Mona Välimäki

SÄHKÖINEN IDENTITEETTI OSANA TIETOJÄRJESTELMIEN PÄÄSYNHALLINTAA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2019

TIIVISTELMÄ

Välimäki, Mona Susanna
Sähköinen identiteetti osana tietojärjestelmien pääsynhallintaa
Jyväskylä: Jyväskylän yliopisto, Informaatioteknologian tiedekunta, 2019, 30 s.
Tietojärjestelmätiede, Kandidaatintutkielma
Ohjaaja: Clements, Kati

Identiteetin- ja pääsynhallinta on merkittävä osa tietojärjestelmien tietoturvaa. Tietojärjestelmän on mahdollistettava sen kohderesurssien suojaaminen luvattomalta tiedonkululta ja muokkaukselta sallien kuitenkin pääsy valtuutetuille käyttäjille ja käyttöoikeuksille. Ennen pääsyoikeuksien toteutumista tulee käyttäjän tai muun pääsyoikeuspyyntöä esittävän sähköisen identiteetin alkuperä todentaa. Sähköisellä identiteetillä tarkoitetaan verkkoympäristössä ilmenevää entiteettiä, johonka liitetyillä attribuuttien arvoilla entiteetti pystytään yksilöimään. Esimerkkinä attribuutin arvoista käy muun muassa käyttäjän sijainti tai puhelinnumero. Identiteetin todentaminen tapahtuu autentikoinnilla, jossa nämä entiteetin ominaisuudet varmennetaan todenmukaisiksi. Sähköisen identiteetin todentaminen on yksi prosesseista, jotka luetaan osaksi identiteetinhallintaa. Pääsynhallinnalla tarkoitetaan puolestaan menettelyitä, joilla varmistetaan, että käyttäjät, laitteet, sovellukset ja järjestelmät pääsevät käyttämään tietojärjestelmissä olevaa tietoa roolinsa mukaisesti. Pääsynhallinnan keskeisin tehtävä on valvoa tietojärjestelmän pääsyoikeuksia siten, että vain valtuutetut pääsyoikeudet voivat tapahtua. Valtuutetulla eli auktorisoidulla pääsyoikeudella tarkoitetaan myönnettyä oikeutta käyttää resursseja todentamisen jälkeen. Eri pääsynhallintamalleja ja -mekanismeja on useita ja tässä kandidaatintutkielmassa tarkastellaan lähemmin harkinnanvaraista, pakollista ja roolipohjaista pääsynhallintaa. Tutkielma on toteutettu kirjallisuuskatsauksena ja siinä pyritään vastaamaan kysymyksiin *"Miten sähköistä identiteettiä hyödynnetään pääsynhallinnassa?"* ja *"Mitä pääsynhallintamalleja on olemassa ja tarjolla?"*.

Asiasanat: Sähköinen identiteetti, todentaminen, pääsynhallinta, valtuuttaminen

ABSTRACT

Välimäki, Mona Susanna
Digital identity as a constituent of information systems access control
Jyväskylä: University of Jyväskylä, 2019, 30 p.
Information Systems, Bachelor's Thesis)
Supervisor: Clements, Kati

Identity and access management is a major part of the security of information systems. The information system must protect its target resources from unauthorized data transmissions and edits while allowing entrance to authorized users and access rights. User or other digital identity requesting access must have their source verified before access rights can be fulfilled. Digital identity signifies to an entity that appears in a network and it can be identified using attribute values that are associated with specific entity. User's location and phone number are examples of attribute values. Identity's attestation takes place through authentication, where entity properties are verified to be true. The authentication of digital identity is one of the processes associated with identity management. Access management, in turn, refers to procedures that ensure users, devices, applications and systems have access to information according to their role. The main task of access control is to navigate access rights to the information system thereby only authorized access rights can take a place. Authorized access rights mean admitted rights to use resources after authentication. There are many recognized access control models and policies. This study examines discretionary, mandatory and role-based access control. The study is made as a literature review and its attempts to answer questions "How is digital identity utilized in access control?" and "What access control models exist and are available?".

Keywords: Digital idenity, authentication, access control, authorization

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Käsite identiteetin- ja pääsynhallinnasta alkoi muotoutua, kun yritysten ja organisaatioiden työntekijöille koettiin tarve yhdenmukaistaa tietojärjestelmiin liittyviä tunnistautumisratkaisuja. Yritysten ja organisaatioiden toimintaympäristössä huomattiin sekä tietoturvallisia heikkouksia että kuormittavia käytänteitä liittyen työntekijöiden käyttäjätunnuksiin eri tietojärjestelmissä. Näitä olivat olleet esimerkiksi useamman eri käyttäjätunnuksen ja salasanan hallinnointi sekä vielä työsuhteen päättymisen jälkeen voimassaoleviksi unohtuneet käyttäjätunnukset. Tämän myötä informaatioteknologian toimialalla syntyi kehittämismahdollisuus tuotteille ja palveluille, jotka liittyivät käyttäjätunnusten ja käyttöoikeuksien hallintaan. (Linden, 2015).

Identiteetin- ja pääsynhallinnalla on merkittävä osa tietojärjestelmien resurssien suojaamisessa ulkopuolisilta. Kummastakin löytyy sekä yhdessä että erikseen esitettyjä menettelytapoja vastaamaan kohdejärjestelmän suojausvaatimuksia (Jajodia, Samarati, Sapino & Subrahmanian, 2001). Tässä kandidaatintutkielmassa tarkastellaan kirjallisten lähteiden perusteella eri käytänteitä ja lähestymistapoja identiteetin- ja pääsynhallintaan. Lisäksi tutkielmassa tarkastellaan erityisesti sähköisen identiteetin käsitettä, joka on verkkopalveluiden yleistyessä noussut verrattain moniselitteiseksi. Tutkielma toteutetaan kirjallisuuskatsauksena, ja sen päämääränä on tarkastella sähköisen identiteetin osaa tunnetuimmissa pääsynhallintamalleissa. Eri pääsynhallintamallien suuren lukumäärän takia rajaus eri mallien välillä on toteutettu lähdeaineiston perusteella muun muassa mallin tunnettavuuden mukaan. Tämän perusteella pääsynhallintamalleista valittiin harkinnanvarainen, pakollinen ja roolipohjainen pääsynhallintamalli läheistä tarkastelua varten.

Lähdeaineistoa on koottu sähköisistä tietokannoista, joita olivat Google Scholar, IEEE ja Wiley Online Library. Lähteet koostuvat pääosin informaatioteknologian toimialan tieteellisistä artikkeleista, konferenssijulkaisusta ja muusta kirjallisuudesta. Tieteellisten artikkeleiden, konferenssijulkaisuiden ja kirjakustantajien kohdalla luotettavuutta on arvioitu Julkaisufoorumin julkaisukanavahaulla. Lähteiksi on pyritty valitsemaan vähintään perustasoon kuuluvia julkaisuja silti painopisteen ollessa korkeatasoisimmissa julkaisuissa, kuten

IEEE Security & Privacy, Software-Practice and experience ja ACM Transactions on Database Systems. Tutkielman tutkimuskysymyksiä ovat *"Miten sähköistä identiteettiä hyödynnetään pääsynhallinnassa?"* ja *"Mitä pääsynhallintamalleja on olemassa ja tarjolla?"*. Lähdeaineistoa kerättiin käyttämällä hakusanoja "digital identity", "social identity", "identity and access management", "identity management architecture" "access control framework", "role-based access control", "mandatory access control" ja "discretionary access control".

Tutkielma koostuu johdannosta, kolmesta sisältöluvusta ja yhteenvedosta. Johdannon jälkeisessä toisessa luvussa määritellään sähköinen identiteetti huomioiden myös sosiaalitieteellinen näkökulma ennen identiteetin käsittelyä verkkoympäristöissä. Toisessa luvussa käsitellään identiteetinhallinnan viitekehystä, identiteetin roolia tietojärjestelmien kokonaisarkkitehtuurissa ja sähköiseen identiteettiin liitettäviä ominaisuuksia. Kolmannessa luvussa määritellään pääsynhallinta sekä siihen liittyvät termit kuten todentaminen ja valtuuttaminen. Lisäksi kolmannessa luvussa käydään pääsynhallinnan viitekehyksen kautta läpi eri pääsynhallintakäytänteitä ja tarkastellaan lähemmin harkinnanvaraista, pakollista ja roolipohjaista pääsynhallintamallia. Neljännessä luvussa perehdytään sähköisen identiteetin ja käyttäjäoikeuksien osaan aiemmin käsiteltyjen kolmen eri pääsynhallintamallin kohdalla. Lisäksi tarkastellaan käyttöoikeuksien hallintaa pilvipalveluiden ja esineiden internetin kohdalla. Lopuksi viidennessä luvussa esitetään yhteenveto tutkielmasta.

2 SÄHKÖINEN IDENTITEETTI

Palveluntarjoajan ja asiakkaan välillä tapahtuva transaktio verkkopohjaisessa ympäristössä vaatii palvelun käyttäjän identifiointia tavalla, joka eroaa fyysisessä liiketilassa tapahtuvasta toimituksesta. Windley (2005) selvittää teoksensa johdannossa sähköisen identiteetin merkitystä palveluun tunnistautuessa. Automatisoidut verkossa toimivat palvelut sisältävät asiakkaan ja palveluntarjoajan lisäksi lukuisia muita käyttäjiä, kuten työntekijöitä, toimittajia ja muita sidosryhmien jäseniä. Useissa tapauksissa anonyymisoitu transaktio näiden käyttäjien välillä on mahdotonta tai epätoivottu tapa toteuttaa palvelua. Tämän myötä on koettu tarpeelliseksi määritellä sähköinen identiteetti ja sen hallinta. (Windley, 2005).

