Juho Taipale

TUNNISTAUTUMISMENETELMÄT TIETOJÄRJESTELMISSÄ

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2019

TIIVISTELMÄ

Taipale, Juho
Tunnistautumismenetelmät tietojärjestelmissä
Jyväskylä: Jyväskylän yliopisto, 2019, 37 s.
Tietojärjestelmätiede, kandidaatin tutkielma
Ohjaaja: Palonen, Teija

Tässä kandidaatin tutkielmassa tarkasteltiin erilaisia tunnistautumismenetelmiä tietojärjestelmissä. Tavoitteena oli selvittää, minkälaisia erilaisia tunnistautumismenetelmiä on olemassa ja mitkä tekijät vaikuttavat niiden valintaan. Tutkielmassa saatiin selville, että tunnistautumismenetelmät voidaan jakaa ominaispiirteidensä perusteella tietoon, hallussapitoon ja erityiseen ominaisuuteen perustuviin menetelmiin. Menetelmästä riippumatta tietoturva ja käytettävyys joutuvat usein vastakkainasettelun kohteiksi, ja siksi onkin tärkeää, että tietojärjestelmää suunniteltaessa ja sen tunnistautumismenetelmää valittaessa kiinnitetään huomiota sekä tietoturvaan että käytettävyyteen, mutta myös valitusta menetelmästä aiheutuviin kustannuksiin kohdejärjestelmän erityispiirteet huomioon ottaen. Voimakkaasti digitalisoituva toimintaympäristö avaa hyökkääjille jatkuvasti uusia portteja erilaisiin tietojärjestelmiin, jotka tänä päivänä vaikuttavat yhä enemmän myös yhteiskunnan toimintoihin. Tunnistautuminen on yksi tietoturvallisen tietojärjestelmän pääkomponenteista, joka oikein toteutettuna vahvistaa järjestelmän tietoturvaa. Viimeaikaisten laajojen tietovuotojen juurisyyt ovat liittyneet sekä järjestelmien teknisiin puutteisiin että yksittäisten käyttäjien huolimattomuuteen. Tämä kandidaatin tutkielma on toteutettu aikaisempaan tutkimukseen perustuvana kirjallisuuskatsauksena ja tunnistautumisen osalta aihe on rajattu käsittelemään ihmistä tunnistautuvana tietojärjestelmän faktorina.

Asiasanat: tunnistautuminen, tunnistautumismenetelmä, tietojärjestelmä, tietoturva

ABSTRACT

Taipale, Juho
Authentication Methods in Information Systems
Jyväskylä: University of Jyväskylä, 2019, 37 pp.
Information Systems, Bachelor's Thesis
Supervisor: Palonen, Teija

This bachelor's thesis examined different authentication methods in information systems. The aim was to find out what kind of different authentication methods exist and what factors influence their selection. The thesis discovered that authentication methods can be divided into methods based on knowledge, possession, or special characteristics. Regardless of the method, security and usability are often subject to confrontation. Therefore, it is important that attention is paid to both security and usability when designing the information system and selecting its authentication method. In addition, the costs of the selected authentication method and the specificities of the target system need to be taken into account. The heavily digitized operating environment constantly opens new gateways to attackers for various information systems, which today are increasingly affecting the activities on a societal level. Authentication is one of the key components of a secure information system that, when properly implemented, strengthens system security. The root causes of recent large-scale information leaks have been related to both the technical failures of the systems as well as the negligence by individual users. This bachelor's thesis has been carried out as a literature review based on previous research, and in terms of authentication, the topic is limited to dealing with a person as an authenticable information system factor.

Keywords: authentication, authentication method, information system, data security

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Yksilön henkilökohtainen identiteetti ja siihen liittyvä pääsynhallinta ovat tärkeässä roolissa kovaa vauhtia digitalisoituvassa maailmassa. Palvelut verkottuvat vauhdilla ja erilaisten tietojärjestelmien määrä kasvaa. Samalla käyttäjien luottamus digitaalisiin palveluihin on heikentynyt esimerkiksi viimeaikaisten säännöllisten ja massiivisten tietovuotojen seurauksena (Sitra, 2019). Näiden kaikkien seikkojen myötä myös tietoturvan merkitys korostuu väistämättä nykyaikaisten digitaalisten palveluiden suunnittelussa entistä enemmän.

Tietoturvan suunnitteluun kuuluu oleellisena osana myös käyttäjän autentikoiminen eli tunnistautuminen. Tunnistautuminen on yksi tietojärjestelmän tärkeimmistä komponenteista (Barkadehi, Nilashi, Ibrahim, Fardi & Samad, 2018), ja siihen perustuen käyttäjälle voidaan asettaa esimerkiksi henkilökohtaiset suoritusoikeudet, jolloin kullekin käyttäjälle voidaan tunnistautumisen ansiosta asettaa tietoturvallisesti vain ne oikeudet, jotka käyttäjä tarvitsee. Tunnusten joutuessa vääriin käsiin, voi ilkeämielisellä tunkeutujalla olla pääsy toisen käyttäjän henkilökohtaisiin tietoihin tai tietojärjestelmästä riippuen mahdollisuus aiheuttaa merkittävääkin tuhoa kyberfyysisessä rajapinnassa. Tätä riskiä pienentääkseen yhä useampi palvelu tarjoaa käyttäjilleen tietoturvallisempaa monivaiheista tunnistautumista (Barkadehi ym., 2018). Erityisiä paineita henkilökohtaisen tietoturvan toteuttamiselle organisaatioissa luovat erilaiset lait ja määräykset, kuten EU:n alueella vuoden 2018 keväästä lähtien sovellettu yleinen tietoturva-asetus GDPR, joka omalta osaltaan on asettanut organisaatioille uusia vaatimuksia tietoturvallisuuden suhteen. Verkko avaa jatkuvasti uusia portteja hakkereille, mutta suojautuminen niitä vastaan on usein liian heikkoa. Identiteetin ja luottamuksellisten tietojen suojaaminen on tärkeää, ja hyökkäysteknologioiden kehittyessä myös yleisen tietoturvallisuuden sekä käytettävien tunnistautumismenetelmien on kehityttävä.

Tämä kandidaatin tutkielma käsittelee tietojärjestelmien tunnistautumismenetelmiä, ja sen tavoitteena on vastata seuraaviin tutkimuskysymyksiin:

- Minkälaisia erilaisia tunnistautumismenetelmiä on olemassa?
- Mitkä tekijät vaikuttavat tietojärjestelmän tunnistautumismenetelmän valintaan?

Tutkimuskysymysten laajuuden vuoksi tutkielmaan on tehty tietoisia rajauksia. Kaikkia erilaisia tunnistautumismenetelmiä ei ole tarkoituksenmukaista esitellä erikseen, vaan ne on jaoteltu teknisten ominaisuuksien ja muiden samankaltaisuuksien perusteella. Samoin tunnistautumismenetelmän valintaan vaikuttavien tekijöiden tarkastelussa tutkimus on rajattu lähdeaineistosta esiin kumpuaviin kirjoittajan arvion mukaan olennaisimpiin tekijöihin.

Tutkielma on toteutettu kirjallisuuskatsauksena, ja sen lähdeaineisto koostuu pääosin informaatioteknologian alan tieteellisistä artikkeleista, konferenssiraporteista sekä alan muusta kirjallisuudesta. Aineistohaussa on hyödynnetty muun muassa Jyväskylän yliopiston kirjaston tarjoaman JYKDOK-tietokannan lisäksi Googlen Scholar -tietokantaa. Lähteen luotettavuutta ja paikkansapitävyyttä on aina arvioitu muun muassa sen julkaisijan tai siihen viittaavien artikkelien määrän mukaan. Julkaisijan luotettavuuden arvioinnissa on käytetty apuna Julkaisufoorumia, joka on ”suomalaisen tiedeyhteisön toteuttama, tutkimuksen laadunarviointia tukeva julkaisukanavien tasoluokitus” (Julkaisufoorumi, 2019). Lähteiksi on pyritty valitsemaan Julkaisufoorumin vähintään perustasoon luokittelemien lehtien artikkeleita.

Tutkielma koostuu johdannosta, kolmesta sisältöluvusta ja yhteenvedosta. Tutkielman luvussa 2 esitellään tietoturvaa yleisesti määritelmän kautta ja pohditaan tietoturvan merkitystä yksilön ja organisaation näkökulmasta. Luvussa 3 esitellään tunnistautumisen peruskäsite ja perehdytään erilaisiin tunnistautumismenetelmiin jakamalla ne ominaispiirteidensä mukaan kolmeen eri ryhmään. Jokaisesta ryhmästä annetaan kaksi esimerkkimenetelmää, jotka esitellään tarkemmin omissa alaluvuissaan. Luvussa 4 nostetaan esiin erilaisia tietojärjestelmän tunnistautumismenetelmän valintaan vaikuttavia tekijöitä luvussa 3 esiteltyjen menetelmätyyppien valossa. Luvussa 5 on tutkielman yhteenveto sekä kirjoittajan havaintoja lähdeaineistosta.

2 TIETOTURVA YKSILÖN JA ORGANISAATION NÄKÖKULMASTA

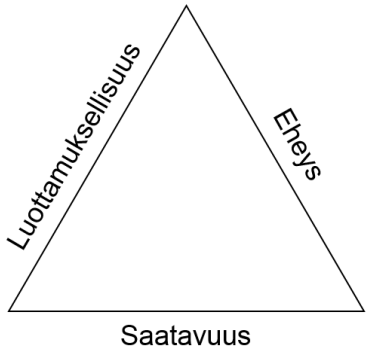
Tässä luvussa esitellään tietoturva yleisesti tieteellisissä julkaisuissa esiintyvien määritelmien valossa sekä käsitellään tietoturvan merkitystä organisaation ja yksilön näkökulmasta. Luvun jälkeen lukija ymmärtää, mistä rakenneosista tietoturva koostuu ja miten tietoturvallisuus näyttäytyy yksilölle sekä miten se tulee huomioida organisaatiossa.

2.1 Tietoturva yleisesti

Useat lähteet määrittelevät tietoturvan koostuvan kolmesta peruskäsitteestä, jotka ovat tiedon eheys (engl. integrity), tiedon saatavuus (engl. availability) ja tiedon luottamuksellisuus (engl. confidentiality) (Anderson, 2003; Metalidou ym., 2014; Sanastokeskus TSK, 2018). Tietoturvan käsitettä kuvataankin usein kolmiona, jonka sivut kuvastavat edeltävän määritelmän mukaisia tietoturvan rakenneosia (KUVIO 1). Sanastokeskuksen (2018) määritelmän mukaan saatavuudella tarkoitetaan tiedon hyödynnettävyyttä haluttuna aikana. Eheydellä tarkoitetaan tiedon yhteneväisyyttä alkuperäiseen tietoon verrattuna sekä sitä, että tietoa ei ole mahdollista muokata ilman siihen myönnettyä oikeutta ja asianmukaisia työkaluja. Luottamuksellisuudella puolestaan tarkoitetaan sitä, että tieto säilytetään luottamuksellisena ja sivullisten saavuttamattomissa. Tietoturvalla voidaan tarkoittaa myös sellaisia ”oloja, joissa tietoturvariskit ovat hallinnassa” (Sanastokeskus TSK, 2018). Sanastokeskus (2018) on täydentänyt määritelmäänsä seuraavasti:

> Tietoturvan järjestelyjä ovat esimerkiksi kulunvalvonta, tilojen lukitus, asiakirjojen turvallinen säilytys ja hävitys, tietojen salaus ja varmuuskopiointi sekä palomuurin, virustorjuntaohjelman ja varmenteiden käyttö. Tietoturvaan kuuluu muun muassa tietoaineistojen, laitteistojen, ohjelmistojen, tietoliikenteen ja toiminnan turvaaminen.

Tässä tutkielmassa laajalti käsitellyn käyttäjän tunnistamisen voidaan katsoa osaltaan varmistavan tietoturvan määritelmässä mainittua tietoaineistojen, laitteistojen ynnä muiden verkon osien turvaamista. Tunnistautumista käsitellään tarkemmin seuraavassa luvussa.



KUVIO 1 Tietoturvan kolme peruskomponenttia

Anderson (2003) on kritisoinut tietoturvan määritelmää merkitykseensä nähden liian abstraktiksi. Jotta tietoturvaa voisi riittävässä määrin toteuttaa, sen tulisi olla mitattavaa. Eheyden, saatavuuden ja luottamuksellisuuden käsitteiden katsotaan olevan kuitenkin liian vaikeaselkoisia mitattaviksi, saati keskusteltavaksi. Anderson (2003) onkin itse määritellyt tietoturvan seuraavasti:

> Hyvin tietoinen varmuus siitä, että informaatioriskit ja valvonta ovat tasapainossa.

