28.2.2022

UNIFI ry

Tietoturvallinen tunnistautuminen yliopisto-opiskelussa

1 TYÖRYHMÄ

Lakimies Laura Aivio, Itä-Suomen yliopisto
Tietohallintojohtaja Kari Keinänen, Oulun yliopisto
Järjestelmäasiantuntija Juha Martikainen, Aalto-yliopisto
Opintoasiainjohtaja Petri Sjöblom, Turun yliopisto
It- och avtalsjurist Ia Wilson, Åbo Akademi

2 TOIMEKSIANTO

Työryhmän tehtävänä on luoda kokonaiskuva sähköisen tunnistautumisen käyttötarkoituksista ja laatia yliopistojen yhteinen käsitys siitä, milloin a) opiskelijalta voidaan ylipäätään edellyttää tunnistautumista; b) missä Digitaalisten palveluiden tarjoamisesta annetun lain (306/2019, ”digipalvelulaki” tai ”DPL”) tarkoittamaa vahvaa tunnistautumista tarvitaan ja c) millaista tunnistautumisjärjestelmää voidaan käyttää.

Toimeksiannon yksityiskohtainen sisältö oli seuraava:

Työryhmän työssä tulee huomioida käynnissä oleva OKM:n CSC:lle toimeksiantama Level of Assurance -selvitys identiteetin hallinnan kysymyksistä, yhteydet Digivisio 2030 -hankkeen työhön sekä FUCIO:n piirissä tehtävä tekninen selvitystyö.

Digitaalisten palveluiden tarjoamisesta annettu laki (306/2019, digipalvelulaki tai DPL) tuli voimaan 1.4.2019. Digipalvelulaissa säädetään ensimmäistä kertaa kansallisen lain tasolla vahvan tunnistautumisen vaatimuksista viranomaisen digitaalisiin palveluihin (eli verkkosivustoihin ja mobiilisovelluksiin). Käytännössä digipalvelulaki edellyttää vahvaa sähköistä tai tätä vastaavaa muuta tietoturvallista tunnistustapaa digitaaliseen palveluun, mikäli palvelu pitää sisällään salassa pidettävää tietoa.

Yliopistoilla on käytössä useita erilaisia organisaatiokohtaisia ja organisaatioiden yhteisiä oppimisympäristöjä tai niihin läheisesti liittyviä ratkaisuja, jotka ovat digipalvelulain tarkoittamia digitaalisia palveluita (esim. Moodle, Exam sekä O365/Teams). Yliopistojen yhteistä tulkintaa vahvasta tunnistuksesta

oppimisympäristöihin tarvitaan yliopistojen digitaalisiin oppimisympäristöihin liittyvän sujuvan yhteistyön turvaamiseksi.

Taustavalmistelun perusteella on todettu yliopistojen yhteistä tulkintaa ja ratkaisua tarvittavan erityisesti seuraavissa kysymyksissä:

- *Missä tilanteissa opiskelijalta voidaan edellyttää tunnistautumista?*
- *Missä tilanteissa tulee edellyttää vahvaa tunnistautumista?*
- *Mikä on tunnistuspalvelu, joka täyttää digipalvelulain vahvan tunnistamisen vaatimukset? Voiko kaksivaiheinen tunnistus (kuten MFA) jo itsessään olla DPL 6.2 §:ssä viitattua ”vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain 2 §:n 1 momentin 1 kohdassa tarkoitettua vahvaa sähköistä tunnistamista”?*

3 TYÖRYHMÄN YHTEYDET MUIHIN TYÖRYHMIIN

SEC-työvaliokunnan asettaman ryhmän selvitystyö

Kansallisella tasolla korkeakoulut ovat pitkään tehneet yhteistyötä tietoturvaan liittyvissä asioissa FUCIO-verkoston ja sen nimittämän, korkeakoulujen tietoturvapäälliköiden muodostaman, SEC-työvaliokunnan kautta. Tietoturvaan liittyvissä asioissa korkeakoulujen osaaminen on kansallisella tasolla tunnustettu ja tietoturvapäälliköt ovat osallistuneet aktiivisesti mm. VM:n koordinoimaan julkisen hallinnon digitaalisen turvallisuuden valmistelu- ja kehittämistyöhön (Vahti).

Työryhmän työssä on huomioitu SEC-työvaliokunnan nimittämän SEC-työryhmän asiaan liittyvä erillinen selvitystyö. Työryhmän ja SEC-työryhmän välillä ei ole olennaista näkemyseroa toimeksiannon piiriin kuuluvista asioista.

OKM:n CSC:lle toimeksiantama Level of Assurance –selvitys, yhteydet DigiVisio 2030 -hankkeen työhön ja muut kansalliset hankkeet

Työryhmä on toimeksiannon kuluessa kokoontunut säännöllisesti keskustelemaan selvitystyöstä ja tulkinnoista yhdessä CSC:n, OKM:n sekä DigiVision edustajien kanssa jakaakseen tietoa oman työnsä edistymisestä ja keskustellakseen siinä esitettävistä tulkintalinjauksista. Itse LoA -selvitys tai DigiVisio -työ ei kuitenkaan ole ollut työryhmän toimikauden aikana vielä siinä vaiheessa, että niistä olisi ollut työryhmälle tukea.

