Jani Haiko

VAHVAN SÄHKÖISEN TUNNISTAMISEN MENETELMÄT JA NIIDEN KÄYTTÖÖNOTTO

Opinnäytetyö

Liiketalouden ammattikorkeakoulututkinto

Tietojenkäsittelyn koulutus

2020

Kaakkois-Suomen ammattikorkeakoulu

Kaakkois-Suomen ammattikorkeakoulu

Tutkintonimike	Tradenomi (AMK)
Tekijä	Jani Haiko
Työn nimi	Vahvan sähköisen tunnistamisen menetelmät ja niiden käyttöönotto
Toimeksiantaja	Disec Oy
Vuosi	2020
Sivut	42 sivua
Työn ohjaaja	Janne Turunen

TIIVISTELMÄ

Opinnäytetyön tavoitteena oli tehdä toimeksiantajan käyttöön laaja selvitys eri vaihtoehdoista verkossa toimivan palvelun käyttäjän vahvaan sähköiseen tunnistamiseen sekä toteuttaa prototyyppitason versio kyseisestä ominaisuudesta. Työssä käydään läpi yleisimmät vahvan sähköisen tunnistamisen menetelmät, erinäisten lakien ja asetusten niille asettamat vaatimukset sekä eri vaihtoehtojen hyvät ja huonot puolet. Tarkasteltavina tunnistusvälineinä olivat pankkitunnukset, Mobiilivarmenne sekä kansalaisvarmenne. Tunnistusvälineiden esittelyn lisäksi opinnäytetyössä tutustutaan TUPAS-tunnistuksen korvanneen Luottamusverkoston toimintaan.

Luottamusverkoston syntyminen ja TUPAS-tunnistuksen käytön loppuminen ovat avanneet ”tunnistusmarkkinat” kilpailulle ja markkinoille onkin tullut monia uusia kaupallisia palveluntarjoajia. Eri palveluntarjoajia vertailtiin ja niiden sopivuutta toimeksiantajan ja sen asiakkaiden käyttöön pohdittiin opinnäytetyössä. Kaupallisten palveluntarjoajien lisäksi mielenkiinnon kohteena oli Digi- ja väestötietoviraston ylläpitämä Suomi.fi-tunnistus.

Työssä kerrotaan myös Suomi.fi-tunnistuksen käyttöönottoon liittyvistä yksityiskohdista, kuten tieto- ja käyttölupien hakemisesta sekä muun muassa eri tasoisista tietoluvista ja niiden eroista. Lisäksi Suomi.fi-tunnistuspalvelun ylläpidolle käyttöönottoa varten toimitettavat XML-metatiedot käydään läpi tärkeimmiltä kohdiltaan.

Prototyyppiversio toteutettiin toimeksiantajan Yksa-arkistonhallintajärjestelmään. Toteutus tehtiin SAML 2.0 -protokollaa käyttävän Suomi.fi-tunnistuksen käyttöönottoa silmällä pitäen, mutta sitä voi pienin muutoksin käyttää minkä tahansa samaa protokollaa hyödyntävän palvelun käyttöönottamista varten.

Prototyyppiversion toteutuksen raportoinnissa keskitytään tarvittavien ominaisuuksien toteuttamiseen Yksa-järjestelmään lähinnä Java-ohjelmointikieltä käyttäen. Varsinainen SAML 2.0 -protokollaan liittyvien tunnistuspyyntöjen ja -vastausten käsittely tapahtuu kuitenkin erillisessä pääsynhallintajärjestelmässä.

Asiasanat: sähköinen tunnistaminen, ohjelmointi, pankkitunnukset, mobiilivarmenne, kansalaisvarmenne, SAML 2.0

South-Eastern Finland University of Applied Sciences

Degree	Bachelor of Business Administration
Author	Jani Haiko
Thesis title	Methods and deployment of electronic identification in online services
Commissioned by	Disec Oy
Time	November 2020
Pages	42 pages
Supervisor	Janne Turunen

ABSTRACT

The objective of the thesis was to perform an extensive study of the various methods for the strong electronic identification of an online service's user. The most common methods of strong electronic identification, the requirements imposed on them by law and regulations, and the pros and cons of different alternatives were examined.