Rannenberg, Royer & Deuker (2009) kuvaavat kirjassaan identiteetin asemaa tietoyhteiskunnassa. Käsitteelle tietoyhteiskunta ei ole tällä hetkellä universaalia määritelmää, mutta sillä tarkoitetaan tavallisesti yhteiskuntaa, jossa esimerkiksi teknologisilla innovaatioilla, tiedonjakelulla ja verkostoituneilla toimintatavoilla on suuri merkitys (Webster, 2014). Rannenberg ym. toteavat sähköisen identiteetin synnyn osasyiksi turvallisempien ja soveltavampien tapahtumien mahdollistamiseen verkkoympäristössä. Kun fyysisessä ympäristössä niin sanottu luonnollinen identiteetti on näkynyt yksilön esiintymisenä palvelutilanteessa, niin sähköisessä ympäristössä identiteetti voi esiintyä sähköpostina tai matkapuhelinnumerona. Nämä virtuaalisesti moniarvoiset identiteetit sekä niiden takana olevat paradigmat heijastuvat tavallisesti kuitenkin fyysisestä ympäristöstä, jossa toimivat prosessit niiden käsittelemiseksi ja esimerkiksi tunnistautumisen mahdollistamiseksi. Kirjoittajat toteavat, että uudet teknologiat ja artefaktit haastavat perinteistä identiteetin käsitettä (Rannenberg, ym., 2009).

Sähköisten palveluiden ja sosiaalisten verkkoyhteisöjen suosion kasvu on nostanut myös huolenaiheen sähköisen identiteetin turvaamisesta ja yksityisyydestä. Verkkoviestinnän käytettävyyden ja yksityisyyttä parantavien työkalujen välillä vallitsee Wesselin (2012) mukaan kuilu, jonka vuoksi sähköisen identiteetin käsitteen yhteydessä on tärkeää huomioida muun muassa tunnistetietojen riittävästä salauksesta järjestelmän ulkopuolisilta tahoilta.

2.1 Identiteetin määritelmä

Identiteetin määritelmä ei ole yksiselitteinen, vaan se on pitkälti riippuvainen tieteenalakohtaisesta tarkastelusta. Identiteetin käsitettä on perinteisesti selvitetty psykologiassa ja sosiaalitieteissä, mutta käsitteen suosio on kasvanut viime vuosina myös muilla tieteenaloilla (Rautio & Saastamoinen, 2006). Saastamoisen (2006, s. 172) mukaan identiteetti jaetaan sosiaalitieteellisessä tutkimuksessa Goffmanin (1963) määrittelemän jaottelun perusteella sekä persoonalliseen että sosiaaliseen identiteettiin. Goffman määrittelee persoonallisen identiteetin johdonmukaiseksi tunteeksi yksilön kokemuksessa eri elämänvaiheissa, kun taas sosiaalinen identiteetti koskee samaistumisen tunnetta sosiaalisiin yhteisöihin ja ryhmiin. Näin ollen identiteetin määritelmään kuuluvat siis tavat, joilla ihmiset määrittelevät itsensä suhteessa itseensä, sosiaaliseen ympäristöönsä ja kulttuurinsa. Myös englantilaisen sosiologin Jenkinsin (2014) muodostama ja laajalti tunnettu määritelmä identiteetistä tukee aiempaa Goffmanin määritelmää. Jenkinsin sosiaalista identiteettiä käsittelevän kirjan uusimmassa painoksessa määritellään identiteetti tietoisuudeksi omasta itsestä suhteessa toisiin ja ympäristöön rakentuen sekä samanlaisuuden että erilaisuuden käsitteistä. Näihin kahteen käsitteeseen – samanlaisuuden ja erilaisuuden, kuuluu tarve tunnistaa toisista yhdistäviä ja erottavia tekijöitä itse tehdyn luokittelun pohjalta (Jenkins, 2014).

Kun tarkastellaan identiteetin asemaa sähköisissä tietovälineissä, nähdään identiteetti tavallisesti tiettyyn verkkotunnukseen (engl. domain) kuuluvan kokonaisuuden entiteettinä eli esiintymänä. Yleensä identiteettiä käsitellään liitettynä yksittäiseen entiteettiin, mutta tällä yksittäisellä entiteetillä voi olla useita identiteettejä annetulla verkkotunnuksella. Yksi esimerkki tällaisesta entiteetistä tietokannassa olisi henkilö, joka toimii koulussa opettajana, mutta on samalla kyseisen koulussa opiskelevan oppilaan vanhempi. Lisäksi yksittäisellä entiteetillä voi olla eri identiteetit eri verkkotunnuksilla. Valikointi liittyen entiteetin kokonaisuuteen, kuten sallitaanko sille useampi identiteetti tietokannassa, perustuu sen rakenteen määrittelylle ja sallituille attribuutin arvoille. (Jøsang, Zomai & Suriadi, 2007).

Kansainvälisiä standardointeja kehittävä ja kokoava järjestö International Organization for Standardization määrittelee ISO/IEC 24760-standardissaan identiteetin *"valikoimaksi kokonaisuuteen kuuluvia attribuutteja."* Identiteetinhallintaan keskittyvässä standardissa mainitaan tämän määritelmän olevan osa niin kutsuttua osittaista (engl. partial) identiteettiä (ISO-IEC 24760, 2019). Näin ollen sähköisen identiteetin attribuutit ovat usein perua fyysisestä ympäristöstä. Tähän liittyen Cao ja Yang (2010) toteavat artikkelissaan, että pitkällä aikavälillä ihmiset saattavat käsitellä sähköistä identiteettiään samoilla tavoin kuin tosielämänsä identiteettiä. Sähköiseen identiteettiin pystytään liittämään useita määritteitä syntymäpäivästä kauppaostoksiin, vaikkakin käytössä olevat sovellukset ja palvelut tarvitsevat usein vain osaa käyttäjän ominaisuuksista. He täsmentävät, että osittaisella identiteetillä tarkoitetaan sähköiseen identiteettiin

liitettäviä ominaisuuksia ja tunnisteita, jotka ovat yhdistettävissä tiettyyn henkilöön tai yritykseen. Cao ja Yang tiivistävät sähköisen identiteetin olevan käyttäjään liitettävien kokonaisuuksien esitys, mukaan lukien todisteet ja tunnistetiedot, jotka ovat eteenpäin välitettävissä verkkopalvelua tai -sovellusta varten. Sähköinen identiteetti vastaa palveluntarjoajan tarpeeseen käyttäjien erottamiseksi toisistaan ja näin mahdollistaa eri käyttäjäoikeuksien jakamisen eri käyttäjille.

Bertino ja Takahashi (2010) vastaavasti määrittelevät sähköisen identiteetin käsitteen joko tiettyyn henkilöön tai yritykseen liitettävän informaation esitettynä sähköisessä muodossa. Tällaisen henkilöön tai organisaatioon liitettävän informaation tulee olla sellaista, että se tukee henkilön identiteetin todentamista perustuen luvan saamiselle jotakin tiettyä tarkoitusta varten. Bertino ja Takahashi havainnollistavat tätä määritelmää antamalla yhden esimerkin passin käyttämisestä henkilöllisyyden todistamiseen ja toisen esimerkin kuljettajan lisenssin käyttämistä ajolupaa varten. Heidän mukaansa sähköinen identiteetti sisältää yksilöllisiä tietoja, jotka voivat olla myös biometrisiä tietoja, kuten silmän iiris tai sormenjälki.

2.2 Identiteetinhallinnan viitekehys

Identiteetinhallinnalla tarkoitetaan Sanastokeskuksen (Kyberturvallisuuden sanasto, 2018) mukaan *"menettelyitä, joilla hallinnoidaan käyttäjien ja laitteiden tunnuksia, rooleja ja ryhmiä"*. Identiteetinhallintaan luetaan osaksi myös prosessit, joiden päämääränä on tietoverkossa liikkuvien entiteettien tunnistaminen sähköisiksi identiteeteiksi. Identiteetinhallintaa pidetään yleensä edellytyksenä tietojärjestelmän muille turvallisuusmekanismeille, kuten pääsynhallintaan liittyvälle valtuuttamiselle. Kun tarkastellaan yksinkertaista tapausesimerkkiä identiteetinhallinnassa, perinteisenä lähestymistapana on ollut käyttäjien mahdollisuus tunnistaa itsensä yksilöivillä tunnisteilla ja todentaa itsenä käyttämällä suojaustietoa palveluntarjoajan verkkoalustalla. Yksilöivänä tunnisteena on voinut esimerkiksi olla sähköposti ja suojaustietona puolestaan salasana. Tämän viitekehyksen etuna pidetään sitä, että siihen sisältyvät identiteetinhallinnan vaatimukset perustuvat tavallisesti tietoturva- ja tietosuoja-asetuksiin, jolloin ne ovat helposti ymmärrettävissä palveluntarjoajan ja käyttäjän välillä. (Jøsang, Fabre, Hay Dalziel & Pope, 2005).

Erilaisten tekniikoiden kirjo on laaja käsiteltäessä sähköisten identiteettien, kuten vahvistusten ja tunnuslukujen, hallintaa tietojärjestelmissä. Yleensä sovelluskehittäjät käyttävät omakohtaisia tekniikoitaan identiteettien hallintaan, joten sovellusohjelmat tallentavat ja hallinnoivat niitä monin tavoin. Tekniikoiden vaihtelu aiheuttaa yksittäisten sovellusohjelmien kohdalla niille vaikeuksia liittää erityyppiset sähköiset identiteetit osaksi pääsytietoja. Sovellusohjelmien tulisi tietää, kuinka saavuttaa tunnistamiseen tarvittava data sähköisestä identiteetistä ja osoittaa niiden oikeellisuus eri kohdissa käyttöjärjestelmää. Yksi näkökulma on toteuttaa identiteetinhallinta ohjelmointirajapinnan ja sähköisen

identiteetin hallintajärjestelmän kautta. (Cross, Hallin, Thomlinson & Jones, 2010).