Lausunnon valmistelussa on tunnistettu meneillään olevat asiaan liittyvät kansalliset hankkeet mm. OKM:n asettama opetuksen ja koulutuksen toimialan identiteetinhallinnan kehittämishanke, CSC:n laatima esitys sähköisen tunnistamisen varmuustasoista (Level of Assurance, LoA) ja Digi-ja väestötietorekisterin selvityksessä oleva Valtiovarainministeriön digitaalisen henkilöllisyyden kehittämishanke

(VM161:00/2020, 8.10.2020–30.6.2023) ja siihen liittyvä digitaalista henkilöllisyyttä koskevan lainsäädännön valmistelu (VM092:00/2021, 1.8.2021–31.8.2022)[1]. Lisäksi yllä mainitun DigiVisio 2030 -hankkeen yhtenä osa-alueena (TP3: Arkkitehtuuri, tekniset ratkaisut ja tietoturva) tarkastellaan myös tämän työryhmän toimeksiantoa lähellä olevia kysymyksiä liittyen tieto-, tietojärjestelmä-, tietoturva- ja tietosuoja-arkkitehtuuriin, identiteetinhallintaan (ulkomaalaisten opiskelijoiden tunnistaminen, identiteettiin kytkeytyvien perustietojen hallinta, tunnusten ja oikeuksien elinkaaren hallinta) sekä digitaalisten palveluiden teknisiin vaatimuksiin.

Edellä mainituista hankkeista tulokset valmistuvat vasta myöhemmin.

Korkeakoulujen lakimiesverkoston ja IT-asiantuntijoiden yhteinen tulkinta DPL 6.2 §:sta

SEC-työryhmän jäsenet ja yliopistojen IT-asioita käsittelevät lakimiehet kokoontuivat toimeksiannon kuluessa lisäksi erilliseen kokoukseen keskustelemaan lakimiesverkoston ja tietoturvapäälliköiden näkemyksistä koskien DPL 6.2 §:n tulkintaa. Näkemys niin vahvaan tunnistautumiseen liittyvästä menettelystä, vaadittavista tunnistustavoista kuin digipalvelulain soveltamisesta suhteessa opiskelijoihin oli yhteneväinen tämän työryhmän selvityksen johtopäätösten kanssa.

Yhteenvetona digipalvelulain soveltamiseen liittyvistä kysymyksistä voidaan todeta, että eri työryhmien kesken vallitsee yhteisymmärrys siitä, että digipalvelulain esiin tuomat tunnistamiseen liittyvät haasteet on ratkaistavissa jäljempänä esitetyllä tulkinnalla ja nykyisiä menettelyitä edelleen kehittämällä.

Työryhmän keskeisten johtopäätösten voidaan siten todeta olevan toimeksiannon edellyttämällä tavalla yliopistojen yhteinen näkemys:

[1] Euroopan komissio antoi 3.6.2021 ehdotuksen (COM (2021) 281 final) asetukseksi eurooppalaisesta digitaalisesta identiteetistä. Eurooppalainen digitaalinen identiteetti olisi EU:n kansalaisille, EU:ssa asuville henkilöille sekä yrityksille tarkoitettu väline tunnistautumista ja henkilöön liittyvien tietojen osoittamista varten. Sitä voitaisiin käyttää sekä julkisissa että yksityisissä sähköisissä ja muissa palveluissa. Jokainen kansalainen ja EU:n alueella asuva saisi käyttöönsä valtion takaamaan identiteettiin liittyvän henkilökohtaisen digitaalisen lompakon.

Asetusehdotuksen tarkoituksena on uudistaa vuonna 2014 annettua eIDAS-asetusta sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla. Ehdotuksessa pyritään edistämään rajat ylittävää sähköistä tunnistamista kahdella rinnakkaisella keinolla.

Työryhmän keskeiset näkemykset tiivistetysti	
1.	Tietoturvallisen tunnistautumisen osalta digipalvelulain vaatimusten täyttymistä voidaan ja tulee yliopisto-opiskelijan osalta arvioida kontekstisidonnaisesti eli ottaen huomioon sekä a) yliopistojen hallinnollinen asema, b) niiden omat tietoturvajärjestelyt ja tietoturvatyö, että c) opiskelijoiden ja yliopiston suhteen yliopistolaista johtuva erityisluonne. Näin myös riippumatta siitä, katsotaanko yliopisto-opiskelija juridis-hallinnollisesti ”yleisöksi” vai ei.
2.	Yliopistoilla on autonomia myös digipalvelulain tulkintaan, ja tulkintojen lainmukaisuutta arvioivat kanteluiden kautta lopulta kansallisen tason laillisuusvalvojat.
3.	Tapa, jolla yliopistot nykytilanteessa suunnittelevat ja toteuttavat opiskeluun liittyviä digitaalisia palveluitaan ja huolehtivat opiskelijoidensa tietoturvallisesta tunnistautumisesta, täyttää keskeisiltä osiltaan digipalvelulain vaatimukset, kun MFA:ta hyödynnetään O365 -ympäristössä ja Haka-kirjautumisessa.
4.	Yliopistoissa on tunnistettu tämän alueen keskeiset kehittämiskohteet ja niiden eteen tehdään aktiivisesti työtä. Lisäksi yliopistot kehittävät muutenkin ammattimaisesti, proaktiivisesti ja yhteistyössä tietoturvaan liittyviä toimintatapojaan.
5.	Jatkossa yliopistojen (tai korkeakoulujen) tietoturvallisen tunnistamisen alueella tulisi olla Suomen tasolla yksi nimetty, kaikkien toimijoiden tunnistama pääkontakti, joka ylläpitää keskitettyä tietoa nykytilanteesta ja työn alla olevasta kehityksestä.

4 JOHDANTO

4.1 Tehtävän rajaus

Työryhmä on toimeksiantonsa mukaisesti rajannut tarkastelun koskemaan yliopistoja ja yliopisto-opintoja. Tehtävään käytettävissä olleen ajan ja resurssien näkökulmasta tämä on ollut myös välttämätöntä, sillä tehtävä on ollut jo yliopistokontekstiin rajattunakin vaativa ja monitahoinen. Ammattikorkeakoulujen edustajan kanssa käydyn keskustelun perusteella näyttää kuitenkin siltä, että johtopäätökset ovat mahdollisesti sovellettavissa sellaisenaan myös ammattikorkeakouluympäristössä.