Different bank IDs, Mobile ID and Citizen Certificate were all taken a look at during the process. In addition to these, the Finnish Trust Network, which has replaced the old TUPAS identification service, was studied in more detail.

The replacement of TUPAS with the FTN has caused many new commercial service providers to emerge into the markets. Different service providers were compared and their suitability for the thesis commissioner and its customers were considered. In addition to commercial service providers, the Suomi.fi identification service maintained by the Digital and Population Data Services Agency was of interest.

The thesis also described different things to keep in mind when planning the deployment of the Suomi.fi identification service, such as applying for the access license. In addition, the most important parts of the XML metadata submitted to the administration of the identification service were shown and explained.

As part of the thesis, a prototype version of the strong electronic identification in Disec's Yksa archive management system was implemented. The prototype version was built with the deployment of Suomi.fi identification service in mind, but it could be used with only minor modifications to implement any service utilizing the same SAML 2.0 protocol as the Suomi.fi identification did.

The reporting of the implementation of the prototype version mostly focused on the implementation of the necessary features in Yksa, mainly using the Java programming language. In the commissioner's environment, authentication requests and responses related to SAML 2.0 protocol were handled in a separate Access Manager, the use and configuration of which was also superficially addressed in the thesis.

Keywords: electronic identification, programming, Bank ID, Mobile ID, Citizen Certificate, SAML 2.0

SISÄLLYS

1 JOHDANTO 5
2 VAHVA SÄHKÖINEN TUNNISTAMINEN 6
2.1 Määritelmä 6
2.2 Vahvan sähköisen tunnistamisen menetelmät 8
2.2.1 Pankkitunnukset 8
2.2.2 Mobiilivarmenne 9
2.2.3 Kansalaisvarmenne ja muut menetelmät 10
2.3 Sähköinen tunnistaminen muutosten keskellä 12
2.3.1 Luottamusverkosto 13
2.3.2 Palveluntarjoajat 15
3 VAHVA SÄHKÖINEN TUNNISTAMINEN YKSA-JÄRJESTELMÄSSÄ 17
3.1 Sähköisen tunnistamisen käyttötapaukset Yksa-järjestelmässä 18
3.2 Palveluntarjoajien vertailu ja sopivan valinta 18
3.2.1 Suomi.fi-tunnistus 21
3.2.2 Johtopäätökset 22
4 TOTEUTUS YKSA-JÄRJESTELMÄSSÄ 23
4.1 Suomi.fi-tunnistuksen testiympäristö ja asiointipalvelun metatiedot 23
4.2 SAML-tunnistustapahtuman kulku 26
4.3 Tunnistustapahtuman käynnistys ja käyttäjän ohjaus tunnistuspalveluun 28
4.4 Tunnistustietojen vastaanotto 30
4.5 Muut käyttötapaukset 34
5 PÄÄTÄNTÖ 35
LÄHTEET 38
KUVALUETTELO

1 JOHDANTO

Tämän opinnäytetyön tavoitteena on tehdä toimeksiantaja Disec Oy:n käyttöön selvitys eri vaihtoehdoista verkossa toimivan sovelluksen, sivuston tai palvelun käyttäjän vahvaan sähköiseen tunnistamiseen, eri vaihtoehtojen hyvistä ja huonoista puolista sekä niiden käyttöönotosta Disecin Yksa-arkistonhallintajärjestelmässä. Lisäksi toteutetaan prototyyppitason versio edellä mainitusta ominaisuudesta.

Toisessa luvussa avataan vahvaa sähköistä tunnistamista käsitteenä, sen määritelmää sekä erinäisten lakien ja asetusten sille asettamia vaatimuksia. Luvussa käydään läpi myös läpi kaikki kirjoitushetkellä Suomessa käytössä olevat vahvan sähköisen tunnistamisen tunnistusvälineet. Tärkeinä käsiteltävinä asioina ovat myös vuoden 2019 aikana tapahtuneet TUPAS-tunnistuksen käytön loppuminen sekä sitä seuranneet muutokset tunnistuspalveluissa ja niiden käytössä.