Windley (2005) esittää kolme ensisijaista elementtiä organisaatioiden identiteetinhallinnan arkkitehtuurista, jotka ovat prosessiarkkitehtuuri, tietoarkkitehtuuri ja tekninen viitearkkitehtuuri. Prosessiarkkitehtuurissa määritellään menetelmä sille, kuinka organisaatio suoriutuu identiteettiin liittyvistä tehtävistä. Tietoarkkitehtuuri sen sijaan kattaa identiteetinhallintaan liittyvän tiedon tallentamisen, rakentamisen ja kehittämisen. Tekninen viitearkkitehtuuri sisältää periaatteet identiteetinhallinnan käyttöönotosta ja ylläpidosta. Identiteetinhallinnan viitekehyksessä on myös oleellista tunnistaa käsite yhteensopivuudesta, jolla Windley tarkoittaa hyväksi havaittujen menettelytapojen toteuttamista tietojärjestelmien välillä. Organisaatioiden kohdalla tämä tarkoittaa esimerkiksi listausta standardeista, joita identiteetinhallinnan arkkitehtuurissa noudatetaan. (Windley, 2005).

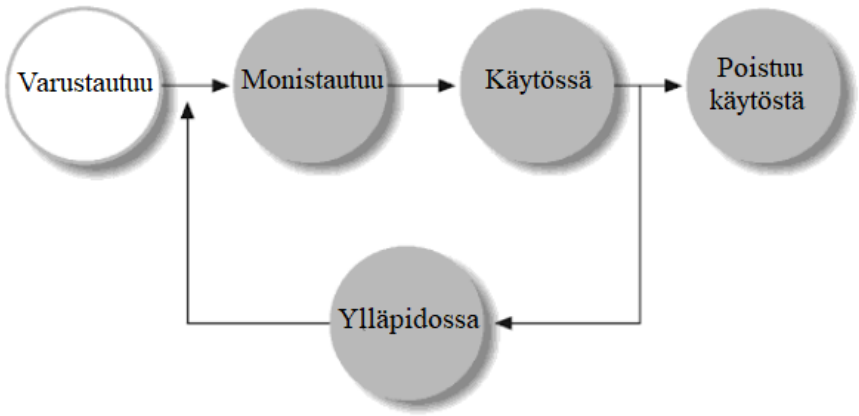
2.2.1 ISO/IEC 24760

International Organization for Standardization ja International Electrotechnical Commision määrittelevät kehittämässään viitekehyksessä identiteetinhallintaan liittyvää terminologiaa. Kyseessä on ISO/IEC 24760 -sarja, joka sisältää identiteetinhallinnan perusteet ja toimintakehotukset siten, että tietojärjestelmät pystyvät täyttämään niitä koskevat velvoitteet niin liiketoiminnallisella kuin oikeudellisella saralla. Tässä kappaleessa keskitytään erityisesti järjestön määrittelemään terminologiaan viitekehyksen sisällä. Näiden käsitteiden avaamisella järjestö on pyrkinyt edistämään yhteistä ymmärrystä koskien identiteetinhallinnan aihealueita. (ISO/IEC 24760, 2019).

Määriteltäessä edellä sähköisen identiteetin käsitettä mainittiin termit entiteetti koskien identiteetin esiintymää ja attribuutti koskien identiteetin saamia arvoja. ISO/IEC 24760 -standardin asiakirjassa tarkennetaan, että entiteetti on verkkotunnuksen tarkoitusta palveleva muuttuja, joka on tunnistettavissa erilliseksi toimintojensa ja ominaisuuksiensa kautta. Mahdollisia entiteettejä ovat esimerkiksi henkilö, yritys tai verkkosivu. Attribuutit luokitellaan puolestaan entiteettiin kuuluvaksi ominaisarvoksi tai ominaisuudeksi. Molemmat entiteetti ja attribuutti liittyvät olennaisesti verkkotunnuksen käsitteeseen, sillä ne toimivat sen ympäristössä tunnistautumisen mahdollistamiseksi osana identiteetin- ja pääsynhallintaa. Tällöin kyseessä on prosessi, jossa tunnistetaan verkkotunnuksella tietty entiteetti erilliseksi toisista entiteeteistä. Tunnistusprosessin tarkoituksena on mahdollistaa vuorovaikutus entiteetin ja palvelun välillä sallimalla pääsyoikeus verkkotunnuksen ympäristöön ja resursseihin. Identiteetinhallinta määritellään tiivistetysti standardia koskevan asiakirjan mukaan *"niihin prosesseihin ja käytäntöihin, joilla hallinnoidaan tietyllä verkkotunnuksella olevien identiteettien attribuuttien elinkaarta ja arvoa sekä tyyppiä ja valinnaisia metatietoja."* (ISO/IEC 24760, 2019).

2.3 Sähköisen identiteetin ominaisuudet

Windleyn (2005) mukaan sähköisillä identiteeteillä on oma elinkaarensa. Elinkaaren tarkastelu on avuksi, kun arvioidaan miten sähköisen identiteetin ominaisuudet ja toiminnot käyttäytyvät eri vaiheiden aikana. Elinkaarimallien käyttäminen on tuttua ohjelmistosuunnittelusta, josta niitä on sovellettu osaksi myös identiteetin- ja pääsynhallinnan viitekehyksiä (Gunter, Liebovitz & Malin, 2011). Windley esittää elinkaaren alkavan identiteetin varustautumisesta tulevaa käyttöä varten eli toisin sanoen kyseessä on sähköisen identiteetin luonti. Sähköisestä identiteetistä muodostuu oma kokonaisuutensa, jossa attribuutit saavat niille tarkoitetut arvot. Kuten edeltävässä luvussa mainittiin, nämä arvot voivat olla ominaisarvoja tai ominaisuuksia. Windley antaa attribuutin arvojen esimerkiksi käyttäjän sijainnin tai puhelinnumeron. Varustautumisen jälkeen identiteetti monistautuu eli levittäytyy sen käyttöä koskeviin järjestelmiin. Sähköisen identiteetin ollessa käytössä siihen kohdistuu aika ajoin ylläpidollisia toimia, kuten salasanaan muuttamista tai attribuutin arvojen lisäystä. Tietojen muutos päivittyy monistautumisen muodossa muihin järjestelmiin ja sen tulee tapahtua luotettavasti. Sähköinen identiteetti poistuu käytöstä, kun se on palvellut käyttötarkoituksensa ja muuttunut tarpeettomaksi. Sähköisen identiteetin deaktivoinnin tai sen poistamisen epäonnistuessa asettuu tietojärjestelmä turvallisuusuhkien ulottuviin, kun ulkopuolisille muodostuu mahdollisuus päästä käyttämään tietoja (Windley, 2005).



KUVIO 1 Sähköisen identiteetin elinkaari, Windley (2005)

Sähköisen identiteetin kohdalla erityisesti ne ominaisuudet, jotka johtavat identiteetin tunnistamiseen ovat keskeisiä tarkasteltavia. Campin (2004) mukaan tunnisteella erotetaan henkilöt, paikat ja asiat toisistaan tietyn nimiavaruuden (engl. namespace) yhteydessä. Nimiavaruus ryhmittelee muun muassa luokkia ja tunnisteita konfliktien välttämiseksi käsitteiden esiintyessä samannimisinä – mutta eri konteksteissa ohjelmointikielen sisällä (Linden, 2015). Kun henkilökohtaiset tunnisteet yhdistettään osaksi yksittäisiä ominaisuuksia on tapahtumassa kyseessä tunnistaminen. On siis huomioitava, että tunniste on yleensä

yksilöllinen vain sille tarkoitetussa yhteydessä (Jøsang, ym., 2005). Tunnistaminen siis vaati tunnisteen, joka voi olla esimerkiksi ajoneuvon valmistenumero. Lisäksi Jøsang ym. täydentävät, että mitä tahansa tunnusomaista tekijää voidaan kutsua tunnisteeksi, kun sitä käytetään tunnistamistarkoituksiin.

Tällä hetkellä on olemassa monia eri lähestymistapoja siihen, kuinka sähköinen identiteetti esitetään kokonaisarkkitehtuurissa. Seuraavaksi käsitellään niistä vallitsevat muodot perustuen Jøsangin, Fabren, Hayn, Dalzielin ja Popen (2005) artikkeliin identiteetinhallinnasta. Nämä muodot ovat eristetty identiteetti, yhdistetty identiteetti, keskitetty identiteetti ja henkilökohtainen todentaminen. Eristetyn identiteetin kohdalla palveluntarjoajat toimivat sekä valtuutusten että tunnisteiden tarjoajana asiakkailleen. He hallitsevat identiteettiin liitettävää verkkotunnuksen nimiavaruutta ja kohdentavat jokaiselle käyttäjälle erilliset käyttöoikeustiedot tunnisteineen. Yhdistetyn identiteetin kohdalla määritellään joukko sopimuksia, standardeja ja teknologioita, jotka tekevät palveluntarjoajille mahdolliseksi tunnustaa käyttäjien tunnisteet ja käyttöoikeustiedot. Tekniikka toteutetaan siten, että eri palveluntarjoajat pystyvät erottamaan toisistaan muiden palveluntarjoajien käyttäjätunnukset ja -oikeudet. Tarkoituksena on liittää käyttäjän eri tunnisteet samalle käyttäjätunnukselle palveluntarjoajien kesken ja antaa käyttäjän todentaa itsensä yhdellä tunnuksella yhdelle palveluntarjoajista. Tämän jälkeen käyttäjää voidaan pitää tunnistettuna ja todennettuna myös kaikkien muiden palveluntarjoajien toimesta. Keskitetty identiteetti kytkeytyy verkkotunnukselle, jota hallinnoi yksi tunniste- ja valtuutustietojen tarjoaja, jonka alla palvelut toimivat. Jokaiselle palveluntarjoajalle käytetään siis samaa tunnistetta ja valtuutustietoja, vaikka todentamistapahtuma toteutettaisiin eri muodoissa. Näitä eri muotoja voivat olla esimerkiksi kertakirjautuminen tai sallittujen verkkotunnusten käyttäminen. Henkilökohtaiseen todentamiseen perustuva menetelmä käsittää henkilökohtaisen välineen, kuten puhelimen, älykortin tai tunnuslukulaitteen, jonka tarkoituksena on suorittaa todennus. Henkilökohtaisen todentamisen välinettä (engl. personal authentication device, PAD) pystytään käyttämään useissa eri todennus- ja pääsynhallintamenetelmissä. Sen käyttöön liittyy olennaisesti, että käyttäjän on muistettava vain yksi valtuutustieto, kuten PIN -koodi. Tämän lähestymistavan etu on, että se voidaan yhdistää osaksi aiempia sähköisen identiteetin hallinnoinnin muotoja eli eristettyä, yhdistettyä tai keskitettyä identiteettiä. (Jøsang, Fabre, Hay, Dalziel & Pope, 2005).