4.2 Opiskelijan käsite

Opiskelijalla tarkoitetaan tässä raportissa yliopistojen kaikkia niitä opiskelijaryhmiä, joille myönnetään yliopiston käyttäjätunnus eli esimerkiksi myös avoimen yliopiston opiskelijoita.

4.3 Yliopistojen toimivalta DPL:n tulkinnassa ja tulkinnan laillisuusvalvonta

Yliopistoilla on toimivalta tulkita niitä koskevia lakeja autonomisesti, silloin kun lain sanamuoto on tulkinnanvarainen eikä lain valmisteluasiakirjoistakaan löydy yksiselitteistä vastausta.

Digipalvelulain valmisteluasiakirjojen mukaan 2 luvussa säädettyjen vastuiden ja velvollisuuksien valvonta tapahtuu yleisen laillisuusvalvonnan toimesta eikä lain 2 luvun valvonta kuulu digipalvelulaissa tarkoitetun valvontaviranomaisen toimivaltaan. Käytännössä valvonta tapahtuu eduskunnan oikeusasiamiehen ja valtioneuvoston oikeuskanslerin toimesta. Yliopistojen tulkinnan lainmukaisuus voidaan siis testata kantelumenettelyllä, ja yliopistot luonnollisesti muuttavat käytäntöään, mikäli niiden tulkinta todettaisiin lainvastaiseksi.

4.4 Yliopisto-opiskelijat yliopiston sähköisten palveluiden käyttäjinä vs. kansalaiset yleisesti viranomaisten palveluiden käyttäjinä

Digipalvelulain soveltamisalasäännöksen (3 §) mukaan sen 2 luvun säännöksiä sovelletaan **yleisölle** tarjottaviin viranomaisen digitaalisiin palveluihin. Tunnistautumiseen liittyvä sääntely on nimenomaisesti lain 2 luvussa, minkä vuoksi sekä tämä työryhmä että muut samaa aihetta koskevia kysymyksiä syksyn 2021 aikana pohtineet tahot ovat joutuneet ottamaan kantaa myös soveltamisalakysymykseen. Koska yleisön käsite on ratkaiseva digipalvelulain säännösten soveltamisen kannalta, digipalvelulain mukaista yleisön käsitettä on syytä arvioida lyhyesti yliopiston näkökulmasta ja lisäksi suhteessa siihen, mikä vaikutus tällä käsitemäärittelyllä on yliopisto-opiskelijoilta edellytettävään tunnistautumiseen ja siinä tehtäviin tulkintoihin.

Ovatko yliopisto-opiskelijat digipalvelulaissa tarkoitettua ”yleisöä”?

Yliopiston tutkinto-opiskelijoiden on perinteisesti katsottu olevan oikeudelliselta asemaltaan suhteessa yliopistoon hallinnon palveluiden käyttäjiä.[2] Digipalvelulaissa yleisön käsite esiintyy hieman eri yhteyksissä (saavutettavuusvaatimukset / tunnistautumiseen liittyvä sääntely). Määritelmä tukee opiskelijoiden yleisö-roolia myös digipalvelulain tarkoittamalla tavalla. Yleisöllä tarkoitetaan digipalvelulain 2 luvussa ”*hallinnon asiakkaita, joita ovat viranomaisen organisaation ulkopuolinen palvelusta riippuen ennalta rajattu tai rajaamaton luonnollisten henkilöiden tai oikeushenkilöiden joukko”.*[3] Tätä voidaan pitää yleisemminkin yleisön määritelmänä digipalvelulaissa.

Digipalvelulain soveltamista yliopistoissa koskevassa oikeuskirjallisuudessa[4] on asiaa pohdittu laajemmin todeten mm. seuraavaa: *”Opiskelijoiden kohdalla on nimittäin huomioitava, että opiskelijat ovat yliopistolain (558/2009) 4 §:n nojalla yliopistoyhteisön jäseniä, samoin kuin opetus- ja tutkimushenkilöstö sekä muu henkilöstö”.*[5] Yliopistolain määritelmän perusteella opiskelijat eivät siis vaikuta yliopisto-organisaation ulkopuolisilta sillä tavalla, miten DPL:ssa yleisöstä on säädetty. Digipalvelulain soveltamisalan kokonaisuuden huomioiden DPL:n yleisön käsitettä on kuitenkin tulkittava laajasti. *Voutilaisen* mukaan *”Digipalvelulain näkökulmasta yleisön käsitteen piiriin kuuluvat asianosaisten, ve-*

[2] Esim. *Tiukkanen 1995*: Opiskelijan oikeusasema.
[3] HE 60/2018 vp, s. 54.
[4] *Hiltunen-Sariola 2020: Digipalvelulain soveltamisesta yliopistoissa* (https://jyx.jyu.fi/handle/123456789/72441).
[5] Yliopistoyhteisöön luetaan yliopistolain 4 §:n perusteella myös kaikki opiskelijat (HE 7/2009 vp, s. 53).

rovelvollisten, kunnan asukkaiden, etuisuuksien saajien, luvanhakijoiden, ilmoituksen tekijöiden, yritysten ja yhteisöjen ohella myös opiskelijat. Ratkaisevaa on se, ettei digitaalista palvelua käytetä palvelussuhteen perusteella".[6]

Näin ollen, vaikka opiskelijat ovatkin osa yliopistoyhteisöä, he ovat digipalvelulain soveltamisen osalta yleisöä. Samaan tulkintaan päädyttiin myös edellä kohdassa 3 mainittujen muiden työryhmien kanssa käydyissä keskusteluissa, vaikkakin vaihtelevin painotuksin. Työryhmän näkemys on lisäksi, että yleisökäsitteen juridisen määrittely ei sinänsä ohjaa yliopistojen suhtautumista ja toimenpiteitä, sillä yliopistot joka tapauksessa katsovat tehtäväkseen parhaan kykynsä mukaan toteuttaa digipalvelulain 1 §:ssä mainittua lain tarkoitusta ”edistää digitaalisten palvelujen saatavuutta, laatua ja tietoturvallisuutta” – mikä edellyttää seuraavassa suositeltuja ratkaisuja.

