Anne Madetoja

Tapaustutkimus perusopetusoppilaiden todentamismenetelmistä

Tietotekniikan
pro gradu -tutkielma
25. toukokuuta 2021

Jyväskylän yliopisto

Informaatioteknologian tiedekunta

Kokkolan yliopistokeskus Chydenius

Tekijä: Anne Madetoja
Yhteystiedot: -
Puhelinnumero: -
Ohjaaja: Risto T. Honkanen
Työn nimi: Tapaustutkimus perusopetusoppilaiden todentamismenetelmistä
Title in English: Case study of authentication methods for primary school students
Työ: Tietotekniikan pro gradu -tutkielma
Sivumäärä: 66+8
Tiivistelmä: Tämän pro gradu -tutkimuksen tarkoituksena oli käydä lävitse perusopetusoppilaiden todentamismenetelmien vaihtoehdot. Koska todentamismenetelmän turvallinen käyttö ja se, että todentamismenetelmä on kunkin henkilön omassa henkilökohtaisessa käytössä, ovat tärkeitä tekijöitä henkilön yksityisyyden suojan toteutumisen kannalta. Tässä tutkimuksessa käydään myös lävitse perusopetusoppilaiden yksityisyydensuojaan toteutuminen ja toteutuuko tietosuojan vaatimukset. Tutkimuksen tutkimuskysymykset olivat: "Miten perusopetusoppilaiden identiteetinhallintaan liittyvä yksityisyyden suojan opetus toteutuu?", "Mitkä ovat perusopetusoppilaiden todentamismenetelmän toteuttamisen vaihtoehdot?" ja "Toteutuuko perusopetusoppilaiden identiteetin- ja pääsynhallinnassa tietosuojan vaatimukset?" Tutkimusmenetelmä oli tapaustutkimus. Tutkimus toteutettiin lomakekyselynä sekä teemahaastatteluna. Opetuksenjärjestäjät huolehtivat tietosuojan toteutumisesta ja oppilaiden yksityisyydensuojasta. Mutta opetus on laaja kenttä ja koska yleensä identiteetin- ja pääsynhallinta toteutetaan opetuksenjärjestäjän it-tuen puolesta ei todentamismenetelmien kehittämiseen ole mahdollisuutta laajalti. Tietosuojan toteutumiseen käytännössä tulisi vielä saada linjauksia ja menetelmiä kuinka tietosuojan toteutuminen opetuksessa saadaan käytäntöön. Tutkimuksen tuloksena voidaan yhteenvetona todeta, että todentamismenetelmän kehittämistä ei ole mietitty vaan nykytilaan ollaan pääsuuntaisesti tyytyväisiä. Perusopetusoppilaiden todentamismenetelmät vaativat kehittämistä, jotta pääsynhallinta täyttää tämänpäivän tietosuoja vaatimukset.
Avainsanat: Perusopetusoppilaiden identiteetinhallinta, identiteetin- ja pääsynhallinta, todentaminen
Abstract: The purpose of this Master's Thesis study was to go through the options for authentication methods for primary school students. Because the secure use of the authentication method and the fact that the authentication method is for each person's own personal use are important factors in achieving the protection of per-

son's privacy. This study also goes through the implementation of basic student privacy and whether data protection requirements are met. The research questions of the study were: "How is privacy education related to identity management for primary school students implementer?"," What are the options for implementing the primary school students authentication method?" and "Are data protection requirements met in identity and access management for primary school students?" The research method was a case study. The research was carried out as a questionnaire and a thematic interview. Education providers take care of data protection and the privacy of students. But teaching is a broad field and because identity and access management are usually implemented on behalf of the IT organizer of the teaching provider, there is no opportunity to develop authentication methods widely. For the implementation of data protection in practice, guidelines and methods on how to implement the implementation of data protection in teaching should be obtained. as a result of the study, it can be stated that the development of the verification method has not been considered, but the current situation is generally satisfying. Authentication methods for primary school students need to be developed in order for access control to meet today's data protection requirements.
Keywords: Identity management of primary school students, identity and access management, authentication

Sanasto

AD	Käyttäjähakemisto, hakemistopalvelu - Active Directory
AM	Pääsyn hallinta - Access Management
CoT	Luottamusverkosto federoídussa identiteetinhallinnassa - Circle of Trust
FIM	Identiteetinhallintajärjestelmä - Forefront Identity Management
GDPR	Yleinen tietosuoja-asetus - General Data Protection Regulation
GUA	Graafinen käyttäjän todennus - Graphical User Authentication
IAM	Identiteetin- ja pääsynhallinta - Identity and Access Management
ICT	Tieto- ja viestintätekniikka - Information and Communication Technology
IdM	Identiteetinhallinta - Identity Management
IdP	Identiteetin tarjoaja - Identity Providers
LDAP	Hakemistopalvelujen käyttöön tarkoitettu verkkoprotokolla - Lightweight Directory Access Protocol
MFA	Kirjautumisessa käytetään vähintään kahta todentamistapaa - Multi-Factor Authentication
PIN	Henkilökohtainen tunnusluku - A Personal Identification Number
Provisiointi	Käyttäjäobjektin ja siihen linkitettyjen attribuuttien luominen kohdejärjestelmään sekä muokkaaminen ja poistaminen (de-provisiointi) kohdejärjestelmästä
RBAC	Roolipohjainen pääsynhallinta - Role-Based Access Control
SP	Palvelun tarjoaja - Service Provider
SSO	Kertakirjautuminen - Single Sign-On
RP	Luotettava osapuoli - Relying Party

Sisältö

1 Johdanto

Perusopetuksessa opetuksen apuna käytetään erilaisia web-pohjaisia oppimisympäristöjä ja oppimispelejä sekä digitaalisia oppimateriaaleja. Oppilaalle luodaan sähköposti ja oppilas saa mahdollisesti käyttöönsä opetuksenjärjestäjältä tietokoneen tai mobiililaitteen. Voidakseen käyttää näitä digitaalisia ympäristöjä sekä kirjautua opetuksessa käytettäville laitteille, oppilas tarvitsee kirjautumiseen vaadittavan todentamismenetelmän tai -välineen, esimerkiksi käyttäjätunnuksen ja salasanan. Keskitetyn identiteetinhallinnan avulla perusopetuksessa olevalle oppilaalle luodaan digitaalinen identiteetti, jota ylläpidetään identiteetin elinkaaren ajan opetuksenjärjestäjän identiteetinhallintajärjestelmissä. Opetuksen identiteetin- ja pääsynhallinta on opetuksenjärjestäjän organisoimaa toimintaa ja tavoitteena on oppilaan sujuva, helppo ja turvallinen digitaalisten ympäristöjen käyttö opetuksessa.

Tieto- ja viestintäteknologia on olennainen osa monipuolisia oppimisympäristöjä [33]. Perusopetuksen opetussuunnitelmassa on vuosiluokittain määritelty laaja-alaisen osaamisen osa-alueet, joista osa-alue L3 määrittää, että oppilaita opetetaan tunnistamaan keskeiset turvallisuuteen liittyvät symbolit sekä suojaamaan yksityisyyttään ja henkilökohtaisia rajojaan [33]. Laaja-alainen osaamistavoite L5 määrittää tieto- ja viestintäteknologisen osaamisen [33]. Tieto- ja viestintäteknologian osa-alue jakaantuu neljään pääalueeseen, joista yksi on "Oppilaita opastetaan käyttämään tieto- ja viestintäteknologiaa vastuullisesti, turvallisesti ja ergonomisesti" [33]. Opetuksenjärjestäjät ovat määritelleet opetussuunnitelman tieto- ja viestintäteknologian osaamisen pääalueiden mukaiset oppijan taitotasotavoitteet eri luokka-asteille. Tieto- ja viestintäteknologian taitotasotavoite ensimmäisen luokan oppilaalle voi olla esimerkiksi, että oppilas ymmärtää käyttäjätunnuksen merkityksen tai ymmärtää käyttäjätunnuksen ja salasanan yksityisyyden suojaamisen merkityksen. Taitotasotavoitteet kasvavat oppilaan mukana.

Tässä pro gradu -tutkielmassa ongelmanasettelun lähtökohta oli perusopetuksen oppilaiden identiteetin- ja pääsynhallintaan liittyvä todentaminen, miten se on tällä hetkellä toteutettu? Mitkä tekijät vaikuttavat todentamismenetelmän valintaan? Mitä vaihtoehtoja on toteuttaa perusopetuksen oppilaan turvallinen ja käytettävä todentamismenetelmä? Ongelma rajattiin käsittelemään perusopetuksen 1-9 luo-

kan oppilaita ja erillisesti käsiteltiin vielä pienet 1-2 luokan oppilaat. Identiteetin- ja pääsynhallinta liittyy kunkin henkilön yksityisyyden suojaan. Ongelmanasettelussa tutkimukseen liittyvästä pääongelmasta muodostetaan tutkimuksen pääkysymys. Tutkimuksen johtoajatus kiteyttää tutkimuksen pääongelman, josta johdetaan osaongelmat [12]. Tutkimusongelmaksi muotoutui seuraava tutkimustehtävä: Mitä vaihtoehtoja on perusopetuksen oppilaille turvallisen ja käytettävän todentamismenetelmän valitsemisessa? Tutkimuskysymykset, joiden avulla tutkimusongelmaa lähdettiin selvittämään, olivat:

1. Miten perusopetusoppilaiden identiteetin- ja pääsynhallintaan liittyvä yksityisyyden suojan opetus toteutuu?

2. Mitkä ovat perusopetusoppilaiden todentamismenetelmän toteuttamisen vaihtoehdot?

3. Toteutuuko perusopetusoppilaiden identiteetin- ja pääsynhallinnassa tietosuojan vaatimukset?

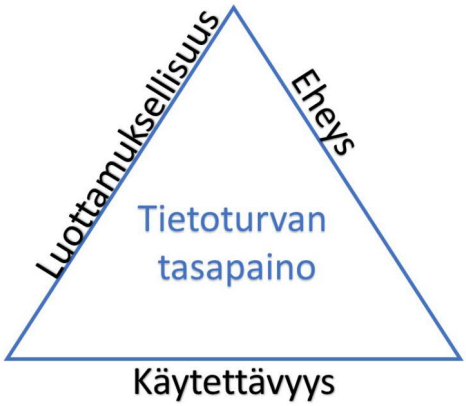
Pro gradu -tutkielma koostuu kirjallisuuskatsauksesta sekä empiirisestä tutkimuksesta. Kirjallisuuskatsauksen tavoitteena oli identiteetin- ja pääsynhallintaan liittyvän tietosuojan kuvaaminen sekä identiteetin- ja pääsynhallinnan osa-alueiden kuvaaminen. Empiirinen osuus toteutettiin tapaustutkimuksena, joka sisältää pienimuotoisen kyselytutkimuksen, teemahaastattelun sekä satunnaisesti valittujen kuntien tieto- ja viestintäteknologian taitotasotavoite dokumenttien tarkastelun.

Tapaustutkimuksen tavoitteena on ymmärryksen kasvattaminen eikä niinkään ratkaista ongelmaa. Tämän tutkimuksen tavoite oli niin ikään ymmärryksen lisääminen. Tutkimuksen tuloksena tuli esille, että todentamismenetelmien kehittämistä toivotaan. Tässä kehittämisessä näkökulma tulisi olla oppilaan ikäkauden ja valmiuksien mukainen todentamismenetelmä. Perusopetuksen oppilaat ovat vielä alaikäisiä lapsia ja heidän osaltaan henkilötietojen käsittelyn tietosuojalainsäädännön vaatimukset ovat tiukemmat. Vaadittavan tietosuojan toteuttaminen vaatii aktiivista kouluttamista ja ohjeistuksia. Opetuksessa käytetään nykyään monipuolisesti sähköisiä palveluita ja pääsääntöisesti tietosuoja toteutuu tyydyttävällä tasolla. Voidaan sanoa, että oppilaiden identiteetin- ja pääsynhallinta sekä todentaminen ovat opetuksenjärjestäjillä hallinnassa. Kehittämistoimenpiteitä kuitenkin tarvitaan, siinä missä yritykset kehittävät identiteetin- ja pääsynhallintaa sekä todentamista vahvan tunnistamisen suuntaan, on oppilaiden osalta tämä sama toiminta jäänyt kehityksestä jälkeen.

Tutkielman toisessa luvussa käydään lävitse tietosuojan ja tietoturvan perusteita henkilötietojen käsittelyssä. Kolmannessa luvussa käydään lävitse identiteetin- ja pääsynhallinnan osa-alueet. Näistä osa-alueista tarkemmin avataan todentamisenmenetelmät. Neljännessä luvussa käydään lävitse lapset ja nuoret digitaalisten palveluiden käyttäjinä tematiikkaa. Viidennessä luvussa käydään lävitse yleisimpiä tutkimus- ja aineistonkeruumenetelmiä sekä tämän tutkimuksen toteutus. Luvussa kuusi käydään lävitse empiirisen osion tuloksia. Luvussa seitsemän käydään tutkimukseen perustuvaa pohdintaa perusopetusoppilaiden todentamismenetelmien vaihtoehdoista ja luvussa kahdeksan on pro gradu -tutkimuksen yhteenveto ja johtopäätökset.

2 Tietosuoja ja tietoturva

Tietosuojan ja tietoturvan menetelmin suojataan sekä henkilöitä, tietoa että organisaatioita. EU:n yleinen tietosuoja-asetus (GDPR) tuli noudatettavaksi toukokuussa 2018. [1] Tietosuoja on perusoikeus, joka turvaa rekisteröidyn oikeuksien ja vapauksien toteutumisen henkilötietojen käsittelyssä [38]. Rekisteröity on henkilö, jonka tietoja käsitellään esimerkiksi tallentamalla tietojärjestelmiin. Tietoturva on yksi tietosuojan toteuttamisen keino, jonka avulla on tarkoitus suojata tietoaineisto ja tietojärjestelmät [38]. Tietosuoja perustuu lainsäädäntöön ja siinä on kysymys rekisteröidyn oikeuksista ja yksityisyyden suojasta. Tietoturva tarkoittaa muun muassa organisatorisia ja teknisiä toimenpiteitä, joilla varmistetaan tiedon luottamuksellisuus ja eheys, järjestelmän käytettävyys sekä rekisteröidyn oikeuksien toteutuminen [38].



Kuva 2.1: Luottamuksellisuus (Confidentiality), eheys (Integrity), käytettävyys (Availability), CIA triad

Toimintaympäristöt ovat muuttumassa yhä enemmän On-Premises toimintaympäristöistä pilvipalveluympäristöiksi, jolloin tietoturvan toteutumiseen ja tietoihin pääsyyn sekä ylläpitoon liittyvät vaatimukset kasvavat. Pilvipalveluissa tehokas

[1] Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus)

identiteetin- ja pääsynhallinta (IAM, Identity and Access Management) on merkittävä pilveen tallennettujen tietojen luottamuksellisuuden (Confidentiality), eheyden (Integrity) ja käytettävyyden (Availability) säilyttämiseksi [7]. Asiaa on havainnollistettu kuvassa 2.1. Luottamuksellisuus liittyy datan suojaamiseen luvattomalta käytöltä, eheys koskee tietojen oikeellisuuden suojaamista ei-toivotuilta muutoksilta, ja käytettävyydellä tarkoitetaan tietojen (ja järjestelmien) käytettävyyttä valtuutetuille henkilöille ja prosesseille tarvittavassa muodossa [48]. Tietojärjestelmien suojaamisessa ei enää riitä tekniikka suojaamaan hyökkäyksiltä, vaan ihmisestä on tullut kriittinen tekijä tässä turvallisuus prosessissa. Esimerkkinä tästä on salasanakäytännöt [10].

2.1 EU tietosuoja-asetus ja henkilötietojen käsittely

EU tietosuoja-asetuksen tavoitteena on tarkentaa ohjeistuksia henkilötietojen suojaamisessa digitaalisissa ympäristöissä. Tietosuojasääntelyiden avulla pyritään takaamaan ihmiselle oikeus yksityisyyteen sekä estämään hänen tietojensa tarpeeton ja epäasiallinen käyttö [16]. EU tietosuoja-asetusta sovelletaan kaikkeen automaattiseen henkilötietojen käsittelyyn sekä muuhun henkilötietojen käsittelyyn, kun henkilötiedot muodostavat rekisterin osan [26]. Henkilötietoja ovat tiedot, joiden avulla henkilö voidaan tunnistaa. Näitä ovat esimerkiksi nimi, osoite, biometriset tiedot ja viestitiedot. Henkilötietojen käsittelyllä (data processing) tarkoitetaan kaikkia toimintoja, joita kohdistetaan henkilötietoihin. Näitä toimintoja ovat esimerkiksi tietojen kerääminen, tallentaminen ja luovuttaminen [26].

EU:n yleisen tietosuoja-asetuksen mukaiset tietosuojaperiaatteet ovat käsittelyn lainmukaisuus, kohtuullisuus ja läpinäkyvyys, käyttötarkoitussidonnaisuus, tietojen minimointi, tietojen täsmällisyys, säilytyksen rajoittaminen sekä eheys ja luottamuksellisuus [26]. EU tietosuoja-asetus velvoittaa rekisterinpitäjää huolehtimaan siitä, että henkilötietoja käsitellään tietosuojaperiaatteiden mukaisesti koko henkilötietojen elinkaaren ajan. Henkilötietojen elinkaari tarkoittaa ajanjaksoa henkilötietojen keräämisestä niiden poistoon tai anonymisointiin. Asiaa on havainnollistettu kuvassa 2.2.

Henkilötietojen käsittelyn lainmukaisuuden mukaisesti käsittelylle on oltava aina jokin peruste, kuten suostumus, sopimus tai rekisterinpitäjän lakisääteinen velvoite [41]. Opetuksenjärjestäjän peruste henkilötietojen käsittelyyn opetuksen järjestämiseksi perustuu lakisääteiseen velvoitteeseen. Henkilötietojen käsittelystä on

Kuva 2.2: Henkilötiedon käsittelyn elinkaari [13]

kerrottava asianomaisille selkeästi ja ymmärrettävästi [41]. Henkilötietoja saa käsitellä vain nimenomaista ja laillista tarkoitusta varten ja vain niitä tietoja, mitkä ovat toiminnan toteuttamista varten olennaisia [41]. Henkilötietojen täsmällisyys ja säilytyksen rajoittamisen periaatteiden mukaisesti henkilötietojen oikeellisuuteen täytyy voida luottaa sekä tietoja saa säilyttää vain sallitun ajan [41].

Henkilötietojen käsittelyn tietosuojaperiaatteissa määritellään niin ikään käsittelyn luottamuksellisuus (Confidentiality), eheys (Integrity) ja käytettävyys (Availability). Tietosuojaperiaatteiden mukaisesti henkilötietoja tulee suojata luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta hävittämiseltä, tuhoutumiselta tai vahingoittumiselta [41].

Tietosuoja ja yksityisyyden suoja ovat tekniikan sekä kehittyvien toimintaperiaatteiden, käytäntöjen, instituutioiden sekä tarkoitusten kokonaisuus [37]. Jotta tietosuojaperiaatteet toteutuvat, palveluiden tarjoajien tulee ottaa tarjoamissaan sovelluksissa ja palveluissa huomioon tietosuoja-asetuksen vaatimukset. EU:n yleisen tietosuoja-asetuksen artiklassa 25 ”Sisäänrakennettu ja oletusarvoinen tietosuoja”

säädetään, että

- Yrityksiä/organisaatioita kannustetaan panemaan täytäntöön teknisiä ja organisatorisia toimenpiteitä käsittelytoimintojen suunnittelun alkuvaiheessa, jotta yksityisyys- ja tietosuojaperiaatteita suojellaan alusta saakka ('sisäänrakennettu tietosuoja') esimerkiksi tietojen pseudonymisointi ja salaaminen.

- Yritysten/organisaatioiden on oletusarvoisesti varmistettava, että henkilötiedot käsitellään korkea yksityisyydensuoja varmistaen (esimerkiksi vain välttämättömiä tietoja olisi käsiteltävä, lyhyt säilytysaika, rajoitettu pääsy) ja että henkilötiedot ovat oletusarvoisesti vain rajattujen henkilöiden käytettävissä ('oletusarvoinen tietosuoja') esimerkiksi sosiaalisen median alustojen käyttäjäasetuksien avulla rajoitetaan käyttäjien profiileihin pääsy vain rajoitetulle henkilömäärälle.

Keväällä 2020 koronapandemian vuoksi suuri osa peruskoulujen opetuksesta järjestettiin etäopetuksena. Etäopetuksen aikana oppiaineisiin soveltuvien sovellusten käyttö joutui opetuksen järjestämisen ja tietosuojan väliseen ristiriitaan. Koska etäopetustilanne oli Suomessa uusi, ei kaikille oppiaineille ollut suunniteltua ja testattua EU-tietosuojan vaatimukset toteuttavaa sovellusta. Etäopetuksen aikana tietoisuus siitä, miten ja milloin oppilaan profiilin voi lisätä mobiilisovelluksiin sekä mitä tietoja (attribuutteja) profiilia luodessa sovelluksen palveluntarjoajalle oppilaasta välitetään, aiheutti huolta niin huoltajissa kuin opetuksen järjestäjien kesken.

EU:n yleisessä tietosuoja-asetuksessa on otettu huomioon erityisesti lasten suojaaminen digitaalisissa ympäristöissä. EU:n yleisen tietosuoja-asetuksen voimaantulon myötä lasten ikärajan tarkennus digitaalisten palveluiden käytön suhteen tarkentui ja tarkoituksena on suojata lasten henkilötietoja. Tietosuojalainsäädännön henkilötietojen käsittelyn perusteissa avataan tarkemmin lasten henkilötietojen käsittely seuraavasti [15, s. 14]

> "Erityisesti lasten henkilötietoja on pyrittävä suojaamaan, koska he eivät välttämättä ole kovin hyvin perillä henkilötietojen käsittelyyn liittyvistä riskeistä, seurauksista, asianomaisista suojatoimista tai omista oikeuksistaan. Tällaista erityistä suojaa olisi sovellettava etenkin lasten henkilötietojen käyttämistä markkinointitarkoituksiin tai käyttäjäprofiilien luomiseen ja lapsia koskevien henkilötietojen keräämistä, kun käytetään suoraan lapsille toteutettuja palveluja."

Kyselyn Nuoret verkossa [27] vastausten mukaan nuoret eivät osaa ottaa huomioon sellaisia uhkia, kuten identiteettivarkaudet tai henkilötietojen kaupalliseen käyttöön liittyvät riskit. Tietosuojalainsäädännön avulla pyritään asettamaan palveluntarjoajat ja aikuiset vastuuseen nuorille tarjottavien digitaalisten palvelujen sopivuudesta ikä huomioiden. Nuorten eniten käyttämiä verkkopalveluja ovat WhatsApp ja YouTube [27]. Näitä molempia palveluja on mahdollista kuitenkin käyttää, vaikka nuoren ikä ei siihen riittäisikään. Lapsia ja nuoria ei voi edellyttää lukemaan ja ymmärtämään eri palvelutarjoajien tietosuojaselosteita palvelujen käytön hyväksymisen yhteydessä. Lastensuojelun keskusliiton mukaan [26]:

- Lapset tarvitsevat erityistä suojaa henkilötietojensa käsittelyssä, koska he eivät välttämättä tiedä henkilötietojen käsittelyyn liittyvistä riskeistä.
- Lapsen henkilötietoja käsittelevien tahojen tulee huomioida tämä erityinen suoja ja suunnitella järjestelmät ja prosessit sen mukaisesti.
- Lapsella on samat tietosuoja-asetuksen mukaiset rekisteröidyn oikeudet kuin aikuisella.
- Tarjottaessa tietoyhteiskunnan palveluja lapsille, on alle 13-vuotiaan kohdalla hankittava vanhemman tai muun huoltajan suostumus.
- Lapset tarvitsevat erityistä suojaa markkinointia vastaan.
- Lapsilla on oikeus saada tietoa henkilötietojensa käsittelystä ymmärrettävällä ja selkeällä tavalla.
- Oikeus tulla unohdetuksi koskee erityisesti lapsia.