3 PÄÄSYNHALLINTA

Konseptina pääsynhallinta on esiintynyt aina niiltä ajoilta asti, kun ihmisillä on ollut vastuullaan suojaamisen arvoista omaisuutta. Tarve pääsynhallinnalle synnytti vuonna 1879 James Rittyn patentoiman ensimmäiseksi suojatuksi tietojenkäsittelyjärjestelmäksi luettavan laitteen. Tätä laitetta kutsuttiin nimellä ”Ritty’s incorruptible cashier” ja myöhemmin se tuli tunnetuksi kassakoneena. Työntekijän pääsy laitteen kassalaatikkoon sallittiin vasta myyntisumman syöttämisen jälkeen myynnin rekisteröinnin varmistamiseksi. Nykyään puhuttaessa käyttäjälle sallitusta pääsystä tietojärjestelmän resursseihin on informaatioteknologian toimialalla vakiintunut käsite valtuuttaminen (engl. authorization) kuvaamaan niitä keinoja, joita pääsyoikeuksien myöntämiseen eri käyttäjille kuuluu. (Ferraiolo, Kuhn & Chandramouli, 2003).

Pääsynhallinta on Bishopin (2003) mukaan osa organisaatioiden tietoturvaa järjestelmien suojaamiseksi. Organisaatioitten mukaan vaatimukset pääsynhallinnalle voivat olla hyvin erilaiset. Esimerkiksi on tavallista, että yliopistot haluavat varmistaa henkilöstölle, opiskelijoille ja toisille tutkijoille pääsyn tietojärjestelmiinsä verkon kautta. Toisaalta taas arkaluontoisia tietoja käsittelevän yrityksen tietojärjestelmiin pääsy halutaan vain harvoissa tapauksissa sallia etäyhteydellä verkon kautta. Vaatimusten määrittely on yleinen tapa aloittaa menettely sopivan pääsynhallintamekanismin valitsemiseksi suojaamista varten. Eri pääsynhallintamekanismeja on useita ja niitä voidaan jaotella muun muassa teknisiin ja operatiivisiin. (Bishop, 2003). Pääsynhallintamalleihin ja -mekanismeihin palataan tarkemmin luvuissa 3.2 ja 3.3.

Ferraiolo ym. toteavat, että pääsynhallintaan liittyy muita muotoja sen lisäksi, millä tavoin käyttäjä tavoittaa yhteyden järjestelmän resursseihin. Näitä ovat muun muassa sen määrittely mille käyttäjälle kuuluvat mitkäkin oikeudet ja mille ajanjaksolle pääsyoikeudet sallitaan. Pääsy järjestelmän resursseihin voidaan sallia esimerkiksi vain työajalla. Abadin (2003) mukaan pääsynhallinnan monet eri muodot näkyvät sovelluksissa, virtuaalikoneissa, käyttöjärjestelmissä ja palomuureissa. Ohjelmistojen lisäksi myös tietokoneen laitteiston fyysinen suojaus on osa pääsynhallinnan eri muotoja, mutta fyysistä suojausta ei käsitellä tässä kirjallisuuskatsauksessa (Abad, 2003).

3.1 Pääsynhallinnan määritelmä

Sandhu ja Samarati (1994) määrittelevät artikkelissaan pääsynhallinnan periaatteita ja harjoitteita. Pääsynhallinta rajoittaa käyttäjien kohdalla heidän suorittamiaan toimintoja ja ohjelmistojen kohdalla sitä, mitä ohjelmia voidaan suorittaa käyttäjille heille myönnettyjen oikeuksien puolesta. Näillä tavoilla yritetään ehkäistä ja estää toimintaa, joka voisi johtaa tietoturvan murtumiseen tietojärjestelmissä. Pääsynhallintaa valvotaan Sandhun ja Samaratin mukaan valtuutustietokannan kautta, jossa määritellään se, onko operaatiota yrittävä käyttäjä valtuutettu suorittamaan haluamansa toiminnot. Artikkelissa painotetaan, että erottelu pääsynhallinnan ja todentamisen (engl. authentication) termien välillä on kirjoittajien näkökulmasta tarpeellista. Pääsynhallinnan toiminta edellyttää, että käyttäjän todennus on tapahtunut onnistuneesti ennen pääsyoikeuksien toteuttamista. Tällöin pääsynhallinnan tehokkuus on osittain riippuvainen kelvollisesta todentamisesta. Sanastokeskuksen (2018) mukaan todentaminen on menettelytapa, jonka tarkoituksena on varmistua kohteen todenmukaisuudesta tai alkuperästä. Kun taas valtuuttamisella eli auktorisoinnilla tarkoitetaan luvan antamista käyttää suojattua kohdetta todentamisen jälkeen. Pääsynhallinta puolestaan käsittää Sanastokeskuksen (Kyberturvallisuuden sanasto, 2018) mukaan *"menettelyt, joilla varmistetaan, että käyttäjät laitteet, sovellukset ja järjestelmät pääsevät käyttämään tietojärjestelmissä olevaa tietoa roolinsa mukaisesti."* Tämän mukaan voidaan siis olettaa, että todentaminen ja valtuuttaminen ovat osa pääsynhallinnan menettelyitä.

Benantarin (2006) mukaan tietojärjestelmien käyttäjämäärien kasvu on johtanut järjestelmäkehityksessä korkeampaan käyttäjien suojaamistarpeeseen ja samanaikaisesti suoritettavien toimintojen sekä prosessien erotteluun. Ennen pääsynhallintamalleihin pohjautuvia ratkaisuja varhaiset suojaustavat käsittivät lähinnä laitteiston ja käyttöjärjestelmien komponentit. Benantar esittää, että pääsynhallinnan tarkoituksena on taata auktorisoiduille entiteeteille pääsyoikeus tietojärjestelmän tietoihin ja resursseihin. Entiteetille myönnettyjä pääsyoikeustapoja voivat olla esimerkiksi luku- tai kirjoitusoikeus. Pääsyoikeudet voidaan esittää suoraan entiteetille tai vaihtoehtoisesti ne voidaan esittää välillisesti esimerkiksi järjestelmässä suoritettavien tehtävien kautta. Samaan aikaan on myös oleellista määrittää se, käytetäänkö oikeuksia vain suoritettavassa prosessissa vai sallitaanko ne esimerkiksi toissijaisessa tallennustilassa. (Benantar, 2006).

International Organization for Standardization määrittelee ISO/IEC 29146-standardissaan pääsynhallinnan prosesseiksi, joilla joko myönnetään tai evätään resurssille suoritettava operaatiopyyntö (ISO-IEC 29146, 2016). Myös de Capitani di Vimercati, Paraboschi ja Samarati (2003) mukailevat samansuuntaista määrittelyä, jossa pääsynhallinta mielletään kokonaisuudeksi prosesseja, jotka koskevat järjestelmän resursseihin kohdistettujen pyyntöjen käsittelyä. Nämä pyynnöt välitetään eteenpäin pääsynhallintajärjestelmälle, joka joko hyväksyy tai hylkää ne. Pääsynhallinnan keskeisin tehtävä on di Vimercatin ym.

mukaan valvoa järjestelmän sekä sen resurssien pääsyoikeuksia siten, että vain valtuutetut pääsyoikeudet voivat tapahtua. Pääsynhallintajärjestelmään sisältyy tavallisesti niin sanottu pääsynvalvontapalvelu (engl. access control service), joka määrittelee toteutettavat pääsynhallintakäytännöt sille tarkoitetulla ohjelmointikielellä. Pääsynhallintajärjestelmään syötettävien käytäntöjen määritteleminen on usein monimutkaista, kun esimerkiksi reaalimaailmasta tulevat turvallisuuspolitiikan säädökset tulee kääntää tietojärjestelmälle yksiselitteiseksi säännöiksi. Tietojärjestelmän pääsynhallinnan tulisi olla tarpeeksi joustava vastaamaan eri vaatimuksiin, mutta samalla riittävän yksinkertainen sekä käyttöehtojen että käyttöönoton kannalta. (de Capitani di Vimercati, ym., 2003).

3.2 Pääsynhallinnan viitekehys

Pääsynhallinta näyttäytyy prosessina, jossa jokainen tietojärjestelmän ylläpitämiin resursseihin välitetty pyyntö tulee joko hyväksyä tai evätä. Päätös siitä, miten pyyntöön reagoidaan, perustuu järjestelmässä käyttöön otettuihin turvallisuusmekanismeihin. Eri pääsynhallinnan käytänteitä on mahdollista soveltaa ja toteuttaa vastaamaan järjestelmän vaatimuksia (Samarati & de Capitani di Vimercati, 2000). Yhdessä järjestelmässä voi näin ollen olla toteutettuna useampia tunnettuja pääsynhallinnan toimintaperiaatteita. Esimerkiksi eri käyttäjille, ryhmille, tai rooleille voidaan soveltaa erilaisia toimintoja perustuen valittuun tietoturvalliseen linjaukseen. Myös pääsynhallinnan kohteena olevan objektin luokitus vaikuttaa toimintaperiaatteiden valintaan (Jajodia, Samarati, Sapino & Subrahmanian, 2001).

