

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

Naudojimasis interneto paslaugomis 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 neretai prašo naudotojų autentifikuotis. Interneto naudotojų skaičiui perkopus 4 milijardus [Min18], o kiekvienam naudotojui vidutiniškai turint po 7 skirtingas socialines paskyras [MM17], asmenų autentifikavimas tampa vis didesniu iššūkiu.

Susidariusi situacija 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 paskyras, reikalaujančias slaptažodžių 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 tą pačią paskyrą. 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* neleistino duomenų perdavimo 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:

TURINYS

ĮVADAS	3
1. SKAITMENINĖS TAPATYBĖS VALDYMO APŽVALGA	6
1.1. Tapatybės patvirtinimo poreikis	6
1.2. Skaitmeninės tapatybės valdymo samprata	6
1.3. Skaitmeninės tapatybės valdymo sistemų charakteristikos.....	7
1.4. Skaitmeninių tapatybių valdymo sistemos	8
REZULTATAI IR IŠVADOS	9
LITERATŪRA	10
SAVOKŲ APIBRĖŽIMAI	12

1. Skaitmeninės tapatybės valdymo apžvalga

1.1. Tapatybės patvirtinimo poreikis

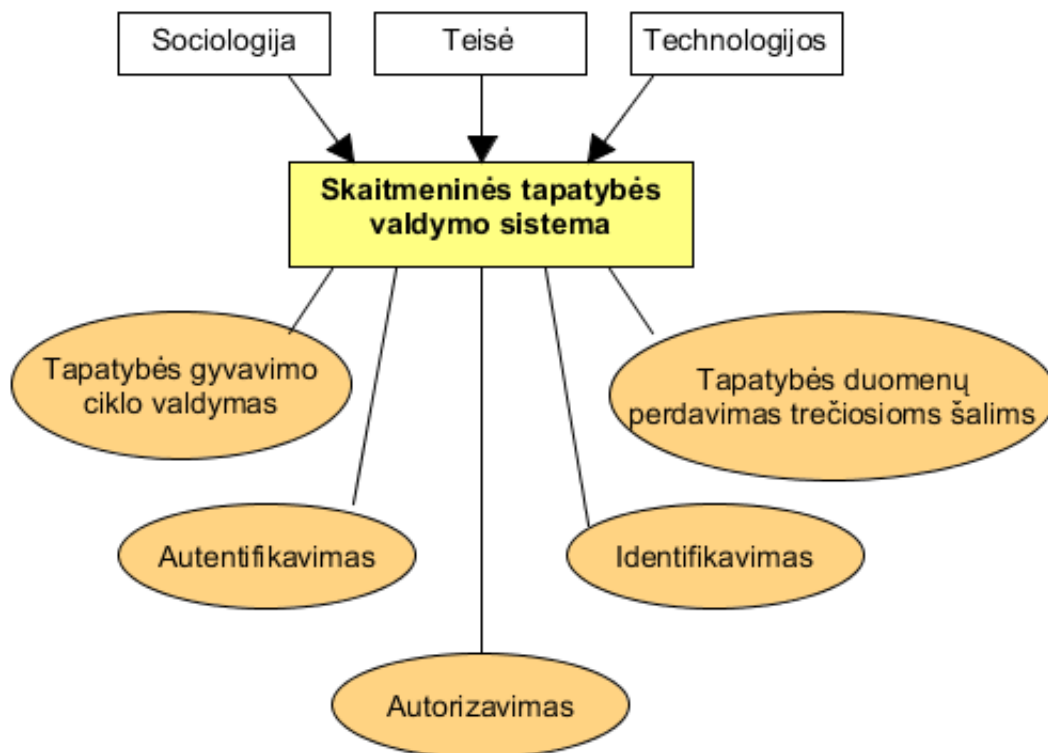
Šiais laikais naudotojo identifikavimas yra svarbi interneto taikomųjų programų dalis. Paslaugų tiekėjai identifikuoja savo naudotojus norėdami [Ral14]:

- 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 anonininių 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 saugoti naudotojų suteiktus asmens duomenis ir užtikrinti jų 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]. Sprendžiant šį iššūkį, sukurta skirtingų skaitmeninės tapatybės valdymo sistemų, siekiančių išspręsti naudotojų tapatybės atpažinimo problemas. 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 pavaizduotas 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 dažniausiai 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 bei paslaugų tiekėjų reikalavimus tapatybės valdymo sistemoms, pateikiamos skirtingos technologijos bei sprendimai, naudojami identiteto valdymui internete, jų privalumai bei trūkumai.