Opinnäytetyön kohteena on perusopetusoppilaiden pääsynhallintaan liittyvä todentaminen. Pääsynhallinta on tärkeä osa tietoturvaa ja tietosuojaa. Oppimisympäristöt, joita oppilaat perusopetuksessa käyttävät, sisältävät muun muassa oppilaan oppimistehtäviä, tehtävien pisteytyksiä ja oppilaan portfolioita. Perusopetuksessa käytettävät digitaaliset ympäristöt tulee olla helposti saatavilla ja helposti käytettäviä. Jotta tämä toteutuu, saatetaan tinkiä luotettavuudesta, joka vaikuttaa tietosuojan ja tietoturvan tasoon heikentävästi. Tärkeä tekijä on myös, että oppilaille opetetaan oman yksityisyyden suojan tärkeys, jotta he osaavat suojata itseään myös vapaa-ajalla digitaalisissa ympäristöissä toimiessaan.

2.2 Tietoturva

Tietoturvalla tarkoitetaan tietojen, järjestelmien ja palvelujen suojaamista sekä normaali- että poikkeusoloissa hallinnollisten ja teknisten toimenpiteiden avulla [34]. Tietoturvan peruskäsitteet ovat [34]:

- Luottamuksellisuus (confidentiality).
- Eheys (integrity).
- Käytettävyys (availability).
- Pääsynvalvonta (access control).
- Osapuolten todentaminen (authentication).
- Kiistämättömyys (accountability).
- Tunnistaminen (identification).

Tietoturvallisuus rakentuu tiedon kolmen ominaisuuden - luottamuksellisuuden, eheyden ja käytettävyyden - turvaamisesta [34]. Näitä käsiteltiin myös aikaisemmin tässä luvussa. Luottamuksellisuudella tarkoitetaan sitä, että tiedot, järjestelmät ja palvelut ovat vain niihin oikeutettujen saatavissa eikä niitä luvatta paljasteta tai muutoin saateta sivullisten tietoon [34]. Luottamuksellisuuden yksi toteuttamiskeino on pääsynhallinnan mallintaminen siten, että käyttövaltuudet perustuvat esimerkiksi työtehtäviin. Eheydellä tarkoitetaan sitä, etteivät tiedot, järjestelmät tai palvelut ole laitteisto- tai ohjelmistovikojen, luonnontapahtumien tai oikeudettoman inhimillisen toiminnan seurauksena muuttuneet tai tuhoutuneet [34]. Käytettävyydellä tarkoitetaan sitä, että tiedot, järjestelmät ja palvelut ovat tarvittaessa niihin oikeutettujen esteettä hyödynnettävissä [34].

Näiden kolmen ominaisuuden rinnalle on lisätty tietoturvan tavoitteet, kuten pääsynvalvonta, osapuolten todentaminen, kiistämättömyys ja tunnistaminen. Tietoturvan tavoitteita on laajennettu, koska on katsottu, että nämä kolme (luottamuksellisuus, eheys ja käytettävyys) eivät riitä kattamaan tietoturvallisuuteen liittyviä tavoitteita. Pääsynvalvonnalla tarkoitetaan, että tietoa tai tietojärjestelmää ei voi käyttää ilman lupaa [34]. Pääsynvalvonta voidaan toteuttaa esimerkiksi siten, että kirjautuja todennetaan käyttäjätunnuksen ja salasanan avulla. Osapuolten todentamisella (autentikointi) tarkoitetaan osapuolten (henkilö tai järjestelmä) luotettavaa

tunnistamista [34]. Kiistämättömyydellä tarkoitetaan todisteiden luomista sen varmistamiseksi, ettei yksikään tietojen käsittelyn tai siirron osapuoli voi jälkikäteen kiistää osuuttaan siihen (juridinen sitovuus) [34]. Tietojen ja tietoaineistojen osalta kiistämättömyys voi koskea muun muassa tietoa siitä, kuka on muokannut tietoja [34]. Tunnistamisella tarkoitetaan menettelyä, jolla yksilöidään kohde, kuten käyttäjä tai järjestelmä [34]. Tunnistaminen ja todentaminen ymmärretään usein yhdeksi kokonaisuudeksi.

Henkilötietojen tietoturvaloukkauksella tarkoitetaan tapahtumaa, jonka seurauksena henkilötietoja tuhoutuu, häviää, muuttuu, henkilötietoja luovutetaan luvattomasti tai niihin pääsee käsiksi taho, jolla ei ole käsittelyoikeutta [42]. Tietoturvaloukkauksesta voi seurata esimerkiksi henkilötietojen valvomiskyvyn menettäminen, identiteettivarkaus tai petos [42]. Kun identiteettivarkaus tapahtuu, toinen henkilö esiintyy identiteettivarkauden kohteena, käyttämällä luvattomasti kohteen henkilötietoja. Identiteettivarkauksia tapahtuu myös nuorten keskuudessa. Nuorten tarkoituksena on usein pilailu, mutta toisinaan myös kiusaaminen.

Jotta tietosuojaperiaatteet eheys ja luottamuksellisuus toteutuvat ja EU tietosuoja-asetuksen mukainen tietojen suojaaminen luvattomalta ja lainvastaiselta käsittelyltä toteutuvat, täytyy rekisterinpitäjän osoittaa toteuttavansa vaadittavat tekniset ja organisatoriset toimenpiteet.

Teknisillä ja organisatorisilla toimenpiteillä tarkoitetaan esimerkiksi henkilöstön koulutusta, sisäisiä ohjeistuksia ja määräyksiä, salassapitosopimuksia ja -sitoumuksia, tilivalvontaa ja käytönvalvontaa, tietojen salausta, tietojen anonymisointia tai pseudonymisointia, tietojärjestelmien ja rekistereiden auditointeja, etäkäyttöyhteyksiä, käytönvalvontaa, teknisiä rajoituksia, tarkastus- ja valvontajärjestelmiä [25]. Hyvin suunniteltu ja toteutettu identiteetin- ja pääsynhallinta toteuttaa tietoturvan ominaisuudet ja tavoitteet.

3 Identiteetin ja pääsynhallinta

Kyberturvallisuuden sanaston mukaan identiteetinhallinta on menettely, jolla hallinnoidaan käyttäjien ja laitteiden tunnuksia, rooleja ja ryhmiä [47]. Tietojärjestelmissä ja sovelluksissa sekä palveluissa henkilöiden digitaalinen identiteetti koostuu henkilön ominaisuuksista ja kiinnostuksen kohteista. Näitä tietoja kerätään digitaalisen profiilin luomiseen, jotta henkilö voi käyttää suojattuja resursseja ja digitaalisia palveluita. Identiteetin- ja pääsynhallinta tarjoaa sovelluksiin ja palveluihin oikean pääsyn oikealle käyttäjälle oikeaan aikaan oikeasta syystä [30]. Identiteetinhallinta on toiminta, joka koostuu prosesseista, käytännöistä ja tekniikoista, joilla hallitaan käyttäjän identiteettien koko elinkaarta sekä käyttäjien pääsyä järjestelmän resursseihin yhdistämällä käyttäjän oikeudet ja rajoitukset [39]. Resursseja, joita identiteetinhallinnan avulla suojataan, voivat olla esimerkiksi tieto, eri palvelut, rakennukset tai tilat sekä omaisuus. Identiteetinhallinta oli aikaisempina vuosina yrityksen sisäistä toimintaa, jonka avulla hallinnoitiin rajatusti työntekijöiden tunnuksia ja pääsyä muutamaan järjestelmään ja ICT-alustoille [2]. Tänä päivänä identiteetinhallintaa hyödynnetään niin organisaation omien toimintojen tuottamisessa kuin palvelujen tuottamisessa asiakkaille. Identiteetinhallinta on muuttunut monimutkaiseksi prosessiksi, joka käsittelee monia sovelluksia käsittäen useita organisaatioita [2].

Identiteetinhallinnan avulla selkeytetään ja määritellään organisaation käyttöoikeuksien anomis- ja luovutustoimenpiteet, sekä käyttöoikeuksien muodostumiseen vaikuttavat vaatimukset. Samanaikaisesti pyritään tehostamaan palvelun tietoturvallisuutta. Identiteetin- ja pääsynhallinta muodostaa organisaation käyttäjähallinnan toimenpiteille yhtenäiset säännöt ja toteuttamismuodot tavoitteenaan saavuttaa seuraavat hyödyt [39]:

- Yhteisten sääntöjen ja käytäntöjen noudattaminen, organisaation identiteetin elinkaaren tapahtumien raportointi ja auditointi.
- Käyttökustannukset pienenevät identiteetin hallinnan automatisoinnin avulla ja kertakirjautumisen käyttöönotto parantaa tuottavuutta.
- Tietoturva paranee, käyttöoikeuksien toteuttaminen nopeutuu, tuki useille todennusmenetelmille.

- Tuottavuus paranee, henkilökohtainen käyttäjien pääsy tietoihin, palveluihin ja työkaluihin, laajennettu ja parannettu pääsy resursseihin yrityksen ulkopuolelta.

Identiteetinhallinnan yhteydessä identiteetillä tarkoitetaan sähköistä identiteettiä, joita kullakin reaalielämän identiteetillä voi olla useita, niin työ- ja opiskeluelämään kuin yksityiselämään liittyen. Identiteetinhallinnan toiminnan mukana jokaiselle käyttäjälle luodaan henkilökohtainen digitaalinen identiteetti, jonka mukana hän saa yksityisen tunnisteen, kuten käyttäjänimen tai kirjautumisnimen järjestelmään kirjautumista varten [39]. Identiteetinhallinnan automatisoiduilla prosesseilla hallinnoidaan digitaalisen identiteetin muodostumista tai poistumista sekä identiteettiin liittyviä muutoksia digitaalisen identiteetin elinkaaren aikana (kuva 2.2). Opetuksenjärjestäjän tarjotessa oppilaille opetuksenjärjestämiseen vaadittavia sovelluksia keskitetyn identiteetinhallinnan kautta, henkilö tunnistetaan ja hän kirjautuu omalle opetuksessa käytössä olevaan digitaaliseen ympäristöön. Tässä tilanteessa, jotta oikea digitaalinen profiili kohdentuu oikeaan henkilöön, palvelu vaatii kirjautujan tunnistamisen. Yksityisyydensuojan kannalta on tärkeää, että tunnistusratkaisu tukee myös pseudonyymiä tai anonyymia asiointia [36]. Kun asioinnin tunnistusratkaisuissa otetaan huomioon yksityisyyden suoja, on hyväksyttävä ainakin seuraavat periaatteet [36]:

- Kaikkia tapahtumia ei tarvitse tunnistaa. Tunnistaminen rajataan tapahtumiin, joissa se on tarpeen turvallisuuden ja yksityisyyden kannalta ja milloin tunnistettava on vapaasti suostunut tunnistettavaksi.
- Pitää tukea mahdollisuutta asioida ja toimia anonyymisti. Tästä mahdollisuudesta on kerrottava tunnistettavalle.
- Pitää tukea pseudonyymien käyttöä silloin, kun anonyymi asiointi ei riitä, mutta täydellistä tunnistusta ei tarvita.
- Tunnistaminen täytyy perustella ja perustelut julkistaa, jotta tunnistettava kykenee arvioimaan tunnistuksen tarpeellisuuden ja toimimaan sen mukaisesti.
- Annetaan tunnistettavalle mahdollisuus kontrolloida tunnistustaan.

Keskitetty identiteetinhallinta opetuksenjärjestäjän toiminnassa parantaa oppilaiden yksityisyydensuojaa henkilötietojen käsittelyssä. Yksityisyydensuojaan liittyviä tärkeitä näkökohtia liittyy muun muassa tietojen keräämiseen, tietojen käyt-

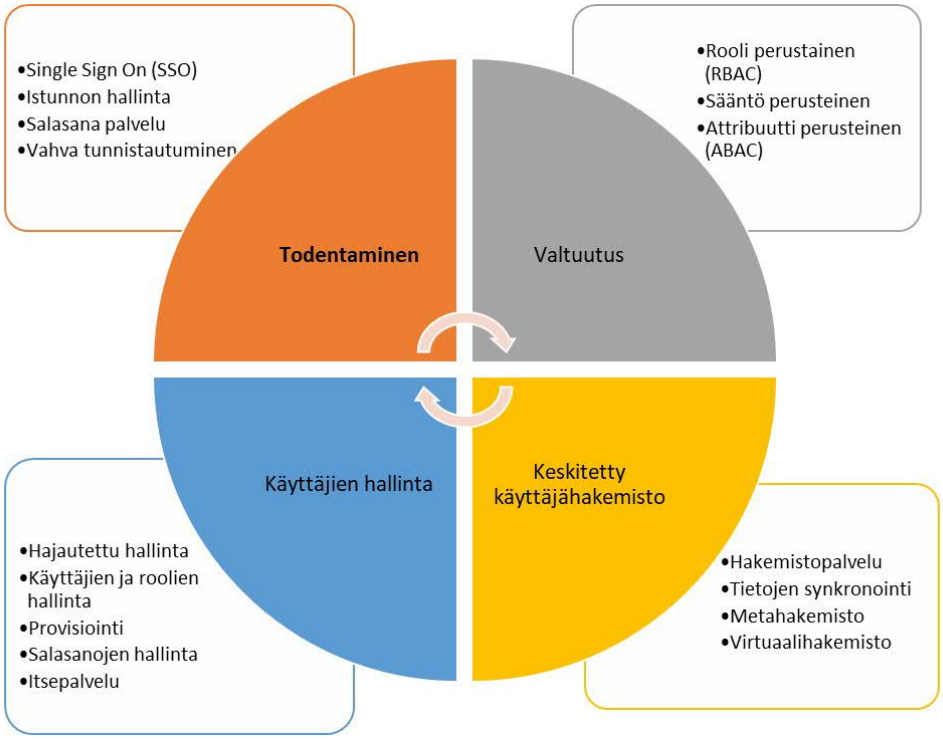
töön, tietojen tallentamiseen, tietojen minimointiin, anonymisointiin ja pseudonymisointiin sekä siihen, missä määrin henkilöt itse hallitsevat omia henkilökohtaisia tietojaan [1]. Keskitetyssä identiteetinhallinnassa henkilö ei yleensä pääse vaikuttamaan omaan digitaaliseen identiteettiin vaan se on organisaation identiteetin- ja pääsynhallinnan prosessin mukainen. Tässä prosessissa tuetaan henkilötietojen elinkaaren mukaista voimassaoloa, joten kun henkilön esimerkiksi oppilaan opiskelu opetuksenjärjestäjän oppilaitoksessa päättyy, samalla poistuu digitaalinen identiteetti. Huomioitavaa kuitenkin on, että yksityisten ja kaupallisten toimijoiden kuten Googlen, Facebookin organisoimaan identiteetinhallintaan ei oteta tässä pro gradu -tutkimuksessa kantaa.

Keskitetty identiteetin- ja pääsynhallinta opetuksessa tarkoittaa muun muassa sitä, että oppilailla on yksi digitaalinen identiteetti, jonka avulla heillä on oikeus käyttää heille opetuksenjärjestäjän mahdollistamia resursseja. Keskitetyn identiteetinhallinnan piirissä on yleensä opetuksenjärjestäjän hyväksymät sovellukset ja palvelut. Näiden palveluntuottajien kanssa on tehty opetuksenjärjestäjän puolesta keskitetysti henkilötietojen käsittelyyn liittyvät sitoumukset. Keskitetty identiteetinhallinta varmistaa myös henkilötietojen elinkaaren noudattamisen.

Siinä missä identiteetinhallinta tarkoittaa käyttäjän kannalta usein näkymättömissä tapahtuvaa käyttäjätiedon hallintaa ja virtaamista taustajärjestelmien välillä, pääsynhallinta tarkoittaa käyttäjälle näkyvää tapahtumasarjaa, jossa yksinkertaisimmillaan pyydetään käyttäjää antamaan käyttäjätunnuksensa ja salasanansa, ja onnistuneen tunnistuksen perusteella kerrotaan, onko käyttäjällä käyttöoikeus palveluun [28]. Pääsynhallinta tarkoittaa menettelyä, jolla varmistetaan, että käyttäjä, laitteet, sovellukset ja järjestelmät pääsevät käyttämään tietojärjestelmässä olevaa tietoa roolinsa mukaisesti [47].

Tyypillisessä identiteetinhallintajärjestelmässä voidaan erottaa kolme osapuolta: käyttäjät, identiteetintarjoajat (Identity Providers, IdP) ja luotettavat osapuolet (Relying Party, RP), joita voidaan kutsua myös palvelun tarjoajiksi (Service Providers, SP) [2]. Identiteetinhallinta prosessissa käyttäjä pyytää todentavalta osapuolelta (RP) palvelua, joka luottaa identiteetin tarjoajaan (IdP) toimittamaan todentamiseen liittyvät tiedot käyttäjästä [2]. Identiteetinhallinta vastaa käyttäjien ja käyttövaltuuksien hallinnasta ja niihin liittyvistä prosesseista työsuhteen tai opiskelusuhteen koko elinkaaren ajan (aloittaa työt, vaihtaa työtehtäviä, lopettaa työt) [4].

Yleisimmin identiteetin- ja pääsynhallinta jaetaan neljään osa-alueeseen kuten kuvassa 3.1 esitetään. Identiteetinhallinnan osa-alueita ovat tämän jaottelun mu-



Kuva 3.1: Identiteetin- ja pääsynhallinnan osa-alueet [13]

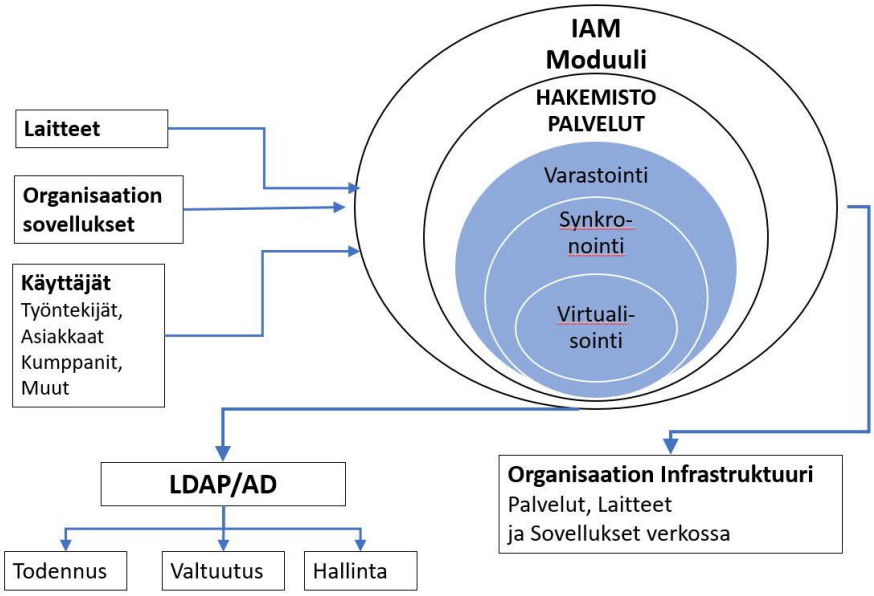
kaan keskitetty käyttäjähakemisto ja käyttäjien hallinta. Pääsynhallinnan osa-alueita ovat todentaminen ja valtuutus.

3.1 Keskitetty käyttäjähakemisto

Hakemisto on identiteetinhallintajärjestelmän keskeinen toiminto, joka tallentaa kaikki identiteetit ja niihin liittyvät tiedot järjestelmään käyttäjiltä, käyttäjäryhmiltä, palveluilta, palveluryhmiltä, resursseilta, resurssiryhmiltä jne [39]. Identiteetinhallinnan toiminnan piiriin voi kuulua erilaisia hakemistoja. Identiteetinhallinnan toiminnot ja sovellukset keskustelevat näiden muiden hakemistojen kanssa. Sovellukset ja pääsynhallinnasta vastaavat tietojärjestelmäpalvelut käyttävät hakemistoja sekä käyttäjien tunnistamiseen (autentikointi) että käyttövaltuuksien tarkistamiseen (autorisointi) [4]. Käyttäjähakemistosta käytetään myös nimitystä keskitetty käyttäjäarkisto. Keskitetty käyttäjähakemisto varastoi ja toimittaa identiteetti tietoja toisiin palveluihin ja tunnistaa käyttäjän antamat käyttäjätiedot [13]. Käyttäjä- ja käyttövaltuustietoja ei haeta koskaan identiteetin hallinnasta, vaan joko hakemistosta tai

kohdesovelluksesta itsestään [4].

Identiteetinhallinnan lähdejärjestelmänä toimii jokin toiminnanjärjestelmä, esimerkiksi taloushallintojärjestelmä, henkilöstöjärjestelmä tai oppilashallintojärjestelmä. Hallintajärjestelmän ytimen muodostaa keskitetty tietovarasto, jossa hallinnoidaan järjestelmän piirissä olevien käyttäjien ja heidän palvelujärjestelmissänsä olevien käyttövaltuuksien tietoja [45]. Tietovarasto voi olla käytännössä yhdistetty useista eri lähteistä, joita voivat olla käyttäjähakemistot, erilaiset tietokannat ja tiedostot [45]. Tätä keskitettyä tietovarastoa kutsutaan myös metahakemistoksi. Tietovaraston tietoja pidetään yllä lähdetietovarastoihin synkronoimalla sekä ennen kaikkea käyttövaltuuksien hallintaprosessien kautta [45]. Metahakemisto esittää identiteetit yhtenä näkymänä identiteetinhallintajärjestelmälle. Metahakemisto voi olla esimerkiksi SQL –tietokanta, joka on liitetty Active Directoryyn (AD) tai Lightweight Directory Access Protocol (LDAP) -järjestelmään. Kun hakemistot ja tietovarastot sisältävät henkilötietoja esimerkiksi käyttäjätietoja sekä käyttöoikeustietoja muodostavat ne henkilörekisterin tietosuoja ja tietoturva huomioiden.



Kuva 3.2: Kuvaus hakemistopalvelusta [7]

Hakemistotoimintoihin identiteetinhallinnassa ei ole olemassa yhtä selkeää mallia vaan toiminnot ja hakemistot sekä hakemistojen hierarkia määritellään organisaation tarpeiden mukaisesti. Kuvassa 3.2 on yksi esimerkki identiteetinhallinnan toteutuksesta. Hakemistopalveluratkaisu on kehitetty kolmen peruspalvelun ym-

pärille [7]:

1. Varastointi - ylläpitää identiteettejä.
2. Synkronointi - synkronoi identiteettitietoja useiden identiteettivarastojen välillä.
3. Virtualisointi - hyödyntää tunnistetietoja useista, heterogeenisista arkistoista ilman fyysistä datan siirtämistä.

Hakemistopalveluratkaisu on integroitu osa erittäin turvallista, saatavilla olevaa, tarkastettavaa ja yhtenäistä identiteetinhallintajärjestelmää (IDM) [7]. Identiteetinhallintajärjestelmä ja sovellukset vaativat vakiomekanismin, jolla pääsee identiteettimääritteisiin, kuten käyttäjäprofiilitietoihin (hallinta), käyttöoikeuksiin (valtuutus) ja käyttäjän tunnistetietoihin (todennus) [7]. Lightweight Directory Access Protocol (LDAP) tai Active Directory (AD) ovat yleisesti käytettyjä identiteetinhallintajärjestelmiä.