5 DPL 6.1 § EDELLYTTÄMÄ TUNNISTAUTUMINEN JA YLIOPISTOJEN NYKYKÄYTÄNNÖT

5.1 Missä tilanteissa opiskelijalta voidaan edellyttää tunnistautumista?

Digipalvelulain 6.1 §:n mukaan viranomainen voi vaatia digitaalisessa palvelussa käyttäjältä sähköistä tunnistamista vain, jos se on tarpeen palvelun tai sen tietosisältöön liittyvien käyttöoikeuksien varmistamiseksi tai palvelussa tehtävään toimeen liittyvien oikeusvaikutusten vuoksi.

Opiskelijan yliopistoissa käyttämät sähköiset palvelut, esim. oppimisympäristöt tai tenttisovellukset ovat kaikki sellaisia, joissa lainkohdan vaatimukset täyttyvät ja tunnistautuminen on välttämätöntä.

Yliopisto ei sen sijaan voi vaatia tunnistusta esimerkiksi tyhjille lomakkeille pääsyyn tai digitaalisissa palveluissa yleisesti tarjolla olevaan informaatioon.[7]

5.2 Yliopistojen nykykäytännöt opiskelijoiden tunnistamisessa

5.2.1 Yleistä

Yliopiston opiskelijoille tarjoamat palvelut ovat itsehallinnollisesti järjestettyjä organisaation sisäisiä palveluita jo ennestään tunnistetuille käyttäjille**.** Lisäksi Korkeakoulujen Haka-federaation kautta yliopistojen käyttäjät käyttävät ristiin toistensa sisäisiä digitaalisia palveluita.

Opiskelijoiden yliopistoissa käyttämät digitaaliset palvelut (kuten oppimisympäristöt) ovat kaikki sellaisia, joihin on pääsy vain opiskeluoikeuden perusteella ja siihen liittyvän vahvan ensitunnistautumisen kautta myönnettävällä henkilökohtaisella käyttäjätunnuksella. Järjestelmäkohtainen käyttö tapahtuu tämän jälkeen käyttäjätunnuksen ja salasanan yhdistelmällä tai jäljempänä tarkemmin eritellysti kaksivaiheisen tunnistautumisen avulla.

[6] *Voutilainen 2020*: Digitaalisten palvelujen sääntely, s. 189.
[7] HE 60/2018 vp

5.2.2. Yliopistoissa opiskelijan tunnistaminen suoritetaan vahvasti opiskelun alkaessa (ensitunnistaminen) ja aina käyttäjätunnuksen käyttöoikeutta luovutettaessa

Korkeakouluissa opiskelijan tunnistaminen suoritetaan nykyisen käytännön mukaan vahvasti (paikan päällä henkilötodistuksen avulla tai vahvan sähköisen tunnistautumisen kautta suomi.fi -palvelussa) opiskelun alkaessa (ensitunnistaminen) ja näin ollen aina ennen kuin opiskelijalle luovutetaan korkeakoulujen sähköisiin ympäristöihin kirjautumiseen vaadittavan henkilökohtaisen käyttäjätunnuksen käyttöoikeus.

Poikkeuksena tästä pääsäännöstä ovat ne kv-opiskelijat, jotka eivät tule fyysisesti paikan päälle ja joilla ei ole mahdollisuutta suomi.fi -tunnistautumiseen (ei suomalaista henkilötunnusta). Eri yliopistoissa (mm. Jyväskylän ja Lapin yliopistot) on kuitenkin parhaillaan käynnissä pilotteja, joissa kv-opiskelija tunnistetaan passin ja videon avulla (biometrinen tunnistus). Kansainvälisten opiskelijoiden ensitunnistamisen haasteet on tunnistettu yliopistoissa ja asian ratkaisemiseksi vaadittavan biometrisen tunnistamisen käyttöönoton vaihtoehtojen selvitys on meneillään ja tullee yhdessä digitaaliseen henkilöllisyyteen liittyvän laajemman lainsäädäntöhankkeen etenemisen kanssa tuomaan ratkaisuja tähän.

Yliopistojen Haka -luottamusverkoston ensitunnistuskäytäntö kuitenkin muuttuu 1.2.2022 alkaen mahdollistaen kolmiasteisesti nousevan vaatimusjärjestyksen. Tämä mahdollistaa kotiorganisaatioille tunnistamisen keveimmillään esimerkiksi sähköpostin avulla. Tähän liittyen Haka -luottamusverkoston tunnistamisattribuutteihin on lisätty uusi ”eduPersonAssurance -attibuutti”, johon tunnistamistaso merkitään. Muutos vaatii Haka -organisaatioilta teknistä muutosta identiteetinhallintaan sekä palveluiden kirjautumiskäytäntöihin silloin, kun palvelun sisältöä on rajattava kevyesti tunnistettujen käyttäjien osalta. Suhteessa digipalvelulain asettamiin tunnistamisen vaatimuksiin ja jäljempänä kohdassa 6 esitettäviin ratkaisumalleihin opiskelijoiden vahvan tunnistamisen tavasta ja sen DPL 6.2 §:n mukaisista perusteita, tulee yliopistojen ehdottomasti huomioida vahvan ensitunnistuksen vaatimus myös 1.2.2022 jälkeen Haka -luottamusverkostoa koskevissa ratkaisuissaan.