Andersonin määritelmää tukee osaltaan Sanastokeskuksen (2018) määritelmä, jossa mainitaan tietoturvan tarkoittavan nimenomaisesti niitä järjestelyjä, joiden avulla tietoturvan kolme elementtiä voidaan toiminnassa varmistaa. Tämän kaltainen määritelmä esimerkiksi auttaa organisaatiota ymmärtämään paremmin tietoturvan merkityksen ja soveltamaan sitä osaksi strategiaansa. Tietoturvaa organisaation näkökulmasta käsitellään tarkemmin luvussa 2.3.

2.2 Tietoturva yksilön näkökulmasta

Palvelut digitalisoituvat nopeammin kuin koskaan, mutta samaan aikaan luottamus digitaalisia palveluita kohtaan heikentyy niihin viime aikoina kohdistuneiden tietoturvaloukkausten ja tietovuotojen seurauksena. Sitran (2019) teettämän kyselyn mukaan palveluntarjoajiin kohdistuva luottamuksen puute estää 43 % suomalaisista käyttämästä digitaalisia palveluita. Kyselyn mukaan luottamus palveluntarjoajia kohtaan oli heikoin 25—34-vuotiaiden, johtavassa asemassa olevien ja toimihenkilöiden keskuudessa.

Euroopan Unioni on viime aikoina aktivoitunut isojen kybermaailmaa muuttavien direktiivien osalta. Unionin uusi yleinen tietosuoja-asetus 2016/679 (engl. general data protection regulation, lyhenne GDPR) tuli täytäntöönpano-

kelpoiseksi huhtikuussa 2018 kahden vuoden siirtymisajan jälkeen. Asetus lisäsi EU:n kansalaisten määräysvaltaa erilaisiin tietojärjestelmiin tallennettavan henkilödatan osalta ja korvasi vuonna 1995 annetun tietosuojadirektiivin (95/46/EC). (Council of the European Union, 2015.)

Ihmistä on tietojärjestelmän käyttäjänä usein tituleerattu sen tietoturvan heikoimmaksi lenkiksi (O'Gorman, 2013). Tietojärjestelmän suunnittelussa sen käytettävyys ja tietoturva joutuvatkin usein vastakkainasettelun kohteeksi. Adams ja Sasse (1999) ovat todenneet, että yksittäisten käyttäjien kehno tietoturvakäytänteiden noudattaminen ja huono motivaatio tietoturvaa kohtaan voivat johtua muun muassa käytettävyyttä ja käyttäjän työskentelykäytänteitä huomioon ottamattomasta tietoturvamekanismien suunnittelusta. Esimerkiksi parhaillaan laajalti eri verkkopalveluissa yleistyvä monivaiheinen tunnistautuminen voi aiheuttaa käyttäjille turhautumista hidastaessaan tunnistautumistapahtumaa (ks. 3.1 Tunnistautuminen yleisesti) (Barkadehi ym., 2018). Käytettävyyttä ja tietoturvaa käsitellään tarkemmin tämän tutkielman neljännessä luvussa (ks. 4.1 Käytettävyys ja 4.2 Turvallisuus). Jotkin tietoturvallisiin järjestelmiin tai toimintoihin kohdistuvat hyökkäystekniikat voivat olla monimutkaisia ymmärtää. Yksi tietoturvan toteuttamisen ongelma onkin se, että usein käyttäjä ei ymmärrä tekniikkaa hyökkäyksen takana eikä siten osaa huomioida tietoturvaa riittäviltä osin omassa toiminnassaan (Adams & Sasse, 1999).

2.3 Tietoturva organisaatiossa

Tietoturvaloukkauksista johtuvat tietovuodot voivat aiheuttaa organisaatioille suuria kustannuksia ja mainehaittaa, minkä vuoksi niihin pyritään varautumaan ennalta ja ehkäisemällä niitä. Vuonna 2018 julkaistun raportin mukaan lähes puolet tietovuodoista oli tietoverkkorikollisuuden organisoimaa, ja vuodon havaitsemiseen kului keskimäärin jopa 197 päivää. Tietovuodosta aiheutuva kustannus kansainvälisellä mittapuulla oli vuonna 2018 keskimäärin 3,86 miljoonaa dollaria, mikä oli 6,4 % enemmän vuoteen 2017 verrattuna. Suurin kustannus on arvioitu yhdysvaltalaisille organisaatioille, joissa kustannus arvioitiin jopa 7,91 miljoonan dollarin arvoon, mikä oli 49 % enemmän kuin toisella sijalla olevilla Lähi-idän mailla. (IBM Security, 2018.)

Esimerkiksi edellä mainittu EU:n yleinen tietosuoja-asetus (ks. luku 2.2) pyrkii lisäämään läpinäkyvyyttä muun muassa EU:n kansalaisten henkilötietojen käsittelyyn organisaatioissa. Näiden määräysten implementointi on aiheuttanut yrityksille kustannuksia, kun olemassa olevia tietojärjestelmiä ja prosesseja on pitänyt tarvittaessa muuttaa siten, että ne täyttävät uuden tietosuoja-asetuksen määräykset. Adamsin ja Sassen (1999) mukaan organisaatioissa käytetään usein yhteiskäyttötunnuksia eri palveluihin, mikä estää esimerkiksi täydellisen kirjausketjun (engl. audit trail) syntymisen. Muun muassa kirjausketjun ja jäljitettävyyden merkitys kasvanee muun muassa uuden tietosuoja-asetuksen ansiosta. Syksyllä 2019 saatetaan täytäntöönpanokelpoiseksi myös EU:n uusi verkon rahaliikenteeseen kantaa ottava niin kutsuttu toinen maksupalveludi-

rektiivi PSD2 (engl. second payment services directive), joka osaltaan aiheuttaa jälleen muutoksia yritysten järjestelmiin. Maksupalveludirektiivin 4 artiklan 30 kohdan mukaan jatkossa verkkomaksutapahtumien varmistuksen yhteydessä edellytetään vahvaa asiakastunnistusta (engl. strong customer authentication, lyhenne SCA). Vahva asiakastunnistautuminen edellyttää vähintään kahden tunnistautumistyypin yhtäaikaista käyttöä. (Direktiivi (EU) 2015/2366.) Alkaen 14. syyskuuta 2019 pankit eivät enää hyväksy sellaisia maksutapahtumia, jotka edellyttävät vahvan asiakastunnistautumisen käyttöä, mutta eivät täytä sille asetettuja ehtoja. Erilaiset tunnistautumistyypit (tieto, hallussapito ja erityinen ominaisuus) on käsitelty tarkemmin luvussa 3.

Edellisessä kappaleessa tietoturvaa lähestyttiin yksilön näkökulmasta ja todettiin, että yleisen käsityksen mukaan ihminen, tässä tapauksessa esimerkiksi organisaation työntekijä, on turvallisen tietojärjestelmän heikoin lenkki. Vaikka kohdejärjestelmä olisi hyvin tietoturvallinen, voi käyttäjä oman huolimattomuutensa, välinpitämättömyytensä tai inhimillisen virheen vuoksi heikentää sen tietoturvaa (O'Gorman, 2013). Siksi monille organisaatioille muodostuukin paine saada työntekijänsä tietojärjestelmän faktoreina ymmärtämään tietoturvallisen toiminnan perusperiaatteet ja toimimaan niiden mukaisesti. Tästä huolimatta organisaatiot usein lähestyvät tietoturvaa teknologiakeskeisesti ja jättävät huomioimatta ihmisen, joka on yksi tietoturvan tärkeimmistä tekijöistä (Metalidou ym., 2014). Peruskäyttäjälle liian monimutkaiset tietoturvakäytänteet tai turhan korkealentoinen tietoturvapolitiikka eivät kuitenkaan motivoi työntekijää noudattamaan tietoturvallisia käytänteitä. Siksi tietoturvaan liittyvät ohjeistukset ja viestintä pitäisi suunnitella niin, että ne tukevat organisaation strategiaa eivätkä turhaan hankaloita työntekijöiden työskentelyä (Adams & Sasse, 1999).

3 TUNNISTAUTUMINEN JA SEN ERI MENETELMÄT

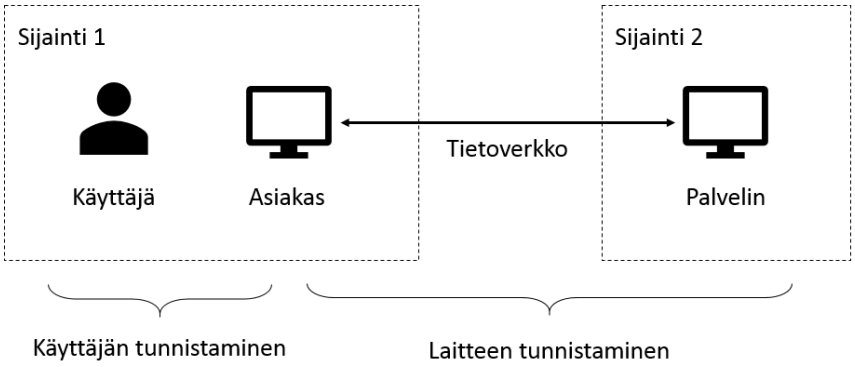
Tässä luvussa käsitellään tunnistautumisen käsite yleisesti. Lisäksi erilaiset tunnistautumismenetelmien kategoriat esitellään kukin kahden esimerkin avulla. Luvun jälkeen lukijalla on käsitys siitä, mitä tunnistautumisella tarkoitetaan ihmisen ja tietojärjestelmän vuorovaikutuksen kontekstissa. Lisäksi lukija tuntee, miten erilaiset tunnistautumismenetelmät jaotellaan ryhmiin ominaisuuksiensa perusteella ja tunnistaa eri ryhmissä esiintyvien menetelmien peruselementtejä.

3.1 Tunnistautuminen yleisesti

Tunnistautuminen (engl. authentication) on yksi tietojärjestelmän tärkeimmistä komponenteista (Barkadehi ym., 2018). Käsitteen tasolla se tarkoittaa menettelyä, jossa varmistetaan henkilön identiteetti tai esineen tai asian tunniste (Sanastokeskus TSK, 2018). Tietojärjestelmistä puhuttaessa se on hajautetussa tietojärjestelmässä tai muussa tietoverkossa tapahtuva prosessi, jonka avulla jokin tietojärjestelmäkokonaisuuteen vaikuttava tekijä todentaa toiselle oman identiteettinsä. Todennettavia tietojärjestelmän faktoreita voivat olla esimerkiksi ihminen, tietokone tai jokin verkon palvelu. (Altinkemer & Wang, 2011; O'Gorman, 2013.) Tunnistautumistapahtuma koostuu kahdesta osasta, tietojärjestelmän faktorin identifioinnista sekä oletetun identiteetin verifioinnista (Bailey, Okolica & Peterson, 2014). Tässä kirjallisuuskatsauksessa ei käsitellä tietoverkon laitteiden tai palveluiden keskinäistä tunnistautumista (engl. machine-to-machine authentication; machine authentication, lyhenne M2M), vaan keskiössä on ihminen tunnistautujana tietojärjestelmässä (engl. human-to-machine authentication, user authentication) sekä se, minkälaisia erilaisia tunnistautumismenetelmiä ihminen voi käyttää todistaessaan identiteettiään tietojärjestelmän laitteille tai palveluille. Ihmisen ja koneen tai palvelun tunnistautuminen on havainnollistettu tarkemmin alla (ks. KUVIO 2 Käyttäjän ja laitteen tunnistaminen). Tämä tutkielma ei myöskään käsittele kahden ihmisen tietojärjestelmävälitteistä tun-

nistautumista, vaan ihmisen tunnistautumista johonkin tietojärjestelmän palveluun. Tunnistautuvan tietojärjestelmäfaktorin ollessa ihminen, tunnistautumisprosessin tärkein tehtävä on vastata kysymykseen ”Onko tämä henkilö se, joka hän sanoo olevansa?” (O’Gorman, 2013).

Tunnistautuminen on usein edellytys kohdejärjestelmän resurssien käytölle (Braz & Robert, 2006), ja sitä pidetäänkin yhtenä tietoturvainfrastruktuurin keskeisimmistä pääkomponenteista (Burrows, Abadi & Needham, 1990; Velásquez, Caro & Rodríguez, 2018). Oikein toteutetun tunnistautumisen avulla kyetään pienentämään tehokkaasti esimerkiksi impersonaation eli toisena henkilönä tai organisaationa esiintymisen uhkaa, mitä pidetään yhtenä suurimmista tietojärjestelmien tietoturvauhkista. O’Gormanin (2003) mukaan ihmisen ja tietokoneen tai muun verkon palvelun välinen tunnistautuminen on paljon turvattomampaa verrattuna kahden verkon tietokoneen tai palvelun väliseen tunnistautumiseen. Ihmisellä tunnistautujana on rajoitteita ja heikkouksia muun muassa kapasiteetin ja suorituskyvyn suhteen; käyttäjän tunnistautumista voidaankin pitää tietoturvallisten järjestelmien akilleenkantapäänä (O’Gorman, 2003). Useimmiten tunnistautuminen perustuu johonkin salausavaimeen tai muuhun osapuolten jakamaan tietoon (Burrows ym., 1990; Velásquez ym., 2018.) Näistä erilaisista tunnistautumismenetelmistä kerrotaan laajemmin seuraavissa kappaleissa.