3.2 Käyttäjien hallinta

Digitaalisen identiteetin luominen ja identiteetinhallintaan kuuluva käyttäjien hallinta lähtee liikkeelle, kun henkilö kirjataan henkilöstöjärjestelmään, oppilashallintojärjestelmään tai muuhun identiteetinhallinnan lähdejärjestelmään. Digitaalisen identiteetin luomiseen määritellyt tiedot (attribuutit) siirtyvät yleensä automaattisen prosessin myötä identiteetinhallintajärjestelmään. Käyttäjien hallinta sisältää työkalut, joiden avulla identiteettejä voidaan lisätä, muokata ja poistaa hakemistosta sekä auditointityökalun. Esimerkiksi Microsoftilla Forefront Identity Management (FIM) on yksi identiteetinhallinnanjärjestelmä. Henkilön lisääminen identiteetinhallintajärjestelmään sisältää kullekin käyttäjälle toimintaan sopivien resurssien luomisen, kuten käyttöoikeuksien hallinnan [39]. Kuvassa 3.1 on kuvattu käyttäjähallinnan toiminnot, joita ovat muun muassa hajautettu hallinta, käyttäjien ja roolien hallinta, joka sisältää käyttöoikeuksien ylläpidon, henkilön provisiointi eli luominen järjestelmään ja myös deprovisiointi eli poistaminen kun henkilö ei ole enää organisaatiossa. Lisäksi käyttäjähallintaan kuuluu salasanojen hallinta ja itsepalvelu toiminnot. Käyttäjienhallinta käsittää käyttäjän digitaalisen identiteetin hallinnan järjestelmässä koko elinkaaren ajan [39].

Digitaalisen identiteetin luomisen yhteydessä identiteetinhaltija saa yksilöllisen tunnisteen, kuten käyttäjänimen tai kirjautumisnimen järjestelmään kirjautumista

varten [39]. Digitaaliseen identiteettiin sisältyy myös muita attribuutteja henkilöllisyyden määrittämiseksi ja yksilöimiseksi kuten esimerkiksi nimi, syntymäaika, osoite tai henkilötunnus, lisäksi muita mahdollisia järjestelmään liittyviä attribuutteja kuten rooli ja asema [39].

Käyttäjien hallinnassa osa käyttäjien ylläpitotoimista on keskitetty ja osa voidaan hajauttaa organisaatiossa käyttäjän yksikköön. Hajautetun ylläpidon tarkoituksena on identiteetinhallinta järjestelmätietojen parantaminen [13]. Käyttäjähallintaan kuuluvan itsepalvelutoiminnan avulla käyttäjä voi ylläpitää omia henkilöllisyystietoja, tarkastaa tietojaan sekä palauttaa salasanan ja anoa käyttöoikeuksia resursseihin.

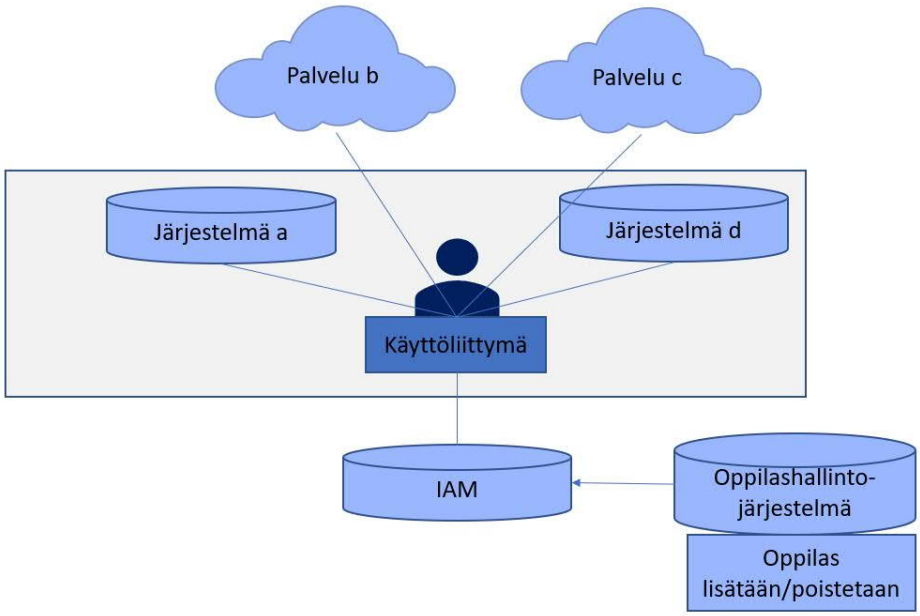
3.3 Todentaminen

Pääsynhallinnan yhteydessä puhutaan tunnistamisesta (identification) ja todentamisesta (authentication). Tunnistaminen on väite siitä, keitä me olemme, todentaminen sisältää väitetyn henkilöllisyyden tarkistamisen (verification) ja vahvistamisen (validation) [3]. Esimerkiksi tunnistaminen tapahtuu, kun käyttäjä antaa käyttäjätunnuksen ja todentaminen tapahtuu, kun hän antaa salasanan. Tässä tutkimuksessa käsitellään tunnistamista ja todentamista samana kokonaisuutena jatkossa todentaminen.

Todentaminen (Authentication) on prosessi, jolla käyttäjän, laitteen tai muun tekijän identiteetti tarkistetaan tietojärjestelmässä edellytyksenä järjestelmän käytön sallimiselle [32]. Todentamisen avulla kirjautujalle annetaan riittävät valtuudet kirjautua sovellukseen tai resurssiin [13]. Kun kirjautuja on todennettu, luodaan istunto, johon viitataan koko sen ajan, kun kirjautuja ja sovellus ovat vuorovaikutuksessa, kunnes sovelluksen käyttäjä kirjautuu ulos tai istunto lopetetaan muilla tavoin (esimerkiksi aikakatkaistaan) [13].

Pääsynhallinnan toteutustapa vaikuttaa siihen, kuinka kirjautuja pääsee identiteetinhallinnan piirissä oleviin järjestelmiin ja palveluihin, kirjautumalla jokaiseen erikseen tai kertakirjautumisella. Kertakirjautuminen on mekanismi, joka mahdollistaa käyttäjälle yhdellä kirjautumisella pääsyn tarvittaviin resursseihin [39]. Käyttäjän tarvitsee suorittaa todentaminen (esim. syöttää käyttäjätunnus ja salasana) vain kerran, ja sen jälkeen kaikki kertakirjautumisen piirissä olevat palvelut avautuvat käyttäjälle ilman uutta todentamista. Kertakirjautuminen on eri asia kuin yhden käyttäjätunnuksen ja -salasanan periaate, jossa palvelut ovat kyllä yhden ja saman

käyttäjätunnuksen ja salasanan takana, mutta ne tulee syöttää kuhunkin palveluun aina erikseen [28].



Kuva 3.3: Keskitetty identiteetinhallinta

Kertakirjautumisen (Single Sign-On, SSO), voidaan toteuttaa organisaation sisäisenä kertakirjautumisena siten, että organisaation sisäiset järjestelmät ovat kirjautujan käytössä, kun hän avaa todentamisen yhteydessä istunnon. Kun kertakirjautumisen piiriin on mahdollistettu organisaation ulkopuolisia toimijoita, puhutaan federoidusta identiteetinhallinnasta. Kuvassa 3.3 on esimerkki keskitetystä identiteetinhallinnasta. Kuvan mukaisesti kirjautuja kirjautuu käyttöliittymän kautta kerran ja organisaation sisäiset palvelut (järjestelmä a ja järjestelmä b) sekä organisaation ulkopuolisiin (palvelut b ja c) ovat kirjautujan käytössä tällä yhdellä kirjautumisella.

Kertakirjautumisen tietojärjestelmäpalvelu ei poista sovelluskohtaisia käyttäjätunnuksia ja salasanoja, vaan poistaa käyttäjän sisäänkirjautumistarpeen tallentamalla käyttäjän käyttäjätunnukset ja salasanat talteen ja syöttämällä ne käyttäjän puolesta kohdesovellukselle [4].

Federoidussa pääsynhallinnassa käyttäjä tunnistautuu jossain verkoston identiteetin tarjoajan palvelussa, jonka jälkeen palveluntarjoajat eivät enää vaadi häntä tunnistautumaan uudelleen, vaan luottavat alkuperäiseen tunnistukseen ja käyttä-

vät sitä käyttövaltuuspäätöksissään [4].

Federoitu pääsynhallinta perustuu luottamusverkkoon (Circle of Trust, CoT), joka muodostuu tyypillisesti identiteetin tarjoajista ja palveluiden tarjoajista [4]. Luottamusverkosto on yhtä kuin joukko palveluita, jotka kuuluvat yhdelle federaatiolle [2]. Palvelu voi kuulua useaan federaatioon ja siten kuulua useaan luottamusverkostoon [2]. Federoitu pääsynhallinta — tietojärjestelmäpalvelu, sisältää identiteetin tarjontaan ja palveluntarjontaa liittyvät tunnistuspalvelut ja tiedon välittämisen sekä luottamusverkoston tietojen ylläpitoon liittyvät toiminnot. Korkeakoulujen käyttämä HAKA ja perusopetuksessa sekä toisella asteella käytettävä MPASSid-käyttäjätunnistusjärjestelmät perustuvat federoituun identiteetinhallintaan. MPASSid on alun perin opetus- ja kulttuuriministeriön tarjoama tunnistusratkaisu. Vuoden 2021 alusta MPASSid palvelua ylläpitää Opetushallitus. Oppilaat voivat MPASSid avulla kirjautua niihin oppimisympäristöihin sekä niihin opetuksessa käytettäviin palveluihin, jotka ovat MPASSid luottamusverkoston piirissä ja opetuksenjärjestäjällä käytössä, koulun antamilla käyttäjätunnuksella ja salasanalla. Oppilas pääsee samalla käyttäjätunnus-salasanaparilla MPASSid palvelun piirissä oleviin palveluihin. MPASSid tunnistusratkaisu ei ole täysi federaatio kuten HAKA tunnistusratkaisu on. MPASSid luottamusverkoston piirissä oleviin palveluihin oppilaalla täytyy tehdä erillinen kirjautuminen.

Vapaa-ajan toiminnoissa Google ja Facebook tarjoavat valtuutusta omalla tunnuksellaan joihinkin palveluihin. Käyttäjän ei tarvitse keksiä uutta salasanaa jokaiseen kohteeseen. Jos esimerkiksi Facebook on kerran tarkistanut henkilöllisyyden, sen antama valtuutus riittää [16].

Todentamismenetelmien varmuuden taso vaatii joko yhden tekijän todennuksen (Single-Factor authentication) tai monen tekijän todennuksen (Multi-Factor authentication, MFA) käyttämällä jotain todennusteknologiaa [31]. Todentamismenetelmät jaotellaan kolmeen eri kategoriaan seuraavasti:

1. Todentamisväline, jonka todentamisvälineen haltija tietää, "Jotain, mitä tiedän" esimerkiksi salasana, PIN -koodi.

2. Todentamisväline, joka todentamisvälineen haltijalla on hallussaan, "Jotain, mitä minulla on" esimerkiksi mobiilitunnistautuminen.

3. Todentamisväline, joka perustuu todentamisvälineen haltijan johonkin fyysiseen ominaisuuteen, "Jotain, mitä minä olen" esimerkiksi sormenjälki tunnistautuminen.

Eri todentamismenetelmiä voidaan arvioida käytettävyyden, käyttöönoton helppouden ja turvallisuuden, joka sisältää yksityisyyden vaatimukset, näkökulmasta [8]. Seuraavissa alaluvuissa käydään lävitse joitain tunnetuimpia todennusmenetelmiä. Lisäksi alaluvussa 3.3.5 tarkastellaan sitä, miten todennusväline soveltuu perusopetusikäisten lasten käyttöön.

3.3.1 Tiedossa oloon perustuva todentamistekijä

Yleisimmin käytetty todentamismenetelmä on käyttäjätunnus ja salasana. A Memorized Secret -todentamismenetelmä on tarkoitettu käyttäjän itse valittavaksi ja muistettavaksi. Yleensä se viittaa salasanaan tai, jos todentamismenetelmä on numeerinen, viittaa se PIN–koodiin [31]. Kirjautujan tiedossa oleva todentamistekijöistä yleisimpiä ovat salasana, salalause, PIN–koodi tai graafinen salasana. Todentamistekijä perustuu kysymyksiin "Mitä tiedät?" ja "Mitä muistat?".

Kirjaimista, numeroista ja erikoismerkeistä muodostettu salasana käyttäjätunnuksen kanssa on tunnetuin ja käytetyin todentamismenetelmä. Salasanan muodostamiseen on useita ohjeita. NIST standardin mukaan, mikäli salasana on käyttäjän itsensä muodostama, täytyy se olla vähintään kahdeksan merkkiä pitkä ja mikäli salasana muodostetaan satunnaisena merkkijonona tai numeraalisena, pitää se olla vähintään kuusi merkkiä pitkä [31].

Järvisen [16] mukaan pitkä salasana ilman erikoismerkkejä on parempi vaihtoehto kuin kahdeksan merkkiä pitkä salasana, jossa on esimerkiksi prosentti-merkki. Petteri Järvinen viittaa salalauseeseen – menetelmää suositaan esimerkiksi kahdeksan merkkiä pitkän salasanan sijaan. Salalauseen muodostamisperiaatteina ohjeistetaan käyttämään erilaisia muistisääntöjä, esimerkiksi lempirunon sanojen ensimmäiset kirjaimet voivat muodostaa salalauseen.

Perinteinen salasana on helppo käyttää ja helppo ylläpitää. Vahvan salasanan eli monimutkaisen ja hankalasti muistettavan salasanan heikkous on, että se kirjoitetaan usein muistiin johonkin tallennusvälineeseen tai paperille. Kun samaa salasanaa käytetään useaan eri palveluun tai salasana vuotaa Internetiin, muodostaa se huomioon otettavan ongelman käyttäjähallintaan. Salasanojen perusongelmat ovat, että helposti muistettavan salasana on helppo hyökkääjän arvata tai etsiä ja pitkä, satunnainen ja vaihtuva salasana on vaikea muistaa [32].

Salasanojen määrä on suuri eikä niiden muistaminen ole enää hallittavissa. Salasanojen muistiin kirjoittaminen paperille tai kalenteriin ei ole suositeltavaa. Sen sijaan tietoturvallisempia ja suositeltavampia keinoja ovat salasanahallintasovelluk-

set tai salasanojen muodostamiseen luodut muistisäännöt. Erilaiset salasanakäytännöt olisi hyvä luoda myös käytettävän sovelluksen tai palvelun tietosisällön kriittisyys huomioiden. Vahvinta salausta vaativiin sovelluksiin luodaan vahvat salasanakäytännöt tai vahva tunnistautuminen ja ei niin kriittisiin tietosisältöihin helpommin muistettavat salasanakäytännöt.

Kuva 3.4: GUA recognation -menetelmä, käyttäjä valitsee viisi kuvaa, joiden avulla muodostaa graafisen salasanan

Graafinen käyttäjän todennus (Graphical User Authentication, GUA) graafisen salasanan avulla tarkoittaa käyttäjien todentamista kuvansyötön ja hiiren/kynän, kosketusnäytön tai eleiden avulla [22]. Graafisen käyttäjän todennuksen avulla tai graafisen salasanan avulla kirjaudutaan kuvaan perustuvalla salasanalla järjestelmään tai palveluun. GUA todennusmenetelmiä on kahdenlaisia: recall-menetelmä (palautusmenetelmä) ja recognition-menetelmä (tunnistusmenetelmä) [22]. Recall-pohjainen GUA-menetelmä vaatii käyttäjää muistamaan ja toistamaan piirustuksen, esimerkiksi taustakuvan avulla [22]. Recognition-pohjainen GUA-menetelmä vaatii

käyttäjää tunnistamaan ja valitsemaan kuvia tietystä ennalta valitusta kuvasarjasta. Tästä on esitetty esimerkki kuvassa 3.4 [22].

Recall-menetelmässä käyttäjä tunnistautuu esimerkiksi valitsemalla ennalta valitut pisteet kuvasta, jolloin kuvan valittujen pisteiden järjestys toimii salasanana. Recognition-menetelmä aiheuttaa vähiten kognitiivista taakkaa, koska kirjautujan täytyy vain valita vastaavatko esitetyt kuvat hänen muistamiaan kuvia [5]. Recall-menetelmässä vastaavasti käyttäjän täytyy muistaa salasana ilman mitään vihjeitä [5]. Käytettävyyden näkökulmasta graafinen salasana on helppo oppia ja mikäli salasana unohtuu, on graafinen salasana helposti palautettavissa [8]. Mikäli henkilöllä on erityisvaatimuksia esimerkiksi näkemiseen tai motoriseen toimintaan liittyviä vaikeuksia ei graafisen salasanan käyttö useinkaan tule kyseeseen.

A Personal Identification Number (PIN) on numeerinen salasana, jonka avulla käyttäjä kirjautuu järjestelmään [44]. PIN-koodi on salasanan tapaan käytettävä numerokoodi. ISO 9564-1 -standardi määrittää PIN-koodin minimipituudeksi 4 numeroa ja maksimipituudeksi 12 numeroa. Yleisimpiä PIN-koodin käyttökohteita on pankkikortin tunnusluku ja matkapuhelimen avauskoodi. Jotkut järjestelmät tarjoavat oletus PIN-koodin, joka ohjeistetaan ensimmäisen kirjautumisen yhteydessä vaihtamaan. PIN-koodi tulisi olla käytettävä ja turvallinen [23]. Käytettävä PIN-koodi on helppo muistaa ja turvallisuus lisääntyy, kun PIN-koodi vaihdetaan säännöllisesti, eri tileillä käytetään eri PIN-koodia ja PIN-koodi muodostetaan satunnaisena numerosarjana [23]. PIN-koodin luomista koskee samat säännöt kuin salasanan muodostamista, PIN-koodi ei saisi olla esimerkiksi syntymäpäivä tai muu helposti henkilöön johdettavissa ja helposti arvattava numerosarja esimerkiksi 1234. PIN-koodia käytetään, joko näppäilemällä numerosarja tai piirtämällä kosketusnäyttöön.

Tietoon perustuvaan tunnistautumiseen liittyvät tunnistautumismenetelmät ovat alttiita hyökkäyksille, kuten olan yli kurkkimiselle (shoulder surfing), brute force–hyökkäykselle, sanakirja-hyökkäykselle, arvaus-hyökkäykselle, vakoiluohjelma-hyökkäykselle ja sosiaaliselle käyttäjän manipuloinnille. Salasanakäytännöt (Password Policy) tehostavat tietoturvaa. Salasanakäytäntöjä ovat muun muassa ohjeistus, miten salasana luodaan ja hallitaan esim. pakottamalla käyttäjä vaihtamaan salasana säännöllisin väliajoin. Mitä pitempi salasana on, sitä vaikeampi se on murtaa. Järjestelmä voi pitää kirjaa aikaisemmista salasanoista, joten niitä ei voi toistaa uudelleen (vanhojen salasanojen valvonta). Salasanakäytäntöihin kuuluu myös tilin lukituskäytäntö, jossa tiettyjen ehtojen täytyttyä tili lukittuu.

3.3.2 Hallussapitoon perustuva todentamistekijä

Jotain, mitä minulla on todentamisvälineitä ovat esimerkiksi toimikortti, erilaiset token–laitteet ja mobiililaitteet. Toimikortti (älykortti, smart card) sisältää muistipiirin eli sirun, johon on upotettu yksityinen salausavain [16]. Toimikortti toimii kuten erittäin pieni tietokone, jossa on upotettu käyttöjärjestelmä, joka ohjaa sovelluksen suoritusta, pääsyn rajoituksia ja viestintää ulkomaailman kanssa [6].

Token on fyysinen laite, joka suorittaa todennuksen tai avustaa todennuksessa [32]. Token voi olla laite, joka sisältää salasanoja tai aktiivinen laite, joka antaa kertakäyttöisiä pääsykoodeja [32]. Pääsykoodi on salanumero, kuten salasana, sillä poikkeuksella, että se on laitteen generoima tai laitteeseen tallennettu, joten se voi olla pidempi, satunnaisempi ja ehkä muuttuva [32].

Token tarjoaa vahvan suojan esimerkiksi brute force-hyökkäystä vastaan, koska se voi tallentaa ja luoda paljon pidemmän salasanan, kuin muistettava salasana ja siten vähentää satunnaisen arvauksen riskiä. Token on kuitenkin altis varkauksille [32]. Token tunnistautumismenetelmää käytetään usein yhdistettynä toiseen todentamismenetelmään esimerkiksi salasanatodentamiseen. Kun token-laitetta käytetään todentamismenetelmänä yhdistettynä salasanaan, henkilön tarvitsee muistaa vain yksi salasana sekä token-laitteen pääsykoodi ja token-laite generoi useita pääsykoodeja todentamiseen, tällöin henkilön ei tarvitse muistaa useita monimutkaisia salasanoja. Token-laite tarjoaa salasanaan yhdistettynä turvallisen todentamismenetelmän. Mikäli token-laite katoaa sen puuttuminen on havaittavissa, mutta salasanan kaappaaminen voi jäädä huomaamatta. Lisäksi mikäli salasana joutuu vääriin käsiin ei tiliä voi hyödyntää ellei kaappaajalle päädy myös token-laite [32]. Token-laitteen avulla on myös mahdollista toteuttaa kertakirjautuminen käytössä oleviin palveluihin.

Mobiilivarmenne perustuu SIM-korttiin liitettyyn todennuskoodiin, joka avaa varmenteen ja todistaa kirjautujan henkilöllisyyden [16]. Mobiilitodentamisessa kirjautumisen yhteydessä palvelusta lähtee kirjautujan matkapuhelimeen tekstiviesti, jossa on satunnainen numerosarja [16]. Mobiilitodentamisen heikkous on, että puhelin täytyy olla aina kirjautumisen yhteydessä kirjautujan hallussa. Kun mobiilitodentaminen yhdistetään salasanaan, muuttuu todentaminen vahvaksi [16].

3.3.3 Luontainen todentamistekijä

Biometrinen tunnistus hyödyntää ihmisen yksilöllisiä ominaisuuksia. Esimerkiksi sormenjäljet, puheääni, kasvonpiirteet ja verkkokalvon rakenne ovat jokaisella ihmisellä erilaiset [16]. Biometrinen tunnistautuminen jaetaan kahteen kategoriaan [35].

1. Fysiologinen biometriikka: perustuu ihmiskehon osan suoriin mittauksiin. Sormenjälki, kasvot, iiris ja käsiskannaustunnistus kuuluvat tähän ryhmään.

2. Käyttäytymisen biometriikka: perustuu käyttäjän tekemästä toiminnasta saatuihin mittauksiin ja tietoihin, ja siten mittaa epäsuorasti joitain ihmiskehon ominaisuuksia. Allekirjoitus, kävely, eleet ja näppäinpainallukset kuuluvat tähän ryhmään.

Biometrisen tunnistautumisen menetelmässä järjestelmä tallentaa ensin näytteen käyttäjän biometrisistä ominaisuuksista käyttämällä sopivaa tunnistinta tunnistautumisen aikana - esimerkiksi kasvoja tunnistettaessa kameraa [14]. Tämän jälkeen näytteestä poimitaan merkittävimmät ominaisuudet, kuten sormenjäljen yksityiskohdat. Järjestelmä tallentaa ominaisuudet mallina tietokantaan yhdessä muiden tunnisteiden, kuten nimen tai identiteettinumeron kanssa [14]. Todentamiseksi käyttäjä esittää toisen biometrisen näytteen sensorille ja järjestelmä vertaa tätä näytettä tietokannassa olevaan malliin [14]. Järjestelmä hyväksyy identiteetin pyynnön vain jos vertailu tulos on ennalta määritetyn rajan yläpuolella [14].