Jajodia ym. esittävät artikkelissaan viitekehyksen, jossa käsitellään useamman eri pääsynhallintakäytänteiden toimintojen tukemista joustavasti yhdessä järjestelmässä. Viitekehys perustuu ohjelmointikieleen, jonka avulla käyttäjät pystyvät määrittelemään tiettyjä tietoturvakäytäntöjä valvottavaksi tietyille pääsyoikeuksille. Käytetty ohjelmointikieli sisältää käsitykset valtuuttamisen johtamisesta, erottelukyvystä ja päätöksentekostrategioista. Lisäksi se mahdollistaa sekä myönteiset että kielteiset valtuuttamispäätökset. Artikkeli tarkastelee aiempia virallisia pääsynhallintaan liittyviä valtuutusmalleja, joidenka käyttöönoton kohdalla toimeenpanoon tulee osaksi myös mallia vastaava turvallisuusmekanismi. Tämän seurauksena teoriassa mahdolliset erilaiset pääsynhallintakäytänteet on käytännössä jouduttu toteuttamaan yksittäisessä järjestelmässä sitoutuen tiettyyn tietoturvalliseen toimintaperiaatteeseen. Tällaisen järjestelmän haittana on ettei yksittäinen toimintaperiaate pysty vastaamaan elinkaarensa aikana kohtaamiinsa suojausvaatimuksiin. Jajodia ym. toteavat artikkelissaan, että tämän myötä järjestelmän käyttäjien tulee mukautua toimimaan valitun linjauksen asettamissa rajoissa, ellei toimintaperiaatetta lähdetä täydentämän osana sovelluskoodia, joka on tavallisesti tietoturvan kannalta puutteellinen ratkaisu. Kirjoittajien esittämän viitekehyksen etuna on puolestaan toisistaan eroavien pääsynvalvontakäytänteiden mahdollisuus toimia samanaikaisesti samassa järjestelmässä. Viitekehys kattaa esimerkiksi perinteisten pääsynhal-

lintakäytäntöjen toimimisen nykyisissä tietojärjestelmissä ja niiden käyttöönoton tarvittaessa samalle palvelimelle. (Jajodia ym., 2001).

Kyky suojata ja hallita erityisesti arkaluontoisen tiedon saatavuutta pidättyen sovituissa pääsynhallintakäytänteissä on Ferraiolon, Atlurin ja Gavrilan (2011) mukaan yksi keskeisimmistä tietoturvaan liittyvistä vaatimuksista. He esittävät artikkelissaan viitekehyksen pääsynhallintamallien käyttöönottoon perustuen kolmeen havaittuun näkökulmaan. Ensimmäiseksi huomioidaan pääsynhallinnan osa suhteutettuna isäntäjärjestelmään, sillä tavallisesti vain suppea osa kokonaisesta pääsynhallintamekanismista sisällytetään isäntäjärjestelmään. Toiseksi sallitaan järjestelmän resurssien valvontaa varten tarkat määritelmät, jolloin minimoidaan mahdollisten tukemattomien käytäntöjen toteuttaminen sovelluskoodina. Kolmanneksi viitekehys sisältää näkökulman, jossa rajoitusten asettuminen ulottuu laittoman tiedonkulun estämiseen myös malleissa, joissa se ei perinteisesti ole ollut mahdollista (Ferraiolo ym., 2011). Artikkelissa esitetään sovellus viitekehyksen konfiguroinnista pariin tunnetuimpaan pääsynhallintamalliin, joidenka luokittelua käsitellään tulevissa kappaleissa.

Pääsynhallinnan alle on muotoutunut monia viitekehyksiä riippuen muun muassa käytetystä pääsynhallintamallista tai pääsynhallinnan kohteena olevan objektin luokittelusta. Esimerkiksi pilvilaskennalle (Yu, Wang, Ren & Lou, 2010) ja esineiden internetille (Seitz, Selander & Gehrmann, 2013) on tunnistettu niitä koskevia menettelytapoja. Samaratin ja de Capitani di Vimercatin mukaan tiedonhallintajärjestelmän tärkeimpiä vaatimuksia on suojata sen resursseja luvattomalta tiedonvälitykseltä ja luvattomalta muokkaamiselta. Nämä ovat kriittisiä tekijöitä sen ohella, että vain valtuutetuille pääsyoikeuksille varmistetaan resurssien tehokas käyttö. Viitekehykset lisäävät riippumattomuutta pääsynhallinnassa toteutettavien suojausvaatimusten ja käyttöönottoa koskevien mekanismien välille. (Samarati & de Capitani di Vimercati, 2000).

3.2.1 ISO/IEC 29146

International Organization for Standardization ja International Electrotechnical Commissin määrittelevät kehittämässään viitekehyksessä pääsynhallintaan liittyvää terminologiaa, jota voidaan soveltaa pääsynhallintamenetelmiin verkkoympäristöissä. Järjestelmäresurssit on mahdollista sijoittaa hajautettuihin verkkoihin, jolloin niihin pääsyä on hallittava sovittujen menettelytapojen mukaisesti. Identiteetinhallinta on tärkeä osa pääsynhallintaa, jonka vuoksi näistä viitekehyksistä tavataan välillä yhteisnimitystä identiteetin- ja pääsynhallinta (engl. identity and access management, IAM). Pääsynhallintaan liittyvät pääsyoikeudet välitetään tunnistamalla ja todentamalla subjektit, jotka pyrkivät pääsemään kohdejärjestelmän resursseihin. Tässä kappaleessa keskitytään erityisesti järjestelmän määrittelemään terminologiaan pääsynhallinnan viitekehyksen sisällä. (ISO/IEC 29146, 2016).

Pääsynhallinta määritetään kyseisessä standardissa prosesseiksi, joilla hallinnoidaan käyttöoikeuksia resursseihin joko hylkäämällä tai hyväksymällä

pyynnöt. Käyttöoikeustunniste toimii luotettavana objektina, joka järjestää identifioidulle käyttäjälle tai käyttäjäryhmälle pääsyn resursseihin. Käyttöoikeustunnus sisältää tavallisesti tiedot käyttöoikeuksista pääsyn esittäneelle subjektille sekä tunnistetiedot subjektista valtuutuspäätöksen tekijälle. Käyttöoikeustunnisteen taustalla toimii turvatunnistepalvelu, joka allekirjoittaa, julkaisee ja vaihtaa tunnisteita sovittujen käytänteiden perusteella. Nämä päätökset tapahtuvat eräänlaisessa päätöksentekopisteessä (engl. policy decision point), joka toteuttaa sovitun pääsynvalvontakäytännön arvioidessaan subjektien pyyntöjä käyttää resursseja ennen niiden vientiä toimeenpantavaksi. (ISO/IEC 29146, 2016).

3.3 Pääsynhallintamallien luokittelua

Eri pääsynhallintamalleilla on oma kokoelmansa käytänteistä, joilla organisaatio hallitsee, kenellä on pääsy mihinkin resursseihin. Pääsynhallintamallilla viitataan tiettyyn menetelmään, työkaluun tai toimenpiteeseen pääsynhallinnan toteuttamiseksi. Pääsynhallintamallin tulee noudattaa pääsynvalvontapolitiikan lisäksi organisaation toteuttamaa tietoturvapolitiikkaa (Benantar, 2006). Butler Lampsonin 1970 -luvun alussa esittämää pääsynvalvontamatriisia pidetään ensimmäisenä virallisena matemaattisena mallina pääsynvalvonnan kuvauksen määrittelylle. Pääsynvalvontamatriisi on yksinkertainen esitys, jossa matriisin merkinnät määrittelevät subjektin eli tavallisesti käyttäjän käyttöoikeudet suojattuihin objekteihin (Ferraiolo, ym., 2003).

	Objekti 1	**Objekti 2**	**Objekti 3**	**Objekti 4**
Käyttäjä 1	{luku, kirjoitus}	{luku, kirjoitus}		
Käyttäjä 2	{kirjoitus}	{kirjoitus}	{luku}	{luku}
Käyttäjä 3	{luku}		{luku}	{luku}

TAULUKKO 1 Pääsynvalvontamatriisi, mukailtu lähteestä Ferraiolo, Kuhn & Chandramouli (2003)

Pääsynvalvontamatriisin sarakkeet muodostavat pääsynhallintalistan (engl. access control list, ACL) ja rivit puolestaan käyttäjän käyttöoikeudet eli valmiudet ominaisuuksista, joita käyttäjän sallitaan harjoittavan objektissa. Pääsynvalvontamatriisin heikkoutena nähdään sen ylläpito kapasiteetin kasvaessa uusien käyttäjien ja vaihtelevien suojattavien kohteiden takia. Seurauksena ovat kehittyneet pääsynhallintamallit, jotka vähentävät pääsynvalvontamatriisissa esiintyvää kompleksisuutta. (Linden, 2015). Seuraavissa kappaleissa käydään läpi tunnetuimpia pääsynhallintamalleja.