KUVIO 2 Käyttäjän ja laitteen tunnistaminen, mukailtu lähteestä O’Gorman (2013)

Ennen tietojärjestelmiä ihmisten välinen tunnistautuminen on perustunut visuaaliseen tunnistukseen tai henkilökohtaiseen viestintään perustuvaan arviointiin tai formaalimmin yhteisesti sovittuun tunnistautumismenetelmään. Tietojärjestelmien aikana tunnistautuminen on kuitenkin muuttunut monimutkaisemmaksi ja haastavammaksi, sillä samat ihmisten välisessä vuorovaikutuksessa käytettävät tunnistautumismenetelmät eivät sellaisenaan ole sovellettavissa ihmisen ja teknologian vuorovaikutuksessa tapahtuvaan tunnistautumiseen tai kahden ihmisen tietoverkkovälitteiseen tunnistautumiseen. Tällöin tunnistautuvaa osapuolta ei suoraan voi nähdä ja tarkastella, joten kyseessä voi olla joko oikea henkilö, tietokone tai hyökkääjä. Näin ollen tunnistautuminen tietojärjestelmässä vaatiikin joitakin sovelluskerroksen ratkaisuja ja käytettävän tunnis-

tautumismenetelmän mukaan myös mahdollisesti joitakin fyysisiä sensoreita tai muuta laitteistoa. (O'Gorman, 2003.)

Menkus (1988) on jakanut käytettävät tunnistautumismenetelmät kolmeen eri kategoriaan (engl. authentication factor). Hänen mukaansa tunnistautuminen voi perustua joko henkilön tietoon (engl. knowledge), hallussapitoon (engl. possession) tai erityiseen ominaisuuteen (engl. inherence). Joissakin lähteissä esimerkiksi tunnistautumislokaatioon ja -aikaan perustuvat tunnistautumismenetelmät luetaan omiin kategorioihinsa, mutta tässä tutkielmassa käsiteltävät menetelmät rajataan kolmeen ensiksi mainittuun kirjallisuudessa yleisimmin esiintyvään kategoriaan. Tässä kirjallisuuskatsauksessa käytettävät tunnistautumismenetelmäkategorioiden suomennokset perustuvat Euroopan Unionin uuden maksupalveludirektiivin (EU) 2015/2366 4 artiklan 30 kohdassa käytettyihin suomenkielisiin termeihin.

Usean tunnistautumismenetelmän yhdistämistä eli niin kutsuttua monivaiheista tunnistautumista (engl. multi-factor authentication, lyhenne MFA; myös kaksivaiheinen tunnistautuminen, lyhenne 2FA) pidetään kasvavana trendinä (Barkadehi ym., 2018). Monivaiheinen tunnistautuminen perustuu Boolen logiikkaan, ja lauseiden validiteettia vertaillaan AND-operaattoreilla, jolloin kaikkien tunnistautumiseen liittyvien vaiheiden tulee olla valideja tunnistautumisen loppuun saattamiseksi. Esimerkki monivaiheisesta tunnistautumisesta on pankkikortti, jonka käyttöön tarvitaan sekä varsinainen kortti (hallussapitoon perustuva menetelmä) että tunnusluku (tietoon perustuva menetelmä). (O'Gorman, 2013.)

3.2 Tietoon perustuvat menetelmät

Tietoon perustuvat tunnistautumismenetelmät ovat yleisimmin käytettyjä menetelmiä tietojärjestelmiin tunnistauduttaessa. Ne perustuvat kysymykseen ”mitä tiedät” tai ”mitä muistat”. Kategorian tunnetuin tunnistautumistyyppi on perinteinen merkkijonoon perustuva salasana, joka on säilyttänyt asemansa käytetyimpänä tunnistautumistyyppinä (Spender, 1987; Jain, Ross & Prabhakar, 2004; Biddle, Chiasson & van Oorschot, 2012; Bonneau, Herley, van Oorschot & Stajano, 2012; O'Gorman, 2013; Velásquez ym., 2018; Barkadehi ym., 2018), vaikka tutkijat ovat jo 40 vuoden ajan demonstroineet siihen liittyviä tietoturva- ja käytettävyysongelmia (Bonneau ym., 2012). Tietoon perustuvan menetelmän varjopuolena voidaan pitää sitä, että tunnistautumiseen tarvittava tieto, kuten salasana, voi paljastua ja siten joutua väärän henkilön käyttöön, mikä altistaa kohdejärjestelmän impersonaatiolle (Bailey ym., 2014).

3.2.1 Merkkijonosalasana

Kaikkein käytetyimpänä tunnistautumismenetelmänä pidetään merkkijonosalasanaa juontuen osittain siitä, että sen implementointi on kustannustehokasta

ja useimmat tietojärjestelmät tukevat sitä valmiiksi (Spender, 1987; Biddle ym., 2012). Merkkijonosalasana on tietoon perustuva tunnistautumismenetelmä, joka perustuu siihen, että tunnistautumiseen vaaditaan tietty ennakkoon määritetty salasana, joka on jaettu vain valtuutettujen tahojen tietoon.

Useissa tietoturvasuosituksissa todetaan, että saman salasanan ei tulisi olla kahdessa eri palvelussa. Mikäli toiseen palveluun kohdistuu tietomurto ja hyökkääjä saa salasanan haltuunsa, sitä voidaan pyrkiä hyödyntämään toiseen palveluun kirjauduttaessa. Salasanan suurimpana tietoturvaongelmana onkin pidetty tarvetta sen muistamiselle, sillä useat käyttäjät valitsevat lyhyitä salasanoja muistin kuormituksen vähentämiseksi (Spender, 1987; Adams & Sasse, 1999, Biddle ym., 2012), mikä muodostaa dilemman turvallisuuden ja käytettävyyden välille (De Angeli Coventry, Johnson & Renaud, 2005).

Tämän päivän pilvilaskenta mahdollistaa salasanojen tehokkaan murtamisen entistä tehokkaammin muun muassa niin kutsutun väsytyshyökkäyksen (myös raakahyökkäys tai brute-force -hyökkäys, engl. brute-force attack) avulla, minkä toteuttaminen on entistä helpompaa, mikäli kohdejärjestelmää ei ole teknisesti suojattu hyökkäystyyppiä vastaan (Antonopoulos, 2010). Myös perinteinen kotitietokone kykenee arvaamaan vain viikossa noin 80% yleisistä salasanoista, ja laitteiston ja ohjelmistojen kehittyessä määrä vain kasvaa (Barkadehi ym., 2018).

Toinen salasanoihin kohdistuva järjestelmällinen hyökkäystyyppi on niin kutsuttu näppäilyn tallentaja (engl. keylogger), joka on tietokoneen USB- tai PS2-porttiin kytkettävä fyysinen laite tai tietokoneeseen asennettava ohjelma, jonka tehtävänä on tallentaa näppäimistön painalluksia. Näppäimistön kuuntelijaa voidaan verrata esimerkiksi niin kutsuttuun välistävetohyökkäykseen (engl. man-in-the-middle attack, lyhenne MITM), joka on tietoturvahyökkäys, jossa kaikki verkkoliikenne välitetään jonkin tunkeutujan palvelimen kautta (Barkadehi ym., 2018). Näppäimistökuuntelijassa kaikki näppäimistön painallukset välitetään ulkopuolisen laitteen tai ohjelman kautta ilkeämieliselle tunkeutujalle automaattisesti tai manuaalisesti. Välistävetohyökkäystä vastaan voi pyrkiä suojautumaan käyttämällä aina salattua HTTPS-yhteyttä. Paras tapa suojautua näppäimistön kuuntelulta on pitää laite päivitettynä ja haittaohjelmasuojat ajan tasalla. Monet merkkijonosalasanaan kohdistuvat uhkat ovat torjuttavissa käyttämällä monivaiheista tunnistautumista, mutta näppäimistökuuntelijan tapauksessa on huomioitava se, että hyökkääjän haltuun päätyy pelkkien tunnistautumistietojen lisäksi kaikki muukin näppäimistöllä kirjoitettu teksti. (Sodiya, Folorunso, Komolafe & Ogunderu, 2011; Barkadehi ym., 2018.)

Ihmismuistin rajallisuus on ongelma, joka johtaa muun muassa liian yksinkertaisiin salasanoihin tai samojen salasanojen käyttämiseen eri palveluissa. Muistettavien salasanojen määrän on ennustettu kasvavan 207 salasanaan vuoteen 2020 mennessä, kun se vuonna 2007 oli ainoastaan 25 salasanaa (Florêncio, Herley & Van Oorschot, 2014; Bras, 2015). Usein monimutkaiset suuren entropia-arvon salasanat (ks. 4.2 Turvallisuus) ovat erityisen vaikeita muistettavia, jolloin käyttäjä päätyy kirjoittamaan sen muistiin ja aiheuttaa tietoturvariskin. Tämän ongelman avuksi on kehitetty muun muassa salasananhallintaohjelmia

(alan kaupallisia toimijoita ovat esimerkiksi 1Password, LastPass, Dashlane ja KeePass), jotka mahdollistavat usean salasanan tallentamisen yhden vahvan pääsalasanan taakse. Käytettäessä salasananhallintaohjelmaa käyttäjä ei välttämättä itse tiedä salasanaansa, vaan ohjelma on generoinut sen automaattisesti tunnusta luotaessa, jolloin saadaan aikaan usein käyttäjän itse valitsemaa salasanaa turvallisempi salasana. (Biddle ym., 2012.)

Salasananhallintaohjelmat herättävät myös tietoturvakysymyksiä ja niiden tietoturvasta onkin viime aikoina kiistelty. Viimeisimmät tutkimukset ovat osoittaneet, että ainakin kaikki edellä mainitut salasananhallintaohjelmat jättävät tietokoneen muistiin salasanan selkokielisen muistijäljen, kun salasana kopioidaan ohjelmasta leikepöydälle (Independent Security Evaluators, 2019). Useat salasananhallintaohjelmat tarjotaan myös pilvipalveluna, mikä voi huolettaa osaa käyttäjistä ja yritys joutuukin huomioimaan mahdollisen tietovuodon uhkan pohtiessaan salasananhallintaohjelman käyttöönottoa (Gyorffy, Tappenden & Miller, 2011): pääsalasanan joutuessa vääriin käsiin mahdollinen hyökkääjä saa pääsyn käyttäjän kaikkiin salasanoihin (Gyorffy ym., 2011; Biddle ym., 2012).

Kuten edellä todettiin, tietoon perustuvat menetelmät ja niistä erityisesti salasana on eniten käytetty tunnistautumismenetelmä. Tämä juontanee juurensa salasanan pitkästä historiasta: erilaisia tunnussanoja on kautta aikojen käytetty tunnistautumismenetelmänä niin sodankäynnissä kuin myös lasten leikeissä ja muussa siviilien rauhanomaisessa kanssakäymisessä. Toinen osatekijä liittyy salasanan asettamiin järjestelmävaatimuksiin. Salasana implementoidaan sovelluskerroksella, joten sen käyttöön ei tarvita näppäimistön lisäksi mitään fyysisen kerroksen laitteita tai sovelluksia. Salasanan implementointi on siis verrattain edullista sisältäen ainoastaan sovelluskerroksen suunnittelu- ja toteutustyön.

3.2.2 Graafinen salasana

Vanhan sanonnan mukaan ”kuva kertoo enemmän kuin tuhat sanaa”, ja tunnetun merkkijonoon perustuvan alfanumeerisen salasanan rinnalle onkin myöhemmin tuotu graafinen salasana (Barkadehi ym., 2018), jonka aktiivinen kehitys aloitettiin viime vuosituhannen lopussa (Biddle ym., 2012). Se on yleistynyt muun muassa mobiililaitteiden kentällä, missä näytön osoittaminen on yleisempää kirjoitettuun syötteeseen verrattuna. Graafinen salasana perustuu suurelta osin salasanan muistamisen korvaamiseen kuvien tunnistamisella. (De Angeli ym., 2005.) Alun perin kiinnostus graafisen salasanan tutkimiseen ja kehittämiseen on syntynyt siitä olettamuksesta, että kuvien muistaminen ei generoi niin paljon kognitiivista kuormitusta (Biddle ym., 2012), ja ne ovat tunnistautumismenetelmänä turvallisempia kuin merkkijonot (De Angeli ym., 2005). Olettamusta vahvistaa kognitiivisen psykologian ilmiö, niin sanottu *picture superiority effect* (ei suom.), jolla viitataan ihmisen lähes rajattomaan visuaaliseen muistiin ja siihen, että ihmisen kyky muistaa kuvia on sanoihin verrattaessa paljon parempi (De Angeli ym., 2005; Gyorffy ym., 2011).

