, autorizavimą) tiek kartų, kiek paslaugų siekiama naudotis. Tai vargina naudotojus ir kuria blogą naudotojo patirtį. Tačiau, izoliuotas tapatybės valdymas pasižymi nuoseklia vartotojo sąsaja (dėl visų tapatybės valdymo procesų įgyvendimo tame pačiame paslaugų tiekėjo puslapyje), tad tai šiek tiek pagerina bendrą naudotojo patirtį.

1.4.2. Centralizuotas tapatybių valdymas

Modelis

Centralizuotame skaitmeninių tapatybių valdyme egzistuoja vienas tapatybės tiekėjas, į kurį kreipiasi visos paslaugos, esančios to paties paslaugų tiekėjo domene [JP05]. Paslaugų tiekėjo ir tapatybės tiekėjo funkcijos tampa atskirtos - tapatybės tiekėjas rūpinasi naudotojo identiteto valdymu, o paslaugų tiekėjas koncentruojasi į savo paslaugos tobulinimą. Naudotojui šiame modelyje užtenka vieno identifikatoriaus ir slaptažodžio, su kuriais jis gali prisijungti prie visų to paties paslaugų tiekėjo paslaugų. Šis modelis iliustruotas 3-iame paveiksle.



3 pav. Centralizuotas skaitmeninės tapatybės valdymas [CY10]

jei reik, pastraipa paslaugų tiekėjo bruožams.

Realizacijos

Centralizuotas modelis tinkamas naudoti vieno paslaugų tiekėjo ribose [JP05]. Vienas iš pavyzdžių - „Atlassian“ įmonės paslaugos. Naudotojui pakanka turėti vieną „Atlassian“ paskyrą ir jis gali naudotis skirtingais šio paslaugų tiekėjo produktais, tokiais kaip „Jira“, „Confluence“, „Bitbucket“ bei kitais. „Atlassian“ turi ir vienkartinio prisijungimo sąlygas - paslaugas galima sukonfigūruoti taip, kad prisijungus prie vienos iš jų, naudotojas automatiškai tampa prisijungęs ir prie kitų paslaugų.

pridėt Kerberos

Patrauklumas naudotojams

Iš naudotojo perspektyvos, šis modelis yra patogesnis nei izoliuotas. Naudotojui pakanka turėti vieną identifikatorių, kuris bus tinkamas visoms paslaugoms. Priklausomai nuo realizacijos, naudotojui gali tekti iš naujo prisijungti prie kiekvienos paslaugos arba vieną kartą prisijungti prie betkurios iš paslaugų ir tapti autentifikuotu visose kitose paslaugose [JP05]. Naudotojo asmens