5.2.3 Yliopistoyhteisön sisäinen asiakirjojen ja tietojen käsittely tapahtuu käyttäjätunnuksen kautta, tarvittaessa monivaiheista todentamista (MFA) soveltaen:

Useassa yliopistossa on vahvan ensitunnistamisen ohella käytössä jo nykyisellään sähköisiin ympäristöihin kirjauduttaessa lisäksi pelkän käyttäjätunnus-salasana-parin ohella jäljempänä tarkemmin kuvattava MFA (Multi-Factor-Authentication) muun muassa Microsoft-ympäristössä käytettäviin digitaalisiin järjestelmiin kirjautumiseksi. Käytäntö on kuitenkin toistaiseksi kirjavaa, vaikka MFA-tunnistautumisen käyttöala onkin laajenemassa yliopistokentässä. Myös yliopistojen luottamusverkoston Haka-tunnistautumiseen on mahdollista liittää MFA-tunnistuspalvelu, kuten esimerkiksi Tampereen yliopisto ja Aalto yliopisto ovat jo tehneet.

Käyttäjätunnuksen hallinta on järjestetty sisäisesti ja sen turvajärjestelyissä noudatetaan kulloinkin tarpeellisia turvajärjestelyjä siten, kuin laki julkisen hallinnon tiedonhallinnasta (906/2019, ”tiedonhallintalaki” tai ”TihL”) edellyttää. Yliopistojen omat tunnistuspalvelut on rakennettu tietoturvallisiksi, poikkeusoloissa toimiviksi ja vikasietoisiksi ja niiden tietoturvallisuus perustuu jatkuvaan riskiarviointiin ja todenmukaiseen uhka-arvioon.

5.3 Tarkemmin ensitunnistamisesta

Ensitunnistamisella tarkoitetaan tunnistusvälineen hakijan henkilöllisyyden todentamista välineen hankkimisen yhteydessä. Vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain (617/2009; ”tunnistuslaki”) mukaan ensitunnistaminen tulee tehdä henkilökohtaisesti tai sähköisesti siten, että sähköisen tunnistamisen korotetulle tai korkealle varmuustasolle säädetyt vaatimukset täyttyvät. Passeja, henkilökortteja ja vahvoja sähköisiä tunnistusvälineitä voi pitää sekä luotettuina identiteetin lähteinä että henkilöllisyyden verifiointitapoina.

Ensitunnistamismenettelyt voidaan jakaa viiteen eri tapaan[8]:

1) Henkilöllisyys tarkistetaan käyntiasioinnissa henkilön esittämästä viranomaisen asiakirjasta eli yleensä passista tai henkilökortista ja erikseen vielä väestötietojärjestelmästä.

2) Henkilöllisyys tarkistetaan etäyhteydellä henkilön esittämästä viranomaisen asiakirjasta eli yleensä passista tai henkilökortista (niin kutsuttu etäidentifiointi, remote identification) ja erikseen vielä väestötietojärjestelmästä. Viranomaisen asiakirjan esittämisessä on voitava varmistua siitä, että asiakirja on aito ja että asiakirja on esittäjän oma. Näiden varmistamiseen liittyy useita luotettavuuskysymyksiä, joiden takia tällaisia menettelyjä on vasta tulossa käyttöön, ja vaatimusten tulkinta tai arviointikriteerit ovat vasta muotoutumassa. Tuoreinta yhteiseurooppalaista näkemystä asiasta löytyy komissionvarmuustasoasetuksen soveltamisohjeesta (niin kutsuttu LOA-guidance, jossa asiaa käsitellä termillä videoidentification).

3) Henkilöllisyys tarkistetaan toisella vahvalla sähköisellä tunnistusvälineellä (niin kutsuttu ensitunnistamisen ketjuttaminen), jonka varmuustaso on vähintään sama kuin haetun vahvan sähköisen tunnistusvälineen, ja erikseen vielä väestötietojärjestelmästä.

4) Henkilöllisyys tarkistetaan tai on tarkistettu muita menettelyjä vastaavan varmuuden takaavalla menettelyllä (niin kutsuttu aikaisempi tai muu asiakkuus)

5) Poliisin tekemä ensitunnistus.

[8]Dnro Traficom/10078/09.02.00/2021 21.10.2021 (Liikenne- ja viestintäviraston tulkintamuistio ensitunnistamisessa hyväksyttävistä asiakirjoista ja asiakirjojen tutkinnasta)

6 DIGIPALVELULAKI JA OPISKELIJAN VAHVA TUNNISTAMINEN

6.1 Mikä on tunnistuspalvelu, joka täyttää DPL 6.2 §:n vahvan tunnistuksen vaatimukset?

Vahvalla sähköisellä tunnistamisella tarkoitetaan luonnollisen henkilön yksilöimistä ja tälle annetun tunnisteen aitouden ja oikeellisuuden todentamista sähköisellä menetelmällä eli tunnistusvälineellä, joka täyttää sähköistä tunnistamista ja luottamuspalveluja koskevassa EU-sääntelyssä määritellyt korotetun tai korkean varmuustason vaatimukset.