Kolmannessa luvussa esitellään Yksa-arkistonhallintajärjestelmä siltä osin kuin tämän opinnäytetyön kannalta on oleellista sekä kerrotaan, että millaisia käyttötapauksia vahvalle sähköiselle tunnistamiselle siinä on. Luvun jälkimmäisellä puoliskolla vertaillaan eri tunnistuspalveluiden tarjoajia ja otetaan tarkempaan tarkasteluun muutama niistä, tärkeimpänä Digi- ja väestötietoviraston Suomi.fi-tunnistus. Avaan myös hieman toimeksiantajan kanssa tässä vaiheessa tehtyjä päätöksiä ja niiden perusteluja.

Prototyyppiversion toteutuksesta ja sen ohjelmointityöstä kerrotaan neljännessä luvussa. Prototyyppiversio toteutettiin Suomi.fi-tunnistuksen käyttöönottoa silmällä pitäen, mutta tunnistustapahtuman kulkua SAML 2.0 -protokollaa käytettäessä käydään läpi myös yleisellä tasolla. Luvussa kerrotaan myös toimeksiantajan käyttöympäristön asettamista vaatimuksista, sillä tasolla kuin se on mahdollista.

Opinnäytetyön toimeksiantajana oleva Disec Oy on vuodesta 2007 asti itsenäisenä toiminut mikkeliläinen yritys, joka SaaS-palveluna tarjottavan arkiston- ja kokoelmanhallintajärjestelmä Yksan lisäksi tarjoaa muun muassa digitointi-

ja terveydenhuollon kuvantamispalveluja. Opinnäytetyö tulee suoraan toimeksiantajan käyttöön, ja vahvaa sähköistä tunnistamista on myöhemmin tarkoitus käyttää Yksassa laajasti.

2 VAHVA SÄHKÖINEN TUNNISTAMINEN

Vahva sähköinen tunnistaminen tarkoittaa palvelun käyttäjän henkilöllisyyden todentamista. Tunnistamisen perusajatus on, että jokin luotettavana pidetty toimija taikka taho takaa tunnistautujan henkilöllisyyden. Tällaisia luotettavana pidettyjä tahoja ovat muun muassa pankit ja teleoperaattorit, mutta eivät esimerkiksi sosiaalisen median sivustot, joille kuka tahansa voi itse luoda tilin. Suomessa vaatimukset vahvalle sähköiselle tunnistamiselle on määritelty laissa melko tarkkaan. (Kyberturvallisuuskeskus 2020a; Metsola 2018.)

2.1 Määritelmä

Laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (7.8.2009/617) säädetään, että vahvan sähköisen tunnistamisen tulee aina perustua tunnistusvälineisiin, joiden avulla tunnistautuja voidaan yksiselitteisesti tunnistaa ja joita ainoastaan tunnistusvälineen oikeutettu haltija voi onnistuneesti käyttää.

Samaisessa laissa (Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista 8 a §) säädetään myös, että tunnistusvälineen toiminnan tulee aina perustua vähintään kahteen seuraavista todentamistekijöistä:

Tiedossa oloon perustuva todentamistekijä tarkoittaa jotakin asiaa, jonka voidaan olettaa olevan vain tunnistautujan itsensä tiedossa. Tällainen on yleensä salasana, tai jokin salasanan kaltainen asia, kuten PIN-koodi (Kyberturvallisuuskeskus 2020a).

Hallussapitoon perustuva todentamistekijä on jokin fyysinen asia, jonka voidaan olettaa olevan vain tunnistautujan itsensä hallussa. Esimerkkinä tällaisista Kyberturvallisuuskeskus (2020a) mainitsee tunnuslukulaitteen, mobiilisovelluksen sekä tunnuslukulistan. Näistä viimeksi mainittu ei kuitenkaan enää kaikilta osin täytä EU:n tiukentunutta lainsäädäntöä, joten sen käytöstä on suurelta osin luovuttu (Niiranen 2019). Tästä lisää myöhemmässä luvussa.

Luontainen todentamistekijä on jokin henkilöön liittyvä luontainen fyysinen ominaisuus, esimerkiksi sormenjälki tai iiris (Kyberturvallisuuskeskus 2020a). Luonnollisesti ominaisuuden tulee olla jokaisella ihmisellä uniikki, ja sellainen, että sitä ei pysty vaihtamaan tai ”väärentämään”.

Kaiken tämän voi tiivistää niin, että tunnistautujalta voidaan vaatia jotakin mitä vain hän tietää, jotakin mitä vain hänellä on ja/tai jotakin mitä vain hän itse on.