Biddle ym. (2012) esittelevät graafisia tunnistautumismenetelmiä niiden tyyppien mukaan kolmessa eri alakategoriassa, jotka ovat tunnistaminen (engl. recognation), muistaminen (engl. recall) ja avustettu muistaminen (engl. cued recall). De Angeli ym. (2005) ovat jakaneet menetelmät niin ikään kolmeen kategoriaan, mutta kutsuvat niitä käytäntöä kuvaavammilla vähemmän abstrakteilla termeillä: tunnistamiseen (engl. cognometric), piirrokseen (engl. drawmetric) ja lokaatioon (engl. locimetric) perustuvat menetelmät (englanninkieliset termit vapaasti suomennettu). Tässä lokaatioon perustuvat menetelmät vastaavat Biddlen ym. (2012) esittelemää avustettua muistamista, ja piirrokseen perustuvat menetelmät vastaavat muistamista. Ensiksi mainittu tunnistamiseen perustuva menetelmä viittaa esimerkiksi toteutukseen, jossa käyttäjän tulee tunnistaa tunnusten luonnin yhteydessä hänelle näytetyt kuvat suuremmasta kuvajoukosta. Lokaatioon ja avustettuun muistamiseen perustuva menetelmä viittaa esimerkiksi toteutukseen, jossa käyttäjän tulee muistaa ja osoittaa tietyn kuvan määrättyjä kohtia. Toteutus perustuu samannimiseen paikkamenetelmään (engl. method of loci), joka on eräs tunnettu psykologinen muistitekniikka. Viimeiseksi mainitulla piirrokseen ja muistamiseen perustuvalla menetelmällä tarkoitetaan esimerkiksi sellaista toteutusta, jossa käyttäjän tulee tuottaa tietty piirros esimerkiksi ruudukkoon tai tyhjälle kanvaasille hiiren, kosketusnäytön tai muun ohjauslaitteen avulla. Piirrokseen perustuva graafisen tunnistautumisen toteutus onkin hyvin samankaltainen behavioristiseen analyysiin perustuvan tunnistautumismenetelmän kanssa. (De Angeli ym., 2005.) Viimeksi mainittua erityisiin ominaisuuksiin perustuvien tunnistautumismenetelmien kategoriaan lukeutuvaa menetelmää käsitellään tarkemmin luvussa 3.4.2 Behavioristinen biometria.

Graafisen salasanan on tarkoitus tarjota ratkaisu perinteisen merkkijonosalasanan muistamis- ja turvallisuusongelmiin hyödyntämällä jo valmiiksi olemassa olevaa perinteistä laitteistokokonaisuutta eli näyttöä, näppäimistöä ja hiirtä. Menetelmä on kuitenkin perinteistä merkkijonosalasanaakin alttiimpi esimerkiksi niin sanotulle shoulder surfing -hyökkäykselle (Barkadehi ym. 2018), jossa hyökkääjä pyrkii vakoilemaan tunnistautumistapahtumaa esimerkiksi kirjautujan näytöltä ”olan yli”. Tämä johtuu siitä, että kuvat näytetään näytöllä usein tunnistettavampina verrattuna perinteisiin merkkijonosalasanoihin, jotka yleensä esitetään piilotettuna korvaamalla merkit asteriskeillä tai muilla vastaavilla merkeillä. Kuvaan perustuvaa salasanaa pidetään merkkijonosalasanaa turvallisempana, mutta tämä turvallisuushyöty ei aina toteudu, sillä kuvakin voi olla entropiasta riippuen yhtä arvattava kuin merkkijono.

Graafisen salasanan käyttö ei myöskään suojaa täysin merkkijonosalasanojen yhteydessä esiintyviltä näppäimistöä kuuntelevilta haittaohjelmilta, sillä niitä voidaan vastaavasti ”kuunnella” hyödyntämällä esimerkiksi näyttökaappauksia eli näytön tapahtumien tallentamista. Myös lokaatioon perustuvassa graafisen salasanan menetelmässä turvallisuus heikkenee, jos järjestelmä antaa käyttäjän valita tunnistautumisessa klikattavat kuvan kohdat, sillä ihmisen katse kiinnittyy ensin tiettyihin kuvan loogisiin ja selkeisiin pisteisiin, joita käyttäjät todennäköisimmin valitsevat. Tähän on kehitetty muiden muassa ratkaisu,

jossa järjestelmä ohjelmallisesti korostaa kuvasta satunnaisia pisteitä ja tarjoaa sillä tavoin käyttäjälle ehdotuksen valittavasta kohdasta (Bonneau ym., 2012). Vastaava ongelma syntyy piirrokseen perustuvassa menetelmässä, kun käyttäjä voi vapaasti piirtäessään valita jonkin helposti arvattavan satunnaisuuteen perustumattoman piirroksen, kuten omat nimikirjaimensa. Tällöin tunnistautumisessa käytettävän salaisuuden entropia eli satunnaisuus laskee, mikä vaikuttaa heikentävästi myös tietoturvaan. (Gyorffy ym., 2011; De Angeli ym, 2015.) Entropian käsitettä esitellään enemmän seuraavassa luvussa (ks. 4.2 Turvallisuus).

3.3 Hallussapitoon perustuvat menetelmät

Hallussapitoon perustuvalla tunnistautumismenetelmällä (engl. possession-based authentication method) tarkoitetaan sitä, että tunnistautumiseen tarvitaan jokin fyysinen esine, kuten pankki- tai älykortti. Laite voi olla myös esimerkiksi aktiivinen laite, joka generoi käyttäjälle kertakäyttöisiä tunnistautumiskoodeja. Hallussapitoon perustuvat menetelmät perustuvat kysymykseen ”mitä omistat”. (O’Gorman, 2003.)

Hallussapitoperusteisen tunnistautumismenetelmän varjopuolena voidaan pitää sitä, että tunnistautumiseen käytettävä väline voi kadota tai tulla varastetuksi, jolloin se voi joutua vääriin käsiin (O’Gorman, 2003; Bailey ym., 2014). Muutoinkin tunnistautuminen tai koko järjestelmän käyttö estyy, jos tunnistautumisväline ei ole saatavilla.

3.3.1 Älykortti

Älykortti (engl. smart card) on usein organisaation sisällä käytettävä useimmiten sirullinen luottokortin kokoinen tunnistautumisväline. Se voi yhä useammin perustua myös tiedon etälukuun ja tallentamiseen käytettävään RFID- eli saattomuistiteknologiaan (engl. radio frequency identification), johon myös NFC-teknologia perustuu (engl. near field communication). Tällöin tunnistautumistapahtumassa käytettävä älykortti ei ole välttämättä perinteisen kortin mallinen, vaan esimerkiksi avaimenperässä kuljetettava tagi. Kuten aikaisemmin on todettu, hallussapitoon perustuvan tunnistautumismenetelmien riskinä on tunnistautumisvälineen hukkuminen tai varastetuksi tuleminen (O’Gorman, 2003; Bailey ym., 2014). Älykorttien osalta riskiä vääränä henkilönä tunnistautumiseen on pyritty usein estämään yhdistämällä hallussapitoon ja tietoon perustuvia tunnistautumismenetelmiä niin kutsuttuun monivaiheiseen tunnistautumiseen. Tällöin älykortin avulla kirjautumiseen tarvitaan kortin esittämisen ohella myös esimerkiksi PIN-koodi tai muu salasana. Älykortti tarvitsee toimiakseen jonkin fyysisen laitteen, jolla kortin tiedot voidaan lukea tietojärjestelmään. Tällainen laite voi olla sisällytettynä käyttölaitteeseen, kuten kannettavaan tietokoneeseen, tai se voidaan liittää laitteeseen esimerkiksi USB-liitännällä. (Spender, 1987.)

Suomessa varmennekorteille tallennettavista yleisistä varmenteista vastaava Väestörekisterikeskus on henkilörekisteriä ylläpitävä viranomainen, joka myöntää muun muassa sähköisissä palveluissa tunnistautumisvälineenä käytettäviä sirullisia henkilökortteja, organisaatiokortteja sekä erilaisia sosiaali- ja terveydenhuollon varmennekortteja. Sen toiminta perustuu muun muassa väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista annettuun lakiin (661/2009). Väestörekisteri tuottaa kansalaisvarmenteita (henkilökortti), organisaatiovarmenteita (organisaatiokortti), ammattivarmenteita (sosiaali- ja terveydenhuollon ammattikortti), palvelujen antajien henkilötoimijavarmenteita (sosiaali- ja terveydenhuollon toimijakortti), sosiaali- ja terveydenhuollon muun henkilöstön varmenteita (sosiaali- ja terveydenhuollon toimijahenkilöstökortti) sekä tilapäisvarmenteita organisaatioiden varakorteille. Myönnettävät varmennekortit sisältävät todentamis- ja salausvarmenteen ja allekirjoitusvarmenteen, jotka kumpikin perustuvat julkisen avaimen infrastruktuuriin (engl. public key infrastructure, lyhenne PKI) ja joita varten generoidaan kaksi 2048-bittistä RSA-avainparia. Kaikki väestörekisterikeskuksen myöntämät varmennekortit sisältävät PIN-tunnusluvut, ja sähköisten palveluiden käyttö edellyttää joko perus- tai allekirjoitustunnusluvun käyttöä, joten korteissa hyödynnetään monivaiheista tunnistautumista. (Väestörekisterikeskus, 2017.)

3.3.2 Älylaite

Erilaisia älylaitteita (engl. hardware token) käytetään erityisesti monivaiheisen tunnistautumisen välineenä enenevissä määrin eri palveluissa. Älylaite voi olla esimerkiksi käyttäjän henkilökohtainen puhelin, USB-porttiin kytkettävä avain tai niin kutsuttu avainlukulaite. Tässä tutkielmassa älylaitteella tarkoitetaan myös muita laitteita tai laitteissa olevia ohjelmistoja, jotka tuottavat kertakäyttöisiä tunnistautumisessa käytettäviä koodeja. Kaupallisia esimerkkejä tällaisista palveluista ovat muiden muassa RSA SecurID, Google Authenticator ja LastPass Authenticator. (Gleischhacker, Manulis & Azodi, 2014.) Gyorffy ym. (2011) ovat esitelleet teknologian, jonka avulla älylaitetta voidaan soveltaa myös esimerkiksi graafisten salasanojen syöttämiseen.

Brownin (2004) mukaan älylaitteeseen perustuvan tunnistautumismenetelmän implementointi ja käyttöönotto on vaivatonta, sillä laitteet eivät vaadi erillistä lukijalaitetta ja ovat useimmiten helppokäyttöisiä erityisesti käyttäjille tuttua mobiililaitetta hyödynnettäessä. Fyysisten älylaitteiden turvallisuus on kuitenkin joutunut kritisoinnin kohteeksi muun muassa siksi, että useimmat niiden valmistajat eivät ole julkaisseet algoritmejaan yleiseen vertaisarviointiin (Brown, 2004).

3.4 Erityiseen ominaisuuteen perustuvat menetelmät

Erityiseen ominaisuuteen perustuvalla tunnistautumismenetelmällä (engl. inherence-based authentication method) tarkoitetaan sitä, että yksittäinen käyttäjä voidaan tunnistaa jonkin tietyn fyysiseen tai kemialliseen ominaisuuteen tai käyttäytymiseen perustuvan mitattavan erityisen ominaispiirteen perusteella. Sen sijaan, että tunnistautuminen vastaisi kysymyksiin ”mitä omistat”, ”mitä tiedät” tai ”mitä muistat”, henkilön erityiseen ominaisuuteen perustuvan tunnistautumismenetelmän avulla voidaan vastata kysymykseen ”kuka olet”. Tietoon ja hallussapitoon perustuvien tunnistautumismenetelmien rinnalla erityiseen ominaisuuteen perustuva menetelmä vastaa paremmin kysymykseen tunnistautuvan henkilöön identiteetistä yhdistäen molemmat tunnistautumisen rakenneosat eli käyttäjän identifioinnin ja identiteetin verifioinnin (Bailey ym., 2014), sillä tunnistautumiskysymys kohdistuu henkilöön itseensä eikä jaettavaan tietoon tai irralliseen fyysiseen esineeseen. Vaikka henkilön erityisiin ominaisuuksiin perustuva tunnistautumisväline on turvallinen, on välineen kopiointi tai jäljittely mahdollista, joskin hyvin paljon haastavampaa muihin tunnistautumismenetelmiin verrattuna. (O’Gorman, 2013; Jain & Ross, 2007, s. 1—2.)

Biometria jaetaan yleensä fysiologiseen ja behavioristiseen biometriaan (Bergadano, Gunetti & Picardi, 2002). Seuraavissa alaluvuissa esitellään esimerkein näihin kahteen biometrian tyyppiin perustuvia ominaisuusperusteisia tunnistautumismenetelmiä. Fysiologiseen ja behavioristiseen biometriaan perustuvat menetelmät on tässä tutkielmassa käsitelty omina alalukuinaan, sillä vaikka molemmat lukeutuvat biometrian käsitteeseen, ne ovat tietojärjestelmän osana lähdekirjallisuuteen perustaen hyvin erilaisia käytettävyydeltään ja teknisiltä vaatimuksiltaan.