Digipalvelulain tarkoittama vahvan sähköisen tunnistamisen määritelmä perustuu eIDAS -asetukseen (Euroopan parlamentin ja neuvoston asetus (EU) N:o 910/2014 sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla) ja Lakiin vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (617/2009, ”tunnistus- ja luottamuspalvelulaki), jonka 2.1 §:n 1-kohdassa vahva sähköinen tunnistaminen määritellään seuraavasti:

> *”Vahvalla sähköisellä tunnistamisella sellaista henkilön, oikeushenkilön tai oikeushenkilöä edustavan luonnollisen henkilön yksilöimistä ja tunnisteen aitouden ja oikeellisuuden todentamista sähköistä menetelmää käyttäen, joka täyttää sähköisestä tunnistamisesta ja luottamuspalveluista annetun EU:n asetuksen 8 artiklan 2 kohdan b alakohdassa tarkoitetun korotetun varmuustason tai mainitun kohdan c alakohdassa tarkoitetun korkean varmuustason vaatimukset”*

DPL 6.2 §:ssä määritelty vahva sähköinen tunnistautuminen, joka käytännössä tarkoittaa vahvaa tunnistusta. DPL 6.2 § jättää kuitenkin harkinnanvaraa tunnistusmenetelmän valinnan osalta:

- hallinnon yhteisistä sähköisen asioinnin tukipalveluista annetun lain (571/2016) lain 3 §:n 1 momentin 4 kohdassa tarkoitettuun luonnollisen henkilön tunnistuspalvelu; tai
- vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain (617/2009, ”tunnistus- ja luottamuspalvelulaki”) 2 §:n 1 momentin 1 kohdassa tarkoitettuun vahva sähköinen tunnistaminen; tai
- painavasta perustellusta syystä muu tietoturvallinen tunnistuspalvelu.

Vahvalla sähköisellä tunnistamisella tarkoitetaan siis luonnollisen henkilön yksilöimistä ja tälle annetun tunnisteen aitouden ja oikeellisuuden todentamista sähköisellä menetelmällä eli tunnistusvälineellä, joka täyttää sähköistä tunnistamista ja luottamuspalveluja koskevassa EU-säätelyssä määritellyt korotetun (esim. verkkopankkitunnistautuminen tai mobiilivarmenne) tai korkean varmuustason vaatimukset (esim. suomi.fi -tunnistus). Tunnistus- ja luottamuspalvelulaki, eIDAS-asetus ja Liikenne ja viestintäviraston (Traficom) määräys 72 määrittävät vahvaan sähköiseen tunnistamiseen ja sähköisiin luottamuspalveluihin kohdistuvat konkreettiset vaatimukset.

Lain määrittelemän vahvan sähköisen tunnistamisen palvelut ovat yliopiston ulkopuolisia. Vahvoja sähköisiä tunnistuspalveluita ovat:

- pankkien verkkopankkitunnukset;
- teleyritysten mobiilivarmenteet;

- Digi- ja väestötietoviraston kansalaisvarmenne poliisin myöntämällä henkilökortilla ja eräät muut tunnistusvarmenteet; ja
- erilaisilla organisaatiokorteilla rekisteröidyt tunnistusvälityspalvelut.

Vahva sähköinen tunnistus voi perustua lisäksi teknisesti eri menetelmiin. Yhteistä menetelmille on se, että niissä on käytettävä vähintään kahta seuraavista todentamistekijöistä ja dynaamista todentamismekanismia:

- tiedossa oloon perustuva todentamistekijä, jonka henkilön on osoitettava olevan tiedossaan (esim. salasana, PIN-koodi);
- hallussapitoon perustuva todentamistekijä, jonka henkilön on osoitettava olevan hallussaan (esim. tunnuslukulaite, mobiilisovellus, tunnuslukulista); tai
- luontainen todentamistekijä, joka perustuu johonkin luonnollisen henkilön fyysiseen ominaisuuteen (esim. sormenjälki, iiris).

Dynaamisella todentamisella tarkoitetaan sähköistä prosessia,

- jossa käytetään salausta tai muita tekniikoita;
- joiden avulla voidaan pyynnöstä luoda sähköinen todiste siitä, että henkilöllä on hallinnassaan tai hallussaan tunnistetiedot; sekä
- jossa voidaan muuttaa sitä jokaisessa uudessa henkilön ja hänen henkilöllisyytensä varmentavan järjestelmän välillä tapahtuvassa todentamisessa.

Useassa palvelussa tarjolla oleva ja myös osassa yliopistoista nykyisellään käytössä oleva tunnistautumismenetelmä eli MFA (multifactor-authentication) tai kaksivaiheinen tunnistus (2FA, two-factor-authentication) perustuu siihen, että käyttäjän tiliin sähköisessä asiointipalvelussa liitetään jokin selaimesta tai sovelluksesta riippumaton yhteystieto, yleensä puhelinnumero tai sähköposti. Kaksivaiheisessa tunnistamisessa käytetään käyttäjätunnuksen ja salasanan lisäksi tällä toisella yhteydellä toimitettavaa vahvistusta, kuten puhelimeen lähetettyä kertakäyttöistä koodia tai sähköpostiin lähetettyä vahvistuspyyntöä, jolla varmistetaan, että käyttäjä on käyttäjätunnukseen liitetyn puhelinnumeron tai sähköpostin haltija.

MFA tai kaksivaiheinen tunnistus *ei* kuitenkaan ole sähköisen asiointipalvelun tarjoajan kannalta kokonaisuutena vahva menetelmä eikä siksi täytä edellä kuvattua eIDAS -asetuksen ja siinä määrättyyn perustuvan digipalvelulain määräyksiä vahvasta sähköisestä tunnistamismenetelmästä. Yliopistoillakin käytössä olevat MFA-tunnistuspalvelut (Microsoft MFA ja Duo Mobile) on kuitenkin arvioitu tietoturvallisiksi tunnistuspalveluiksi ja siten ne voidaan katsoa DPL 6.2 §:ssä tarkoitetuksi ”muuksi tietoturvalliseksi tunnistuspalveluksi”, erityisesti yhdistettynä yliopistoyhteisön jäsenyyteen ja sen edellyttämään vahvaan ensitunnistamiseen.