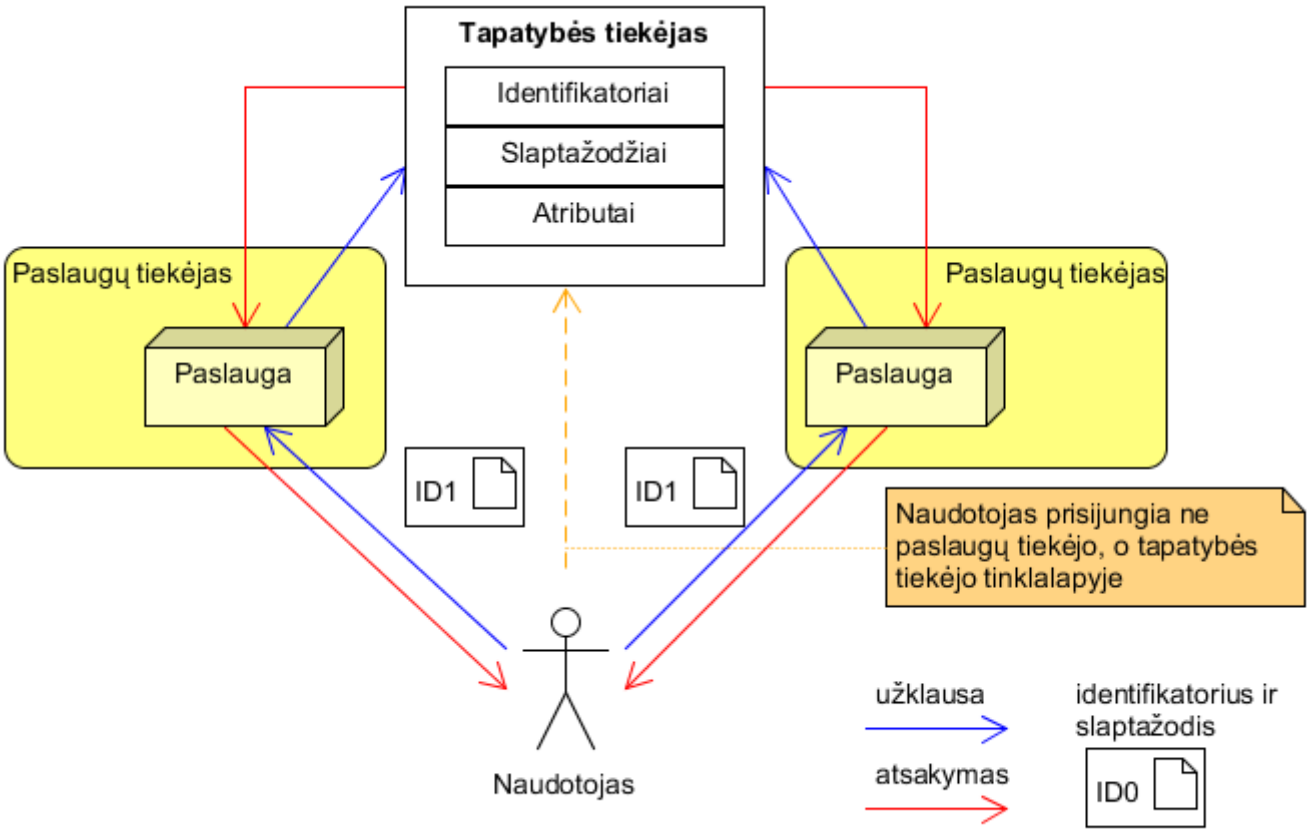
duomenų kontrolė yra geresnė nei izoliuotame skaitmeninės tapatybės valdyme, nes naudotojas asmens duomenis patiki mažesniam kiekiui esybių (vietoj kiekvienos paslaugos, kiekvienam paslaugų tiekėjui).

Pagrindinis šio modelio trūkumas yra tas, kad jis galimas naudoti tik vieno paslaugų tiekėjo srityje (angl. *scope*). Tai palieka laisvės paslaugų tiekėjui tapatybės valdymo sistemos realizavimui (tai gali būti centralizuota platforma įmonės ribose), tačiau naudotojas negali turimo identifikatoriaus naudoti kito paslaugų tiekėjo sistemose.

1.4.3. Jungtinis tapatybių valdymas

Modelis

Centralizuotas modelis reikalauja visų naudotojų būti tame pačiame domene, tačiau naudotojams reikia paslaugų ir iš kitų domenų [CY10]. Jungtinis (angl. *federated*) tapatybių valdymas yra aibė technologijų ir procesų, kurie leidžia sistemoms dalintis tapatybės informacija ir deleguoti tapatybės valdymo užduotis tarp skirtingų paslaugų tiekėjų [MR08]. Šis tapatybių valdymo modelis įgalina naudotojus turėti vieną identifikatorių, kurį gali naudoti skirtingų paslaugų tiekėjų tinklalapiuose. Žemiau pateikiama schema, nusakanti šio modelio architektūrą:



4 pav. Jungtinis skaitmeninės tapatybės valdymas [CY10]

Jungtiniame tapatybės valdyme tapatybės tiekėjas yra atskira sistema, su kuria turi integruotis paslaugų tiekėjas. Tapatybės duomenys bei su tapatybe susiję veiksmai (autentifikavimas, autori-

zavimas) yra deleguojami šiai sistemai. Naudotojas turi vieną identifikatorių, su kuriuo prisijungia tiesiogiai tapatybės tiekėjo puslapyje. Prisijungus šioje sistemoje, naudotojas tampa autentifikuotas visose paslaugose, kurios palaiko šį tapatybės tiekėją [MR08].