Biometrisen tunnisteiden käytössä on omat ongelmat. Ihmisellä on rajattu määrä biometrisiä tunnisteita eivätkä ne ole korvattavissa. Biometrinen tunnistautuminen voi epäonnistua myös laiteongelmien vuoksi. Tällaisia ovat muun muassa sieppauslaitteen epäpuhtaus, huono valaistus tai järjestelmän sopeutumattomuus ympäristötekijöihin (kylmä, sade, auringon häikäisy) tai käyttäjien vaihtuminen päivittäin [32]. Linden mainitseekin kirjoituksessaan [28], että biometrisessä tunnistuksessa käytettävä tunnistusalgoritmi tyytyy siihen, että näyte ja mallinne kuuluvat esimerkiksi 99% todennäköisyydellä samalle henkilölle. Palvelun käyttö voi estyä tilanteessa, missä järjestelmä ei tunnista oikeaa käyttäjää, kun taas tunkeutuminen viittaa tilanteeseen, jossa järjestelmä tunnistaa kirjautujan väärin valtuutetuksi käyttäjäksi [14]. Tunnetuimmat biometrisen tunnistautumisen kohteet ovat muun muassa passi, rikostutkinta, puhelimelle kirjautuminen, kulunvalvonta. Biometrinen tunniste yhdistettynä sähköiseen identiteettiin muodostaa erityisen henkilötiedon. EU:n yleisen tietosuoja-asetuksen artikla 9 kieltää erityisiä henkilötietoja

koskevan käsittelyn ja määrittää soveltamisehdot milloin biometrisiä tietoja henkilön yksiselitteiseen tunnistamiseen saa käyttää.

Biometrisistä tunnistautumisista yksi tunnetuin ja käytetyin tunnistautumismenetelmä on sormenjälkitunnistautuminen. Juhani Korja on väitöskirjassaan Biometrinen tunnistaminen ja henkilötietojen suoja [24], jakanut biometrisen tunnistautumisen koviin ja pehmeisiin menetelmiin. Jako perustuu siihen, kuinka tunnistautuminen vaikuttaa yksilön yksityisyyteen ja muihin oikeuksiin [24]. Kovia tunnistautumismenetelmiä ovat esimerkiksi sormenjälki ja iiristunnistusmenetelmät. Koviin biometrisen tunnistamisen menetelmiin luetaan ne menetelmät, joilla on vaikutuksia yksilön fyysiseen koskemattomuuteen esimerkkinä sormenjälkitunnistus [24]. Pehmeät biometrisen tunnistamisen menetelmät ovat sellaisia, joiden vaikutus yksityisyydelle jää vähäisemmäksi ja eivät puutu yksilön fyysiseen koskemattomuuteen [24]. Pehmeitä biometrisen tunnistautumisen menetelmiä ovat esimerkiksi käyttäytymisen piirteisiin liittyvät tunnistusmenetelmät. Biometrisen tunnuksen ominaisuuksia ovat muun muassa [46]

- Universaalius, biometrinen ominaisuus on kaikilla ihmisillä.
- Ainutlaatuisuus, kahdella henkilöllä ei ole samanlaisia biometrisiä tietoja.
- Pysyvyys, biometristen tietojen ei tulisi muuttua ihmisen elämän aikana.
- Kerättävyys, biometrisen tunnuksen tulisi olla mitattavissa jollakin laitteella.
- Hyväksyttävyys, biometrisen ominaisuuden keräämistä ei vastusteta.

3.3.4 Monivaiheinen tunnistautuminen (MFA)

Multi-Factor Authentication (MFA) tarkoittaa vahvaa tunnistautumista tai monivaiheista tunnistautumista, puhutaan myös kaksivaiheisesta tunnistautumisesta. Vahvasta tunnistautumisesta ja sähköisistä luottamuspalveluista annetun lain (617/2009) 8 a §:n mukaan vahvassa tunnistautumisessa on käytettävä vähintään kahta erilaista todentamismenetelmää. Esimerkiksi pankkiautomaatilla asioidessaan henkilö käyttää todentamismenetelmiä mitä henkilöllä on hallussaan (sirullinen pankkikortti) ja mitä henkilö tietää (PIN-koodi). Yleisimmin käytössä on todentamismenetelmät: Jotain mitä omistan ja jotain mitä tiedän.

Identiteettivarkauksien ja tietojen kalastelun lisäännyttyä nykypäivänä suositellaan todentamisessa käytettävän vähintään kahta todentamistapaa kirjautumisen

yhteydessä, jolloin tunnistautuminen muuttuu vahvaksi (MFA). Monivaiheisesta tunnistautumisesta voidaan mainita esimerkkinä käyttäjätunnuksen ja salasanan lisäksi matkapuhelimeen lähetetty PIN-koodi. Matkapuhelimeen tekstiviestinä lähetettyjen PIN-koodien ongelma on mikäli matkapuhelinnumero vaihtuu, puhelin joutuu vääriin käsiin tai viesti on mahdollista kaapata. Toinen monivaiheinen todentamismenetelmä on käyttäjätunnuksen ja salasanan lisäksi token-laitteen avulla tapahtuva kirjautuminen. Tässä tilanteessa on mahdollista toteuttaa kirjautuminen kertakirjautumisena.

3.3.5 Lapset ja eri todentamismenetelmät

Kun verrataan tunnetuimpia todentamismenetelmiä PIN-koodia, salasanaa, biometristä todennusmenetelmää sekä erillisellä, esimerkiksi token-laitteella, tapahtuvaa todentamista ja lisäksi graafiseen salasanaan perustuvaa todennusmenetelmää, niin voidaan todeta kaikista löytyvän omat heikot ja hyvät puolensa lasten ja nuorten todentamismenetelmänä.

Kuten yllä jo todettiin käyttäjätunnus ja kirjoitettu salasana jäävät liian helposti heikon salasanan varaan. Salasanaan ei voida laittaa vaadittavaa vaikeusastetta, koska lapset eivät tätä muista ja mikäli siinä on erikoismerkkejä tuo se pienten lasten osalta myös ymmärtämisen vaikeuden. Koska PIN-koodi on useimmiten 4–6 merkkiä pitkä numerosarja, olisi tämä lasten kirjautumiseen varteenotettava vaihtoehto. Tunnetuin PIN-koodi on laitekohtainen. Tämä vaihtoehto aiheuttaa sen, että lapselta vaaditaan sovelluskohtainen kirjautuminen vielä erikseen. Kuvassa 3.5 on yhteenveto tunnetuimmista todentamismenetelmistä.

Mikäli henkilön täytyy muistaa useita salasanoja, johtaa se mahdollisesti siihen, että salasanasääntöjä ei noudateta niiden vaatimalla tasolla, vaan niistä joustetaan, jotta saadaan luotua muistettavia salasanoja. Fyysisen laitteen ongelmia ovat, että laite täytyy muistaa kantaa mukana ja sen mahdollinen katoaminen. Biometrisen todennuksen haaste on mahdolliset ongelmat tunnisteen lukemisessa sekä biometrinen tieto kuuluu erityisiin henkilötietoihin ja niiden käyttöä on rajoitettu.

Käyttäjätunnus ja salasana tunnistautumismenetelmänä luokitellaan heikoksi tunnistautumismenetelmäksi. Salasanan laadun vaatimuksilla voidaan parantaa tunnistautumismenetelmän tietoturvallisuutta. Salasana halutaan yleensä luoda helposti muistettavana, mikä heikentää tunnistautumisen vaadittavaa suojaa. Lapset luovat yleensä salasanoja, jotka sisältävät heidän henkilökohtaisia tietojansa tai joitain nuorten maailman termejä. Lapset ja nuoret uskovat, että näitä salasanoja on

	Tiedossaoloon perustuva todentamistekijä	Hallussapitoon perustuva todentamistekijä	Luontainen todentamistekijä
Yleisesti kutsutaan:	Salasanaksi, salaisuudeksi	Tokeniksi	Biometriseksi tunnistautumiseksi
Tukee todennusta	Salassapidon avulla	Hallussapidon avulla	Ainutlaatuisuuden ja personoinnin avulla
Turvallisuuteen liittyvä tekijä	Pidetään muistissa	Pidetään mukana	Vaikea väärentää
Digitaalinen esimerkki	Tietokoneen salasana	Avaimeton auton avaus	Sormenjälki
Turvallisuus ongelma	Salaisuus heikkenee jokaisen käytön jälkeen	Turvaton mikäli hukataan	Vaikea korvata

Kuva 3.5: Käytetyimmät todennusmenetelmät [32]

vaikea arvata [29]. Lapsilla ja nuorilla on luottamus siihen, että tunnistautumismenetelmiään ei käytetä väärin tai sillä ei ole merkitystä, mikäli he käyttävät heikkoa tunnistautumismenetelmää.

Graafinen salasana ei ole yleisesti käytetty vaikkakin Windows 10 sen tarjoaa kirjautumisvaihtoehtona. Windows 10:ssä puhutaan kuvasalasanasta. Henkilö valitsee tässä kirjautumistavassa kuvan, jota haluaa käyttää todennusmenetelmänä. Kuvan valittuaan kirjautujaa pyydetään piirtämään kolme kuviota, jotka voivat olla viivoja, ympyröitä ja napautuksia. Todentaminen tapahtuu toistamalla kuviot samassa järjestyksessä ja samassa paikassa kuvassa. Pienillä oppilailla graafinen salasana tai kuvaan perustuva salasana voisi olla toimiva ratkaisu.

Koska token-laite on altis menemään hukkaan sekä varkauksille, ei sitä tulisi käyttää ainoana todentamismenetelmänä [32]. Token-laitteen ja salasanan yhdistelmä todentamismenetelmänä tuo enemmän turvallisuutta kuin salasana yksinään [32]. Lasten todentamismenetelmänä käyttäjätunnus ja salasana yhdistettynä token-laitteen todentamismenetelmään voisi olla toimiva ja turvallinen ratkaisu. Biometrisen tunnistautumisen etuja ovat muun muassa [43]

- Yhden tai kahden sormen yhdistelmä on helpompi muistaa kuin monimutkainen salasana.

- Se on nopea käyttää.
- Biometrinen tunnistautuminen ei ole niin altis urkinnalle kuten arvaus-hyökkäykselle tai olan yli urkkiminen.
- Todentamismenetelmä on mahdollista lapsille, jotka vielä opettelevat lukemaan.

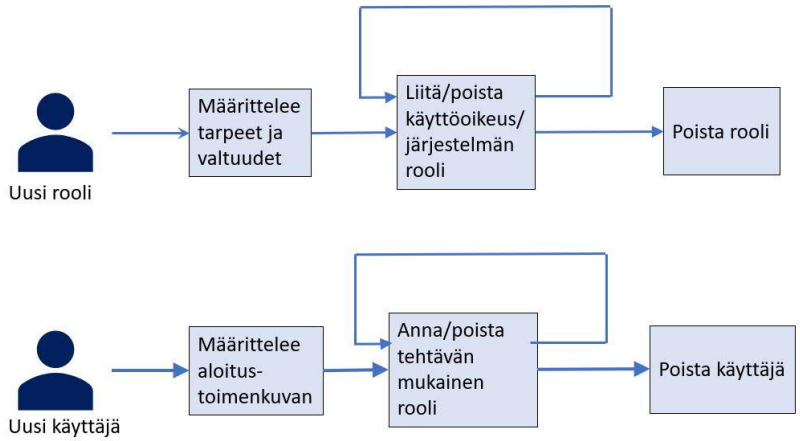
Kun lasten tunnistamiseen käytetään biometriikkaa, vaatii se erityistä huolellisuutta [46]. Lasten biometristen tietojen käyttöä tunnistautumiseen estää niin tekniset kuin eettiset syyt. Esimerkiksi lasten sormenjälkitunnistautuminen voi olla hankalaa mikäli lapsen sormet ovat vielä pienet. Lasten biometriikkaa käsiteltäessä on myös eettisiä näkökohtia. Lasten biometrisiä tietoja tulisi käsitellä erittäin huolellisesti, ja menettelyjen on oltava tietosuojaperiaatteiden mukaisia [46]. Huomioitavaa on myös, että lasten biometrisen tunnistautumisen käyttöön tulee vanhemmilta olla aina kirjallinen suostumus.

3.4 Valtuutus

Tunnistautumisen jälkeen järjestelmä tarkistaa identiteetille myönnetyt valtuudet, jonka jälkeen kirjautuja voi toimia valtuuksien mukaisesti järjestelmässä tai pääsy estetään. Tällöin kysymys on pääsynvalvonta päätöksestä (access control decision). Valtuutus on identiteetinhallinnan alue, joka määrittää, onko kirjautujalla oikeus käyttää tiettyä resurssia [13]. Valtuutus vastaa kysymyksiin, mitä on oikeus tehdä tai mihin on oikeus kirjautua. Valtuutus suoritetaan vertaamalla resurssiin pääsypyyntöä valtuutus käytäntöihin, jotka ovat varastoituina IAM käytäntövarastoon [13]. Valtuutus on päätös sallia tietty toiminto tunnisteen tai attribuutin perusteella [40].

Rooliin perustuvassa pääsynvalvonnassa (Role-Based-Access Control, RBAC) käyttäjän ja käyttövaltuuden väliin on luotu abstraktio: käyttäjälle annetaan rooleja, jotka kuvaavat esimerkiksi hänen työtehtäviään organisaatiossa. Käyttövaltuudet puolestaan annetaan rooleille [28]. Esimerkki kuva 3.6 havainnollistaa roolien ja käyttäjien toimenkuvan ja niihin liittyvien valtuuksien hallinnan elinkaarta [45]. Organisaatio muodostaa tehtäväkohtaiset roolit ja roolien käyttöoikeudet. Henkilölle liitetään käyttöoikeuteen hänen tehtävänsä mukainen käyttöoikeusrooli.

Työrooli (tai rooli) on käyttäjäryhmä, jossa on yksi tai useampi jäseniä [45]. Roolit on suunniteltava tukemaan tietoturva- ja liiketoimintasääntöjä [9]. Karkeimmillaan



Kuva 3.6: Roolien ja käyttöoikeuksien elinkaaret [45]

perusroolit voivat olla esimerkiksi oppilas ja opettaja. Opettaja rooli on mahdollista tarkentaa lisävaltuuksilla. Tällaisia voivat olla esimerkiksi erityisopettaja tai rehtori. Rooleihin perustuva identiteetin- ja pääsynhallinta selkeyttää käyttäjähallintaa vaikkakin roolien tunnistaminen ja määrittely voi olla työläs ja haastava tehtävä. Mikäli pääsynhallinnan valtuudet perustuvat rooleihin, täytyy roolit määritellä ennen identiteetin- ja pääsynhallintajärjestelmän käyttöönottoa. Organisaatio voi määritellä roolit esimerkiksi työntekijän perusrooleihin, jossa kaikilla organisaation työntekijöillä on esimerkiksi oikeus sähköpostiin ja kirjautuminen intraan. Tämän jälkeen roolit eriytetään esimerkiksi työtehtävien mukaisiin rooleihin. Työtehtäviin perustuvassa roolien määrittelyssä pääsynhallinnan haasteeksi muodostuu ristiin menevät roolit sekä työntekijän tehtävien vaihtoon liittyvät roolin muutokset.

Attribuuttiperusteinen pääsynhallinta (Attribute-Based-Access Control, ABAC) käyttää pääsynvalvonnassa joustavasti käyttöoikeuksien sijaan nimettyjä objekteja ja käyttäjäattribuutteja [9]. Attribuutteja ovat esimerkiksi nimitiedot ja työtehtävä. Attribuutti perusteisessa pääsynhallinnassa käyttöoikeus myönnetään, mikäli kirjautujalla on attribuutteja, jotka reflektoivat kohteessa, johon kirjautuja haluaa päästä [9].

4 Lapset ja nuoret digitaalisten palveluiden käyttäjinä

Lapset ja nuoret toimivat yhä nuorempina eri digitaalisissa ympäristöissä niin vapaa-ajalla kuin kouluaikana. Tietosuojalain (1050/2018) 5 §:n mukaisesti alle 13 -vuotiaan osalta vanhempainvastuunkantajan tulee antaa suostumus, mikäli lapsi tai nuori käyttää tietoyhteiskunnan palveluja, joihin hänen ikänsä ei riitä. Tietoyhteiskunnan palvelu tarkoittaa etäpalveluna sähköisessä muodossa palvelun vastaanottajan henkilökohtaisesta pyynnöstä toimitettava palvelu, joka toimitetaan siten, että osapuolet eivät ole samanaikaisesti läsnä [26]. Palveluja ovat esimerkiksi sosiaaliset mediat, blogialustat, videosivustot, online-pelit ja erilaiset pelisovellukset [26].

Perusopetuksen opetussuunnitelman [33] mukaisesti tieto- ja viestintäteknologia on olennainen osa monipuolisia oppimisympäristöjä. Uusia tieto- ja viestintäteknologisia ratkaisuja otetaan käyttöön oppimisen edistämiseksi ja tukemiseksi [33].

Digitaalisiin palveluihin kirjautuessaan käyttäjä luovuttaa henkilötietojaan palveluntarjoajalle. Käsiteltävät henkilötiedot riippuvat palvelusta, näitä voivat olla mm. käyttäjän nimi, syntymäaika, käyttäjätunnus tai paikkatieto. Nuorille tehdyn kyselyn mukaisesti nuoret ymmärtävät sosiaalisen median käyttöön liittyvät riskit osittain. Nuoret eivät kuitenkaan kyselyn mukaan maininneet riskeinä henkilötietojen luovuttamiseen ja käsittelyyn liittyviä uhkia kuten identiteettivarkaudet tai henkilötietojen kaupalliseen hyväksikäyttöön liittyvät riskit [27]. Lapsilla ei useinkaan ole ymmärrystä ja kiinnostusta siitä, kuinka he voivat suojata yksityisyyttään internetissä ja heikot salasanat lisäävät heidän turvattomuuttaan [29]. Lasten luomat salasanat ovat yksinkertaisia ja sisältävät henkilökohtaista tietoa heistä itsestään [29]. Kirjaimista, numeroista ja erikoismerkeistä muodostuva salasana on lasten käytössä haastava ja lapset unohtavat salasanan. Lapsia tulisikin opastaa muodostamaan salasanan lapsen ikä huomioiden. Graafisen salasanan ollessa käytössä lapset valitsevat mielellään salasanoihin kuvia, jotka kiinnostavat heitä, kuvat sisältävät yleensä leluja tai eläimiä [5]. Lasten on helpompi muistaa kuvia kuin merkityksettömiä sanoja. Tätä ominaisuutta on mahdollista hyödyntää myös salasanan muodostamisessa.

Suunniteltaessa lapsille todentamismenetelmiä, tulisi ottaa huomioon lapsen kognitiiviset kyvyt ja mieltymykset, koska näillä tekijöillä on merkittävä vaikutus lasten

kykyyn käyttää järjestelmiä [5]. Lasten on vaikea muistaa pitkiä kirjaimista ja numeroista sekä erikoismerkeistä muodostettuja hankalia salasanoja, etenkin jos nämä sanat eivät merkitse heille mitään.

Perusopetuksessa identiteetin- ja pääsynhallinnan menetelmät sisältävät mm. työasemalle kirjautumiseen tarvittavan tunnuksen, sähköpostin, oppimisympäristöihin ja oppimista tukevien peliympäristöihin kirjautumisen sekä opetusmateriaalit. Tänä päivänä todentamisen menetelmät ovat kehittyneet ja yhteiskunta panostaa yhä enemmän identiteetin suojaan digitaalisessa ympäristössä. Perusopetus ympäristössä oppilaiden todentamiseen liittyvät vaatimukset ovat kuitenkin jääneet kehityksestä jälkeen. Opetuksen tuomat muut vaatimukset painottuvat ja työasemmille sekä sovelluksiin kirjautuminen tunnin alussa halutaan toteuttaa helposti ja nopeasti.

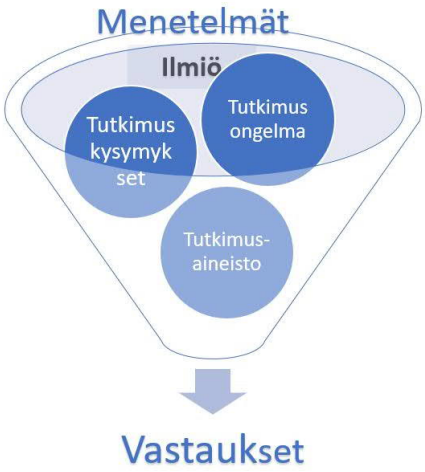
Digitalisaation vaatimukset opetuksessa ovat kuitenkin kasvaneet ja opetuksenjärjestäjillä on paineita kasvattaa opettajien ja oppilaiden osaamista digitaalisten oppimisympäristöjen ja oppimateriaalien käyttöön. Tämä tarkoittaa lähes suoraan sitä, että oppilaiden kirjautumiset erilaisiin web-palveluihin kasvaa ja kirjautumiseen liittyvien tunnusten määrä kasvaa.

Mikäli oppilailla ei ole käyttäjätunnusten ja salasanojen viidakko hallussa opetustunti menee helposti salasanojen muisteluun tai vaihtamiseen. Tämä tuo paineita toteuttaa oppilaiden kirjautuminen opettajavetoisesti.

Perusopetuksen opetussuunnitelman laaja-alaisen osaamisen osa-alueisiin kuuluu L5 tieto- ja viestintäteknologian osaaminen. Tieto- ja viestintäteknologian osaalueita ovat mm. että oppilas ymmärtää tieto- ja viestintäteknologian käyttö- ja toimintaperiaatteet sekä oppilaita opastetaan käyttämään tieto- ja viestintäteknologiaa vastuullisesti, turvallisesti ja ergonomisesti [33]. Tieto- ja viestintäteknologian turvallinen käyttö sisältää mm. oman identiteetin suojaamisen sekä huolehtimisen kirjautumiseen vaadittavista välineistä, käyttäjätunnuksesta ja riittävän vahvasta salasanasta. Vastuulliseen ja turvalliseen toimintaan liittyy että oppilaita opastetaan oman yksityisyyden ja identiteetin suojaamiseen.

5 Tutkimusasetelma ja tutkimuksen toteutus

Opinnäytetyön kohteena on ilmiö, johon liittyy jokin ongelma [19]. Tutkimusongelma muutetaan tutkimuskysymyksiksi, joihin saadaan vastaus tutkimusaineiston avulla [19]. Kuvassa 5.1 opinnäytetyön prosessi ilmiöstä vastauksiin, jossa ilmiöön liittyvät kysymykset ja tutkimusongelma käsitellään tutkimusaineiston avulla.



Kuva 5.1: Opinnäytetyössä ratkaistaan tutkimusongelma tutkimuskysymysten avulla (muokattu) [19]

Tutkimusten lähestymistapojen perusjaottelu perustuu laadulliseen (kvalitatiivinen) ja määrälliseen (kvantitatiivinen) tutkimukseen [19]. Tutkimusotteet (lähestymistavat) ovat kattokäsite ja muodostavat metodologian, jonka alapuolella ovat tutkimusmenetelmät (metodit) [21]. Määrällinen eli kvantitatiivinen tutkimus on tieteellisen tutkimuksen menetelmäsuuntaus, joka perustuu kohteen kuvaamiseen ja tulkitsemiseen tilastojen ja numeroiden avulla [18]. Määrällinen tutkimus perustuu täysin muuttujiin ja niistä tehtäviin operaatioihin [19]. Laadullinen eli kvalitatiivinen tutkimus on tieteellisen tutkimuksen menetelmäsuuntaus, jossa pyritään ymmärtämään kohteen laatua, ominaisuuksia ja merkityksiä [18]. Laadullinen tutkimus pyrkii ymmärtämään ja määrällinen yleistämään [19]. Laadullisessa tutkimuksessa on kyse mielipiteistä, ajatuksista ja sanoista [19].