3.3.1 Harkinnanvarainen pääsynhallinta

Harkinnanvaraiset käytännöt pääsynhallinnassa perustuvat pyynnön esittäjän identiteettiin ja niihin pääsyoikeuden vaatimuksiin, jotka määrittelevät mitä oikeuksia pyynnön esittäjältä joko hyväksytään tai evätään. Harkinnanvarainen pääsynhallinta (engl. discretionary access control, DAC) valvoo pääsyoikeuksia selkeiden sääntöjen perusteella, jotka määrittävät mitä toimenpiteitä kukin voi suorittaa sallituilla resursseilla. Mallia kutsutaan harkinnanvaraiseksi, koska käyttäjä voivat siirtää pääsyoikeutensa toisille käyttäjille, kun käyttöoikeuksien myöntämistä ja peruuttamista säätelee hallinnolliset menetelmät. Kyseessä on käyttäjän suorittama valtuuksien laajentaminen, joka voi toteutua kun sovitut ehdot toteutuvat valtuutusmäärityksissä suhteessa resursseihin eli objekteihin. Toisaalta ehdoilla pystytään myös rajoittamaan pääsyoikeutta objektien sisältökohtaisten ehtojen perusteella. Käytäntöä valtuutuksien laajentamisesta kutsutaan joko suljetuksi tai avoimeksi riippuen lähestymistavasta. Suljettu käytäntö sallii pääsyoikeuden kohteeseen, jos sille löytyy positiivinen valtuutus. Avoin käytäntö puolestaan sallii pääsyoikeuden kohteeseen jatkuvasti ellei se kohtaa negatiivista valtuutusta. Avointa käytäntöä tavataan järjestelmissä, joissa tarve suojaukselle ei ole kovin suuri vaan oletuksena pääsyoikeus myönnetään. Suljettu käytäntö on usein tunnetumpi, koska sillä parannetaan suojausta estämällä pääsy oletusarvoisesti. Sekä avoimen että suljetun käytännön sisältämiä positiivisia ja negatiivisia valtuutuksia pystytään myös käyttämään yhtäaikaisesti. Samarati ja de Capitani di Vimercati (2000) antavat esimerkin, jossa valtuutus halutaan myöntää suurelle käyttäjäryhmälle paitsi sen yhdelle tietylle käyttäjälle. Yhdistämällä positiiviset ja negatiiviset valtuutukset, pystytään määritellä samalla vaatimuksella positiivinen valtuutus käyttäjäryhmälle ja negatiivinen valtuutus yksittäiselle käyttäjälle. (Samarati & de Capitani di Vimercati, 2000).

Käyttäjien suorittamaan valtuuksien laajentamiseen DAC-mallissa sisältyy avoimen ja suljetun käytännön lisäksi valtuutuksien ajalliset rajoitukset. Valtuutuksille voidaan osoittaa tietty voimassaoloaika jaksollisella lausekkeella, joka määrittää ajankohdat sen käytölle. Esimerkki annetusta jaksollisesta lausekkeesta sisältää kellonaikojen ja työpäivien määrittelyn. Aiemmin mainitut harkinnanvaraisen pääsynhallintamallin hallinnolliset menetelmät määrittelevät sen, ketkä ovat oikeutettuja laajentamaan omia pääsyoikeuksiaan tai muuttamaan jo sallittuja pääsyjä. Näitä menetelmiä ovat muun muassa keskitetyt, hierarkkiset ja hajautetut käytännöt sekä yhteistyöhön ja omistajuuteen perustuvat käytännöt. (Samarati & de Capitani di Vimercati, 2000).

3.3.2 Pakollinen pääsynhallinta

Toisin kuin harkinnanvaraisessa mallissa, pakollinen pääsynhallintamalli (engl. mandatory access control, MAC) ei salli resurssin omistajien jakaa käyttöoikeuksia harkintansa mukaan vaan pääsykäytäntö perustuu luokiteltuihin tietoturvatasoihin. Tietoturvatasot määritellään käyttäjien ja objektien eli kohdere-

surssien luokituksiin tietojärjestelmässä. Turvaluokituksien hierarkia osoitetaan suhteilla, ja tekstissä esiintyy seuraava esimerkki:

> Top Secret (TS), Secret (S), Confidental (C) ja Unclassified (U), jossa TS > S > C > U (Samarati & de Capitani di Vimercati, 2000, s. 148)

Tietoturvatasoon perustuvia pääsyoikeuksia hallinnoi luotettu auktoriteetti, tavallisesti järjestelmänvalvoja tai ylläpitäjä. Näin ollen hallinnolliset menetelmät pakollisessa pääsynhallintamallissa ovat melko yksinkertaisia. Tunnetuin MAC -pääsynhallintamallin muoto on monitasoisen tietoturvan menetelmä. Menettelytapa perustuu järjestelmän subjektien ja objektien luokitteluun. Järjestelmänvalvoja tai ylläpitäjä määrittelee subjekteille, jonka perusteella käyttöjärjestelmä huolehtii, että tietyn tason omaava käyttäjä voi saada pääsyoikeuden vain saman tietoturvatason omaavaan objektiin eli resurssiin. Subjektit ovat siis aktiivisia kokonaisuuksia, jotka pyytävät pääsyä passiivisiin objekteihin, joiden tehtävänä on puolestaan tiedon tallentaminen. Vaikka tavallisesti valtuutetuilla subjekteilla tarkoitetaan järjestelmän käyttäjiä tai käyttäjäryhmiä, pakollinen pääsynhallinta erottaa käyttäjät ja subjektit toisistaan. Käyttäjät ovat mallin mukaan järjestelmään pääsyoikeuden saaneita ihmisiä, kun taas subjektit ovat käyttäjien puolesta toimivia prosesseja. Tämä erottelu huolehtii ettei evätty käyttäjä saisi mahdollista pääsyoikeutta välillisesti suoritettavien prosessien kautta. (Samarati & de Capitani di Vimercati, 2000).

Bell ja LaPadula määrittelivät alun perin armeijan käytössä olevat tietoturvatasot vastaamaan niiden asianmukaista käyttöä myös tietokoneiden pääsynhallintajärjestelmissä. Aiempi sotilas- ja julkishallinnosta tuttu tietoturvatason luokittelu noudatti menetelmää, jossa käyttäjä saivat pääsyn vain sellaisiin tietoihin, jotka oli luokiteltu heidän omalle turvatasolleen tai sen alapuolelle. Bell-LaPadula -mallissa määritetään kaksi sääntöä koskien pääsynhallintaa, jotka tunnetaan nimillä ei ylöspäin lukua (engl. no read-up) ja ei alanpäin kirjoittamista (engl. no write-down). Ensimmäisellä tarkoitetaan ettei käyttäjä voi lukea oman turvatasonsa korkeamman tason tietoja ja toisella ettei käyttäjä voi kirjoittaa tietoa, joka saisi alemman turvatason itse käyttäjä. Sääntöjen tarkoituksena on ylläpitää järjestelmän tietoturvaa. (Ferraiolo, ym., 2003)

3.3.3 Roolipohjainen pääsynhallinta

Työnkuvaan liitettäviin tehtäviin on jo pidemmän aikaa tunnistettu eri oikeuksia ja vastuita organisaatioympäristöissä. 1980 – ja 1990 -lukujen vaihteessa tutkijat tunnistivat työtehtävät rooleiksi, joidenka oikeuksia pystyisi hallinnoida sovellusohjelmissa ja tietokannan hallintajärjestelmissä. Organisaatioiden eri työnkuvat ja -virat nähtiin rooleina, joille muodostui oma rakenteensa eroten sovellusohjelman käyttäjän rakenteesta (Ferraiolo, ym., 2003). Tämä roolin rakenne muodosti pääsynhallintamallin perustan, joka tunnetaan roolipohjaisena pääsynhallintana (engl. role-based access control, RBAC). Roolit määrittelevät käyttäjät, joilla on pääsyoikeus resursseihin. Lisäksi ne määrittelevät pääsyoi-

keuden käyttöasteen ulottuvuuden, esimerkiksi voiko resurssien tietoja tallentaa tai muokata. Järjestelmänvalvojat luovat roolit, myöntävät käyttöoikeudet rooleille ja osoittavat käyttäjät oikeille rooleille organisaatiossa olevien työnkuvauksien perusteella. Rooli kuvaa käyttäjälle osoitettuja valtuuksia ja vastuita työtehtävien mukaisesti. (Sandhu, Coyne, Feinstein & Youman, 1996).

Ferraiolo ja Kuhn esittelivät ensimmäisen kerran roolipohjaisen pääsynhallintamallin artikkelissaan vuonna 1992. Tätä ennen oli todettu etteivät DAC- tai MAC -pääsynhallintamallit ominaisuuksiltaan vastanneet kaupallisten ja julkisten organisaatioiden tarpeita. RBAC -pääsynhallintamalli tarjosi edellytykset rajoittaa käyttäjän pääsyoikeuksia toiminnon tai roolin perusteella pystyen silti toteuttamaan DAC – ja MAC -mallien käytännöt ilman komplikaatioita. Mallin taustalla oleva motivaatio on pystyä määrittelemään järjestelmissä yrityskohtaiset tietoturvamenetelmät mukaillen organisaation rakennetta. Ferraiolon ja Kuhnin artikkelissa esitetään kolme perustavanlaatuista vaatimusta, joita varhaisen roolipohjaisen pääsynhallintamallin on olennaista noudattaa. Nämä ovat roolin osoittaminen, roolin valtuuttaminen ja transaktion valtuuttaminen. Roolin osoittamisella tarkoitetaan, että subjekti voi suorittaa transaktion vain jos sille on valittu tai annettu rooli. Siten kaikilla aktiivisilla käyttäjillä tulisi olla osoitettuna aktiivinen rooli. Roolin valtuuttamisella seurataan, että subjektin aktiivinen rooli on valtuutettu subjektille. Tämä varmistaa yhdessä roolin osoittamisen kanssa, että käyttäjät voivat omaksua vain heille valtuutettuja rooleja. Transaktion valtuuttamisella tarkoitetaan, että subjekti voi suorittaa transaktion vain, jos transaktio on valtuutettu subjektille osoitetulle aktiiviselle roolille. Yhdessä roolin osoittamisen ja roolin valtuuttamisen kanssa, tämä vaatimus varmistaa käyttäjien suorittavan vain sellaiset transaktiot, jotka ovat valtuutettuja. (Ferraiolo, ym., 2003).