Šis tapatybių valdymo modelis yra gana patogus naudotojams. Jiems užtenka turėti vieną identifikatorių, su kuriuo gali prisijungti prie tinklalapių iš skirtingų paslaugų tiekėjų. Asmens duomenų saugumas priklauso nuo bendravimo tarp paslaugų bei tapatybės tiekėjų, o šiame modelyje jis sudėtingesnis nei izoliuotame ar centralizuotame tapatybių valdyme, nes jungtinis valdymas paremtas tarpdomeniniu bendravimu [MR08]. Naudotojo duomenų kontrolė jungtiniame modelyje turi tiek privalumų, tiek trūkumų. Viena vertus, naudotojas savo asmens duomenis suteikia mažesniam kiekiui sistemų (tik tapatybės tiekėjams, vietoj visų paslaugų tiekėjų). Tačiau taip paslaugų tiekėjas tampa vieninteliu nesekmės tašku (angl. *single point of failure*) - programišiams įsilaužus į tapatybės tiekėjo sistemą, asmens paskyros visose paslaugose tampa prieinamos [PM03]. Taip pat, naudotojui gali būti sunku kontroliuoti savo duomenų sklaidą tarp tapatybės tiekėjo ir skirtingų paslaugų, ką rodo ir *Cambridge Analytica* incidentas [Gra18].

jei reik, pastraipa paslaugų tiekėjo bruožams.

Realizacijos

paimt iš kursinio

1.5. Tapatybių valdymo sistemų palyginimas

1 lentelė. My caption

Modelis	Identifikatorių kiekis	Patogumas			Asmens duomenų kontrolė
		Prisijungimų kiekis	Papildoma programinė įranga	Naudotojo patirtis	
Izoliuotas					
Centralizuotas					
Jungtinis					

Rezultatai ir išvados

Literatūra

[Baa16] Djuri Baars. Towards Self-Sovereign Identity using Blockchain Technology. Disertacija, University of Twente, 2016. URL: http://essay.utwente.nl/71274/1/Baars%7B%5C_%7DMA%7B%5C_%7DBMS.pdf.

[Cam04] L.J. Camp. Digital identity. IEEE Technology and Society Magazine, 23(3):34–41, 2004. DOI: 10.1109/MTAS.2004.1337889. URL: http://ieeexplore.ieee.org/document/1337889/.

[CY10] Yuan Cao Yuan Cao ir Lin Yang Lin Yang. A survey of Identity Management technology. 2010 IEEE International Conference on Information Theory and Information Security:287–293, 2010. DOI: 10.1109/ICITIS.2010.5689468. URL: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5689468.

[CK01] S Clauß ir M Køhntopp. Identity Management and its Support of Multilateral Security. Computer Networks, 37 (2):205–219, 2001.

[DD08] Rachna Dhamija ir Lisa Dusseault. The Seven Flaws of Identity Management: Usability and Security Challenges. IEEE Security & Privacy Magazine, 6(2):24–29, 2008-03. ISSN: 1540-7993. DOI: 10.1109/MSP.2008.49. URL: http://ieeexplore.ieee.org/document/4489846/.

[DP08] M. Dabrowski ir P. Pacyna. Generic and Complete Three-Level Identity Management Model. 2008 Second International Conference on Emerging Security Information, Systems and Technologies, p. 232–237. IEEE, 2008-08. DOI: 10.1109/SECURWARE.2008.18. URL: http://ieeexplore.ieee.org/document/4622588/.

[FH07] Dinei Florencio ir Cormac Herley. A large-scale study of web password habits. Proceedings of the 16th international conference on World Wide Web - WWW '07, p. 657, New York, New York, USA. ACM Press, 2007. ISBN: 9781595936547. DOI: 10.1145/1242572.1242661. URL: http://portal.acm.org/citation.cfm?doid=1242572.1242661.