3.4.1 Fysiologinen biometria

Biometriikka on tieteenala, joka mittaa yksilön fyysisiä ja kemiallisia ominaisuuksia ja käyttäytymistä. Biometrisen tunnistautumisen juuret ulottuvat kauas historiaan, sillä ihmiset ovat pitkään tunnistaneet toisiaan muun muassa kasvojen ja äänen perusteella. 1900-luvun puolivälissä Pariisin poliisivoimissa keksittiin hyödyntää erilaisia ihmisen mitattavia ominaisuuksia rikollisten tunnistamisessa. Tätä keksintöä tutkittiin ja kehitettiin edelleen myöhemmin samalla vuosisadalla erityisesti sormenjäljen tunnistamisen osalta, ja nykyisin esimerkiksi sormenjäljellä tunnistautuminen on tullut suosituksi esimerkiksi mobiililaitteiden kuluttajamarkkinoilla. (Jain ym., 2004.)

Jain ja Ross (2007, s. 4) ovat kirjassaan *Introduction to Biometrics* esitelleet erilaisia fyysiseen biometriaan perustuvia tunnistautumistapoja, kuten sormenjälki, kasvot, iiris, korvalehti ja kämmenen geometria. Lisäksi on lueteltu yksilön behavioristisiten ominaispiirteiden analyysiin perustuvia tapoja, kuten allekirjoitus, kirjoitusdynamiikka näppäimistöllä ja askellus. Nämä käyttäytymiseen perustuvat tunnistautumismenetelmät on käsitelty seuraavassa alaluvussa

(ks. luku 3.4.2 Behavioristinen biometria), sillä ne eroavat huomattavasti yleisemmin käytetyistä biometriaan perustuvista tunnistautumismenetelmistä, kuten sormenjäljen tai kasvon tunnistuksesta, niin käyttökohteidensa kuin teknisen toteutuksensa puolesta.

Biometriaa hyödyntävän tunnistautumismenetelmän etuna on tunnistautumisvälineen vaikea kopioitavuus sekä se, että tunnistautumistietoja ei juurikaan voi luovuttaa toisen henkilön käyttöön, joten menetelmän avulla voidaan esimerkiksi tehokkaasti estää usean henkilön kirjautuminen samoilla käyttäjätiedoilla (Wayman, 2001; O'Gorman, 2013). O'Gormanin (2013) mukaan staattisia biometrisiä signaaleja voidaan kuitenkin helposti kaapata ilman riittävää laitteiston ja verkon tietoturvaa, joten biometristä tunnistautumista ei tulisi käyttää ilman monivaiheista tunnistautumista. Kaapattua biometristä signaalia voidaan hyödyntää esimerkiksi toistohyökkäyksen välineenä (engl. replay attack).

Tunnistautumisen perustuessa henkilön ominaisuuksiin tunnistautumisen väline on myös aina saatavilla. Varjopuolena voidaan kuitenkin nähdä se, että tunnistautuminen ominaisuusperusteista menetelmää käyttäen estyy, jos jokin henkilön tunnistamisessa käytetty ominaisuus muuttuu esimerkiksi ikääntymisen seurauksena. Ihmisen ikääntymisellä on suoria vaikutuksia muun muassa ihon elastisuuteen, keuhkojen hapenottokykyyn ja lihasvoimaan, mikä vaikuttaa esimerkiksi kasvojen, sormenjäljen, kämmenen geometrian ja äänen ominaisuuksiin. Luonnollisen ikääntymisen aiheuttamien suorien vaikutusten lisäksi ihmisen biometriikkaan vaikuttavat myös erilaiset vammat ja sairaudet, kuten esimerkiksi diabetes (ylipaino; kasvojen tunnistus), glaukooma (silmä; iiriksen tunnistus), kurkkusyöpä (äänihuulet; äänen tunnistus) tai Parkinsonin tauti (liikkuvuus; behavioristinen analyysi). (Lanitis, 2010.)

Biometristen tunnistautumismenetelmien luotettavuutta voidaan arvioida väärinhyväksymisasteella (engl. false acceptance rate, lyhenne FAR) ja väärinhylkäysasteella (engl. false rejection rate, lyhenne FRR). Väärinhyväksymisasteella mitataan sitä todennäköisyyttä, jolla biometrinen tunnistautumismenetelmä hyväksyy väärän henkilön kirjautumisyrityksen. Sen sijaan väärinhylkäysastetta käytetään mittaamaan todennäköisyyttä oikean henkilön kirjautumisyrityksen hylkäykselle. Mitä pienemmät mittareiden arvot ovat, sitä luotettavampi biometrinen tunnistautumismenetelmä on. (Jain ym., 2004.)

3.4.2 Behavioristinen biometria

Behavioristinen biometria mittaa yksilön käyttäytymisen ominaispiirteitä. Sitä voidaan käyttää tunnistusmenetelmänä erilaisissa tietojärjestelmissä perustuen kirjoitusdynamiikkaan (Bergadano ym., 2002), hiiren dynamiikkaan (Ahmed & Traore, 2017) tai esimerkiksi graafisen käyttöliittymän ja käyttäjän välisen interaktion analyysiin (Bailey ym., 2014). Menetelmä perustuu käyttäytymisen analysointiin hyödyntämällä käyttäjän aikaisemmin tallennettua käyttäytymisdataa.

Behavioristista biometriaa hyödyntävä tunnistautuminen ei aina edellytä järjestelmältä mitään fyysisiä laitteita, jotka osaltaan lisäisivät tunnistautumisprosessin kompleksisuutta, sillä tunnistautumisessa käytettävä sensoridata perustuu yleensä järjestelmän luonnollisiin osiin, kuten näppäimistöön, hiireen tai ohjauslevyyn (Bergadano ym., 2002; Bailey ym., 2014). Fysiologiseen biometriaan perustuvat menetelmät puolestaan tarvitsevat lähes aina jonkin erityisen sensorin (Bergadano ym., 2002). Behavioristisen tunnistautumismenetelmän implementointi on näin ollen laitteiston osalta edullinen, joskin tunnistautumisessa käytettävä ohjelmisto saattaa aiheuttaa kustannuksia. Fyysinen laitteisto aiheuttaa kustannuksia kuitenkin silloin, jos behavioristisen biometrian menetelmää sovelletaan käyttäen tunnistautumiskeinona esimerkiksi käyttäjän kävelyä (kamera tai muu sensori), allekirjoitusta (piirtolevy, kamera tai muu kuvantunnistuksen väline) tai muuta järjestelmän luonnollisiin osiin suoraan liittymätöntä menetelmää (Ahmed & Traore, 2017).

Behavioristiseen biometriaan perustuvia tunnistautumismenetelmä voidaan ajatella myös käytettävyydeltään hyväksi ja hyväksyttäväksi teknologiaksi, sillä käyttäjä ei ole suoraan vuorovaikutuksessa teknologian kanssa pelkästään tunnistautumistapahtumaa varten, vaan tunnistautuminen tapahtuu muun toiminnan ohessa. Behavioristiseen biometriaan verrattuna fysiologisen biometrian sovellukset ovat tällä hetkellä kuitenkin luotettavampia ja enemmän käytettyjä, sillä ihmisen fysiologiset ominaisuudet pysyvät paremmin vakiona, kun taas behaviorististen ominaisuuksien ilmentymät saattavat muuttua ajassa huomattavan paljon (Bergadano ym., 2002; Ahmed & Traore, 2017). Useimpia behavioristista biometriaa hyödyntäviä tunnistautumismenetelmiä ei voida vielä hyödyntää kaupallisesti fysiologista biometriaa heikomman suorituskyvyn vuoksi (Bailey ym., 2014). Esimerkiksi hiiren dynamiikan analyysiin perustuvan menetelmän väärinhyväksymisaste on 2,47 prosenttia ja väärinhylkäysaste 2,46 prosenttia, minkä takia menetelmä ei ole vuonna 2007 täyttänyt suorituskykynsä puolesta Euroopan Unionin kaupallisille sovelluksille asettamia standardeja. (Ahmed & Traore, 2007; Bergadano, ym., 2002.)

Behavioristiseen biometriaan perustuva tunnistautumismenetelmä voi olla joko staattinen tai dynaaminen. Staattinen tunnistautuminen tarkoittaa sitä, että käyttäjä tunnistetaan kerran esimerkiksi kirjautumisen yhteydessä, mikä on useimmissa tietoon, hallussapitoon ja erityiseen ominaisuuteen perustuvissa tunnistautumismenetelmissä käytettävä toteutus. (Ahmed & Traore, 2007.) Behavioristisen tunnistautumismenetelmän etuna on dynaaminen tunnistautuminen, joka tarkoittaa sitä, että käyttäjää voidaan tunnistaa jatkuvasti käytön ohessa taustalla myös varsinaisen kirjautumistapahtuman ulkopuolella. Dynaaminen tunnistautuminen estää suojatun tietojärjestelmän käyttäjän vaihtamisen jo autentikoidun session aikana. (Bailey ym., 2014; Ahmed & Traore, 2007.)

3.5 Tunnistautumismenetelmien koonti

Edellä käsiteltiin esimerkein tietoon, hallussapitoon ja erityiseen ominaisuuteen perustuvia tietojärjestelmissä käytettäviä tunnistautumismenetelmiä.

Perinteisesti kaupallisissa tietojärjestelmissä on useimmiten käytetty tietoon perustuvia tunnistautumismenetelmiä, kuten salasanaa tai PIN-koodia. Valtiollisissa sovelluksissa käytetään usein hallussapitoon perustuvia tunnistautumismenetelmiä, kuten älykorttia, ja sen rinnalla jotakin tietoon perustuvaa menetelmää monivaiheisen tunnistautumisen välineenä. Barkadehin ym. (2018) mukaan tunnistautumismenetelmät eivät kuitenkaan yksittäin ole tarpeeksi luotettavia. Tietoon perustuvat menetelmät ovat alttiita sosiaaliselle manipuloinnille, erityiseen ominaisuuteen perustuvat menetelmät ovat alttiita tunnistautumisvälineen, kuten kasvojen tai sormen 3D-mallinnukselle, ja hallussapitoon perustuvien menetelmien rinnalle on kehitettävä prosessi, jolla tunnus voidaan nopeasti lukita esimerkiksi tunnistautumisvälineen kadotessa. Kaikkia tietoturvariskejä ja hyökkäysvariaatioita huomioivaa tunnistautumismenetelmää voi olla vaikea löytää, mutta monivaiheisen tunnistautumisen avulla voidaan parantaa turvallisuutta ja ehkäistä tietoturvapoikkeamia (Barkadehi ym., 2018).

Henkilön erityiseen ominaisuuteen perustuvat tunnistautumismenetelmät ovat pitkään olleet laajasti käytössä tietojärjestelmiin tunnistautumisen lisäksi myös forensiikkaan liittyvissä tunnistamissovelluksissa, kuten esimerkiksi vainajan tunnistamisessa tai rikostutkinnassa, mutta ne ovat yleistyneet viime aikoina yhä enemmän myös kuluttajille suunnatuissa tietojärjestelmäsovelluksissa erityisesti mobiiliteknologiassa käytössä olevan kasvojen ja sormenjäljen tunnistuksen ansiosta. (Jain ym., 2004.)

Tietoon perustuvat tunnistautumismenetelmät ovat implementoinnin puolesta kaikkein edullisimpia, sillä niiden käyttöönotto ei normaalisti edellytä laitteistohankintoja (Spender, 1987; Biddle ym., 2012), vaan toteutus tehdään tietojärjestelmän sovelluskerroksessa. Hallussapitoon ja erityiseen ominaisuuteen perustuvat tunnistautumismenetelmät vaativat useimmiten laitteistohankintoja, kuten lukijan älykortin tai sormenjäljen lukemista varten (Spender, 1987; Bergadano ym., 2002). Sekä tietoon että hallussapitoon perustuvat tunnistautumismenetelmät ovat kuitenkin alttiita tiedon tai tunnistautumisvälineen vääriin käsiin joutumiselle. Väärän henkilön tunnistautumisen riskiä on pyritty pienentämään käyttämällä ristiin yhtä tai useampaa tunnistautumismenetelmää, jolloin esimerkiksi tietoon perustuvaa menetelmää käytettäessä salasanan lisäksi syötetään älylaitteesta saatu koodi tai hallussapitoon perustuvassa menetelmässä käytetään älykortin lisäksi myös PIN-koodia (Barkadehi ym., 2018). Tietoon perustuvissa menetelmissä voidaan käyttää myös erilaisia salasananhallintaohjelmia, jotka pienentävät riskiä samojen salasanojen käyttämiseen eri palveluissa (Biddle ym., 2012).

Alle on koottu vertaileva yhteenvetotaulukko tässä kirjallisuuskatsauksessa esiteltyjen tietoon, hallussapitoon ja erityiseen ominaisuuteen perustuvien tunnistautumismenetelmien vahvuuksista ja heikkouksista (ks. TAULUKKO 1).