4 SÄHKÖINEN IDENTITEETTI OSANA PÄÄSYNHALLINTAA

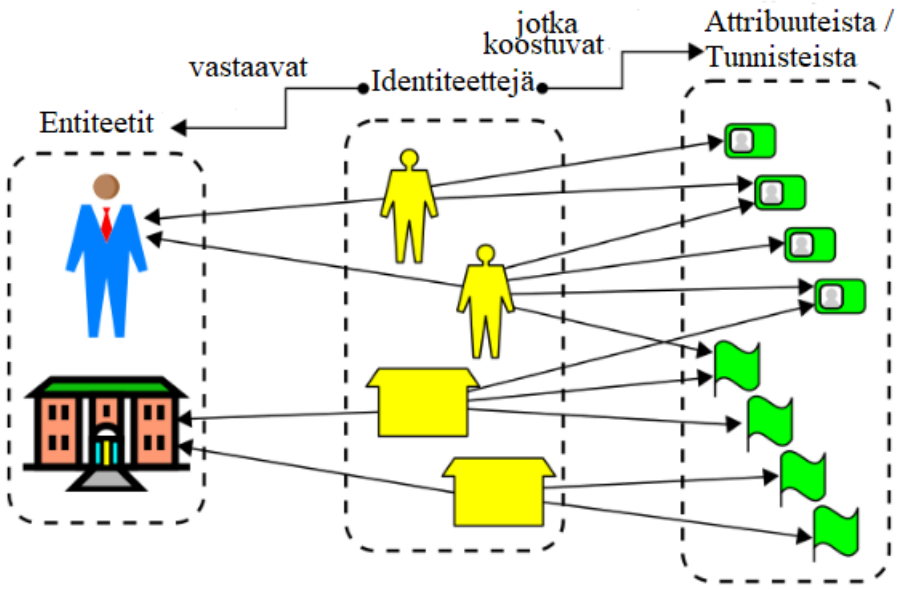
TAULUKKO 2 Sähköisen identiteetin tunnistaminen ja käyttöoikeuksien hallinta tunnetuimmissa pääsynhallintamalleissa, pääsynhallintamallien jaottelu toteutettu mukaillen Samaratin ja de Capitani di Vimercatin (2000) artikkelia.

Pääsynhallintamalli	**Identiteetin/ subjektin tunniste**	**Identiteetin ja käyttöoikeusien hallinta**	**Käyttö ja sovellutus**	**Lähteet**
Harkinnanvarainen pääsynhallinta, DAC	tiedot käyttäjän toiminnoista, identiteetin attribuutit	mm. keskitetyt, hajautetut, hierarkkiset ja omistajuuteen perustuvat menetelmät	nykyiset käyttöjärjestelmät ja tietokantojen hallintajärjestelmät mm. UNIX DAC ja DBMS DAC	Bertino & Takahashi, 2010; Jøsang ym., 2005; Li, 2011
Pakollinen pääsynhallinta, MAC	auktoriteetin myöntämä	mm. yhdistettyyn identiteettiin perustuvat menetelmät	monet tietoturvasovellukset ja monitasoiset turvallisuusjärjestelmät, mm. HP-UX Trusted System ja TrustedBSD	Bertino & Takahashi, 2010; De Capitani di Vimercati & Samarati, 2011; Jøsang ym., 2005;

Roolipohjainen pääsynhallinta, RBAC	identiteetille määrätty aktiivinen rooli	mm. DAC- ja MAC malleissa esiintyneet menetelmät sekä niiden yhdistelmät	laaja käyttö erityisesti yritysjärjestelmissä sisältäen mm. käyttöjärjestemät, tietokannan hallintajärjestelmät ja työnkulun hallintajärjestelmät	Alturi & Ferraiolo, 2011; Bertino & Takahashi, 2010; Jøsang ym., 2005;

4.1 Tunnistaminen ja todentaminen

Identiteetin tunnistaminen tapahtuu yksilöivillä tunnisteilla, kun puolestaan identiteetin todentaminen tapahtuu autentikoinnilla, jossa varmistetaan entiteetin ominaisuudet todenmukaisiksi (Jøsang, ym., 2005). Sähköisen identiteetin kohdalla näitä ominaisuuksia ovat muun muassa käyttäjän biometriset tiedot, tiedot käyttäjän toiminnoista ja käyttäjän hallinnoimat sähköiset tunnukset (Bertino & Takahashi, 2010). Taulukosta (ks. TAULUKKO 2) havaitaan, että DAC -pääsynhallintamallin kohdalla muun muassa tiedot käyttäjän toiminnoista ja omistajuuteen perustuvat menetelmät vaikuttavat identiteetin ja käyttöoikeuksien hallinnoimiseen. Näin ollen DAC -mallissa käyttäjä voi myöntää eteenpäin käyttöoikeutensa resurssi-omistaja -menetelmän pohjalta, kun sen tiedossa on toisen käyttäjän toiminnot valtuuttamispäätöksen tekemiseksi. Myös identiteettiin liitetyillä attribuuteilla voidaan suorittaa todennus, koska attribuutit ovat sekä identiteetin että entiteetin ominaisuuksia. Erityyppiset tunnisteet poikkeavat luonteeltaan. Ne voivat olla esimerkiksi tilapäisiä tai pysyviä; luontaisia tai sovellettuja; itsekeksittyjä tai ulkopuolisen myöntämiä (Jøsang, ym., 2005). Taulukosta nähdään, että esimerkiksi MAC-pääsynhallintamallin kohdalla identiteetin todentaminen perustuu pääsynhallintajärjestelmässä hallinnoivalta luotetulta auktoriteetilta myönnettyyn lupaan.



KUVIO 2 Entiteettien, identiteettien ja attribuuttien väliset suhteet (Jøsang, 2005).

Sähköinen identiteetti muodostuu, kun kootaan sähköiset tunnisteet tietojärjestelmälle soveltuvaksi kokonaisuudeksi prosessoida niihin liitettyä dataa. Jøsang ym. painottavat artikkelissaan, että tunnisteille varattu nimiavaruus tulee valita huolellisesti, jotta varmistetaan tunnisteen yksiselitteisyys identiteetille. Tarkastellessa taulukon RBAC-pääsynhallintamallin riviä nähdään, että identiteetin tunnisteena tietylle käyttöoikeudelle toimii sille määrätty rooli. Tunnisteiden joukko on kuitenkin tavallisesti suurempi kuin identiteetin joukko, joten usein yhteen identiteettiin liitetään useampia tunnisteita. Sähköisen todennuksen kohdalla on kyse vahvistuksesta, että käyttäjän hallussa oleva tunniste on ominaisuuksiltaan tosi ja tunnisteen omistajuus pätee sille osoitetulle identiteetille. (Jøsang, ym., 2005).

4.2 Käyttöoikeuksien hallinta

Käyttöoikeuksien kohdalla käytetään termiä valtuutus merkitsemään käyttäjän oikeutta suorittaa pyytämänsä toiminto. Pääsynhallintaan kuuluu ratkaisevasti tapahtumaketju, jossa pääsynvalvontapäätös kulminoituu käyttöoikeuksien hallintaan eli auktorisointiin (Linden, 2015). Käyttäjän tunnistaminen ja todentaminen on tapahtunut jo ennen käyttöoikeuksien valtuuttamista, kuten pääsynhallinnan määrittelyä koskevassa kappaleessa käytiin läpi. Käyttöoikeuksia suorittavan mekanismin on toimittava luotettavana monitorina, joka käsittelee jokaisen järjestelmälle osoitetun pyynnön. Tämän vaatimuksen myötä muodostui *reference monitor* nimellä tunnettu malli, jonka mekanismien tulee noudattaa seuraavia ominaisuuksia. Sen tulee olla tarpeeksi kestävä kohtaamaan mahdollisia tietomurtoja. Mekanismin tulee toimia välittäjänä kaikissa järjestelmään ja sen kohderesursseihin esitetyissä pyynnöissä. Sen käyttöjärjestelmäydin toteut-

taa tietoturvatoimenpiteet järjestelmän resurssien käytön hallitsemiseksi. Viimeisenä ominaisuutena mekanismin rakenteen tulee olla tarpeeksi rajoitettu, että se pysyy soveltuvana valitun pääsynhallinnallisen toimintaperiaatteen tarkasteluille ja testeille. (Samarati & de Capitani di Vimercati, 2000).

Seitz ym. käsittelevät menettelytapoja koskien esineiden internetin (engl. internet-of-things, IoT) käyttöoikeuksien hallintaa. Internettiin kytkettyjen elektronisten laitteiden kohdalla haasteeksi osoittautuu usein laitteiden rajallinen käsittelyteho ja muisti. Tilanteessa, jossa IoT -laitteet ovat yhdistettynä yhteiseen verkkoon, sen on pystyttävä käsittelemään yhteyksiä muilta laitteilta ja käyttäjiltä, vaikka niillä ei olisi samoja käyttöoikeuksia. Näiden laitteiden pääsynhallinnan kohdalla valtuutuspäätöksien tulee olla hienojakoisia. Seitz ym. esittelevät artikkelissaan käyttöoikeuksien valtuuttamiseen muun muassa seuraavia ehtoja. IoT-laitteen on valvottava pääsyoikeuksia paikallisesti, jotta päätös voi perustua laitteen paikallisiin parametreihin. Lisäksi menettelytapojen tulee perustua voimassaoleviin Internetin ja pääsynhallinnan standardeihin (Seitz, ym., 2013). Hienojakoiset valtuuttamispäätökset ovat osa myös pilvipalveluiden käyttäjäoikeuksien hallintaa (Yu, ym., 2010). Pilvipalveluiden käyttäjät ulkoistavat datansa palveluntarjoajan palvelimelle, jolloin data ei ole sijoitettuna sen käyttäjän omalla luotetulla toimialueella. Nykyisissä ratkaisuissa käytetään tavallisesti salausavaimia, joiden tiedot luovutetaan vain valtuutetuille käyttäjille. Nämä ratkaisut vaativat raskaan laskentatehon salausavainten jakelua, joka voi koitua ongelmaksi yhdessä tavoiteltujen hienojakoisten valtuuttamispäätösten kanssa. Yu ym. ehdottavat pääsynhallintajärjestelmää, joka tavoittaisi samanaikaisesti hienojakoisuuden, skaalautuvuuden ja luottamuksellisuuden. Ehdotettu järjestelmä sisältää muun muassa attribuutteihin perustuvan salauksen ja uudelleensalauksen tekniikoita koskien välityspalvelinta. Ehdotetun järjestelmän avulla suuri osa raskaasta laskentatehosta on mahdollista siirtää datan omistajalta suuritehoiselle pilvipalvelimelle (Yu, ym., 2010).