1.3. Skaitmeninės tapatybės valdymo sistemų charakteristikos

Šiame darbe į skaitmeninių tapatybių valdymą žvelgta iš dviejų perspektyvų: naudotojo bei paslaugų tiekėjo **palikt tik naudotojo?**. Abi pusės, priklausomai nuo savo poreikių, iškelia jiems aktualias identiteto valdymo sistemų savybes. Darbe nagrinėjant skirtingas tapatybės valdymo sistemas, didžiausias dėmesys kreiptas į žemiau aprašytus naudotojams bei paslaugų tiekėjams svarbius

sistemų bruožus.

Tiek naudotojams, tiek paslaugų tiekėjams itin svarbus yra pasirinkto identiteto valdymo sprendimo patikimumas, t.y., asmens duomenų saugumo užtikrinimas. Naudotojai nenori savo asmens duomenų nutekėjimo (angl. *data leakage*) internete, tuo tarpu paslaugų tiekėjai negali rizikuoti prarasti naudotojų pasitikėjimo jų paslauga pasirinkus nesaugų tapatybės valdymo sprendimą. Be patikimumo, naudotojams bei paslaugų tiekėjams aktualios ir kitos skaitmeninio identiteto sistemų savybės. Žemiau pateikiami pagrindiniai abiejų pusių poreikiai.

Naudotojams svarbūs tapatybės valdymo sistemų bruožai:

- identifikatorių kiekis. Naudotojui vidutiniškai turint 25 paskyras, reikalaujančias slaptažodžių [FH07] bei naudojant nuo 2 iki 12-os el. paštų [GC07] naudotojai tampa priversti prisiminti vis daugiau identifikatorių. Tai verčia naudotojus aukoti saugumą dėl patogumo ir naudoti panašius slaptažodžius skirtingose sistemose [PM03; Sam99];
- asmens duomenų kontrolė. Pasak Nyderlanduose atliktų tyrimų, naudotojai jaučia, kad nekontroliuoja 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 dažnai yra tik pašalinis mechanizmas, reikalingas norint pasiekti paslaugą [DD08]. Dėl šios priežasties sistemos naudojimosi patogumas yra svarbus - kuo tapatybės valdymas yra labiau integruota su asmens jau naudojamomis sistemomis ir kuo mažiau jis reikalauja papildomo naudotojo įsitraukimo, tuo labiau naudotojas bus linkęs pasirinkti šį identiteto valdymo sprendimą.

Paslaugų tiekėjams aktualios tapatybės valdymo sistemų savybės:

- kaštai, skirti tapatybės valdymui. Priklausomai nuo pasirinkto sprendimo, paslaugų tiekėjui gali tekti skirti daug arba mažai resursų (programuotojų, laiko, investavimo į technologijas) naudotojų tapatybės valdymo veiksams užtikrinti;
- naudotojo patirties kontrolė (angl. *user experience control*). Paslaugų tiekėjai siekia užtikrinti teigiamą naudotojų patirtį, o tapatybės valdymo sistemos veikimo primesti sprendimai (pvz. nukreipimai į kitą tinklalapį) gali daryti tam įtaką.

1.4. Skaitmeninių tapatybių valdymo sistemos

Skirtingos tapatybių valdymo sistemos yra pagrįstos skirtingomis architektūromis, kurios įgalina konkrečios sistemos veikimą. Šiame skyriuje apžvelgiami 4-i naudojami tapatybių valdymo modeliai bei pateikiami šių modelių įgyvendinimo pavyzdžiai.

- apibrėžt, į kokius aspektus atkreipsiu dėmesį nagrinėdamas (let's go user centric?) - eit per dvi skirtingas dimensijas: > architektūra (lokalī, centralizuota, paskirstyta) > pavyzdžiai (bobotė-spaskola.com, LDAP/AD, OpenIdConnect/SAML 2.0)

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 Kønhtopp. 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. 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>.

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

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 yra slaptyvardžio ir slaptažodžio pora. Autentifikavimo pavyzdys: *tavo pateikta slaptyvardžio 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 tu pateikei administratoriaus prieigos raktą, tau leidžiama ištrinti šį tinklalapio puslapį*.

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 procesų, 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].

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.

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].