[GC07] Benjamin M. Gross ir Elizabeth F. Churchill. Addressing Constraints: Multiple Usernames, Task Spillage and Notions of Identity. CHI '07 extended abstracts on Human factors in computing systems - CHI '07, p. 2393, New York, New York, USA. ACM Press, 2007. ISBN: 9781595936424. DOI: 10.1145/1240866.1241013. URL: http://portal.acm.org/citation.cfm?doid=1240866.1241013.

[Gra18] Kevin Granville. Facebook and Cambridge Analytica, 2018. URL: https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html (tikrinta 2018-03-28).

[GV09] Uwe Glässer ir Mona Vajihollahi. Identity Management Architecture. 9:97–116, 2009. URL: https://link.springer.com/content/pdf/10.1007%7B%5C%%7D2F978-1-4419-1325-8.pdf.

[JP05] Audun Jøsang ir Simon Pope. User Centric Identity Management. AusCERT Conference, 2005. URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.60.1563%7B%5C&%7Drep=rep1%7B%5C&%7Dtype=pdf.

[Kuk11] Ado Kukic. Definitive guide to Single Sign-On (SSO), 2011. URL: https://resources.auth0.com/definitive-guide-to-single-sign-on/.

[Mic07] Microsoft Developer Network. Access Tokens, 2007. URL: https://msdn.microsoft.com/en-us/library/Aa374909.aspx (tikrinta 2018-04-07).

[Min18] Miniwatts Marketing Group. World Internet Users Statistics, 2018. URL: https://www.internetworldstats.com/stats.htm (tikrinta 2018-03-28).

[MM17] Jason Mander ir Felim McGrath. Global Web Index Social. Tech. atask., 2017. URL: https://cdn2.hubspot.net/hubfs/304927/Downloads/GWI%20Social%20Summary%20Q3%202017.pdf.

[MR08] E Maler ir D Reed. The Venn of Identity: Options and Issues in Federated Identity Management. IEEE Security and Privacy, 6(2):16–23, 2008. ISSN: 15407993. DOI: 10.1109/MSP.2008.50. URL: http://innovbfa.viabloga.com/files/IEEESecPriv%7B%5C_%7D%7B%5C_%7D%7B%5C_%7DVenn%7B%5C_%7Dof%7B%5C_%7DIdentity%7B%5C_%7D%7B%5C_%7D%7B%5C_%7D2008.pdf.

[MS07] Tewfiq El Maliki ir Jean-marc Seigneur. A Survey of User-centric Identity Management Technologies. International Conference on Emerging Security Information Systems and Technologies:12–17, 2007. DOI: 10.1109/SECURWARE.2007.6. URL: http://ieeexplore.ieee.org/xpls/abs%7B%5C_%7Dall.jsp?arnumber=4385303.

[PM03] Andreas Pashalidis ir Chris J. Mitchell. A taxonomy of single sign-on systems. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2727 LNCS:249–264, 2003. ISSN: 03029743.

[Ral14] Raluca Budiu. Login Walls Stop Users in Their Tracks, 2014. URL: https://www.nngroup.com/articles/login-walls/ (tikrinta 2017-06-10).

[Sam99] V Samar. Single sign-on using cookies for Web applications. Proceedings IEEE 8th International Workshops on Enabling Technologies Infrastructure for Collaborative Enterprises WET ICE99:158–163, 1999. ISSN: 10801383.

Sąvokų apibrėžimai

Atributas - charakteristika, susieta su esybe, pavyzdžiui fiziniu asmeniu. Galimi asmens atributai: gimimo data, vardas, ūgis, pirštų antspaudai [Cam04]. Atributas gali būti laikinas (pvz. adresas) arba nuolatinis (pvz. asmens kodas).

Identifikatorius - tai atributas, kuris vienareikšmiškai susiejamas su jį pateikiančiu asmeniu ir kurį sunku arba neįmanoma pakeisti. Fizinio asmens identifikatoriaus pavyzdys galėtų būti gimimo data (žmogus gali apie ją meluoti, tačiau gimimo datos pakeisti neįmanoma) [Cam04]. Skaitmeninio identifikatoriaus pavyzdys yra naudotojo elektroninio pašto adresas.