Laadullinen tutkimus lähtee käytännöstä eli reaalimaailmasta ja pyrkii selittämään/ymmärtämään ilmiötä [20, sivu 99]. Lähtökohtana laadullisessa tutkimuksessa on todellisen elämän kuvaaminen [12]. Laadullinen tutkimus vastaa kysymykseen "Mistä tässä on kyse?" [19]. Laadullinen tutkimus tuottaa selityksen käytännöstä eli empiriasta, joten otetta kutsutaan myös induktioksi [19]. Induktio tarkoittaa etenemistä yksittäisestä yleiseen, eli yksittäisen tapauksen avulla pyritään yleistyksiin [19]. Laadullisessa tutkimuksessa tutkimuskohteena olevaan ongelmaan tuotetaan ymmärrys, mutta ongelmaa ei ole tarkoitus ratkaista tai poistaa, ongelmaan voidaan kuitenkin esittää tutkimuksen tuloksena syntyneitä ratkaisumalleja.

Laadullinen tutkimus on yläkäsite joukolle tutkimusmenetelmiä [19]. Jorma Kananen luettelee kirjassaan [19] Creswellin viisi laadullisen tutkimuksen alalajia:

1. Narratiivinen tutkimus, jossa käsitellään yksittäisen henkilön kertomuksia.
2. Fenomenologinen tutkimus, jossa tutkimuskohteena on useampi henkilö ja heidän eletty elämänsä.
3. Grouded theory -tutkimus, perustuu henkilöiden kokemuksiin ja on aineistolähtöinen, tavoitteena on luoda yhteisestä näkemyksestä teoria.
4. Etnografinen tutkimus, tavoitteena on kuvata ja selittää ihmisten toimintaa heidän ympäristössään tai ryhmän jäsenten tulkintoja ja käsityksiä ympäristöstään ja toiminnastaan.
5. Tapaustutkimus (case -tutkimus).

Tapaustutkimukseksi (case-tutkimukseksi) kutsutaan tutkimusstrategiaa, jossa tarkoituksena on tutkia syvällisesti vain yhtä tai muutamaa kohdetta tai ilmiökokonaisuutta [18]. Tapaustutkimus tarjoaa holistisen (kokonaisvaltaisen) ja syvällisen tutkimuksen, jossa hyödynnetään monia eri tietolähteitä [19]. Tapaustutkimuksessa tutkimuskohteena on usein yksi ilmiö, johon pyritään perehtymään syvällisesti ja antamaan hyvä kuva ilmiöstä [19]. Tapaustutkimuksessa tarkastellaan yhtä tai useampaa tapausta, joiden määrittely, analysointi ja ratkaisu on tapaustutkimuksen keskeisin tavoite [11]. Tapaustutkimuksessa on triangulaation piirteitä [21]. Triangulaatio tarkoittaa monimenetelmäistä tutkimusasetelmaa, jossa käytetään erilaisia lähestymistapoja, tiedonkeruumenetelmiä ja analyysimenetelmiä ilmiön ymmärtämiseksi [21]. Monimenetelmäisessä tutkimusasetelmassa osaan tutkittavan ilmiötä voidaan käyttää esim. määrällisen tutkimuksen kyselytutkimusta ja osaan laadullisen tutkimuksen teemahaastattelua [21].

Laadullisen ja määrällisen tutkimuksen yhdistelmiä ovat tapaus-, kehittämis- ja toimintatutkimus sekä konstruktiivinen tutkimus [21]. Näistä muutokseen tähtääviä tutkimuksia ovat toiminta-, kehittämis- ja konstruktiivinen tutkimus, joista käytetään nimitystä interventiotutkimus [21]. Tapaustutkimuksen vaatimukset ovat [19]:

- Ilmiö on tässä hetkessä.
- Tutkimus toteutetaan luonnollisessa ympäristössään (kontekstissaan).
- Tutkimusaineisto koostuu monista eri aineistoista (ja monista menetelmistä).
- Ilmiöstä halutaan saada syvällinen ja rikas kuvaus .
- Tutkimuskohteita (tapaus, case) on yleensä yksi (voi olla useitakin).

Tapaustutkimuksen tutkimuskysymykset ovat miten? ja miksi? [49]. Laadullisen tutkimuksen ja tapaustutkimuksen luotettavuustarkastelu poikkeaa määrällisen tutkimuksen luotettavuustarkastelusta. Tapaustutkimuksen tapausten valinnan yhteydessä ei voida puhua (tilastollisesta) otannasta tai yleistämisestä [19]. Laadullisessa tutkimuksessa tutkimukseen valittujen henkilöiden valinnassa tärkeintä on valita juuri tähän tutkimukseen oikeat henkilöt ja tutkittavien määrällä ei ole merkitystä. Tavoitteena on valita juuri ne henkilöt, jotka tietävät tutkittavasta ilmiöstä eniten [21].

Luotettavuusmittareina käytetään reliabiliteettia ja validiteettia [21]. Reliabiliteetti tarkoittaa tutkimustulosten pysyvyyttä ja validiteetti sitä, että on tutkittu oikeita asioita [21]. Tutkimuksen validiteetti eli se, että tutkitaan oikeita asioita, liittyy tutkimuksen suunnitteluun eli tutkimusasetelmaan ja osittain myös siihen, että aineiston analyysi (syy-seuraussuhteet) tehdään oikein [21]. Reliabiliteetti liittyy lähinnä tutkimuksen toteutukseen [21]. Luotettavuustarkastelussa on kyse tutkimusprosessin eri vaiheissa tehtyjen valintojen ja niiden toteutusten hyvyyden arvioinnista [21]. Jotta tapaustutkimusta voitaisiin pitää laadukkaana eli luotettavana, on perusedellytys, että kaikki tutkimusprosessin valinnat on kirjattu ylös ja valinnoille on esitetty perustelu [21]. Dokumentaatio kohdistuu tutkimusprosessin vaihdeiden, lähtökohtatilanteiden ja lopputuleman sekä menetelmien yksityiskohtaiseen kuvaamiseen ja kirjaamiseen [21].

5.1 Aineistonkeruumenetelmät

Tiedonkeruutavoilla tai aineistonkeruumenetelmillä tarkoitetaan periaatteita ja tapoja, joilla tutkimuksen empiirinen aineisto kootaan tutkijan käyttöön [17]. Määrällisessä tutkimuksessa käytetään kyselyä yleisimpänä aineistonhankintamenetelmänä [21]. Laadullisen tutkimusotteen aineistonkeruumenetelmiä ovat havainnointi, haastattelut, kyselyt ja dokumentit [21]. Näistä haastattelu on käytetyin menetelmä. Havainnoinnin käyttö on perusteltua tilanteissa, joissa ilmiöstä ei ole tietoa tai tieto on vähäistä [21]. Tapaustutkimuksen tiedonkeruumenetelminä käytetään sekä laadullisen että määrällisen tutkimuksen tiedonkeruumenetelmiä. Jorma Kananen kirjoittaa kirjassaan [19], että tapaustutkimus on eräänlainen palapeli, jonka tutkija kasaa eri tietolähteistä kokonaiskuvan saamiseksi. Tiedonkeruun ja aineiston hajanaisuus tekee tutkimuksesta nimenomaan tapaustutkimuksen [19].

Tapaustutkimuksessa aineistonkeruumenetelmänä voidaan hyödyntää valmiita dokumentteja. Valmiit dokumentit tuottavat lisämerkitystä tutkimukselle muiden tiedonkeruumenetelmien rinnalla. Valmiit dokumentit muodostavat niin kutsutun sekundääriaineiston. Sekundääriaineistoa ovat erilaiset dokumentit esimerkiksi tutkimukset ja tilastot. Ominaista näille dokumenteille on, että ne ovat olemassa olevia, niitä ei tuoteta tutkimusta varten [21]. Aineistonkeruumenetelmänä haastattelut voidaan jakaa kysymystyypin mukaan lomakehaastatteluun (kysely), teemahaastatteluun ja syvähaastatteluun (avoin haastattelu). Teemahaastattelu tarkoittaa kahden ihmisen välistä keskustelua aihe kerrallaan [21]. Teemahaastattelun avulla tutkija pyrkii ymmärtämään ja saamaan käsityksen (vangitsemaan) tutkimuksen kohteena olevasta ilmiöstä, jossa on aina mukana ihminen ja hänen toimintansa, jota tutkija pyrkii avaamaan teemojen avulla. Teemahaastattelulle on tyypillistä [21]

- Keskusteltavat aiheet
- Keskustelun eteneminen vastaajan ehdoilla.

Teemahaastattelu olisi hyvä käydä haastateltavan kanssa useaan kertaan. Aineisto analysoidaan heti haastattelun jälkeen ja toisella haastattelukerralla tarkennetaan avoimiksi jääneitä asioita. Teemahaastattelua varten laaditaan runko, jonka mukaan keskustelu etenee ja haastattelija voi tehdä tarkentavia kysymyksiä haastateltavalle. Teemahaastattelussa hyviä kysymyksiä ovat [21]:

- Avoimet kysymykset, ovat kysymyksiä, joihin ei voi vastata kyllä/ei vastauksella

- Jatkokysymykset, ovat asiaan liittyviä tarkentavia kysymyksiä, joita tulee esille haastattelun edetessä
- Hypoteettiset kysymykset, ovat muotoa "Mitä jos..". Oletuskysymysten avulla saadaan tietoa asioista, joista ei ehkä muuten saataisi tietoa.

Lomakekysely on pääasiassa kvantitatiivisen tutkimuksen tiedonkeruumenetelmä. Tapaustutkimuksessa lomakekyselyä voidaan käyttää yhtenä tiedonkeruumenetelmänä ilmiön kuvaamisen ja ymmärtämisen apuna. Lomakekysely on menetelmä, jossa aineisto kerätään standardoidusti ja jossa kohdehenkilöt muodostavat otoksen tai näytteen tietystä perusjoukosta [12]. Tapaustutkimuksessa tapausten valinnan yhteydessä ei kuitenkaan voida puhua (tilastollisesta) otannasta tai yleistämisestä [19]. Tapauksen valinnassa voidaan puhua harkinnanvaraisesta otannasta [19]. Lomakekysely toteutetaan nykyään pääasiassa sähköisenä kyselynä. Sähköinen lomakekysely mahdollistaa tulosten analysoinnin suoraan lomakkeelta. Lomakkeen laadinnassa tärkeää on kysymysten muoto. Kysymykset suositellaankin testattavaksi ennen varsinaisen kyselyn lähettämistä vastaajille. Kysymyksiä voidaan muotoilla yleensä kolmella tavalla [12].

- Avoimet kysymykset
- Monivalintakysymykset
- Asteikkoihin eli skaaloihin perustuvat kysymystyypit

Tapaustutkimuksessa haastateltavien määrä perustuu harkintaan siitä, milloin tutkimukseen on saatu riittävästi aineistoa ja haastattelujen sisältö alkaa toistaa itseään. Haastateltavia otetaan niin paljon, että vastaukset alkavat toistaa itseään, eli vastaukset/tulokset saturoituvat [19]. Saturaation saavuttaminen edellyttää tiedonkeruuja analyysivaiheen jatkuvaa vuorovaikutusta [19].

5.2 Analyysimenetelmät

Laadullisen aineiston analyysivaihe on syklinen prosessi, josta puuttuvat määrällisen tutkimuksen tiukat säännöt [21]. Analyysi on laadullisen tutkimuksen koko tutkimusprosessin eri vaiheissa mukana oleva toiminta, joka ohjaa itsessään tutkimusprosessia ja tiedonkeruuta [21]. Laadullisessa tutkimuksessa aineiston määrää ei voi etukäteen määritellä, sillä sitä kerätään niin kauan, kunnes tutkimusongelma ratkeaa [21]. Tämän vuoksi kerättyä aineistoa analysoidaan samanaikaisesti ja

mikäli todetaan, että aineisto ei ole vielä riittävä, jatketaan keräämistä. Laadullisen aineiston analyysi koostuu aineiston puhtaaksikirjoittamisesta (litterointi), aineiston koodaamisesta (tiivistäminen, hajottaminen), aineiston luokittelusta (kategorisointi) ja aineiston yhdistämisestä (laajentaminen) [21]. Aineiston litterointi on käytännössä äänitteiden ja muiden aineistojen kirjoittamista sellaiseen muotoon, että niitä voidaan käsitellä joko manuaalisesti tai automaattisesti. Tekstimuotoon kirjoitettu aineisto käsitellään siten, että sieltä etsitään pääteemat tutkimusongelmaan. Aineistoa voidaan lähestyä aineistolähtöisesti ja teorialähtöisesti [21]. Teoriapohjaisessa tarkastelussa aineistoa seulotaan ilmiötä selittävien teorian käsitteiden avulla [21]. Aineistolähtöisessä luokittelussa teksti luokitellaan aineistoista löytyvien ilmaisujen mukaan. Koodauksen avulla tiivistetty aineisto luokitellaan. Luokittelu (kategorisointi) tarkoittaa samaa tarkoittavien asioiden tai käsitteiden yhdistämistä [21]. Aineiston käsittelyn aikana täytyy pitää mielessä tutkimusongelma ja pitää siten mielessä mitä aineistosta etsii. Laadullisen aineiston analyysimenetelmät ovat teemoittelu, tyypittely, sisällönerittely, diskurssianalyysi ja keskusteluanalyysi [12].

Tapaustutkimuksessa käytetään tyypillisesti laadullisen tutkimuksen analyysimenetelmiä. Tapaustutkimuksessa analyysi koostuu aineiston tarkastelusta, luokittelusta, taulukoinnista sekä aineiston yhdistelystä, jotta voidaan tehdä empiirisesti perusteltuja johtopäätöksiä [49]. Yin ehdottaa kirjassaan [49] että tapaustutkimustietojen analysointi aloitettaisiin kysymyksillä. Kysymysten kysymistä jatketaan kunnes on käsitelty tutkimuksen pääkysymykset. Aineistoa lukemalla ja kysymysten avulla etsitään vastauksia tutkimuskysymyksiin. Aineistosta etsitään esimerkiksi [19]

- Selitystä ilmiölle (mm. aikasarja, teoria, malli).
- Tyypillistä kertomusta.
- Toiminnan logiikkaa (prosesseja).
- Samanlaisuutta tai erilaisuutta.

Aineiston käsittelyn perusteella luodaan selitys tulkintamenetelmien avulla. Yin [49] on esittänyt viisi tulkintamenetelmää: Teorian/mallin vastaavuus (Pattern Matching), Selityksen rakentaminen (Explanation Building), Time-Series Analysis (Aikasarja-analyysi), Loogiset mallit (Logic Models), Tapausten välinen synteesi (Cross-Case Synthesis). Teorian/mallin vastaavuus menetelmässä tutkija vertaa tapaustutkimus aineiston analyysin tuloksia olemassa oleviin malleihin ja teoriaan. Tapaus-

tutkimuksen yleisin muoto on Kanasen [19] mukaan ilmiölle syvällisen ja rikkaan kuvauksen ja selityksen antaminen. Tässä selityksen rakentamisen tulkintamenetelmässä tulkinta kirjoitetaan tarinan muotoon tai kuvauksena ilmiöstä. Aikasarja-analyysissä tarkastellaan ilmiön ajallista kehitystä.

5.3 Tutkimuksen toteutus

Tässä tutkimuksessa tavoitteena on saada ymmärrys perusopetus oppilaiden todentamisen nykytilanteesta, ongelmista sekä mitä ratkaisumahdollisuuksia voisi olla perusopetusoppilaiden todentamisen kehittämiseksi. Mitä vaihtoehtoja on perusopetuksen oppilaille turvallisen ja käytettävän todennusmenetelmän valitsemiseksi? Jotta ilmiö voidaan kokonaisuutena ymmärtää, täytyy myös todentamisen kokonaisuuteen liittyvä identiteetin- ja pääsynhallinta toimenpiteenä, sekä tähän kiinteästi liittyvä tietosuoja ja tietoturva käydä tutkimuksessa lävitse. Perusopetuksen oppilaiden identiteetin- ja pääsynhallinta sekä siihen liittyvä todentamisen toteuttamiseen liittyy niin hallinnollinen, pedagoginen että taloudellinen näkökulma. Tapausta olisi mahdollista tarkastella myös lasten kehityksen ja siihen liittyvien eri ikäkausina kehittyvien kognitiivisten taitojen kautta.

Tutkimuksen empiirinen osuus on toteutettu tapaustutkimuksena. Tapaustutkimuksen avulla voidaan toteuttaa monipuolisesti eri tutkimusmenetelmiä ja saada siten monipuolinen kuva tutkittavasta ilmiöstä. Empiiriseen osioon aineistonhankintamenetelminä käytettiin sähköistä lomakekyselyä sekä teemahaastattelua. Lisäksi tarkasteluun otettiin eri kuntien dokumentointia perusopetuksen tvt-taitotasojen opetuksesta. Sähköinen lomakekysely toteutettiin ensin. Sähköisen lomakekyselyn haasteena on kyselyn tekijän etäinen asema vastaajaan, jolloin kyselyyn on helppo jättää vastaamatta. Tapaustutkimuksessa ei ole tarpeen saada vastauksia suuria määriä, vaan vastausten määrä on riippuvainen tulosten saturaatiosta. Kun vastaukset alkavat toistamaan itseään ei kysymyksiä tai haastatteluja ole tarpeen jatkaa. Lomakekyselyn aiheet ja teemahaastattelun keskustelujen teemat noudattivat samaa linjaa. Eroavaisuus vastauksissa näkyi vastaajan työskentelypiirin mukaan, vaikkakaan tämä ilmiö ei ollut suuri. Esimerkiksi opettajien vastaukset noudattivat hyvin toiminnanläheistä näkökulmaa oppilaiden kannalta. Tässä luvussa käydään lävitse tutkimuksen empiirisen osan toteutusta, aineiston hankinta sekä aineiston analyysimenetelmät.

Kirjallinen aineisto koostuu eri kuntien tieto- ja viestintäteknologian opetukses-

sa osaamisalueiden taitotasotavoitteista. Taitotasotavoitteita analysoidaan lomakekyselyn ja teemahaastattelun rinnalla ja ymmärryksen lisäämisen tukena. Tapaustutkimuksessa kirjallista aineistoa voidaan käyttää empiirisessä osuudessa ilmiön selittämiseen ja ymmärryksen lisäämiseen. Tässä tutkimuksessa nämä valmiit dokumentit toimivat muun aineiston tukena. Lomakekyselyyn ja teemahaastatteluun valitut henkilöt mietittiin ja valittiin heidän tähän tutkimukseen liittyvän asiayhteyden eli organisaation, työnkuvan ja aseman perusteella. Koska lomakekyselyn ja teemahaastattelun tavoite on perusopetuksen todentamiseen liittyvän nykytilan ymmärtäminen, vastaajaksi valitut henkilöt haluttiin eri toiminnan alueilta mutta siten, että heidän työnkuvansa liittyi opetukseen.

Lomakekysely

Lomakekysely toteutettiin Webropol-ohjelmalla tehdyllä sähköisellä lomakekyselyllä. Kyselylomake on esitetty liitteessä A. Kysely toteutettiin syksyllä 2020 ja kyselytutkimus lähetettiin kahteentoista kuntaan, vastauksia kyselyyn tuli kuitenkin vain kolme. Vallitseva koronapandemia oletettavasti aiheutti, että kyselyyn vastauksia tuli niukasti. Kyselyn tavoitteena oli kartoittaa, miten perusopetuksen identiteetin- ja pääsynhallinta on eri opetuksenjärjestäjien hallinnoimana toteutettu, miten todentaminen on toteutettu ja mitä haasteita todentamiseen liittyy. Kyselytutkimus sisälsi sekä määrällisesti mitattavia että laadullisesti mitattavia avoimia kysymyksiä. Lomakekyselyn analysoinnin yhteydessä tulokset muutettiin taulukkomuotoon teemoittain. Vapaan tekstikentän vastaukset luokiteltiin aineistosta löytyvien ilmaisujen perusteella. Tämän avulla etsittiin teemoittain vastauksia tutkimuskysymyksiin.

Teemahaastattelu

Toisena tiedonkeruumenetelmänä käytettiin teemahaastattelua. Teemahaastattelu runko on esitetty liitteessä B. Koronapandemian vuoksi ja koska haastattelija ja osa haastateltavista sijaitsi pitkien välimatkojen päässä, teemahaastattelu toteutettiin Teams-yhteyden avulla. Haastateltavia oli viisi henkilöä. Teemahaastattelua varten tehtiin haastattelurunko, joka loi keskusteluaiheet. Tyypillisen teemahaastattelun mukaisesti keskustelu eteni haastateltavan ehdoin. Haastattelussa annettiin pääsääntöisesti rungon mukaisesti aihe, joka toimi keskusteluun johtavana kysymyksenä. Teemahaastattelu runko sisälsi avoimia kysymyksiä, joiden avulla haastatelta-

vaa pyydettiin arvioimaan nykytilaa. Lisäksi haastateltavaa pyydettiin vastaamaan muutamaan hypoteettiseen kysymykseen. Näiden hypoteettisten kysymysten avulla pyrittiin saamaan syvempää näkemystä haastateltavan näkemyksistä perusopetuksen oppilaiden todentamismenetelmän kehittämismahdollisuuksiin sekä halukkuuteen tai mahdollisuuksiin kehittää todentamismenetelmiä. Haastattelija kirjasi ylös haastattelun kulun, haastattelun nauhoitusta ei käytetty.

Teemahaastattelu aineisto kirjoitettiin haastattelun aikana Word-tekstinkäsittelyohjelmalla. Haastatteluja ei äänitetty, joten aineiston varsinaista litterointia ei tehty materiaalin käsittelyn alkuvaiheessa. Alkuperäiset haastatteludokumentit kirjoitettiin puhtaaksi. Tämän jälkeen haastatteluaineisto luokiteltiin teemoittain. Lomakekyselyn kysymykset ja teemahaastattelu noudattivat kolmea teemaa, joita olivat tietosuoja, identiteetin- ja pääsynhallinta sekä todentaminen, joten tulosten teemoittelu noudatti tätä samaa teemajakoa. Teemahaastattelun aikana keskustelu lähtee helposti rönsyilemään ja niin oli tapahtunut myös joissain tämän tutkimuksen haastatteluissa, joten tulosten läpikäymisessä karsittiin luokitellusta aineistosta pois tulokset, jotka eivät vastanneet tutkimuskysymyksiin.

6 Tutkimuksen tulokset

Tämän pro gradu -tutkimuksen tutkimuskohteena oleva ilmiö on perusopetusoppilaiden todentaminen, miten se tapahtuu ja mitä ongelmia siihen liittyy. Teoriaosiossa käsiteltiin tietosuoja sekä identiteetin- ja pääsynhallinnan osa-alueet, joita ovat keskitetty käyttäjähakemisto, käyttäjien hallinta, todentaminen ja valtuutus. Jotta kokonaiskuva identiteetin- ja pääsynhallinnasta muotoutuu, on nämä avattu teoriaosuudessa kukin omana osionaan. Lomakekyselyssä ja teemahaastattelussa sivutaan identiteetin- ja pääsynhallinnan merkitystä yksityisyyden suojan näkökulmasta.

Empiirisessä tutkimuksessa sähköinen lomakekysely sekä teemahaastattelu käsittivät neljä teemaa, identiteetin ja pääsynhallintaan liittyvä yksityisyys, perusopetuksen oppilaiden todentamismenetelmät, perusopetuksen oppilaiden identiteetin- ja pääsynhallintaan liittyvä tietosuoja sekä 1-2 luokan oppilaiden todentamiseen liittyvät haasteet. Tässä luvussa esitellään tutkimuksen tuloksia. Tutkimuksen tulokset esitellään teemoittain. Kolme teemaa muodostavat tutkimuskysymykset

1. Miten perusopetusoppilaiden identiteetin- ja pääsynhallintaan liittyvä yksityisyyden suojan opetus toteutuu?
2. Mitkä ovat perusopetusoppilaiden todentamismenetelmän toteuttamisen vaihtoehdot?
3. Toteutuuko perusopetusoppilaiden identiteetin- ja pääsynhallinnassa tietosuojan vaatimukset?