6.2 Missä tilanteissa yliopisto-opiskelijalta tulee edellyttää vahvaa tunnistautumista?

Digipalvelulaki edellyttää vahvaa sähköistä tai tätä vastaavaa muuta tietoturvallista tunnistustapaa digitaaliseen palveluun, *mikäli palvelu pitää sisällään salassa pidettävää tietoa*. Vahvaa sähköistä tunnistamista olisi käytettävä esimerkiksi palveluissa, joissa käyttäjä pääsee näkemään tai käsittelemään terveydentilaansa koskevia tietoja, muita erityisiin henkilötietoryhmiin kuuluvia tietoja, sosiaalihuollon asiakkuutta koskevia tietoja, oppilashuoltoon liittyviä tietoja sekä liike- ja ammattisalaisuuksia[9].

Yliopistojen ei ole käytännössä suurten volyymien vuoksi ja palvelun käytettävyyden vaarantumatta mahdollista eikä lainsäädännön valossa tarvettakaan edellyttää vahvaa tunnistautumista jokaisella yksittäisellä kirjautumiskerralla järjestelmiin, jotka eivät lähtökohtaisesti sisällä salassa pidettävää tietoa. Näissä tilanteissa ei siten ole perusteltua edellyttää DPL 6.2 §:ssä viitattuja ensisijaisia (kaksi ensin mainittua) tunnistustapoja silloin, kun tunnistetaan yliopistoyhteisön jäseniä (joille on jo ensitunnistamisen perusteella luovutettu käyttäjätunnus). Myös hallintolain (434/2003) 7 §:n asettamat vaatimukset toisaalta kustannustehokkaasta hallinnon järjestämisestä, toisaalta viranomaisen palveluiden hyvästä käytettävyydestä puoltavat sitä näkemystä, että opiskelijoiden asema hallinnon asiakkaina ei saa heikentyä eikä oppimisympäristöihin kirjautuminen muodostua suhteettoman haasteelliseksi valittavan vahvan tunnistautumisen menetelmän kautta.

Tilanteissa, joissa käytettävä järjestelmä ei lähtökohtaisesti sisällä salassa pidettävää tietoa, riittävä tietoturvallisen tunnistuspa voisi siten olla edelleen vahvaan ensitunnistamiseen yhdistetty käyttäjätunnus-salasana-parin käyttö. Tosin näissäkin tilanteissa MFA:n hyödyntämien on suositeltavaa, jotta voidaan varmistaa toiminnan laatu sekä lisätä yleistä järjestelmien käyttöön liittyvää tietoturvaa.

Digitaaliset oppimisympäristöt voivat sisältää tällaisia salassa pidettäviä tietoja viranomaisten toiminnan julkisuudesta annetun lain (621/1999, ”julkisuuslaki”) 24.1 §:n 21 tai 30 kohdan perusteella (ks. kuitenkin alla luku 7). Opiskelijat ovat palvelun käyttäjiä ja heiltä tulee vaatia digipalvelulain edellyttämää tunnistautumista tilanteissa, joissa opiskelijalla on mahdollisuus saada oppimisympäristössä salassa pidettäviä tietoja nähtäväksi ja käytettäväksi. Mikäli palveluissa saa nähtäväkseen tai käytettäväkseen salassa pidettäviä tietoja, pelkkä käyttäjätunnus ja salasana kirjautumistapana ei sellaisenaan ole digipalvelulain mukainen. Sen sijaan käyttäjä tulisi tunnistaa DPL 6.2 §:ssä esitetyillä vaihtoehtoisilla vahvan tunnistamisen tavoilla.

Sellaisissa tilanteissa, jotka edellyttävät vahvaa tunnistautumista, yliopistojen ja yliopistoyhteisön erityisluonne julkisyhteisönä ja opiskelijoiden edellä kuvattu ensitunnistamisen menettely (yhdessä yliopistojen muiden tietoturvatoimenpiteiden kanssa) synnyttävät painavan perustellun syyn käyttää digipalvelulain edellyttämissä tunnistamistilanteissa lain mahdollistamaa ns. muuta vastaavaa tietoturvallista tunnistuspalvelua. Painavaksi perustelluksi syyksi muodostuu tässä tilanteessa siis se tosiasia, että kysymys on käyttäjistä, jotka on kertaalleen vahvasti tunnistettu sähköisiin järjestelmiin vaadittavan käyttäjätunnuksen myöntämisen yhteydessä.

[9] HE 60/2018 vp, yksityiskohtaiset perustelut.

Mikäli opiskelijan käyttämä digitaalinen oppimisympäristö taas on luonteeltaan ja tietoturvallisuuteen liittyviltä ominaisuuksiltaan sellainen, että yliopistojen tiedonhallintaohjeistusten mukaisesti sinne *voidaan* tallentaa salassa pidettävää tietoa, on opiskelijan tunnistauduttava lisäksi MFA-tunnistuspalvelulla eli tunnistaminen tehtäisiin DPL 6.2 §:n tarkoittamalla ”muulla tietoturvallisella tunnistuspalvelulla”. Opiskelijoiden käyttämissä digitaalisissa oppimisympäristöissä eli järjestelmissä, jotka sisältävät tai voivat sisältää salassa pidettäviä tietoja, tulee siten jatkossa hyödyntää MFA-tunnistusta, mikäli järjestelmän ominaisuudet sen mahdollistavat eikä järjestelmän käyttövarmuus vaarannu.