TAULUKKO 1 Tunnistautumismenetelmien vertailu

Menetelmä	Vahvuudet	Heikkoudet
Merkkijonosalasana (tieto)	- Käytetyin → käyttäjälle tuttu - Ei erityisiä laitteistovaatimuksia - Toteutukselta yksinkertainen - Edullinen	- Voi paljastua - Käytettävyyshaasteet - Vahvan entropian huono muistettavuus - Altis näppäimistökuuntelulle
Graafinen salasana (tieto)	- Muistettavuus merkkijonoon verrattuna	- Voi paljastua - Altis shoulder surfing -hyökkäyksille
Älykortti (hallussapito)	- Yhdistetään usein PIN-koodiin (monivaiheinen tunnistautuminen) → turvallinen	- Voi kadota tai tulla varastetuksi - Vaatii lukijalaitteen
Älylaite (hallussapito)	- Yleensä monivaiheinen tunnistautumisen väline → turvallinen	- Voi kadota tai tulla varastetuksi - Lukijalaitteen tarve
Fysiologinen biometria (erityinen ominaisuus)	- Käytettävyys nykyaikaisissa mobiililaitteissa - Lähes ääretön entropia - Vaikea kopioida tai varastaa	- Olosuhteiden vaikutus väärinhylkäysasteeseen - Lukijalaitteen tarve
Behavioristinen biometria (erityinen ominaisuus)	- Lähes ääretön entropia - Vaikea jäljitellä - Mahdoton varastaa - Lukijalaite voi olla järjestelmään luonnollisesti kuuluva laite	- Ei tuttu - Herkästi muuttuva - Lukijalaitteen tarve, jos tunnistautuminen ei perustu osoitin- tai syöttölaitteen käyttöön

4 MENETELMÄN VALINTAAN VAIKUTTAVAT TEKIJÄT

Uuden järjestelmän suunnitteluvaiheessa tärkeä huomioon otettava tietoturvan osa-alue on tietojärjestelmässä käytettävän tunnistautumismenetelmän valinta. Kuten tunnistautumista yleisesti käsittelevässä kappaleessa mainittiin, tunnistautuminen on yksi tietojärjestelmän tietoturvainfrastruktuurin pääkomponenteista, mutta se ei kuitenkaan ole välttämätön osa tietojärjestelmän rakennetta. Mikäli tunnistautumisen käyttö ei ole perusteltua tai sille ei muutoin nähdä tarvetta, se voidaan myös jättää kokonaan pois.

Velásquez, Caro ja Rodríguez (2018) ovat esitelleet Kontun-viitekehyksen, jossa tunnistautumismenetelmän soveltuvuutta tietojärjestelmään voidaan arvioida käytettävyyden (engl. usability), turvallisuuden (engl. security) ja aiheutuvien kustannusten (engl. costs) näkökulmasta. Tässä kirjallisuuskatsauksessa esitellään tunnistautumismenetelmän valintaan vaikuttavia tekijöitä näiden kolmen komponentin sekä kohdejärjestelmän erityispiirteiden valossa. Kirjallisuudessa esiintyy muutamia eri malleja tunnistautumismenetelmän valintaan, ja Bonneau ym. (2012) ovat omassa viitekehysmallissaan huomioineet kustannusten sijasta käyttöönoton (engl. deployability) näkökulman. Tässä tutkielmassa kohde rajataan kuitenkin kolmen ensin mainitun mukaan. Tämän luvun jälkeen lukija tuntee oleellisia tietojärjestelmän tunnistautumismenetelmien suunnittelussa huomioitavia seikkoja käytettävyyden, turvallisuuden, kustannusten ja kohdejärjestelmän erityispiirteiden näkökulmasta.

Käytettävyyden ja turvallisuuden sanotaan usein olevan vastakkainasettelun kohteena (Braz & Robert, 2006), ja niiden välille muodostuu paljon yhtymäkohtia erityisesti tässä erilaisia tunnistautumismenetelmiä käsittelevässä kandidaatin tutkielmassa. Selkeyden ja tekijöiden eroteltavuuden vuoksi ne on kuitenkin tässä luvussa käsitelty omina kappaleinaan.

4.1 Käytettävyys

Käytettävyys tarkoittaa ISO 9241-11 -standardin mukaan sitä tuottavuutta (engl. effectiveness), tehokkuutta (engl. efficiency) ja tyytyväisyyttä (engl. satisfaction), jolla tietyt määritellyt käyttäjät saavuttavat määritellyt tavoitteet tietyssä ympäristössä (ISO, 2018). Arvostettu tanskalainen käytettävyysasiantuntija Jakob Nielsen on määritellyt käytettävyyden useammalla käsitteellä. Nielsenin (1994, s. 26) mukaan käytettävyys koostuu opittavuudesta (engl. learnability), tehokkuudesta (engl. efficiency), muistettavuudesta (engl. memorability), virheettömyydestä (engl. errors) ja tyytyväisyydestä (engl. satisfaction). Nielsenin käyttämistä käsitteistä sekä tehokkuus että tyytyväisyys mainitaan myös ISO 9241-11 -standardissa, mutta joukossa on lisäksi muita käsitteitä, joita ei sovi jättää huomiotta arvioitaessa tunnistautumismenetelmän soveltuvuutta kohdetietojärjestelmään käytettävyyden näkökulmasta.

Eräs käytettävyysarvioinnin menetelmä on Nielsenin kehittämä heuristinen arviointi (Ovaska, Aula & Majaranta, 2005). Käytettävyyden arvioinnin tueksi Nielsen on julkaissut kymmenen kohdan heuristiikkalistan, jota voidaan käyttää järjestelmän käytettävyyden arvioinnissa. Potentiaalisia käytettävyyden ja turvallisuuden konflikteja voidaan pyrkiä karsimaan käyttämällä esimerkiksi näitä heuristiikkoja suunnittelun tukena. Nielsenin kymmenen heuristiikan lista tarkastelee käytettävyyttä seuraavista näkökulmista (Ovaska ym., 2005):

1. Palvelun tilan näkyvyys
2. Palvelun ja tosielämän vastaavuus
3. Käyttäjän kontrolli ja vapaus
4. Yhteneväisyys ja standardit
5. Virheiden estäminen
6. Tunnistaminen mieluummin kuin muistaminen
7. Käytön joustavuus ja tehokkuus
8. Esteettinen ja minimalistinen suunnittelu
9. Virhetilanteiden tunnistaminen, ilmoittaminen ja korjaaminen
10. Opastus ja ohjeistus

Brazin ja Robertin (2006) mukaan tietojärjestelmän käytettävyys ja turvallisuus joutuvat usein vastakkainasettelun kohteeksi. Kuten luvussa 2.2 todettiin, käyttäjä mainitaan usein tietoturvallisen tietojärjestelmän heikoimpana lenkkinä, mutta usein vain välillisesti, sillä huonosti suunniteltu hyvä turvallisuus saattaa itsessään aiheuttaa tietoturvariskejä ihmisen ja tietojärjestelmän vuorovaikutuksen tuloksena. On huomioitava, että kohdejärjestelmän käyttäjät eivät välttämättä luontaisesti hallitse tietokoneen käyttöä (Barkadehi ym., 2018), ja mikäli järjestelmän tietoturvan suunnittelussa ei oteta huomioon käytettävyyden aspektia, hyvin suunniteltu tietoturva saattaa epäonnistua käytännössä. (Adams & Sasse, 1999.)

Luvussa 3 esiteltiin ja lopuksi koostettiin erilaisten tunnistautumismenetelmien ominaispiirteitä (TAULUKKO 1). Koonnin perusteella voidaan päätellä, että tietoon perustuvien menetelmien, erityisesti perinteisen salasanan, voidaan katsoa olevan tunnettuutensa puolesta kaikkein käytettävin menetelmä, joskin graafinen salasana noudattelee tietoon perustuvien menetelmien osalta paremmin Nielsenin heuristiikkalistaa. Myös erityiseen ominaisuuteen perustuvat biometriset tunnistautumismenetelmät ovat viime aikoina yleistyneet esimerkiksi mobiiliteknologian saralla sormenjälkilukijan ja kasvojen tunnistuksen muodossa. Käytettävyyttä saattaa heikentää myös sellainen menetelmä, joka vaatii jonkin järjestelmään muuten kuulumattoman laitteen, kuten älykortinlukijan (Bailey ym., 2014), joskin järjestelmän luonnollisena osana esiintyvät fyysiset laitteet voidaan välttää behavioristiseen biometriaan perustuvan menetelmän perustuessa esimerkiksi osoitin- tai syöttölaitteen dynamiikkaan (Ahmed & Traore, 2017). Erityiseen ominaisuuteen perustuvan tunnistautumismenetelmän voidaan katsoa olevan käytettävimmillään silloin, kun väärinhylkäysaste FRR on mahdollisimman pieni. Tähän voivat kuitenkin vaikuttaa myös järjestelmän ulkopuoliset tekijät, kuten ympäristön ilmankosteus lukuhetkellä.

4.2 Turvallisuus

Turvallisuus on abstrakti määre, jota on vaikea mitata. O'Gormanin (2013) mukaan tietojärjestelmän turvallisuuden voidaan katsoa olevan hyvällä pohjalla, jos hyökkääjälle aiheutuvia kustannuksia voidaan pitää suurempina kuin potentiaalista hyökkäyksestä saatavaa hyötyä. Hyökkäyksestä aiheutuvat kustannukset pitävät sisällään rahan lisäksi myös ajan ja esimerkiksi mahdollisen tuomion (O'Gorman, 2013). Tunnistautumismenetelmän turvallisuutta voidaan tarkastella puhtaasti eri tyyppisiin menetelmiin perustuen. Kuten edellisessä luvussa todettiin, tietoon ja hallussapitoon perustuvissa menetelmissä ovat riskeinä tunnistautumiseen käytettävän tiedon paljastuminen sekä fyysisen välineen katoaminen tai anastaminen. Erityiseen ominaisuuteen perustuvan menetelmän kopiointi ja jäljittely on sitä vastoin huomattavasti vaikeampaa, joskin kuitenkin mahdollista (O'Gorman, 2013).

Harkittaessa tietoon perustuvan tunnistusmenetelmän järjestelmäimplementointia, on otettava huomioon muun muassa merkkijonosalasanan vahvuus: annetaanko käyttäjän valita salasanana käytettävä merkkijono täysin itsenäisesti vai ohjaako tietojärjestelmän sovellus käyttäjää noudattamaan tiettyjä ennakkoon syötettyjä parametreja. Järjestelmän asettama vaatimus salasanalle voi olla esimerkiksi se, että salasanan täytyy olla pituudeltaan tietyn mittainen tai siinä täytyy esiintyä tietty määrä jonkin tietyn merkkiryhmän merkkejä, kuten suur- tai pienaakkosia, numeraaleja, tai erikoismerkkejä, kuten huuto- tai kysymysmerkkejä. Järjestelmässä tämänkaltaisten asetettujen ehtojen validiteettia voidaan testata esimerkiksi säännöllisen lausekkeen avulla (engl. regular expression, lyhenne regexp tai regex). (Florêncio ym., 2014.) Britannian kansallisen kyberturvallisuuskeskuksen NCSC:n (2019) mukaan kymmenen yleisimmin

käytetyn salasanan listalta löytyvät esimerkiksi merkkijonot ”123456”, ”qwerty” ja ”password”. Tivi-lehden artikkelin (2019) mukaan kaksi ensimmäistä ja viimeksi mainitun suomenkielinen vastine ”salasana” löytyvät niin ikään suomalaisten suosimien salasanojen listalta. Tällaiset helposti arvattavat salasanat ovat erityisen alttiita niin sanotulle sanakirjahyökkäykselle (engl. dictionary search attack) (Bonneau ym., 2012; Barkadehi ym., 2018). Näin ollen onkin syytä harkita salasanan satunnaista generointia tai sanakirjahyökkäystä vaikeuttavia merkistövaatimuksia salasanalle käyttäjän täysin vapaasti itse asettaman salasanan sijaan.