Neljäs teema 1-2 luokan oppilaiden digitaalisten ympäristöjen käyttö liittyy näihin kaikkiin kolmeen tutkimuskysymykseen. Sähköiseen lomakekyselyyn sekä teemahaastatteluun valikoidut henkilöt olivat eri toimialoilta kuitenkin siten, että kaikkien haastateltavien tehtävänkuva liittyy opetukseen.

6.1 Lomakekyselyn tulokset

Valtaosalla opetuksenjärjestäjien käytössä olevat identiteetin- ja pääsynhallintamenetelmät tukevat käyttäjätunnus ja salasana perusteista todennusmenetelmää. Näin

oli myös näissä kolmessa sähköisen lomakekyselyyn vastanneessa organisaatiossa. Yksi vastaajista ilmoitti, että he olivat harkinneet myös Microsoft-koodin mukaista todennusmenetelmää. Käyttäjätunnusperusteista todennusmenetelmää puolustaa opetuksessa muun muassa se, että se on edullinen ja helposti käyttöön otettavissa.

Kyselyyn vastanneiden opetuksenjärjestäjien kesken yksi vastaajista ilmoitti, että heillä on käytössä federoitu pääsynhallinta. Kahdessa muussa oppilailla on käytössä yhden käyttäjätunnuksen ja salasanan menetelmä. Toisin sanoen sama käyttäjätunnus ja salasana, mutta erillinen kirjautuminen käytössä oleviin järjestelmiin. Perusopetusoppilailla käytössä oleva MPASSid auttaa vähentämään tarvittavien erillisten käyttäjätunnusten ja salasanojen määrää. Mikäli opetuksessa käytetään sovellusta tai palvelua, joka ei kuulu MPASSid luottamusverkon piiriin, luodaan siihen oppilaille erillinen profiili ja kirjautumiseen vaadittavat tunnukset. Oppilaiden eri palveluihin käytettävien käyttäjätunnusten määrä kasvaa, mikäli opetuksenjärjestäjillä ei ole määritelty opetuksessa käytettävien sovellusten käyttöönottoprosessia. Kyselyssä tuli esille, että oppilaalla vaaditaan erillinen kirjautuminen keskimäärin neljään opetuksessa käytettävään palveluun. Vastaajien mukaan tämä johtaa siihen, että oppilailla on käytössään 1-4 käyttäjätunnus-salasanaparia eri palveluihin käytössään opetuksenjärjestäjän antamien AD-tunnusten lisäksi.

Kyselyssä pyydettiin mainitsemaan 1-3 kehitysehdotusta, miten perusopetusoppilaiden tunnistautumismenetelmää voitaisiin kehittää. Yksi kehitysehdotus oli, että

> "MPASS kaikille käyttöön, kaupallinen toimija mukaan lukien."

Toinen kehitysehdotus oli, että kirjautuminen pitäisi olla mahdollisimman helppoa ja nopeaa, mutta turvallista. Lisäksi alla vielä muutama kehitysehdotus, joita tuli kyselyssä esille.

> "YubiKey tai vastaava voisi olla hyvä ratkaisu, mutta toistaiseksi sen käyttöönottoon ei ole ollut resursseja."

YubiKey:llä viitataan erilliseen token-laitteen avulla tapahtuvaan kirjautumiseen. Tässä on kustannukseen liittyvät haasteet, mutta todentamismenetelmänä esimerkiksi yhdistettynä salasanaan token-laite on lasten käytössä toimiva ratkaisu.

> "Muutamat huoltajat vastustavat lapsen tietojen antamista sähköisiin järjestelmiin, sen vuoksi muuhun kuin hetuun tai nimeen perustuvan kirjautumisen pitäisi olla mahdollista."

"Oman salasanan vaihtomahdollisuus."
"Eriasteiset salasanat eri ikäluokille."
"Kokonaisvaltainen kertakirjautuminen."
"Keskitetty mahdollisuus hallita yhteistä työpöytää."

Mikäli opetuksessa oli käytössä sähköinen työpöytä, koettiin sen helpottavan sähköisten järjestelmien käyttöä ja käyttöönottoa. Lomakekyselyyn vastanneista organisaatioista yhdessä käytettiin toimintamallia, jossa oppilas pystyy hallinnoimaan tunnustaan itsepalvelun kautta. Niissä organisaatioissa, missä oppilaalla ei ole mahdollisuus hallinnoida tunnustaan, salasanan unohtaminen ja vaihtamisprosessi onkin usein tekijä, miksi käyttäjätunnus ja salasana halutaan pitää yksinkertaisina ja helposti muistettavana.

Kyselyssä kysyttiin myös pienten 1-2 lk oppilaiden digitaalisten palveluiden käytöstä ja niihin liittyvistä haasteista. 1-2 lk oppilailla on käytössä kyselyyn vastanneissa organisaatioissa muun muassa Wilma, sähköposti, Googlen tai Microsoftin opetukseen tarkoitetut ympäristöt. Pienten oppilaiden tunnistautumiseen liittyviä kehitysehdotuksia kysyttäessä tuli esille, että

"Käyttäjätunnus-salasana voi olla haasteellinen pienille ja graafinen kuvio voisi olla kokeilun arvoinen."

Kyselyssä tuli myös esille kehitysehdotus, että oppilaille pitäisi opettaa enemmän tunnusten hallintaa.

"Lisää opetusta tunnusten hallintaan yhtenä merkittävänä osana 1. ja toisen luokan opetusta."

Kyselyyn vastaajat ehdottivat myös, että salasanojen vaatimuksen kasvattaminen luokka-asteittain voisi olla kokeilemisen arvoinen ja siten 1-2 luokilla salasanojen vaatimukset olisivat matalammat. Tämä toki tuo vaihtoehtona riskin, että pienten oppilaiden käyttäjätilit ovat heikommin suojattuja ja siten alttiimpia identiteettivarkauksille.
Kysymykseen "Kuinka näette, että tvt-taitotaso käyttäjätunnuksen ja salasanan merkityksen opettaminen 1-2 lk oppilaille toteutuu?" tuli seuraavanlaisia vastauksia.

"Osassa kouluista oikein hyvin - osassa ei."

Myös näissä vastauksissa tuli esille se, kuinka opettajan kiinnostus ja osaaminen vaikuttaa siihen, miten opettaja opettaa oppilaille esimerkiksi tvt-taitotasoihin liittyviä taitoja. Mutta myös koulukohtaiset erot tuotiin vastauksissa esille.

"Riippuu koulusta, asia kerrotaan, mutta siihen tuskin panostetaan kovin paljon."

Vaikka sähköisen lomakekyselyn anti oli niukka, noudattaa vastaukset samaa linjaa teemahaastattelun tulosten kanssa. Perusopetuksen todentamiseen kehittäminen voi olla haastavaa jo siitäkin syystä, että opetustilanteet vaativat opettajan kokonaisvaltaisen huomion. Kirjautuminen halutaan tehdä helpoksi ja nopeaksi, mikä on ymmärrettävää, jotta toiminta pysyy luokkatilanteessa hallinnassa.

6.2 Teemahaastattelun tulokset

Teemahaastattelu validoitiin analysointivaiheessa neljän teeman mukaisesti. Ensimmäinen teema oli perusopetusoppilaiden identiteetin- ja pääsynhallinta. Tässä keskityttiin pääasiassa yksityisyyden suojaan. Esimerkkinä käsiteltävistä asioista oli perusopetusoppilaiden kesken tapahtuvat identiteettivarkaudet. Toinen teema oli perusopetusoppilaiden todentaminen. Tässä käsiteltiin aihetta siitä näkökulmasta, voisiko oppilaiden kanssa käyttää jotain muuta todentamismenetelmää kuin käyttäjätunnus ja salasana. Todentamiseen liittyvän teeman kohdalla keskusteltiin myös mahdollisuudesta, voisiko todentamismenetelmä olla oppilaan ikään suhteutettujen vaatimusten mukainen. Kolmas teema oli tietosuoja, kuinka se toteutuu ja kuinka tietosuojan huomioimista perusopetusoppilaiden todentamisessa voitaisiin kehittää. Neljäntenä teemana haastateltavien kanssa käsiteltiin 1-2 luokan oppilaiden digitaalisten ympäristöjen käyttöön liittyviä haasteita ja pääsynhallintaan liittyviä tvt-oppimistavoitteita.

Teemahaastattelussa haastateltavien vastaukset olivat hyvin linjassa toisten haastateltavien kanssa kuten myös lomakekyselyn vastausten kanssa. Perusopetusoppilaiden todentamiseen liittyvät ongelmat ja kehittämistoiveet toistuivat vastauksissa. Vastauksissa tuli myös esille, että perusopetusoppilaiden todentamiseen sekä yksityisyyden suojan tarkentamiseen toivotaan kansallisia linjauksia esimerkiksi Opetushallituksesta.

6.2.1 Identiteetin- ja pääsynhallinta ja yksityisyydensuoja

Vielä 2000 luvulle saakka kouluissa oli oppiaine kansalaistaito. Tämän oppiaineen sisältö oli opettaa oppilaille elämässä tarvittavia yleisiä yhteiskunnassa tarvittavia taitoja ja omien asioiden hoitamiseen tarvittavia taitoja. Haastatteluissa käytiin kes-

kustelua tämän tyyppisestä oppiaineesta nykypäivänä. Oppiaineen sisältö voisi olla yksityisyyden suojaaminen digitaalisessa ympäristössä, kuinka huolehdit yksityisyydestäsi ja kuinka hoidat omia yksityisiä asioita digitaalisesti.

Perusopetuksen oppilaalla on digitaalinen identiteetti palveluissa, joita käytetään opetuksessa esimerkiksi Google G Suite, O365 ja Wilma muiden opetuksessa käytettävien sähköisten palveluiden lisäksi. Opetuksenjärjestäjän ylläpitämän keskitetyn identiteetinhallinnan keinoin huolehditaan, että oppilaan henkilötietojen käsittely identiteetinhallinnan piirissä olevissa järjestelmissä ja sovelluksissa noudattaa henkilötietojen käsittelyn vaatimuksia. Opetuksenjärjestäjän vastuulla on lasten henkilötietojen käsittely, joten erityistä huolellisuutta noudatetaan, että sovellukset noudattavat GDPR vaatimuksia lasten henkilötietojen käsittelyn vaatimuksista.

Keskitetyn identiteetinhallinnan piirissä olevien palveluiden ja sovellusten käyttämiseen vaadittavat tietosuojasitoumukset tehdään opetuksenjärjestäjän toimesta. Oppilaan eikä myöskään opettajan, tarvitse huolehtia näissä tilanteissa henkilötietojen käsittelyn ehdoista, kuten kuka henkilötietoja käsittelee ja kuinka kauan henkilötietoja palveluissa käsitellään.

Haastatteluissa tuli esille, että opetuksenjärjestäjän määrämuotoinen opetuksessa käytettävien sovellusten käyttöönottoprosessi parantaa tietoisuutta siitä, että opetuksessa käytetään henkilötietojen käsittelyn näkökulmasta hyväksyttyjä sovelluksia ja samalla se tuo kustannussäästöjä. Suomessa opettajilla on vielä perinteinen pedagoginen vapaus, joka mahdollistaa, että opettaja voi joissain tilanteissa ottaa käyttöön sovelluksen, joka ei ole keskitetyn identiteetinhallinnan piirissä. Erään haastateltavan kommentti olikin, että Suomessa opetuksessa oleva pedagoginen vapaus aiheuttaa tietoturvaongelman. Tämä tulee esille tilanteissa, joissa opettaja ottaa käyttöön opetukseen sovelluksen, mikä ei noudata henkilötietojen käsittelyn vaatimuksia ja erityisesti lasten henkilötietojen käsittelyn vaatimuksia.

> "Suomessa pedagoginen vapaus ja aiheuttaa tietoturvaongelmia."

Sovelluksen käyttöönottajan tulee huolehtia tietosuojasitoumusten varmistaminen sekä henkilötietojen lainmukainen käsittely. Haastatteluissa tuli esille muun muassa, että käyttöehtosopimuksiin perehtyminen on kiinni osaamisesta ja tiedosta siitä, miten Internet toimii ja mitä riskejä siihen liittyy. Erään haastateltavan mukaan identiteetinhallinnan pitäisi olla tänä päivänä ydintaito.

> "Digitaalisissa ympäristöissä sinulla on profiili ja tunnus, miten tätä tunnusta käytetään ja miten oppilas voi itse säädellä tätä asiaa."

Haastatteluissa tuli myös esille, ettei opettajilla eikä oppilailla ole käsitystä siitä, mitä datan kerääminen tarkoittaa esimerkiksi niissä tilanteissa kun tehdään profiili sovellukseen.

> "Mitä datan kerääminen tarkoittaa ja mitä sen myyminen tarkoittaa ja voidaanko siihen puuttua."

Useamman haastateltavan kanta oli, että oppilaan yksityisyyden suojan kannalta MPASSid ja MPASSid:n piirissä olevien sovellusten käyttö parantaa oppilaan yksityisyyden suojaa ja henkilötietojen käsittelyyn liittyvää tietosuojaa. Eräs haastateltava toi myös esille, että yksityisyyden suojaa ei korosteta riittävästi, oppilas ei ymmärrä mitä yksityisyydensuoja tarkoittaa ja väärinkäytöksiä tapahtuu.

> "Ymmärtääkö oppilas mitä tarkoittaa yksityisyyden suoja."

Digitaalisen identiteetin- ja pääsynhallinnan tulisi tukea yksityisyyttä, olla turvallista ja suojata oppilaita sähköisen identiteetin varkauksilta ja väärinkäytöltä. Perusopetusoppilaiden kesken tapahtuu tänä päivänä jonkin verran identiteettivarkauksia. Nuoret ottavat toisen käyttäjätilin haltuun usein ajattelemattomuuttaan, mutta myös tarkoituksena kiusata varkauden uhria. Identiteettivarkaus on tietoturvaloukkaus, joka nykyään on myös rikoslaissa määritelty. Nuorille toisen käyttäjätilin kaappaaminen voi tuntua harmittomalta pilalta.

> "Oppilaat teki ryhmässä tehtäviä Teamsissa ja kirjoitti keskusteluun toisen oppilaan tunnuksilla."

Opetuksessa tulisi korostaa digitaalisen ympäristön olevan kunkin henkilökohtainen asia, jota ei edes pilailumielessä saa ottaa haltuun ilman seurauksia. Lapset ja nuoret eivät täysin ymmärrä identiteettivarkauden vakavuutta, mitä identiteettivarkaus tarkoittaa ja mitä siitä voi seurata. Haastatteluissa tuli esille, että identiteettivarkauksista tulisi puhua enemmän, jotta jo perusopetusoppilailla olisi ymmärrys, mitä se tarkoittaa. Identiteettivarkauksien vakavuus tulisi tuoda esille, kuten myös niiden seuraukset.

> "Oppilaat kokevat, että toisen nimissä tekeminen on vain läppä ja eivät ymmärrä seurauksia."

Mikäli oppilaiden salasanan muodostaminen noudattaa tiettyä kaavaa, on luokkakaverin käyttäjätunnus ja salasana helposti haltuun otettavissa.

> "Identiteettivarkauksia tapahtuu muun muassa, jos kaikilla on vaki salasana."

Lainsäädännön tuoma ikäraja 13-vuotta tuli myös haastatteluissa esille. Mitä käytännössä voi käydä lapsen kanssa lävitse, ellei hän ikänsä puolesta saa kyseistä palvelua vielä käyttää.

> "Lapsen kanssa ei voi harjoitella some yksityisyyden suojaa, koska hän ei saa niitä käyttää."

Yhteiskäytössä olevat laitteet altistavat myös identiteettivarkauksille. Yhteiskäytössä olevien laitteiden käyttöön kaivataan kansallisia linjauksia. Lapset ja nuoret eivät muista tai huomaa kirjautua ulos sovelluksista tai tallentavat käyttäjätiedot laitteille. Opettajien koulutus ja perehdytys myös tähän aiheeseen nousi esille.

Haastatteluissa tuli esille myös identiteetinhallinnasta puhumisen vaikeus. Opettajan työ vaatii tänä päivänä yhä enemmän aikuista lapselle ja digitaalisten välineiden sekä ympäristöjen käyttö tulisi olla sujuvaa sekä nopeaa, mutta myös hallittua. Opettaja ei kuitenkaan voi olla kaiken aikaa selvillä, mitä oppilaat tekevät esimerkiksi omilla laitteillaan.

> "Identiteetinhallinnasta puhuminen on haastavaa, koska tämä on arka asia ja pedagogiikka täytyy olla edellä."

> "Opettajan työ vaatii yhä enemmän aikuista lapselle ja siinä tilanteessa jää mahdollisesti digi toiseksi."

Opettajien koulutus ja perehdytys identiteetinhallintaan ja henkilötietojen käsittelyyn liittyvän ymmärryksen lisäämiseksi nostettiin haastatteluissa myös esille.

> "Opettajien perehdytys on myös yksi tekijä, jotta digiymmärrys kasvaa."

Opetuksenjärjestäjät ovat määritelleet eri vuosiluokille opetussuunnitelman mukaisesti tieto- ja viestintäteknologiset (tvt) taitotasot. Kuntien tvt-taitotasoissa on todentamiseen ja yksityisyyden suojaan liittyvät taitotasot määritelty vaihtelevasti eri luokka-asteilla alla muutama esimerkki. Esimerkit on valittu satunnaisesti eri opetuksenjärjestäjien tvt-taitotasoista.

- 1. lk Oppilas ymmärtää käyttäjätunnuksen merkityksen

- 1-2. lk Käyttäjätunnuksen ja salasanan yksityisyyden ymmärtäminen (tietosuoja)
- 1-2. lk Oppii käyttämään kirjautumiseen käyttäjätunnusta ja salasanaa
- 2. lk Tietoturvallisuus mm. salasanojen säilyttäminen, turvallinen salasana
- 2. lk Oppilas osaa käyttää henkilökohtaista käyttäjätunnusta ja salasanaa kirjautuessaan laitteelle
- 4. lk Osaa muodostaa turvallisen salasanan
- 7-9. lk Oppilaalla on henkilökohtainen tunnus koulun tarjoamiin palveluihin ja oppilas ymmärtää, että tunnus on henkilökohtainen

Kuten esimerkeistä käy esille, kirjautumiseen liittyvää tietoturvaa ja yksityisyyden suojaa pidetään tärkeänä opettaa oppilaille eri luokka-asteilla. Taitotaso vaatimukset pääsääntöisesti kasvavat luokka-asteelta toiselle siirryttäessä. Haastatteluissa tuli esille, että opettajilta puuttuu kuitenkin selkeät ohjeet, kuinka oppilaille opetetaan yksityisyyden suojaa ja tietoturvallista toimintaa muun muassa tunnusten hallintaan liittyen. Tvt-taitotasot määrittävät myös muita oppilaan digitaalisten välineiden käyttöön liittyviä oppimispolkuja. Näiden mukaan luokka-asteittain eteneminen auttaa oppilasta kasvattamaan digitaalisia taitojaan ja ymmärrystä ja luo etenevän polun oppilaalle.

> "Viidennen luokan oppilailla on jo enemmän tiedonhakuja ja hallintaa, joten toiminta on joustavampaa, jos näitä asioita on harjoiteltu. Vaatii, että noudatetaan tvt-taitotasoja"

6.2.2 Todentaminen

Kuten jo aikaisemmin tässä tutkielmassa on todettu, pääasiallinen todentamismenetelmä perusopetuksessa on käyttäjätunnus ja salasana. Teemahaastattelussa kysyttiin voisiko perusopetusoppilailla käyttää jotain muuta todentamismenetelmää. Todentamisvälineen ja -menetelmän valintaan vaikuttaa muun muassa niiden vaatimat kustannukset. Käyttäjätunnus ja salasana on edullinen ja yleisesti käytetty vaihtoehto. Mikäli tunnistautumiseen käytetään jotain välinettä, esimerkiksi tokenlaitetta, tuo se opetuksenjärjestäjälle lisää kustannuksia. Välineen käyttö tunnistautumisessa oppilaiden kanssa on myös haasteellista laitteiden häviämisen tai rikkoutumisen vuoksi. Biometrinen tunnistautuminen kuuluu erityisiin henkilötietoihin,

joten sen käyttäminen tuo omat erityisiin henkilötietoihin liittyvät haasteet. Alla todentamiseen liittyviä haasteita, joita haastatteluissa tuli esille.

> "Tokenit on hankalia, jos häviää tai menee rikki."

> "Todentaminen on vaikeaa, koska se on tekninen asia ja arki on hektistä."

> "Opettajat kokevat, että tunnistautumiseen menee liikaa aikaa."

Luokassa oppilaat ovat erilaisia ja myös tässä tilanteessa osa oppilaista suoriutuu kirjautumisesta nopeasti ja osa tarvitsee tukea enemmän. Teemahaastattelun kysymykseen, voisiko todentamismenetelmän vaikeusaste kasvaa oppilaan mukana, vastaukset olivat yhtenevät – mikäli se olisi teknisesti mahdollista.

> "Samassa tenantissa (=ympäristössä) olisi salasanavaatimukset pienillä oppilailla helpompi salasana ja yläasteella vaikeampi salasana. Lukiossa mfa, jossa olisi oma puhelin apuna."

Pienillä oppilailla esimerkiksi graafinen salasana voisi olla toimivampi. Vastauksissa tuli myös esille, että tämän pitäisi olla opetussuunnitelman sisältöä. Asiaa lähestytään nyt jo tvt-taidoissa ja monilukutaidoissa. Joissain kunnissa on tehty myös digitaalisia polkuja, joiden toteutuminen on opettajan osaamisesta ja aikataulusta kiinni.

> "Opettajan koulutusta on pyritty kehittämään ja miten eri opettajan koulutuslaitokset ottavat digitaalisuuden mukaan ja ovat kehittäneet tätä."

> "Opettajankoulutuksessa on edelleen kehittämistä opettajan digitaalisten taitojen osalta."

Opetushallitus laatii "Uudet lukutaidot ohjelman", jossa laaditaan kansallisesti osaamisen kuvauksia eri ikätasoille. Tämän mukaan laaditaan eri ikätasoille osaamisen minimitasot. Oppilaiden digitaalisten menetelmien käyttö kasvaa luokka-asteittain ja siten myös harjoitus tässä asiassa kasvaa.
Opetuksenjärjestäjien välillä oppilaiden käyttäjätunnuksen ja salasanan muodostamisen menetelmät vaihtelevat. On mahdollista, että pienten oppilaiden salasanan muodostamiseen käytetään säännönmukaista logiikkaa, jonka avulla helpotetaan oppilaan salasanan muistamista. Pienet oppilaat unohtavat tunnistautumistiedot

helposti ja oppitunnin rajallinen pituus luo paineet luoda heikko salasana. Opettajia haastatellessani tuli kuitenkin esille, että mikäli oppilas pääsee itse vaikuttamaan salasanan sisältöön, oppii hän paremmin muistamaan sen. Tämä vaatii kuitenkin opettajalta alussa hieman enemmän aikaa huomioida salasanan muistamisen tärkeys.

Todentamisen teknisyys tuo omat haasteet arjen hektisyyden vuoksi. Perusopetuksen oppilaiden todentamiseen ja digitaalisten välineiden käyttöön liittyen kehittämistoiveita olivat esimerkiksi sähköinen työpöytä, jonka avulla oppilas saisi yhdellä kirjautumisella työpöydälle näkyviin opetuksessa käytettävät sovellukset ja palvelut. Vastauksissa tuli esille käsitys biometrisen tunnistautumisen helppoudesta ja toive, että sitä voisi käyttää perusopetuksessa. Lisäksi kehitystoiveena tuli esille sähköisen työpöydän käyttö.

> "Olisi sähköinen työpöytä, mihin lapsi kirjautuu esim. Airo, Edison tai muu vastaava, jolloin lapsen täytyy kirjautua vain kerran."