5 YHTEENVETO

Sähköinen identiteetti ja pääsynhallinta tarkoittavat yhdessä niiden toimintaperiaatteiden määrittämistä ja todentamista, joilla valtuutetaan käyttöoikeuksia kohdistuen tietojärjestelmiin ja tietoverkkoihin (Gunter, ym., 2011). Tässä tutkielmassa tarkasteltiin sähköisen identiteetin osaa tietojärjestelmien pääsynhallinnassa. Pääsynhallinnassa vertailevaksi malleiksi otettiin useiden eri menettelytapojen joukosta harkinnanvarainen, pakollinen ja roolipohjainen pääsynhallintamalli. Sähköisen identiteetin kohdalla tarkasteltiin erityisesti sen tunnistamiseen ja todentamiseen vaikuttavia tekijöitä. Pääsynhallinnan kohdalla tarkasteltiin menettelytapojen lisäksi mekanismeja pääsyoikeuden valtuuttamisen taustalla.

Tutkielma toteutettiin kirjallisuuskatsauksena ja sen tavoitteena oli vastata kysymyksiin *"Miten sähköistä identiteettiä hyödynnetään pääsynhallinnassa?"* ja *"Mitä pääsynhallintamalleja on olemassa ja tarjolla?"*. Tutkielmassa todettiin sähköisen identiteetin tunnistaminen kriittiseksi tekijäksi koskien järjestelmien tietoturvaa ja sen myötä myös pääsynhallintaa. Esimerkiksi luotettavien transaktioiden ja arkaluontoisten kohderesurssien pääsyoikeuksien kohdalla sähköisen identiteetin tunnistaminen on välttämätöntä. Sähköisen identiteetin käsitteeseen kuuluu oleellisesti sen näkeminen tietyistä ominaisuuksista tai ominaisarvoista koostuvaksi entiteetiksi. Sähköisen identiteetin tunnistautuminen tapahtuu näiden ominaisuuksien tai ominaisarvojen toimiessa yksilöivinä tunnisteina niille osoitetussa yhteydessä. Lähdeaineistossa annettiin esimerkkejä muun muassa luontaisista tunnisteista ja tunnisteista perustuen käyttäjän toimintoihin. Tutkielman edetessä pääsynhallinnan käsitteen tarkasteluun havaittiin sen tehokkuuden olevan riippuvainen sähköisen identiteetin onnistuneesta todentamisesta. Pääsynhallintamallien kartoittaminen osoitti, että tietojärjestelmän vaatimukset ja pääsynhallinnan kohteena olevan objektin luokitus toimivat tavallisesti perusteina käytänteiden valinnalle. Eri pääsynhallinnan käytänteiden sekä myös identiteetin hallintaan liittyvien menetelmien yhdistäminen on mahdollistanut laajan tarjonnan pääsynhallintamalleista.

Jatkotutkimusaiheeksi esitetään sähköisen identiteetin yksityisyyden suojaamista sen omistajan näkökulmasta sekä pääsynhallintaan liittyviä ratkaisuja

koskien yhä hajautetumpia ja monimutkaisempia järjestelmiä. Sähköisen identiteetin suojaamisen tarkastelu olisi mielenkiintoista Euroopan Unionin tietosuoja-asetuksen oltua noin vuoden verran voimassa. Sähköisen identiteetin määritelmän erotessa sosiaalisesta identiteetistä olisi kiinnostavaa tarkastella myös yksityisyyden käsitteen muotoutumista eri konteksteissa. Yksityisyyden tarkastelu voisi mahdollistaa parempaa luottamusta palveluntarjoajan ja käyttäjän välille koskien muun muassa tiedonkeruuta. Pääsynhallinnan kohdalla olisi mielenkiintoista tarkastella käyttöoikeuksien hallinnan kehitystä koskien esineiden internettiä. Älylaitteiden käyttöympäristö ja -järjestelmä asettaa uusia haasteita esimerkiksi perinteisimmille tunnistautumismenetelmille.

LÄHTEET

Abadi, M. (2003, June). Logic in access control. In *18th Annual IEEE Symposium of Logic in Computer Science, 2003. Proceedings.* (pp. 228-233). IEEE.

Alturi, V., & Ferraiolo, D. (2011). Role-Based Access Control. *Encyclopedia of Cryptography and Security*, 1053-1055.

Benantar, M. (2006). *Access Control Systems: Security, Identity Management and Trust Models*. Springer Science & Business Media.

Bertino, E., & Takahashi, K. (2010). *Identity management: Concepts, technologies and systems*. Artech House.

Bishop, M. (2003). What is computer security?. *IEEE Security & Privacy*, *1*(1), 67-69.

Camp, J. L. (2004). Digital identity. *IEEE Technology and society Magazine*, *23*(3), 34-41.

Cao, Y., & Yang, L. (2010, December). A survey of identity management technology. In *2010 IEEE International Conference on Information Theory and Information Security* (pp. 287-293). IEEE.

Cross, D. B., Hallin, P. J., Thomlinson, M. W., & Jones, T. C. (2010). *U.S. Patent No. 7,703,128*. Washington, DC: U.S. Patent and Trademark Office.

De Capitani di Vimercati, S., Paraboschi, S., & Samarati, P. (2003). Access control: principles and solutions. *Software: Practice and Experience*, *33*(5), 397-421.

De Capitani di Vimercati, S., & Samarati, P. (2011). Mandatory access control policy (mac). *Encyclopedia of Cryptography and Security*, 758-758.

Ferraiolo, D., Atluri, V., & Gavrila, S. (2011). The Policy Machine: A novel architecture and framework for access control policy specification and enforcement. *Journal of Systems Architecture*, *57*(4), 412-424.

Ferraiolo, D., Kuhn, D. R., & Chandramouli, R. (2003). *Role-based access control*. Artech House.

Gunter, C. A., Liebovitz, D., & Malin, B. (2011). Experience-based access management: A life-cycle framework for identity and access management systems. *IEEE Security & Privacy*, *9*(5), 48–55.

ISO – International Organization of Standardizatio: ISO/IEC 29146, Information Technology : Security Techniques : A framework for acccess management. Haettu 27.7.2019 osoitteesta https://www.iso.org/standard/45169.html

ISO – International Organization of Standardizatio: ISO/IEC 24760, IT Security and Privacy: A framework for identity management. Haettu 10.7.2019 osoitteesta https://www.iso.org/standard/77582.html

Jajodia, S., Samarati, P., Sapino, M. L., & Subrahmanian, V. S. (2001). Flexible support for multiple access control policies. *ACM Transactions on Database Systems (TODS)*, *26*(2), 214-260.

Jenkins, R. (2014). *Social identity*. Routledge.

Jøsang, A., Fabre, J., Hay, B., Dalziel, J., & Pope, S. (2005). Trust requirements in identity management. In *Proceedings of the 2005 Australasian workshop on Grid computing and e-research-Volume 44* (pp. 99-108). Australian Computer Society.

Jøsang, A., Zomai, M. A., & Suriadi, S. (2007). Usability and privacy in identity management architectures. In *Proceedings of the fifth Australasian symposium on ACSW frontiers-Volume 68* (pp. 143-152). Australian Computer Society.

Julkaisukanavahaku. (2019). Haettu 2.7.2019 osoitteesta https://www.tsv.fi/julkaisufoorumi/haku.php

Li, N. (2011). Discretionary access control. *Encyclopedia of Cryptography and Security*, 353-356.

Linden, M. (2015). *Identiteetin- ja pääsynhallinta*. Tampere University of Technology. Department of Pervasive Computing. Report; Vuosikerta 6.

Rannenberg, K., Royer, D., & Deuker, A. (2009). *The future of identity in the information society: Challenges and opportunities*. Springer Science & Business Media.

Rautio, P., & Saastamoinen M. (2006) Minuus ja identiteetti. Tampereen Yliopistopaino Oy – Juvenes Print.

Samarati, P., & de Capitani di Vimercati, S. C. (2000). Access control: Policies, models, and mechanisms. In *International School on Foundations of Security Analysis and Design* (pp. 137-196). Springer, Berlin, Heidelberg.

Sanastokeskus TSK. (2018). *Kyberturvallisuuden sanasto*. (TSK 52) Haettu 23.7.2019 osoitteesta http://www.tsk.fi/tepa/fi/

Sandhu, R. S., Coyne, E. J., Feinstein, H. L., & Youman, C. E. (1996). Role-based access control models. *Computer*, *29*(2), 38-47.

Sandhu, R. S., & Samarati, P. (1994). Access control: principle and practice. *IEEE communications magazine*, *32*(9), 40-48.

Seitz, L., Selander, G., & Gehrmann, C. (2013). Authorization framework for the internet-of-things. In *2013 IEEE 14th International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM)* (pp. 1-6). IEEE.

Webster, F. (2014). *Theories of the information society*. Routledge

Wessels, B. (2012). Identification and the practices of identity and privacy in everyday digital communication. *New media & society*, *14*(8), 1251-1268.

Windley, P. J. (2005). *Digital Identity: Unmasking Identity Management Architecture (IMA)*. O'Reilly Media, Inc.

Yu, S., Wang, C., Ren, K., & Lou, W. (2010). Achieving secure, scalable, and fine-grained data access control in cloud computing. In *2010 Proceedings IEEE INFOCOM* (pp. 1-9). IEEE.