Sähköistä tunnistamista Euroopan Unionin alueella säätelevää eIDAS-asetusta täydentävä komission täytäntöönpanoasetus (EU) 2015/1502 (tunnetaan myös nimellä varmuustasoasetus) määrittelee kolme varmuustasoa sähköiselle tunnistustapahtumalle. Ne ovat matala, korotettu ja korkea. Suomessa vahvaksi sähköiseksi tunnistustapahtumaksi hyväksytään ainoastaan korotetun tai korkean varmuustason vaatimukset täyttävillä tunnistusvälineillä ja -palveluilla suoritetut tunnistautumiset (Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista 8. § mom 2). Eurooppalaiselle lainsäädännölle tyypilliseen tapaan varmuustasoista on määrätty hyvin vaikeaselkoisessa lakitekstissä. Perusajatus kuitenkin on, että korkeammalle tasolle siirryttäessä tunnistus on aina edellistä tasoa huomattavasti varmempi.

Esimerkiksi luonnollisen henkilön henkilöllisyyden todentamisesta tunnistusvälinettä myönnettäessä (eli ns. ensitunnistuksesta) matalla varmuustasolla Komission täytäntöönpanoasetuksessa (EU) 2015/1502 säädetään, että tunnistusväline voidaan myöntää, kun *Henkilöllä voidaan **olettaa** olevan hallussaan sen jäsenvaltion hyväksymä todiste ilmoitetusta henkilöllisyydestä, jossa sähköisen tunnistamisen menetelmää haetaan.* Korotetulla tasolla taas vaaditaan, että ko. todisteen täytyy olla **varmistettu** olevan tunnistusvälinettä hakevan henkilön hallussa. Korkealla varmuustasolla täytyy tämän lisäksi varmistaa, että esitetty todiste on luotettavan lähteen mukaan edelleen voimassa ja sen esittäjä täytyy **todentaa** vertaamalla jotakin ihmisen fyysistä ominaisuutta johonkin luotettavaan lähteeseen. (Komission täytäntöönpanoasetus (EU) 2015/1502.)

Kirjoitushetkellä Suomessa käytössä olevista tunnistusvälineistä (esitellään seuraavassa luvussa) toistaiseksi vain Digi- ja väestötietoviraston myöntämät

kansalaisvarmenteet sekä ammatti- ja organisaatiokortit täyttävät korkean varmuustason vaatimukset. Sekä Valtionvarainministeriö (Mitrunen, Salovaara ym. 2019, 21) että Finanssialan keskusliitto (2014, 3) ovat painottaneet julkaisuissaan, että heidän mielestään kaikissa kansalaisille suunnatuissa asiointipalveluissa jo korotettu varmuustaso on täysin riittävä nyt ja myös lähitulevaisuudessa. Julkaisuissa myös muistutetaan, että korotetun varmuustason tunnistusmenetelmien tuottaminen on huomattavasti korkean tason menetelmien tuottamista edullisempaa.

2.2 Vahvan sähköisen tunnistamisen menetelmät

Käytössä on useita erilaisia tunnistusmenetelmiä ja -välineitä, jotka kaikki perustuvat edellä esiteltyihin todentamistekijöihin. Käyttömäärältään ehdottomasti suosituin menetelmä ovat pankin myöntämät pankkitunnukset. Esimerkiksi Valtionvarainministeriön (Mitrunen, Salovaara ym. 2019, 31) mukaan vuonna 2018 julkishallinnon toimijoiden käytössä olevan Suomi.fi-tunnistuksen tunnistustapahtumista 95,3 % perustui juuri pankkitunnuksiin. Toisella sijalla oli Mobiilivarmenne 4,1 prosentin osuudellaan. Muut menetelmät, kuten kansalaisvarmenne, kattoivat vain vaivaisen 0,6 prosentin osuuden tunnistustapahtumista.