Sovellusten käyttöönottoprosessin kehittäminen tuli vastauksissa myös esille.

> "Sovelluskori, jonka avulla voi opettaja valita kaupungin hyväksymät sovellukset, joista voi valita mitä käyttää luokan kanssa."

6.2.3 Tietosuojan toteutuminen

Hyvin suunniteltu ja toteutettu identiteetin- ja pääsynhallinta on olennainen osa organisaation tietosuojaan liittyviä toimenpiteitä. Tästä johtuen tietosuojaan liittyviä kysymyksiä oli sekä lomakekyselyssä sekä teemahaastattelussa. Vastauksissa tuli esille tietosuoja-asetuksen ja lainsäädännön voimaantulon tuomat muutokset ja tiukennukset lasten henkilötietojen käsittelyyn.

Tähän osioon liittyvissä kysymyksissä tavoitteena oli saada ymmärrys, kuinka tietosuojan toteutuminen nähdään perusopetuksen identiteetin- ja pääsynhallinnassa ja tarkemmin vielä todentamiseen liittyvissä tapahtumissa. Tietosuojan toteutuminen nykyisessä perusopetus oppilaiden identiteetin- ja pääsynhallinnassa katsottiin toteutuvan riittävän hyvin.

> "Tietosuoja toteutuu riittävän hyvin, tehdään liian mörkö ja verrataan liikaa somejättien toimintaan."

Lainsäädännön näkökulma tuli haastatteluissa esille. Perusopetuslaki edellyttää oppilastietojen käsittelyn opetuksenjärjestämiseksi ja tämä menee GDPR edelle.

"GDPR ei saa mennä käytettävyyden edelle."

Haastatteluissa tuli esille myös sovellusten kolmannet osapuolet sekä evästekäytännöt. Näiden osalta ei ole mahdollisuutta määrittää, eikä myöskään tarkasti tietää, kuinka paljon oppilaiden tietoja jää näiden osapuolten käyttöön. Haastatteluissa käytiin lävitse, toteutuuko tietosuojan vaatimukset, kun käytetään digitaalisia palveluita. Mikäli opetuksenjärjestäjällä on selkeä sovellusten käyttöönottoprosessi, vastaa opetuksenjärjestäjä tietosuojasitoumuksista ja sovellusten henkilötietojen käsittelyyn vaadittavasta tietosuojan toteutumisesta. Muussa tilanteessa on mahdollista, että koulut tai yksittäiset opettajat voivat ottaa käyttöön sovelluksia opetukseen ilman, että hänellä on mahdollisuutta tai osaamista selvittää sovelluksen sopivuus perusopetuksen käyttöön. Haastateltavat toivatkin esille, että sovellusten käyttöönotto voi olla koulun ja opettajan osaamisen sekä kiinnostuksen mukainen.

"Käytännöntasolla toiminnassa on kouluilla eroavaisuuksia ja on hyvin paljon opettajan näköinen."

Eräs haastateltava sanoikin, että tietosuojan toteutuminen on monisyinen asia, jos ajatellaan opetuksen sisältöihin liittyviä ympäristöjä.

"Esimerkiksi cafe ympäristö, jossa on käytössä oppilaan henkilötietoja ja käsittelyperuste on opetuksen järjestäminen."

Tietosuoja-asetuksen voimaantulon jälkeen opetuksenjärjestäjät ovat järjestäneet koulutusta sekä ohjeistuksia opetuksen tueksi. Tällöin voidaan katsoa, että teorian tasolla ohjeistukset ja koulutukset ovat kunnossa. Käytännössä kuitenkin toiminta tietosuojan huomioon ottamisessa eroaa opetuksenjärjestäjien, koulujen ja opettajienkin välillä.

"Käytännön toteutukset voivat vaatia kehittämistä".

Tietosuojan toteuttamisen vastuukysymyksiä pohdittiin ja haastateltava totesi, että tietosuojan toteutuminen on opetuksenjärjestäjän vastuulla. Tähän liittyen vaaditaan kuitenkin vielä kehittämistä. Tietosuojan toteutumiseen opetuksessa vaikuttaa opetuksenjärjestäjän panostaminen asiaan eli kuinka tärkeänä tietosuoja nähdään. Opetuksen pedagoginen vapaus ja tietosuojan tuomat ohjeistukset eivät saisi olla toisiaan kumoavia tai estäviä. Tietosuojaan liittyvä ohjeistus, koulutus ja viime kädessä opettajan toiminta vaikuttavat siihen, kuinka tietosuoja toteutuu. Koulut ja

opettajat toteuttavat henkilötietojen käsittelyyn liittyvää tietosuojaa toiminnassaan opetuksenjärjestäjän antamien ohjeiden ja koulutuksen mukaisesti. Oppilas toteuttaa opettajan antamia ohjeita. Opettajan taidot ja kiinnostus edesauttavat tietosuojan toteutumista digitaalisten ympäristöjen ja laitteiden käytössä.

Oppimisympäristöjen käyttö ohjatusti edellyttää, että opetuksenjärjestäjä järjestää oppilaille ensinnäkin välineet, mutta myös näihin ympäristöihin kirjautumiseen vaadittavat todennusmenetelmät. Tietosuoja-asetus asettaa erityisesti lasten henkilötietojen suojaamiseen vaatimuksia. Näiden vaatimusten käytäntöön vieminen vaatii opetuksenjärjestäjätasoisia ohjeistuksia ja koulutusta opetushenkilökunnalle.

> "Tämä liittyy opettajan osaamiseen, joillain opettajilla edistyneitä menetelmiä miten tätä opetetaan esim. internetin toiminta ja riskit".

Opetuksen järjestämiseen liittyvät palvelut joutuvat toteuttamaan tietosuojan vaatimuksia lasten henkilötietojen käsittelyssä, joten näitä tulisi voida käyttää turvallisin mielin. Ongelmaksi nähtiin enemmänkin oppilaiden oma digitaalisten palvelujen käyttö. Haastatteluissa käytiin lävitse sitä, kenen vastuulla on tietosuojaan liittyvien ohjeistuksien antaminen. Vastuukysymyksistä tuli esille, että vaikka ohjeistuksia ja suuntaviivoja kaivataan opetushallitukselta, todettiin että vastuu ohjeistuksista ja koulutuksesta on opetuksenjärjestäjän.

> "Lähtökohtaisesti tietosuojan toteutuminen on opetuksenjärjestäjän vastuulla".

Tietosuojan toteutumisen kehittäminen liittyy opettajien perehdytykseen, kouluttamiseen sekä tietoisuuden kehittämiseen.

> "Opettajan tietosuojaosaamisen kehittäminen."

Opetuksessa käytettävät laitekannat tulisi olla ajan tasalla. Järjestelmien ja tunnistautumismenetelmien kehittäminen tuli myös vastauksissa esille. Haastatteluissa tuli myös esille koulujen eriarvoisuus laitekannan osalta. Erilaiset laiteympäristöt ja se onko laite oppilaan omassa käytössä vai yhteiskäytössä vaikuttaa myös tietosuojan toteutumiseen.

> "Laiteympäristöjen ja oppimisympäristöjen hankkiminen pitäisi kuulua valtionosuuksien piiriin."

Perusopetuksen oppilaiden kirjautumiseen liittyvät haasteet ovat pedagogiikan ja opettajan digitaalisten taitojen sekä oppitunnin pituuden rajallisuuteen liittyvät tekijät.

> "Jotta opettaja ehtii ottamaan digitaalisen toiminnan käyttöön tunnilla, tunti on 45 min ja siitä saattaa mennä 30 min kirjautumiseen".

Oppimisympäristöjen kohdalla saattaa vallita myös ajatus, että mitä suojataan, mikäli oppimisympäristö sisältää esimerkiksi "vain" koulutehtäviä. Viranomaisten ohjausvelvoitetta esimerkiksi Opetushallituksen ohjeistuksia ja ohjausta kaivattiin identiteetin- ja pääsynhallintaan sekä todentamiseen liittyvissä kysymyksissä.

6.2.4 1-2 luokan oppilaiden digitaalisten ympäristöjen käyttö

Oppilaille opetetaan pääsääntöisesti, että käyttäjätunnus ja salasana ovat henkilökohtaisia eikä niitä saa näyttää tai kertoa kenellekään. Ykkösluokan oppilailla lukutaidon ja kirjoitustaidon oppiminen on vasta aluillaan. Tässä tilanteessa käyttäjätunnuksen ja salasanan kirjoittaminen on haastavaa. Liian pitkä tunnus tuo omat haasteensa. Muistamista ja kirjoittamista helpottaa, mikäli käyttäjätunnus muodostuu oppilaan omasta nimestä. Kahdeksanmerkkinen salasana, jossa on erilaisia erikoismerkkejä, on ykkösluokan oppilaille haastava. Koska lukemisen ymmärtäminen on vielä puutteellista eivätkä he mahdollisesti tunnista kaikkia kirjaimia, heille täytyy olla malli siitä, kuinka käyttäjätunnus ja salasana kirjoitetaan, jotta he suoriutuvat kirjautumisesta. Tämä tarkoittaa joissain tilanteissa sitä, että opettajalla on esimerkiksi mallikortit kunkin oppilaan tunnuksista. Tunnin alussa opettaja jakaa kortit oppilaille, jotka toteuttavat kirjautumisen mallin mukaisesti. Tämä toimintamalli ei ole tietosuojan mukainen, mutta takaa opettajalle tunnille rauhan toteuttaa opetusta. Kirjautuminen muutoin olisi haastavaa ja aikaa vievää. Eräs haastateltava totesikin,

> "Miten on mahdollista pienelle oppilaalle, joka vasta opettelee lukemaan, opettaa tätä."

Ensimmäiset kerrat ovat yleensä haastavimpia, mutta oppilas oppii kuitenkin nopeasti, mikäli kirjautumista harjoitellaan säännöllisesti.

> "Noin viisi ensimmäistä kertaa tietokoneelle kirjautumiseen menee noin 30 minuuttia."

Haastatteluissa tuli esille, että iPadin käyttäminen on pienten oppilaiden kanssa helpompaa, koska se ei vaadi erillistä kirjautumista tai PIN-koodilla kirjautumisen. Neljänumeroinen PIN-koodi on pienten oppilaiden helpompi muistaa. Mutta toisaalta haastatteluissa tuli myös esille, että pienten oppilaiden kanssa ei ehkä olisikaan tarpeen käyttää digitaalisia välineitä ennenkuin perustaidot lukemiseen ja kirjoittamiseen on hallussa.

> "Oppilaalla täytyy olla jokin ymmärrys mitä tekee, lukemisen taito ennen kuin saa muuta kuin iPad:in käyttöön."

Samoin haastatteluissa pohdittiin pienten oppilaiden kanssa graafisen salasanan käyttöä ja se oletettiin olevan helppokäyttöisempi. Tästä ei kuitenkaan ollut kenelläkään kokemusta. Ennen digitaalisten välineiden käyttöä pienten oppilaiden kanssa tulisi käydä myös mitä yksityisyyden suoja ja käyttäjätunnuksen ja salasanan omistaminen tarkoittaa.

> "Ymmärrys siitä mitä omalla tunnisteella voi tehdä, vastuu ja tieto seuraamuksista eroaa."

> "Ykkösluokkalaiselle sana 'yksityisyyden suoja' ei tarkoita mitään."

Haastatteluissa käytiin myös keskustelua siitä, kuinka opettajalla tulisi olla mahdollisuus hallita oppilaiden laitteita keskitetysti, etenkin pienten oppilaiden kohdalla. Opettajan ohjauksessa ja kontrollin alla kaikki oppilaat olisivat samassa tehtävässä ja opettaja voisi myös seurata mitä oppilas laitteella tekee. Haastatteluissa pohdittiin voisiko tunnistautumismenetelmä kasvaa eli vaikeutua oppilaan kasvaessa. Tässä tilanteessa identiteetin- ja pääsynhallinnan toteutustapa voi vaikeuttaa tätä tai käytössä oleva identiteetinhallintajärjestelmä ei pysty mahdollistamaan erilaisia todennusmenetelmiä. Haastatteluissa käytiin keskustelua myös opetuksenjärjestäjän it-tuen osuudesta erilaisten todennusmenetelmien mahdollistajana.

> "Kun kunnan it-tuki on yhteinen, ei usein mietitä erityistarpeita esimerkiksi 1-2 lk osalta tai yhden opettajan osalta."

Haastatteluissa tuli esille myös biometrisen todennusmenetelmän käyttö oppilailla.

> "Jos olisi resursseja oppilaalla olisi kärryssä oma tietokone, jonne voi tunnistautua esimerkiksi sormenjäljellä."

Pienten oppilaiden osalta todentamismenetelmän helppokäyttöisyys, mutta myös turvallisuus ovat tärkeitä ominaisuuksia. Tässä tilanteessa nopeasti ajateltuna biometrinen todennusmenetelmä näyttäisi hyvältä vaihtoehdolta. Biometrinen todennusmenetelmä kuuluu erityisiin henkilötietoihin ja sen käyttö lasten todennusmenetelmänä opetuksenjärjestäjän toimesta vaatii tarkempaa pohdintaa ja riskiarviointia, mutta ei lähtökohtaisesti ole mahdollista.

7 Perusopetusoppilaiden todentamismenetelmien vaihtoehdot

Mikäli oppilaalla koulussa olisi vain yksi käyttäjätunnus ja salasana muistettavanaan, voisi tässä tilanteessa salasanan turvallisuusvaatimuksia lisätä. Tässä tilanteessa salasanan muodostamiseen voitaisiin käyttää sekä oppilaan itsensä vaikutusta että satunnaisuutta. Mutta mikäli oppilaalla on useita salasanoja, heikentää se hänen käyttäjätunnusten ja salasanojen muistamista sekä käyttöaktiivisuutta. Lapset unohtavat helpommin heille merkityksettömät asiat ja asiat, joita ei harjoitella säännöllisesti. Mikäli käyttäjätunnus ja salasana luodaan satunnaisesti tai kaavamaisesti, mutta ilman oppilaan omaa vaikutusta, jää kirjautumiseen vaadittava toiminnan muistaminen lapselle vieraaksi ja merkityksettömäksi.

Todentamismenetelmien käyttöönotossa painotetaan tänä päivänä vahvaa, monivaiheista tunnistautumista. Tunnistautumismenetelmään paneutumista korostetaan yksityisyyden suojan turvaamisen vuoksi. Kun perusopetusoppilaille otetaan käyttöön todentamismenetelmä, joudutaan punnitsemaan käytettävyyden, kustannusten ja turvallisuuden välillä. Tutkimuksesta kävi ilmi, että perusopetusoppilas oppii vaikeankin käyttäjätunnuksen ja salasanan, mikäli tunnistautumisen opetteluun on mahdollisuus laittaa aikaa.

EU:n yleisen tietosuoja-asetuksen ja tietosuojalain voimaantulon myötä lasten henkilötietojen käsittelyn perusteet ovat tarkentuneet. Opetuksessa käytetään sähköisiä oppikirjoja ja digitaalisia peliympäristöjä, näissä ympäristöissä suoritetaan kokeita, tehdään arviointia, ryhmätöitä, yksilötehtäviä ym. Opetushallitus tarjoaa tunnistuksenvälitysratkaisuksi MPASSid:n. MPASSid:n avulla oppilas voi kirjautua tämän palvelun piirissä olevaan ympäristöön opetuksenjärjestäjän tarjoamilla todentamismenetelmillä. MPASS:n käyttöönotto vähentää oppilailla muistettavien tunnusten määrää. Kaikki opetuksessa käytettävät palvelut ja sovellukset eivät vielä kuulu MPASSid yhteistyöhön, joten näiden sovellusten osalta täytyy opetuksenjärjestäjän pystyä ratkaisemaan voiko sovellusta käyttää opetuksessa apuna. Mikäli tällainen sovellus otetaan käyttöön, kasvattaa se oppilaan muistettavien käyttäjätunnusten ja salasanojen määrää. Opetuksenjärjestäjien olisikin hyvä miettiä yhteisiä ratkaisuja, milloin opetukseen on tarpeen ottaa MPASSid:n ulkopuolinen sovel-

lus käyttöön. Luvussa 3 käytiin lävitse tunnistusratkaisujen periaatteita, jotta yksityisyyden suoja tulee otetuksi huomioon. Näiden periaatteiden mukaisesti, mikäli mahdollista, tulisi käyttää anonyymiä tai pseudonyymiä asiointia, jolloin oppilaan tunnistusta ei tarvitse tehdä näissä MPASSid ulkopuolisissa sovelluksissa.

Perusopetusoppilaiden todennusmenetelminä haastattelujen ja kirjallisen tutkimuksen mukaisesti vaihtoehtoina olisivat perinteisen käyttäjätunnus ja salasanan lisäksi graafinen salasana, PIN-koodi sekä token-laitteen avulla tapahtuva todentaminen.

Perinteinen salasana on tuttu ja toimiva ratkaisu. Tässä vaihtoehdossa haastattelujen mukaan toivottiin mahdollisuutta vaikeuttaa salasanan monimutkaisuutta oppilaan iän mukaisesti. Haastatteluissa tuli myös esille, että mikäli oppilas itse pääsee vaikuttamaan salasanan sisältöön, muistaa hän sen paremmin. Graafisen salasanan käytöstä ei haastateltavien joukossa ollut kokemusta, mutta se koettiin kokeilun arvoiseksi vaihtoehdoksi. Vaihtoehto voisi olla pienillä oppilailla graafinen tai kuvaan perustuva salasana ja isommilla oppilailla korkeamman vaikeusasteen merkkipohjainen salasana. Jotta salasanan vaatimustaso toteutuu, tulisi sen myös vaihtua säännönmukaisesti oppilailla.

Teemahaastattelussa tuli esille mahdollisuus biometrisen tunnistautumisen käytöstä. Kun biometrinen tunnistautuminen yhdistetään oppilaan sähköiseen identiteettiin, kuuluu se erityisiin henkilötietoihin. Mikäli biometrisiä tunnistetietoja käsitellään, tulee rekisterinpitäjän toteuttaa tietosuojalain (1050/2018) 6 §:n mukaan asianmukaiset ja erityiset toimenpiteet rekisteröidyn oikeuksien suojaamiseksi. EU:n yleisen tietosuoja–asetuksen artikla 9 mukaisesti biometrisen tunnistautumismenetelmän käyttäminen vaatii aina suostumuksen ja lasten ollessa kyseessä vaaditaan huoltajan kirjallinen suostumus. Kasvotunnistautuminen biometrisenä tunnistusmenetelmänä voisi tulla kysymykseen lasten kohdalla, koska se on suhteellisen pysyvä, kerättävissä ja on yleisesti hyväksyttävämpi menetelmä, kuin esimerkiksi sormenjälki- tai iiris-tunnistautuminen. Vaikka biometrinen tunnistautuminen olisi nopeaa ja helppoa, tuo se mukanaan kuitenkin erityiset riskit. Kouluilla käytössä olevat yhteiskäyttöiset laitteet eivät sovellu biometrisen tunnistautumisen käyttöönottoon. Biometrisen tunnistautumisen käyttäminen vaatii aina huoltajalta luvan ja kuten eräässä haastattelussa tuli esille, ovat huoltajat varovaisia sen suhteen, mitä tietoja lapsesta välitetään esim. kirjautumiseen liittyvissä tapahtumissa.

Kirjautumisen turvallisuuteen vaikuttaa muun muassa se, että salasana on riittävän monimutkainen, käytetään vahvaa tunnistautumista sekä se, että salasana

on vain omistajansa tiedossa. Kaikki nämä turvallisuuteen vaikuttavat tekijät ovat haasteellisia perusopetuksessa. Oppilaat unohtavat helposti monimutkaiset salasanat ja pienten oppilaiden osalta oppitunnilla tapahtuvaa kirjautumista digitaaliseen palveluun helpottaa, mikäli opettajalla on oppilaan salasana tiedossa, se on kirjoitettu muistilappuun ja opettaja pääsee hallinnoimaan oppilaan salasanaa. Vahva tunnistautuminen tarkoittaisi oppilaiden kohdalla esimerkiksi sitä, että käyttäjätunnus-salasana kirjautuminen vahvistettaisiin token-koodilla. Token-laitteella tapahtuva kirjautuminen ainoana todentamismenetelmänä on turvaton ja token-laitteet ovat alttiita menemään hukkaan. Mikäli token-laite toimisi toisena todentamisvälineenä perinteisen salasanan rinnalla, toisi se vahvempaa suojaa kirjautumiseen. Tässä tilanteessa salasanan vaikeusaste voisi pienillä oppilailla olla heikompi. Token-laitteiden hankinta on kuitenkin suuri kustannuserä opetuksenjärjestäjille ja haastatteluissa tuli myös esille, että näiden menetelmien kehittäminen tulisi kuulua valtionosuuksien piiriin.

8 Yhteenveto ja johtopäätökset

Peruskouluissa käytetään digitaalisia oppimateriaaleja ja oppimisympäristöjä aktiivisesti. Lasten pääsynhallintaan liittyvät menetelmät eivät ole kuitenkaan kehittyneet samaan tahtiin. Tämän pro gradu -tutkimuksen teoriaosan aluksi käytiin läpi tietosuojan ja tietoturvan peruskäsitteitä sekä mitä tietosuoja tarkoittaa henkilötietojen käsittelyssä. Tämän jälkeen teoriaosassa esiteltiin identiteetin- ja pääsynhallinnan osa-alueet ja käytiin tarkemmin lävitse yleisimmät todennusmenetelmät. Teoriaosan lopuksi pohdittiin lasten ja nuorten asemaa digitaalisten palvelujen käyttäjinä. EU tietosuoja-asetus ja tietosuojalaki ovat tuonet yksityisille ihmisille vahvempaa suojautumisen mahdollisuuksia digitaalisissa ympäristöissä. Samalla ihmisten tietoisuus on kasvanut. EU tietosuoja-asetus ja tietosuojalaki nostavat erityisesti esille lasten suojaamisen. Lasten ja nuorten suojaamiseen digitaalisissa ympäristöissä kiinnittää huomiota myös Opetushallitus ja ohjeistaa opetuksenjärjestäjiä käsittelemään lasten tietoja huolellisesti.

Empiirisessä osiossa etsittiin vastausta kysymyksiin, toteutuuko perusopetusoppilaiden identiteetin- ja pääsynhallinnassa yksityisyyden suoja sekä tietosuoja lainsäädännön vaatimukset ja mitkä ovat perusopetusoppilaiden todentamisen vaihtoehdot.

Ensimmäiseen tutkimuskysymykseen miten perusopetusoppilaiden identiteetin- ja pääsynhallintaan liittyvä yksityisyyden suojan opetus toteutuu. Perusopetusoppilaiden identiteetin- ja pääsynhallintaan liittyvä yksityisyyden suojan opetus on kirjattu opetussuunnitelmaan ja mainitaan useiden kuntien tvt–taitotasoissa. Tutkimuksen tulokset näyttävät kuitenkin, että tässä on vielä kehittämistä. Yksityisyyden suojan opettaminen nykypäivän kansalaistaitona olisi haastattelujen mukaan toivottavaa. Toisen tunnuksen käyttämisen seurauksista tulisi puhua enemmän ja oppilaita opettaa kunnioittamaan myös digitaalisen identiteetin yksityisyyttä. Haastatteluissa tuli esille, että yksityisyyden suoja terminä voi olla vieras oppilaille, joten tämän opetus tulisi sisällyttää opetukseen, kuten muutkin digitaalisten ympäristöjen ja välineiden käyttö. Sovelluksissa, jotka eivät kuulu identiteetin- ja pääsynhallinnan piiriin, tulisi voida käyttää anonyymiä tai pseudonyymiä asiointia. Näin oppilaiden henkilötietojen turhaa välittämistä palveluiden tarjoajille voidaan vält-

tää. Sovellusten käyttöönottoprosessissa tulee selvittää henkilötietojen käyttö sekä miten henkilötietojen elinkaaren mukainen käsittely toteutuu. Haastatteluissa tuli esille, että MPASSid käyttöönotto parantaa oppilaiden yksityisyydensuojaa. Tätä tulosta puoltaa se näkökulma, että MPASSid piirissä olevien lasten henkilötietoja käsitellään keskitetyn identiteetinhallinnan kautta ja näin ollen opetuksenjärjestäjä on myös huolehtinut keskitetysti henkilötietojen käyttöehtositoumukset. Keskitetyn identiteetinhallinnan piirissä henkilötietojen käsittelyssä noudatetaan myös henkilötietojen elinkaaren vaatimuksia.