Tavoiteltava tunnistautumistietojen avainavaruus ja entropia sekä yleisellä tasolla käyttäjän tunnistautumisen tarpeellisuus on kuitenkin arvioitava järjestelmän mukaan. Avainavaruudesta puhuttaessa tarkoitetaan mahdollista kombinaatioiden määrää. Salasanan tai muun merkkijonon, jonka pituus on n, ja jonka jokaisella merkillä on c mahdollista arvoa, avainavaruuden koko lasketaan kaavalla $k_p = c^n$. Nelinumeroisen PIN-koodin avainavaruus on $10^4 = 10\,000$, mikä tarkoittaa, että tällaisella koodilla on 10 000 mahdollista kombinaatiota. Tilastollisen entropian avulla voidaan arvioida salasanan tai muun merkkijonon epävarmuutta bitteinä. Esimerkiksi 8 satunnaisen bitin sisältämä entropia on 8 bittiä. Merkkijonon entropia saadaan selville kaavalla $H_{max} = \log_2(k_p)$ (bittiä), jolloin esimerkiksi edellä esitetyn PIN-koodin entropia on $\log_2(10\,000) = 13{,}3$ bittiä. (O’Gorman, 2013.) Käyttäjän valitessa itse samanpituisen salasanan, avainavaruus säilyy samana, mutta salasanan entropia saattaa olla paljon pienempi, sillä käyttäjä valitsee usein salasanansa muistettavuuden eikä satunnaisuuden perusteella (Adams & Sasse, 1999), ja tällöin heikentyvää tietoturvaa ei kyetä palauttamaan esimerkiksi järjestelmän teknistä tietoturvaa vahvistamalla (Biddle ym., 2012). Esimerkiksi päivämäärään perustuvan koodin *ppkk*, jossa $p_1 \in \{0, 1, 2, 3\}$, $p_2 \in \{0, 1, \ldots, 9\}$, $k_1 \in \{0, 1\}$ ja $k_2 \in \{0, 1, \ldots, 9\}$, avainavaruus on ainoastaan $4 \times 10 \times 2 \times 10 = 800$, jolloin samalla sen entropiakin laskee $\log_2(800) = 9{,}6$ bittiin, joka on jo huomattavasti vähemmän kuin täysin satunnaisessa vaikeammin muistettavassa numeroyhdistelmässä. Avainavaruuden ja entropian ollessa hyvällä tasolla ne pienentävät riskiä altistua sanakirja- tai väsytyshyökkäyksille tai muille vastaaville kryptoanalyysihyökkäyksille. (O’Gorman, 2013.) Suunnitellun tunnistautumismenetelmän entropia voidaan laskea mille menetelmälle tahansa menetelmän tyypistä riippumatta.

O’Gormanin (2013) mukaan useimpaan tunnistautumismenetelmään liittyy jokin tunnistautumispalvelimella säilytettävä salainen koodi tai kombinaatio, jota verrataan käyttäjältä saatuun syötteeseen. Tunnistautumistietoa voidaan säilyttää tietokannassa joko selväkielisenä tekstinä (myös ilmiteksti, engl. plaintext) tai salattuna joko kaksi- (engl. reversible) tai yksisuuntaisesti (engl. irreversible). Salausavaimen tallentaminen selväkielisenä tekstinä ei ole hyvä käytäntö, sillä tällöin se ei ole palvelimella salatussa muodossa ja sen tietoturvallisuus on täysin palveluntarjoajan tietoturvan varassa. Selväkielistä tekstiä parempi tapa on tallentaa tieto kaksisuuntaisesti, jolloin sen tallentamiseen käytetään jotakin salausavainta, jonka avulla salattu tieto on myös mahdollista palauttaa selkokieliseksi. Parhaana käytänteenä pidetään kuitenkin yksisuuntai-

sen salauksen käyttöä. Yksisuuntaista salausta ei ole mahdollista palauttaa takaisin selkokieliseen muotoon, mutta tunnistautumisessa annetun selkokielisen syötteen yhdenmukaisuutta voidaan verrata tietokannan salattuun tietoon. Esimerkkejä yksisuuntaisista salausalgoritmeista (myös hajakoodausalgoritmi, engl. one-way hashing algorithm) ovat muun muassa kryptografiset tiivistefunktiot MD5 (nk. message-digest -algoritmi) ja korkeampaa tietoturvaa tarjoava SHA (engl. secure hash algorithm). (O'Gorman, 2013.)

4.3 Kustannukset

Tietoturvan implementointi aiheuttaa kustannuksia organisaatiolle ylläpidon sekä implementoinnin osalta kattaen koko kehitystyön järjestelmäintegraatiot mukaan lukien. Altinkemerin ja Wangin (2011) mukaan tunnistautumista on kuitenkin tutkittu lähinnä teknisestä näkökulmasta taloudellisen näkökulman jäädessä taka-alalle lähinnä taustarooliin jonkin teknisesti orientoituneen tutkimuksen sivutuotteeksi. Yksi aiheutuvien kokonaiskustannuksen osatekijä on myös valittu tunnistautumismenetelmä, joka osaltaan aiheuttaa kustannuksia sekä kehitys- että käyttövaiheessa. Esimerkiksi monivaiheista tunnistautumista voidaan pitää yksivaiheista turvallisempana, mutta se aiheuttaa enemmän implementointikustannuksia muun muassa ohjelmiston, laitteiston ja koulutuksen osalta (Altinkemer & Wang, 2011).

Kuten perinteisen salasanan suosiosta voidaan päätellä, monissa tietojärjestelmissä käytetään tietoon perustuvia tunnistautumismenetelmiä, sillä ne perustuvat useimmiten yksinkertaisempaan tekniikkaan ja ovat näin ollen ylläpidettävämpiä ja laitteistovaatimuksiltaan vaatimattomampia (De Angeli ym., 2005). Hallussapitoon ja erityiseen ominaisuuteen perustuvat tunnistautumismenetelmät tarvitsevat jonkin lukijalaitteen, jolla esimerkiksi varmennekortti tai sormenjälki voidaan lukea (Ahmed & Traore, 2017), mistä aiheutuu lisäkustannuksia. Lisäksi hallussapitoon perustuva menetelmä vaatii fyysisen tunnistautumisvälineen, jonka hankinta myös osaltaan kasvattaa implementoinnin kokonaiskustannuksia.

Lawrence ja Loeb (2002) ovat esitelleet mallin, jonka avulla tietoturvan implementoinnista aiheutuvia kuluja voidaan arvioida. Mallin keskeinen laskentakaava koostuu kolmesta parametrista, jotka ovat a) tietoturvaloukkauksesta aiheutuva taloudellinen tappio, b) tietoturvaloukkauksen todennäköisyys, sekä c) alttius joutua tietoturvaloukkauksen kohteeksi. Tunnistautuminen on tärkeä osa tietoturvallisen järjestelmän kokonaisarkkitehtuuria (Velásquez ym., 2018), joten malli voi olla apuna myös tunnistautumismenetelmän implementoinnista syntyvien kustannusten arvioinnissa.

4.4 Kohdejärjestelmän erityispiirteet

Valintaan vaikuttavien toistensa kanssa ristiriidassa olevien komponenttien puntarointi aiheuttaa usein kompromissin lopputuloksessa. Näin voidaan havaita esimerkiksi käytettävyyden ja turvallisuuden tai turvallisuuden ja kustannusten komponenttien osittaista ristiriitaisuutta: usein ajatellaan, että järjestelmän turvallisuuden kasvaessa sen käytettävyys pienenee esimerkiksi monivaiheisen tunnistautumisen käyttöönoton myötä (Barkadehi ym., 2018), tai parannettaessa järjestelmän tietoturvallisuutta siitä aiheutuvat kokonaiskustannukset kasvavat. Siksi onkin tärkeää asettaa valintaan vaikuttaville komponenteille painoarvot: kuinka paljon tunnistautumisen käytettävyydelle ja tietoturvallisuudelle halutaan antaa painoarvoa ja kuinka paljon tunnistautuminen saa aiheuttaa kustannuksia kohdejärjestelmä ja toimintaympäristö huomioiden. Painoarvot voivat esiintyä hyvin erilaisina riippuen siitä, ollaanko tunnistautumista implementoimassa yhteiskunnallisesti kriittiseen kyberfyysiseen tietojärjestelmään tai esimerkiksi kirjaston aineistohakujärjestelmään.

Velásquezin ym. (2018) kehittämä Kontun-viitekehys muodostuu tämän tutkielman edellisissä kappaleissa käsiteltyjen komponenttien ympärille. Sen avulla tunnistautumismenetelmän valinnassa voidaan huomioida kohdejärjestelmän erityispiirteitä viitekehykseen määritettyjen painoarvojen perusteella. Viitekehys ottaa huomioon käytettävyyden, turvallisuuden ja kustannusten näkökulmat, joita voidaan arvioida komponenttitasolla pilkottuina vielä tarkempiin osatekijöihin, joista jokainen painotetaan kohdejärjestelmän vaatimusten mukaan. Kunkin näkökulman painoarvo voidaan laskea viitekehyksen tarjoaman taulukon avulla (LIITE 1), minkä jälkeen komponentit ovat vertailukelpoisia keskenään suuremmassa mittakaavassa. Tällöin voidaan laskea esimerkiksi tietojärjestelmäkohtainen turvallisuuden ja käytettävyyden tai kustannusten ja käytettävyyden painoarvojen suhde. Kontun-viitekehyksen turvallisuusnäkökulma ottaa huomioon turvallisuuden tärkeyden yleensä, järjestelmässä käsiteltävän informaation luottamuksellisuuden sekä suojautumisen eri tyyppisiltä hyökkäyksiltä. Käytettävyysnäkökulmassa huomioidaan käytön ja opittavuuden helppous, tunnistautumistietojen palautusmahdollisuus käyttäjän unohdettua esimerkiksi käyttäjätunnuksensa tai salasanansa, lukijalaitteen hyväksyttävyys sekä luotettavuus esimerkiksi väärinhylkäysten suhteen. Kustannusnäkökulmassa huomioidaan implementointikustannukset sekä käyttäjästä mahdollisesti aiheutuvat kustannukset. (Velásquez ym., 2018.)

5 YHTEENVETO

Tämä tutkielma toteutettiin kirjallisuuskatsauksena, ja siinä tarkasteltiin tietojärjestelmien tunnistautumismenetelmiä ja niiden valintaan vaikuttavia tekijöitä. Tutkielman tavoitteena oli vastata kahteen asetettuun tutkimuskysymykseen:

- Minkälaisia erilaisia tunnistautumismenetelmiä on olemassa?
- Mitkä tekijät vaikuttavat tietojärjestelmän tunnistautumismenetelmän valintaan?

Tutkielmassa todettiin, että tunnistautuminen on yksi tietoturvallisen järjestelmän pääkomponenteista. Aluksi käytiin läpi tietoturvan peruskäsite ja tarkasteltiin tietoturvaa sekä yksilön että organisaation näkökulmasta. Tämän jälkeen määriteltiin, mitä tunnistautuminen yleisellä tasolla tarkoittaa ja todettiin tunnistautumismenetelmien jakautuvan pääsääntöisesti tietoon, hallussapitoon ja erityiseen ominaisuuteen perustuviin menetelmiin. Jokaista eri tyyppistä tunnistautumismenetelmäkategoriaa esiteltiin kahden esimerkin avulla. Kolmannen luvun lopussa erilaiset tunnistautumismenetelmät koottiin yhteen taulukon muodossa. Tunnistautumismenetelmien läpikäynnin jälkeen neljännessä luvussa tarkasteltiin tunnistautumismenetelmän valintaan vaikuttavia tekijöitä, joiksi tässä tutkielmassa valikoituivat käytettävyys, turvallisuus ja aiheutuvat kustannukset sekä kohdejärjestelmän erityispiirteet.

Tutkielmassa todettiin tietoturvan koostuvan useasta elementistä, joiden toteuttaminen yksitellen on helppoa, mutta niiden yhdistämisen aiheuttavan haasteita. Samaa voitiin todeta tunnistautumisen järjestelmäimplementoinnista, jossa sekä käytettävyys, turvallisuus ja kustannukset näyttelevät tärkeää roolia, mutta niiden tasapaino kohdejärjestelmän vaatimukset huomioiden aiheuttaa komponenttien välillä kitkaa. Käyttäjälle vaadittujen tietoturvakäytänteiden noudattaminen voi olla epämieluisaa, jos tietoturvan käytettävyyttä ei ole saatettu tarpeeksi hyvälle tasolle. Tämä aiheuttaa kuitenkin ongelmia muun muassa organisaatioiden näkökulmasta, jotka lähestyvät usein tietoturvaa teknologialähtöisesti turvallisuus ja kustannukset edellä käytettävyysnäkökulman jäädessä vähemmälle huomiolle. Näistä syistä tietoturvallisten järjestelmien kehit-

tämisessä yleensä onkin syytä pyrkiä konsensukseen eri näkökulmien suhteen, jolloin voidaan pitkällä tähtäimellä saavuttaa jopa tietoturvallisempi tila kuin keskittymällä pelkkään turvallisuuteen.