Identifikavimas - tai procesas, kurio metu asmuo susiejamas su jo identifikatoriumi [Cam04]. Identifikavimo pavyzdys yra asmens ir jo vardo susiejimas: *tu esi Jonas Jonaitis*.

Autentifikavimas - tai procesas, kurio metu patvirtinama sąsaja tarp tapatybės ir jos identifikatoriaus (t.y., įrodoma, kad asmuo iš tikrųjų yra tas, kas sakosi esąs) [Cam04; Kuk11]. Dažniausiai internete autentifikavimui pateikiamas identifikatorius (pvz. slapyvardis) bei slaptažodis, susietas su tuo identifikatoriumi. Autentifikavimo pavyzdys: *tavo pateikta slapyvardžio ir slaptažodžio pora patvirtina, kad tu esi Jonas Jonaitis*.

Autorizavimas - tai procesas, kurio metu leidžiama arba draudžiama asmeniui atlikti konkretų veiksmą, priklausomai nuo jo identifikatoriaus ar atributo [Cam04]. Pavyzdys: *kadangi tau yra daugiau nei 18 metų, tu gali nusipirkti energetinį gėrimą*.

Skaitmeninė tapatybė - abstrakti fizinės esybės reprezentacija, sudaryta iš aibės esybės nuolatinių ar laikinų atributų, kurie susiejami su fizine esybe [Cam04; GV09]. Fizinė esybė gali būti fizinis arba juridinis asmuo. Šiame darbe, jei nenurodyta kitaip, kalbama apie fizinio asmens skaitmeninę tapatybę.

Skaitmeninės tapatybės valdymas (angl. *digital identity management*) - tai veiksmų, skirtų kontroliuoti tapatybę ir su ja susijusius procesus, visuma [DP08]. Į tai įeina autentifikavimas, autorizavimas, prieigų kontrolė, tapatybės gyvavimo ciklo valdymas bei saugus tapatybės atributų perdavimas trečiosioms šalims [CY10].

Skaitmeninių tapatybių domenas - tai sritis, kurioje kiekviena tapatybė yra unikali. Domene esantys unikalūs identifikatoriai leidžia sukurti vienas-su-vienu ryšį tarp šių identifikatorių ir jų tapatybių bei taip vienareikšmiškai identifikuoti tapatybę iš jos unikalaus identifikatoriaus [JP05].

Paslaugų tiekėjas (angl. *service provider*) - tai betkokia taikomoji programa, kuri suteikia naudotojui tam tikrą paslaugą ar norimą turinį. Galimi paslaugų tiekėjai yra interneto tinklapiai, susirašinėjimo programos ar kitos taikomosios programos, į kurias kreipiasi naudotojas [PM03; Sam99]. Paslaugų tiekėjas gali turėti vieną ar kelias paslaugas, kurioms reikia tapatybės valdymo funkcijų. Darbe paslaugų tiekėjas dar gali būti vadinamas pasikliaujančiąja šalimi (angl. *relying party*).

Tapatybės tiekėjas (angl. *identity provider*) - servisas ar taikomoji programa, skirta koordinuoti su tapatybe susijusius duomenis tarp naudotojų, jų naršyklių bei paslaugų tiekėjų [Kuk11]. Pagrindinės tapatybės tiekėjo funkcijos: infrastruktūros naudotojų tapatybės duomenims apdoroti sukūrimas ir užklausų iš paslaugų tiekėjų bei naudotojų apdorojimas [CY10].

Prieigos raktas (angl. *token*) - tai objektas, identifikuojantis skaitmeninę tapatybę [Mic07].

Šis raktas būna išduodamas tapatybės tiekėjo ir skirtas identifikuoti naudotoją. Raktas būna prisegtas prie visų autentifikuoto naudotojo užklausų ir leidžia paslaugos tiekėjui žinoti, koks naudotojas kreipiasi.

Vienkartinis prisijungimas (angl. *single sign on*) - to be added.