Toinen tutkimuskysymys oli mitkä ovat perusopetusoppilaiden todentamismenetelmän toteuttamisen vaihtoehdot. Kaikista vastauksista tuli esille halu kehittää todentamiseen liittyvää toimintamallia. Kehittämisen haasteena ovat nykyiset toimintaympäristöt ja tämän päivän haasteet opettajan työssä oppilaiden kohtaamisissa. Vaikka kiinnostus todentamismenetelmän kehittämiseen tuli haastatteluissa esille, ei kuitenkaan kukaan haastateltavan organisaatio ollut miettinyt todentamismenetelmän vaihtamista tai kuinka toimintaa voitaisiin kehittää. Perinteinen salasana onkin tehokas todennusmenetelmä, kun sen vaikeusaste on riittävä ja se on vain oppilaan itsensä tiedossa. Lomakekyselyssä ehdotettiin myös token-laite, YubiKey tai vastaavan mukaista ratkaisua. Token-laitteen käyttö todentamisvälineenä toimisi oppilailla toisena todentamisvälineenä esimerkiksi perinteisen salasanan rinnalla. Mikäli oppilaiden todentaminen varmistettaisiin token-laitteella, voisi pienten oppilaiden salasanavaatimukset olla lievemmät. Token-laitteella kirjautuminen tukee kertakirjautumista ja helpottaa oppilaiden muistettavien salasanojen määrää. Token-laitteet aiheuttavat kuitenkin kustannuksia ja niiden mukana kuljettaminen saattaa olla oppilaille haastavaa. Perusopetusoppilailla ei voida hyödyntää puhelimen käyttämistä token-laitteena, koska opetuksenjärjestäjä ei voi olettaa eikä velvoittaa oppilaalla olevan omaa puhelinta käytössään.

Kolmas tutkimuskysymys käsitteli aihetta, toteutuuko perusopetusoppilaiden identiteetin- ja pääsynhallinnassa tietosuojan vaatimukset. Tietosuojan vaatimukset katsottiin toteutuvan teorian tasolla riittävän hyvin. Haastatteluissa tuli kuitenkin esille, että käytäntö tietosuojan toteutumisesta vaihtelee. Opetuksenjärjestäjät ovat järjestäneet koulutusta sekä ohjeistuksia opettajille, mutta arki voi kuitenkin olla ihan toisenlainen. Tietosuojan toteutuminen opetuksessa riippuu myös siitä, kuinka tärkeänä se nähdään. Kuten eräs haastateltava totesi "Käytännön toteutukset voivat vaatia kehittämistä". Tietosuojan toteutumisen kehittämiseksi ehdotettiin muun muassa koulujen laitekannan ajantasaistamista sekä todentamismenetel-

mien ajantasaistamista ja kehittämistä. Opetushallituksen roolia tietosuojan toteutumisen vahvistajana toivottiin. Voisiko Opetushallitus luoda linjaukset koulujen laitekannan sekä todentamismenetelmien minimivaatimuksista, kuten myös sovellusten käyttöönottoprosessin yhtenäistämisestä. Sekä teemahaastattelun että sähköisen lomakekyselyn tulosten perusteella tietosuojan toteutuminen paremmin vaatii vielä koulutusta, ohjeistuksia ja toimintamallien tarkennuksia. Jotta kaikki Suomen perusopetusoppilaat olisivat samassa asemassa, vaatisi tämä myös kansallisia minimivaatimuksia identiteetin- ja pääsynhallinnan, tietosuojan sekä todentamiseen liittyvien toimenpiteiden toteutukseen.

Tutkimuksen tuloksena voidaan katsoa, että ymmärrys perusopetusoppilaiden identiteetin- ja pääsynhallinnan nykytilanteesta on saatu kuvattua. Tapaustutkimuksen tavoitteena ei ole varsinaisesti kehittää toimintaa, mutta tutkimuksen tuloksena on mahdollista ehdottaa kehittämiskohteita. Tämän tutkimuksen mukaisesti kehittämiskohteina voidaan nähdä, että oppilaiden pääsynhallintaan liittyvä todentamismenetelmä vaatii laajempaa tarkastelua ja kehittämistä, jotta se noudattaa tämän päivän vaatimuksia. Oppilaiden monivaiheinen todentaminen voi olla mahdollista kun toimenpide suunnitellaan oppilaan ikä huomioiden.

Tässä pro gradu -tutkielmassa käsiteltiin perusopetuksessa olevien lasten ja nuorten todentamismenetelmiä sekä tietosuojan ja yksityisyyden suojan toteutumista. Jatkotutkimuksen aiheena voisi olla kehittää perusopetusoppilaiden monivaiheisen todentamisen menetelmää esimerkiksi token-laitteen avulla ja seurata kuinka se parantaa lasten osaamista ja ymmärrystä oman yksityisyyden suojan hallinnassa. Tähän liittyy tiiviisti opetuksenjärjestäjän ohjaamana opetuksessa käytettävien sovellusten käyttöönottoprosessin kehittämistä, jotta nämä saadaan oppilaille kertakirjautmisen piiriin. Tutkimuksessa tuli myös esille toisena tutkimuskohteena lasten tietojen käsittely tietoyhteiskuntapalveluissa mikä on kokonaisuutena huomionarvoinen asia ja asian laajuuden vuoksi olisi oman tutkimuksen arvoinen.

Lähteet

[1] ADJEI, J., JA OLESEN, H. Keeping Identity Private. *IEEE Vehicular Technology Magazine 6*, 3 (2011), 70–79.

[2] ALPÁR, G., HOEPMAN, J., JA SILJEE., B. The Identity Crisis. Security, Privacy and Usability Issues in Identity Management. *Arxiv.org 1101*, 0427 (2011), 1–15.

[3] ANDRESS, J. *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practise.* Waltham, MA, Syngress, 2014.

[4] ARKKITEHTUURIRYHMÄ, K. *Kuntasektorin käyttövaltuushallinnan viitearkkitehtuuri Versio 1.0.* Kuntaliiton verkkojulkaisu, Helsinki, 2013.

[5] ASSAL, H., IMRAN, A., JA CHIASSON, S. An Exploration of Graphical Password Authentication for Children. *ELSEVIER 18* (2018), 37–46.

[6] AUSSEL, J.-D. Smart Cards and Digital Identity. Kirjassa *Identity Management*, P. H. Lehne, Ed. Telektronikk, 2007, ch. 66, ss. 66–78.

[7] BANDAY, M., JA MEHRAJ, S. Directory Services for Identity and Access Management in Cloud Computing. Julkaisusarjassa *2017 3rd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT)* (2017), IEEE, 334–337.

[8] BONNEAU, J., HERLEY, C., VAN OORSCHOT, P. C., JA STAJANO, F. The Quest to Replace Password: A Framework for Comparative of Web Authentication Schemes. *IEEE* (2012), 553–567.

[9] COYNE, E., JA WEIL, T. ABAC and RBAC: Scalable, Flexible, and Auditable Access Management. *IT Professional 15* (2013), 14–16.

[10] CRANOR, L. F., JA BUCHLER, N. Better Together: Usability and Security Go Hand in Hand. *IEEE Security Privacy 16*, 6 (2014), 89–93.

[11] ERIKSSON, P., JA KOISTINEN, K. *Monenlainen tapaustutkimus.* Kuluttajatutkimuskeskus, Helsinki, 2014.

[12] HIRSJÄRVI, S., REMES, P., JA SAJAVAARA, P. *Tutki ja kirjoita*. Tammi, Helsinki, 2010.

[13] HONG KONG POLYTECHNIC UNIVERSITY. Identity and Access Management (IAM). URL https://www.polyu.edu.hk/ags/Newsletter/news0911/IAM_details.html, viitattu 25.7.2020.

[14] JAIN, A., JA NANDAKUMAS, K. Biometric Authentication: System Security and User Privacy. *Computer 45*, 11 (2012), 87–92.

[15] JÄRVINEN, H. *Lakikokoelma 2019, Tietosuojalait*. Edita, Helsinki, 2019.

[16] JÄRVINEN, P. *Arjen tietoturva, vinkit ja ratkaisut*. Docendo, Jyväskylä, 2012.

[17] JYVÄSKYLÄN YLIOPISTO. Aineistonhankintamenetelmät. URL https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/aineistonhankintamenetelmat/, viitattu 8.11.2020.

[18] JYVÄSKYLÄN YLIOPISTO. Tutkimusstrategiat. URL https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimusstrategiat/, viitattu 12.10.2020.

[19] KANANEN, J. *Case-tutkimus opinnäytetyönä*. Suomen Yliopistopaino Oy, Jyväskylä, 2013.

[20] KANANEN, J. *Opinnäytekirjoittajan kirjoittajan opas*. Edita, Jyväskylä, 2015.

[21] KANANEN, J. *Laadullinen tutkimus pro graduna ja opinnäytetyönä*. Jyväskylän ammattikorkeakoulu, Jyväskylä, 2017.

[22] KATSINI, C., FIDAS, C., BELK, M., Y GEORGE SAMARAS, JA AVOURIS, N. A Human Cognitive Perspective of Users' Password Choices in Recognitionbased Graphical Authentication. *International Journal of Human-Computer Interaction* (2019), 1–23.

[23] KIM, H., JA HUH, J. H. PIN Selection Policies: Are they Really Effective? *Computers security 31* (2012), 484–496.

[24] KORJA, J. *Biometrinen tunnistaminen ja henkilötietojen suoja*. PhD thesis, Lapin yliopisto, 2016. URL: https://lauda.ulapland.fi/bitstream/handle/10024/62397/Korja_Juhani_ActaE_193_pdfA.pdf?sequence=2&isAllowed=y, viitattu 1.5.2021.

[25] KUNTALIITTO. Yleinen tietosuoja-asetus. URL https://www.kuntaliitto.fi/yleiskirjeet/2017/yleinen-tietosuoja-asetus, viitattu 29.11.2020.

[26] LASTENSUOJELUN KESKUSLIITTO. Lapsi verkossa – Näkökulmia lasten oikeuksiin ja tietosuojaan digitaalisessa ympäristössä. URL https://www.lskl.fi/materiaali/lastensuojelun-keskusliitto/Lapsi-verkossa.pdf, viitattu 24.8.2020.

[27] LASTENSUOJELUN KESKUSLIITTO. Nuoret verkossa Raportti nuorille suunnatun kyselyn vastauksista. URL https://www.lskl.fi/materiaali/woocommerce_uploadslastensuojelun-keskusliitto/LSKL_DigiSelvitys_0377.pdf, viitattu 24.8.2020.

[28] LINDEN, M. *Identiteetin ja pääsynhallinta.* Tekninen raportti, Tampereen teknillinen yliopisto, 2017. URL: https://tutcris.tut.fi/portal/files/3087873/linden_identiteetin_ja_paasynhallinta.pdf/, viitattu 10.3.2020.

[29] MAQSOOD, S., MAQSOOD, S., BODDLE, R., JA CHIASSON, S. An Exploratory Study of Children's Online Password Behaviours. Julkaisusarjassa *IDC '18: Proceedings of the 17th ACM Conference on Interaction Design and Children* (2018), Association for Computing Machinery, 539–544.

[30] NAIK, N., JA JENKINS, P. *A Secure Mobile Cloud Identity: Criteria for Effective Identity and Access Management Standards.* Tekninen raportti 16022663, IEEE, 2016.

[31] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *Digital Identity Guidelines Authentication and Lifecycle Management*, 2017.

[32] O'GORMAN, L. Comparing Passwords, Tokens, and Biometrics for User Authentication. *IEEE 91*, 12 (2003), 2021–2040.

[33] OPETUSHALLITUS. Perusopetuksen opetussuunnitelman perusteet 2014.

[34] OPETUSHALLITUS. Tietoturva ja -suoja kouluissa. URL https://www.oph.fi/fi/koulutus-ja-tutkinnot/tietoturva-ja-suoja-koulussa/, viitattu 24.7.2020.

[35] QUADRI, S. L., KAZIM, A., JA ADITYA. Cloud and Biometrics: The Future of Authentication. *International Journal of Advanced Research in Computer Science 8*, 2 (2017), 88–91.

[36] RISTO HEINONEN. Luottamus verkkoasiointiin edellyttää yksityisyyden suojaa. URL `https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/78509/3_2006.pdf?sequence=1`, viitattu 22.5.2021.

[37] ROMMETVEIT, K., TANAS, A., JA VAN DIJK, N. Data Protection by Design: Promises and Perils in Crossing the Rubicon Between Law and Engineering. Julkaisusarjassa *Privacy and Identity Management* (2017), Springer, 25–37.

[38] SUOMEN TIETOSUOJAPALVELUT OY. Yleistä tietosuojasta. URL `https://opitietosuojaa.fi/fi/aloitus/tietosuoja`, viitattu 24.8.2020.

[39] THUAN, D. V. Identity Management Demystified. Kirjassa *Identity Management*, P. H. Lehne, Ed. Telektronikk, 2007, ch. 11, ss. 11–18.

[40] THUAN, D. V., JA JORSTAD, I. The Ambiguity of Identity. Kirjassa *Identity Management*, P. H. Lehne, Ed. Telektronikk, 2007, ch. 3, ss. 2–10.

[41] TIETOSUOJAVALTUUTETUN TOIMISTO. Tietosuojaperiaatteet. URL `https://tietosuoja.fi/tietosuojaperiaatteet`, viitattu 29.11.2020.

[42] TIETOSUOJAVALTUUTETUN TOIMISTO. Tietoturvaloukkaukset. URL `https://tietosuoja.fi/tietoturvaloukkaukset`, viitattu 2.4.2021.

[43] TSVETKOV, K. S., JA GEORGIEV, T. An Alternative Aapproach and Attempt to Come up With a Standard for Biometric User authentication in a network based environment. *ELSEVIER 47* (2012), 74–78.

[44] VAIDYA, S. A., JA BHOSALE, V. Invisible Touch Screen Based PIN Authentication to Prevent Shoulder Surfing. *International Journal for Research in Applied Science Engineering Technology 6*, IV (2018), 3196–3199.

[45] VALTIONHALLINNON TIETOTURVALLISUUDEN JOHTORYHMÄ, V. *Käyttövaltuushallinnon periaatteet ja hyvät käytännöt*. Edita Prima Oy, Helsinki, 2006.

[46] VAN GREUNEN, D. Ethics, Children and Biometric Technology. *IEEE Technology and Society Magazine 35*, 3 (2016), 67–72.

[47] VIESTINTÄVIRASTO, SANASTOKESKUS TSK, HUOLTOVARMUUSKESKUS. Kyberturvallisuuden sanasto. URL https://www.tsk.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf, viitattu 25.4.2020.

[48] WARRKENTIN, M., JA ORGERON, C. Using the Security Triad to Assess Blockchain Technology in Public Sector Applications. *International Journal of Information Management 52*, 102090 (2020), 1–8.

[49] YIN, R. K. *Case Study Research Design and Methods*. Sage publications, United Kingdom, 2009.

A Sähköinen lomakekysely perusopetuksen tunnistautuminen

Perusopetuksen oppilaiden tunnistautuminen

Kyselyssä ei kerätä henkilötietoja. Kyselyn tarkoituksena on selvittää, mitä tunnistautumismenetelmiä perusopetuksen oppilailla on käytössä, kun kirjaudutaan opetuksessa käytettäviin digitaalisiin palveluihin / järjestelmiin. Miten toimivia käytössä olevat tunnistautumismenetelmät ovat perusopetuksen oppilaiden käytössä. Lisäksi tarkastellaan, kuinka 1-2 lk oppilaiden tunnistautuminen on toteutettu ja mitä haasteita 1-2 lk oppilaiden tunnistautumiseen ja tunnistautumismenetelmiin liittyy.

1. Mikä tunnistautumismenetelmä perusopetuksen oppilailla on käytössä? *

- ◯ Käyttäjätunnus ja salasana
- ◯ Kertaluonteinen salasana (esim. token tai pin -koodi)
- ◯ Biometrinen tunniste esim. sormenjälkitunniste
- ◯ Kuvio (esim tabletin aukaisuun)
- ◯ Yubikey
- ◯ Muu, mikä

2. Mikäli perusopetuksen oppilailla on käytössä käyttäjätunnus + salasana tunnistautuminen, oletteko harkinnut oppilaille muuta tunnistautumismenetelmää? *

- ☐ Kertaluonteinen salasana (token)
- ☐ Biometrinen tunnistautuminen (esim. sormenjälki)
- ☐ Graafinen kuvio
- ☐ YubiKey
- ☐ Muu, mikä
- ☐ Muuta tunnistautumismenetelmää ei ole harkittu

Federoitu pääsynhallinta tarkoittaa organisaatiorajat ylittävää pääsynhallintaa ja tarjoaa yleensä sekä organisaation sisäisen että organisaatiorajat ylittävän kertakirjautumisen.

3. Kuinka perusopetuksen oppilaiden identiteetinhallinta ja tunnistautuminen on toteutettu? *

- [ ] Eri tunnistautuminen jokaiseen käytössä olevaan järjestelmään/ palveluun, (esim. eri kt+ss)
- [ ] Yhden käyttäjätunnuksen ja salasanan periaate + erillinen kirjautuminen käytössä oleviin järjestelmiin/ palveluihin
- [ ] Kertakirjautuminen orgnisaation sisäisiin järjestelmiin/palveluihin
- [ ] Federoitu identiteetinhallinta
- [ ] Jokin muu toimintamalli

4. Hallinnoidaanko oppilaiden oppimisympäristön käyttäjätunnuksia Wilman avulla? *

- ◯ Kyllä
- ◯ Ei

5. Onko kunnassanne käytössä MPASSid kertakirjautuminen Wilma tunnuksilla? *

- ◯ Kyllä
- ◯ Ei

6. Onko 1-2 lk oppilailla tunnukset käytössä seuraaviin palveluihin: *

- [ ] Wilma
- [ ] Sähköposti
- [ ] Sähköinen oppimisympätistö
- [ ] Muu, mikä/mitkä

7. Kirjaa 1-3 kehitysehdotusta 1-2 lk oppilaiden tunnistautumiseen liityen *

Perusopetuksen opetussuunnitelmassa on vuosiluokittain määritelty laaja-alaisen osaamisen osa-alueet. Osa-alue L5 määrittää Tieto- ja viestintäteknologisen osaamisen.
Tieto- ja viestintäteknologian osa-alue jakaantuu neljään pääalueeseen, joista yksi on "Oppilaita opastetaan käyttämään tieto- ja viestintäteknologiaa vastuullisesti, turvallisesti ja ergonomisesti".

Opetuksenjärjestäjät ovat määritelleet tvt -taitotasot vuosiluokittain. Tunnistautumiseen liittyen 1. lk oppilaan yksi taitotasoista on "Oppilas ymmärtää käyttäjätunnuksen (ja salasanan) merkityksen".

8. Kuinka näette, että tvt -taitotaso käyttäjätunnuksen ja salasanan merkityksen opettaminen 1-2 lk oppilaille toteutuu?

9. Mikäli teillä on perusopetuksessa käytössä keskitetty identiteetin- ja pääsynhallinta. Kuinka moneen palveluun / järjestelmään oppilas voi tällä tunnistautumismenetelmällä kirjautua? *

- [ ] 1-4
- [ ] 5-9
- [ ] 10-15
- [ ] yli 16

10. Luettele palvelut, joihin perusopetuksen identiteetin- ja pääsynhallinnan kautta oppilaalle luotuja tunnuksia käytetään.

11. Voiko oppilas hallinnoida tunnustaan esim. salasanaa itsepalvelun kautta? *

- ◯ Kyllä
- ◯ Ei

12. Kuinka monta eri tunnusta (tai tunnistautumismenetelmää) oppilaalla on käytössä? esim. kuinka monta kt+ss oppilaalla on käytössä opetukseen liittyen? (keskitetyn identiteetinhallinan luomien tunnusten lisäksi) *

- [ ] 1-4
- [ ] 5-9
- [ ] yli 10

13. Kuinka moneen järjestelmään / palveluun oppilaalla vaaditaan erillinen kirjautuminen? (tunnistautumismenetelmä esim. kt+ss voi olla sama mutta kirjautuminen vaaditaan erikseen) *

- [ ] 1-4
- [ ] 5-9
- [ ] yli 10

14. Onko oppilailla käytössä sähköinen työpöytä?

- [ ] Desku
- [ ] Muu, mikä
- [ ] Edison
- [ ] Ei ole käytössä sähköinen työpöytä

15. Koetteko, että sähköisestä työpöydästä on apua oppilaalle digitaalisten palveluiden käytössä?

16. Oletteko huomioinut identiteetin- ja pääsynhallinnassa turvakiellon alaiset oppilaat erillisenä toimintamallina? *

- ◯ Kyllä
- ◯ Ei

17. Koetko, että nykyisessä perusopetuksen oppilaiden tunnistautumisessa toteutuu tietosuojan vaatimukset *

- ◯ Hyvin
- ◯ Tyydyttävästi

◯ Tietosuojavaatimukset eivät toteudu vaaditulla tavalla. Miten toimintaa tulisi kehittää, jotta tietosuojan vaatimukset toteutuisivat

18. Mainitse 1-3 kehitysehdotusta, miten perusopetusoppilaiden tunnistautumismenetelmää voisi kehittää. *

19. Olen tutustunut sähköpostin liitteenä olevaan tietosuojaselosteeseen *

☐

B Teemahaastattelu runko

Teemahaastattelurunko

Teemat ja päänäkökohdat:

Teema 1: Perusopetuksen oppilaiden identiteetin- ja pääsynhallinta.

a. Opetetaanko oppilaille heidän ikänsä huomioiden riittävällä tasolla identiteetin- ja pääsynhallintaan liittyvää yksityisyyden suojan merkitystä digitaalisissa ympäristöissä?

Teema 2: Perusopetuksen oppilaiden todentamismenetelmä.

a. Perusopetuksen oppilaiden todentaminen on pääsääntöisesti käyttäjätunnus ja salasana. Mikä on sinun näkökulmasi, voisiko perusopetuksen oppilailla kokeilla jotain muuta todentamismenetelmää, esimerkiksi graafista salasanaa?
b. Voisiko todentamismenetelmän vaikeusaste kasvaa oppilaan mukana?
c. Mitä kehittäisit perusopetuksen oppilaiden todentamiseen ja digitaalisten välineiden käyttöön liittyen ensitilassa?

Teema 3: Tietosuoja

a. Toteutuuko sinun mielestäsi perusopetuksen oppilaiden identiteetinhallinnassa tietosuojan vaatimukset?
b. Miten tietosuojaa voitaisiin vielä kehittää?

Teema 4: 1-2 luokan oppilaiden digitaalisten oppimisympäristöjen käyttö

a. Mikä on 1-2 luokan oppilaiden digitaalisten välineiden ja ympäristöjen käytössä haastavinta?
b. Kuntien tieto- ja viestintätekniikan taitotasoissa on useissa mainittu 1 luokan oppimistavoitteiksi, että oppilas ymmärtää käyttäjätunnuksen ja salasanan merkityksen.
   - Mitä haasteita näet tässä?
   - Miten perusopetuksen oppilaat saadaan samanarvoiseen asemaan tämän oppimistavoitteen osalta?