Aineistohaun yhteydessä kiinnitettiin huomiota eri tunnistautumismenetelmiin liittyvien hakusanojen palauttamien hakutulosten julkaisuajankohtiin. Tähän tarkoitukseen käytettiin JYKDOK-aineistotietokannan työkalua, joka näyttää hakutuloksien julkaisuvuosijakauman graafina. Esimerkiksi haettaessa graafiseen salasanaan liittyviä vertaisarvioituja tuloksia, muutamaa poikkeusta lukuun ottamatta kaikki hakutulokset sijoittuivat ajallisesti 2000-luvun puolelle. Googlen Scholar -tietokannan hakutulokset antoivat samansuuntaisia tuloksia. Tästä voitiin päätellä, että graafisten salasanojen osalta kyse on verrattain uudesta keksinnöstä. Biometristen eli erityiseen ominaisuuteen perustuvien tunnistautumismenetelmien osalta hakutuloksia löytyi huomattavasti enemmän, ja niiden tutkimus painottui julkaisuajankohtien perusteella myös 2000-luvun puolelle. Hallussapitoon perustuvien menetelmien ja perinteisen salasanan osalta julkaisut ulottuivat jopa 1980-luvulle, salasanan osalta jopa 1970-luvulle asti, ja näiden tutkimuksen todettiin hakutulosten perusteella lähteneen kasvuun 1990-luvun aikana. Älylaitteisiin liittyviä artikkeleita löytyi määrällisesti paljon vähemmän muihin tunnistautumismenetelmiin verrattuna. Kaikkien tunnistautumiseen liittyvien hakusanojen osalta oli havaittavissa kasvua hakutulosten määrässä viime vuosien aikana, mikä tarkoittaa sitä, että aiheen tutkimus on kiihtynyt. Aihetta onkin tarpeen tutkia, sillä entisestään digitalisoituvassa toimintaympäristössä tunnistautuminen ja identiteetinhallinta korostuu tietoturvan merkityksen kasvaessa.

Koska kandidaatin tutkielma ei yleisluonteeltaan ole kovin laaja, tehtiin tähänkin kirjallisuuskatsauksena toteutettuun tutkimukseen rajauksia aiheen käsittelyn suhteen. Tunnistautumismenetelmien osalta tutkimus kohdistui ihmisen ja laitteen välisiin tunnistautumistapahtumiin sekä ihmiseen tietojärjestelmän faktorina jättäen yleisesti ohjelmistotuotannossa hyödynnettävän laitteiden välisen tunnistautumisen ilman erityistä huomiota. Laitteiden välistä tunnistautumista käsiteltäessä esimerkiksi käytettävyyden näkökulma olisi jäänyt vähemmälle tarkastelulle, kun taas Bonneaun ym. (2012) mallissa esiintyvä käyttöönoton näkökulma olisi saanut muita osa-alueita enemmän huomiota osakseen.

Mielenkiintoinen jatkotutkimusaihe olisi esimerkiksi tunnistautumismenetelmän valintaa ohjaavan viitekehyksen käytön tutkiminen käytännössä; kuinka eri alojen asiantuntijat ja asiakkaat painottavat esimerkiksi Kontun-viitekehyksessä listattuja kriteerejä. Myös jonkin vähemmän tutkitun tunnistautumismenetelmän, kuten esimerkiksi behavioristisen biometrian jatkuvan tunnistautumisen eri sovellusmahdollisuuksia olisi suositeltavaa tutkia. Esimerkki mielenkiintoisesta poikkitieteellisestä tutkimusaiheesta olisi äärettömän entropian tarjoaman DNA:n hyödyntäminen globaalissa tunnistautumisessa ja siihen liittyvät moninaiset tietoturva- ja yksityisyysongelmat.

LÄHTEET

Adams, A. & Sasse, M. (1999). Users are not the enemy. *Communications of the ACM, 42*(12), pp. 40-46. doi:10.1145/322796.322806

Ahmed, A. E. E. & Traore, I. (2007). A New Biometric Technology Based on Mouse Dynamics. *IEEE Transactions on Dependable and Secure Computing, 4*(3), pp. 165-179. doi:10.1109/TDSC.2007.70207

Altinkemer, K. & Wang, T. (2011). Cost and benefit analysis of authentication systems. *Decision Support Systems, 51*(3), pp. 394-404. doi:10.1016/j.dss.2011.01.005

Anderson, J. M. (2003). Why we need a new definition of information security. *Computers & Security, 22*(3), pp. 308-313. doi:10.1016/S0167-4048(03)00407-3

Antonopoulos, A. (2010). Password cracking in the cloud. *Network World, 27*(22), p. 17.

Bailey, K. O., Okolica, J. S. & Peterson, G. L. (2014). User identification and authentication using multi-modal behavioral biometrics. *Computers & Security, 43*(C), pp. 77-89. doi:10.1016/j.cose.2014.03.005

Barkadehi, M. H., Nilashi, M., Ibrahim, O., Fardi, A. Z. & Samad, S. (2018). Authentication systems: A literature review and classification. *Telematics and Informatics, 35*, pp. 1491-1511. doi:10.1016/j.tele.2018.03.018

Bergadano, F., Gunetti D. & Picardi C. (2002). User Authentication through Keystroke Dynamics. *ACM Transactions on Information and System Security, 5*(4), pp. 367-397. doi:10.1145/581271.581272

Biddle, R., Chiasson S. & Van Oorschot, P.C. (2012). Graphical passwords: Learning from the first twelve years. *ACM Computing Surveys, 44*(4), pp. 1-41. doi:10.1145/2333112.2333114

Bonneau J., Herley C., van Oorschot P. C. & Stajano F. (2012). The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. *IEEE Symposium on Security and Privacy*, pp. 553-567. doi: 10.1109/SP.2012.44

Bras, T. L. (2015). [INFOGRAPHIC] online overload – it's worse than you thought. Haettu osoitteesta https://blog.dashlane.com/infographic-online-overload-its-worse-than-you-thought/

Braz, C. & Robert, J. (2006). Security and Usability: The Case of the User Authentication Methods. (s. 199-203) *ACM.* doi:10.1145/1132736.1132768

Britannian kansallinen kyberturvallisuuskeskus NCSC. (2019). PwnedPasswordTop100k [sähköinen tietoaineisto]. Haettu osoitteesta https://www.ncsc.gov.uk/static-assets/documents/PwnedPasswordTop100k.txt

Brown, G. (2004). The use of hardware tokens for identity management. *Information Security Technical Report, 9*(1), pp. 22-25. doi:10.1016/S1363-4127(04)00012-3

Burrows, M., Abadi, M. & Needham, M. (1990). A logic of authentication. *ACM Transactions on Computer Systems, 8*(1), pp. 18-36. doi:10.1145/77648.77649

Council of the European Union. (2015). Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Haettu osoitteesta http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf

De Angeli A., Coventry L., Johnson, G. & Renaud, K. (2005). Is a picture really woth a thousand words? Exploring the feasibility of graphical authentication systems. *International Journal of Human – Computer Studies, 63*(1), pp. 128-152. doi:10.1016/j.ijhcs.2005.04.020

Euroopan parlamentin ja neuvoston direktiivi (EU) 2015/2366, annettu 25 päivänä marraskuuta 2015, maksupalveluista sisämarkkinoilla, direktiivien 2002/65/EY, 2009/110/EY ja 2013/36/EU ja asetuksen (EU) N:O 1093/2010 muuttamisesta sekä direktiivin 2007/64/EY kumoamisesta (ETA:n kannalta merkityksellinen teksti). (2015). Haettu osoitteesta https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32015L2366&from=EN

Florêncio, D., Herley, C. & van Oorschot, P. C. (2014). An Administrator's Guide to Internet Password Research. Haettu osoitteesta https://www.microsoft.com/en-us/research/wp-content/uploads/2014/11/WhatsaSysadminToDo.pdf.

Gyorffy, J. C., Tappenden, A. F. & Miller, J. (2011). Token-based graphical password authentication. *International Journal of Information Security, 10*(6), pp. 321-336. doi:10.1007/s10207-011-0147-0

Independent Security Evaluators. (2019). Password managers: Under the hood of secrets management. Haettu osoitteesta

https://www.securityevaluators.com/casestudies/password-manager-hacking/

International Organization for Standardization. (2018). Ergonomics of human-system interaction – Part 11: Usability: Definitions and concepts (ISO 9241-11). Haettu osoitteesta https://www.iso.org/obp/ui/#iso:std:iso:9241:-11:ed-2:v1:en

Jain, A. & Ross, A. (2007). *Handbook of Biometrics*. Springer Science & Business Media.

Jain, A., Ross, A. & Prabhakar, S. (2004). An Introduction to Biometric Recognition. *IEEE Transactions on Circuits and Systems for Video Technology, 14*(1), pp. 4-20. doi:10.1109/TCSVT.2003.818349

Julkaisufoorumi. (2019). Haettu osoitteesta http://www.julkaisufoorumi.fi/fi/julkaisufoorumi

Lanitis, A. (2010). A Survey of the Effects of Aging on Biometric Identity Verification. *International Journal of Biometrics, 2*(1), pp. 34-52.

Lawrence, G. & Loeb, M. (2002). The economics of information security investment. *ACM Transactions on Information and System Security, 5*(4), pp. 438-457. doi:10.1145/581271.581274

Menkus, B. (1988). Understanding the Use of Passwords. *Computers & Security, 7*(2), p. 132. doi:10.1016/0167-4048(88)90325-2

Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C. & Giannakopoulos, G. (2014). The Human Factor of Information Security: Unintentional Damage Perspective. *Procedia – Social and Behavioral Sciences, 147*, pp. 424-428. doi:10.1016/j.sbspro.2014.07.133

Nielsen, J. (1994). *Usability Engineering*. Academic Press. doi:10.1016/C2009-0-21512-1

O'Gorman, L. (2003). Comparing passwords, tokens, and biometrics for user authentication. *Proceedings of the IEEE, 91*(12), pp. 2019-2040. doi:10.1109/JPROC.2003.819605

Ovaska, O., Aula, A. & Majaranta, P. (2005). *Käytettävyystutkimuksen menetelmät.* (B-2005-1). Tampereen yliopisto.

Sanastokeskus TSK. (2018). *Kyberturvallisuuden sanasto*. (TSK 52). Haettu osoitteesta http://www.tsk.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf

Sodiya, A. S., Folorunso, O., Komolafe, P. B. & Ogunderu, O. P. (2011). Preventing Authentication Systems From Keylogging Attack. *Journal of Information Privacy & Security, 7*(2), pp. 3-27. doi:10.1080/15536548.2011.10855909

Spender, J. (1987). Identifying computer users with authentication devices (tokens). *Computers & Security, 6*(5), pp. 385-395. doi:10.1016/0167-4048(87)90011-3

Tivi. (14.2.2019). Suomalaisten suosikkisalasanat paljastuivat – jos käytät jotakin näistä, vaihda heti. Haettu osoitteesta https://www.tivi.fi/uutiset/suomalaisten-suosikkisalasanat-paljastuivat-jos-kaytat-jotakin-naista-vaihda-heti/181cdf96-1971-3b7e-bd27-af2d826d7084

Wayman, J. L. (2001). Fundamentals of Biometric Authentication Technologies. *International Journal of Image and Graphics, 1*(1), pp. 93-113. doi:10.1142/S0219467801000086

Velásquez, I., Caro, A. & Rodríguez, A. (2018). Kontun: A Framework for recommendation of authentication schemes and methods. *Information and Software Technology, 96,* pp. 27-37. doi:10.1016/j.infsof.2017.11.004

Väestörekisterikeskus. (2017). Väestörekisterikeskuksen tunnistusperiaatteet. Haettu osoitteesta https://vrk.fi/documents/2252790/2448917/V%C3%A4est%C3%B6rekisterikeskuksen+tunnistusperiaatteet+FI/82b34cef-897d-46e8-832d-3ed626f7faf4/V%C3%A4est%C3%B6rekisterikeskuksen+tunnistusperiaatteet+FI.pdf

LIITE 1 KONTUN-VIITEKEHYKSEN PAINOARVOTAULUKKO

	Criteria	Importance	Value	Weight
SECURITY (S)	Importance of security	Security is a crucial aspect for the application	100	45%
		Security is an important aspect for the application	60	
		Security is a secondary aspect for the application	20	
	Information sensitivity	There is sensitive information for the company and the user	100	25%
		There is sensitive information for the company	75	
		There is sensitive information for the user	45	
		There is no sensitive information	20	
	Resistance to observation from third parties	The method should be resistant	100	10%
		The method does not need to be resistant	20	
	Resistance to Phishing	The method should be resistant	100	10%
		The method does not need to be resistant	20	
	Resistance to replay attacks	The method should be resistant	100	10%
		The method does not need to be resistant	20	
USABILITY (U)	Ease of use	The method necessarily needs to be easy to use	100	25%
		The method preferably needs to be easy to use	60	
		It is not necessary for the method to be easy to use	20	
	Ease of learning	A user should take no longer than a day to get used	100	25%
		A user should take no longer than a week to get used	60	
		The time that it takes to get used is not relevant	20	
	Authentication information recovery	The recovery process should be simple	100	10%
		The recovery process should be complex	20	
	Need of using a device	The method does not need the use of a device	100	10%
		The method can use a possession or biometric device	60	
		The method can use both a possession and a biometric devices	20	
	Authentication method's reliability	The method should never or hardly fail during authentication	100	30%
		The method should not fail occasionally during authentication	75	
		The method can fail occasionally during authentication	45	
		It does not matter how often the method fails	20	
COSTS (C)	Implementation Costs	Costs should not be over 10% of the project's budget	100	65%
		Costs should not be over 30% of the project's budget	60	
		There can be any costs regardless of the project's budget	20	
	Costs per user	The method should not present additional costs for each user	100	35%
		The method can present additional costs for each user	20	

(Velásquez ym., 2018.)