Organisaatiot päättävät itse, missä järjestelmissä salassa pidettävää tietoa käsitellään ja jotka siten tulevat muun vastaavan tietoturvallisen tunnistuspalvelun piiriin. Tiedonhallintalaki asettaa vaatimukset tietoaineistojen käsittelytavoille. Kullakin yliopistoilla on omat ohjeet sallituille tietoaineistojen käsittelytavoille ja tallennuspaikoille, joissa huomioidaan tiedonhallintalain ja digipalvelulain vaatimukset, mukaan lukien salassa pidettäviä aineistoja koskevat erityisvaatimukset. Järjestelmät, joihin tallennetaan salassa pidettäviä tietoja sisältäviä tietoaineistoja, tulee yliopistoissa määritellä tiedonhallintalain vaatimusten mukaisesti. Organisaatioiden käyttötavat ja sisäinen ohjeistus järjestelmän käyttöön voivat vaihdella, mikä vaikuttaa tehtyihin ratkaisuihin. Teoreettinen mahdollisuus salassa pidettävän tiedon lataamiseen järjestelmään ei ole riittävä peruste vaadittavan tunnistustavan muuttamiseen, jos organisaatio ohjeistaa, että järjestelmää ei saa käyttää salassa pidettävien tietojen käsittelyyn. Ensisijaisesti on priorisoitava niitä järjestelmiä, joissa salassa pidettävän tiedon käsittely on keskiössä ja joiden käyttäjäkunta on laaja. Useissa yliopistoissa käytössä olevien järjestelmien kohdalla on tehtävä yhteisiä linjauksia erityisesti silloin, kun yhteisellä digikehittämisellä voidaan säästää resursseja.

Organisaatiot arvioivat itse käyttöönottamiensa tunnistusratkaisujen ja järjestelmien pohjalta, tarvitaanko tietosuojaa koskevaa vaikutustenarviointia (DPIA). Tarve ratkeaa EU:n yleisen tietosuoja-asetuksen (EU) 2016/679, ”GDPR”) vaikutustenarviointia koskevan 35 artiklan ja sitä koskevan tulkinnan perusteella.

7 HUOMIOTA SALASSA PIDETTÄVISTÄ TIEDOISTA JA NIIDEN KÄSITTELYSTÄ YLIOPISTO-OPISKELUKONTEKSTISSA

Julkisuuslain 24.1 § ja oppimisympäristöissä käsiteltävät aineistot

Viranomaisen salassa pidettävät tiedot määritellään julkisuuslain 24.1 §:ssä. Yliopistot tunnistavat salassa pidettävään tietoon liittyvät vaatimukset hyvin, ja ne pystyvät toimintaprosesseillaan rajaamaan salassa pidettävän tiedon pysymisen niiden työntekijöiden tietona, joiden työtehtäviin ko. tiedon käsittely kuuluu. Esimerkkinä tästä on opiskelijan rikostaustaotteen käsittely (kunkin yliopiston omilla ohjeilla rajattu, minkä lisäksi opintotietojärjestelmään merkitään vain tieto otteen tarkistamisesta).

Oppimisympäristöissä keskeinen salassa pidettävän tiedon laji ovat opiskelijan koesuoritukset. Sähköisten palveluiden osalta koesuorituksia sisältää ennen kaikkea sähköisen tentin järjestelmä EXAM. Järjestelmä toimii kuitenkin siten, että opiskelija ei näe sen kautta muiden opiskelijoiden koesuorituksia.

Oppimisalustojen toimintalogiikan mukaista sen sijaan on, että opiskelijat näkevät toistensa työt silloin, kun opintojakson suorittamisen osana on myös toisten opiskelijoiden töiden opponointi tai muu kommentointi. Asetelmaa ei kuitenkaan ole pidettävä julkisuuslain tarkoittaman salassapitovaatimuksen näkökulmasta ongelmallisena.

Sen sijaan opinnäytteet ja opinnäytteiden arvostelulausunnot ovat julkisia asiakirjoja. Myöskään arvostelulausuntoja ei siis ole pidettävä saman lainkohdan tarkoittamina henkilökohtaisten ominaisuuksien sanallisena arviointina. Sama koskee myös opiskelijalle esimerkiksi oppimisalustassa annettua sanallista palautetta, joka ei tyypillisessä tilanteessa sisällä lainkohdassa tarkoitettuja henkilökohtaisten ominaisuuksien arviointia.

8 TULEVAISUUDENNÄKYMIÄ JA EHDOTUS KANSALLISEKSI KOORDINAATIOKSI

Tietoturvan varmistaminen ja sen osana tietoturvallinen tunnistautuminen tulee olemaan lähitulevaisuudessa jatkuvasti ja nopeasti kehittyvä alue. Tietojärjestelmien ja niiden välisten yhteyksien monimutkaistuessa tasolle, jolla niiden käyttäjät eivät enää täysin ymmärrä niiden toimintaa ja kokonaisuuksien tulkinta edellyttää monialaista asiantuntijaverkoston yhteistyötä, julkisille viranomaisille asetettavat tietoturvavaatimukset kasvavat entisestään.

Työryhmämme ehdottaa myös tämän kehityksen koordinaation tueksi, että yliopistojen (tai korkeakoulujen) tietoturvallisen tunnistamisen alueella olisi Suomen tasolla yksi nimetty, kaikkien toimijoiden tunnistama pääkontakti, joka ylläpitää keskitettyä tietoa nykytilanteesta ja työn alla olevasta kehityksestä. Yhteisellä toimintamallilla säästettäisiin resursseja, selkeytettäisiin kansallisen tason viestintää yliopistokentässä sekä nopeutettaisiin yhteistä tulkintamallia, mikä on välttämätöntä ottaen huomioon yhteiset oppimisympäristöratkaisut ja yliopistoja velvoittavan digitaalisiin toimintaympäristöihin liittyvän säänte-lyn kehitys.

Ehdotettu pääkontakti voisi olla nimetty työryhmä, jossa olisi sekä juridiikan että ICT-alan asiantuntijoita. Ryhmän tulisi tarkastella laajasti lainsäädännön vaikutuksia ja valmistella yhteisiä linjauksia ICT-palveluiden toteutuksen alueella. Työryhmällä tulisi olla yhteys myös DigiVision kautta tapahtuvaan kehitykseen.