2.2.1 Pankkitunnukset

Pankkitunnukset ovat pankin myöntämä tunnistusväline, joiden ensisijainen käyttötarkoitus on pankin verkkoasiointipalveluun (eli ns. verkkopankkiin) kirjautuminen sekä siellä erinäisten toimenpiteiden, kuten maksujen, vahvistaminen. Mutta ne ovat myös ylivoimaisesti suosituin menetelmä vahvaan sähköiseen tunnistautumiseen muihinkin kuin pankin omiin palveluihin. Suosion syynä lienee se, että lähes jokainen suomalainen on jonkin pankin asiakas. Lisäksi tänä päivänä laki velvoittaa pankkeja myöntämään pankkitunnukset esimerkiksi myös maksuhäiriömerkintäisille asiakkaille. Aiemmin pankeilla ei tällaista velvoitetta ollut. (Palomaa 2016.)

Pankkitunnusten käytännön toteutuksessa ja toiminnassa on jonkin verran eroavaisuuksia eri pankkien välillä. Kaikilla pankeilla asiakkaan tunnistaminen kuitenkin perustuu jonkinlaiseen staattiseen käyttäjätunnukseen (eli tiedossa

oloon perustuvaan todentamistekijään) sekä hallussapitoon perustuvaan todentamistekijään eli esimerkiksi mobiilisovellukseen tai vaihtuvia pääsykoodeja generoivaan ns. tunnuslukulaitteeseen. Esimerkiksi Nordean pankkitunnukset koostuvat kahdeksannumeroisesta pysyvästä käyttäjätunnuksesta sekä asiakkaan älypuhelimeen asennettavan tunnuslukusovelluksen taikka pankin asiakkaalle myöntämän tunnuslukulaitteen generoimasta vaihtuvasta tunnusluvusta. (Nordea Bank Oyj s.a.)

Ennen älypuhelinten yleistymistä pankkitunnukset lähes poikkeuksetta perustuivat pahviseen tai paperiseen tunnuslukulistaan. Ideana oli, että tunnistautumisen yhteydessä tunnistautuja ensin syötti staattisen käyttäjätunnuksensa, jonka jälkeen pankki pyysi tunnistautujaa syöttämään tietyn tunnusluvun numeroidusta tunnuslukulistasta. Tämänkaltainen ratkaisu ei kuitenkaan enää täytä vuonna 2019 voimaan astuneen EU:n maksupalveludirektiivin vaatimuksia, joten pankit ovat joutuneet luopumaan sen käytöstä kokonaan tai lisäämään prosessiin esimerkiksi tekstiviestivarmistuksen. Huomionarvoinen seikka on, että nimensä mukaisesti kyseinen EU-direktiivi koskee vain pankkien maksupalveluita, ei sähköistä tunnistamista. (Niiranen 2019.) Pankit voisivat siis teoriassa sallia pelkän pahvisen tai paperisen tunnuslukulistan käytön sähköisessä tunnistautumisessa oman harkintansa mukaan, mutta koska asiakas ei pelkästään sen avulla enää voi esimerkiksi vahvistaa maksuja verkkopankissa, useimmat pankit eivät enää tarjoa tätä tunnistusvälinettä lainkaan.

2.2.2 Mobiilivarmenne

Mobiilivarmennetta käytettäessä tunnistautujan henkilöllisyyden takaa pankin sijaan teleoperaattori. Mobiilivarmenteen kehittämiseen ovat yhteistyössä osallistuneet DNA, Elisa ja Telia. (Lehtiniitty 2019.) Kuten pankkitunnuksetkin, myös Mobiilivarmenne nojaa vahvasti hallussapitoon perustuvaan todentamistekijään, eli tunnistautujan matkapuhelinliittymään, tai teknisesti katsoen liittymän SIM-korttiin. Tunnistautumisen yhteydessä liittymän puhelinnumeroon lähetetään tunnistautumispyyntö, jonka tunnistautuja kuittaa itse määrittämällään salasanalla.

Teleoperaattorit ovat parhaillaan kehittämässä Mobiilivarmenteen seuraavaa versiota, jossa salasana on tarkoitus korvata sormenjäljellä, kasvojentunnistuksella tai muulla biometrisellä tunnisteella. Uuden Mobiilivarmenteen käyttöönoton odotetaan alkavan vuosien 2020 - 2021 aikana. (Lehtiniitty 2019.) Toteutuessaan tämä olisi ensimmäinen laajassa käytössä oleva tunnistusväline, joka perustuisi lain määrittelemään luontaiseen todentamistekijään. Kolmen edellä mainitun suuren operaattorin yhteisesti julkaisemassa lehdistötiedotteessa (Vauhdilla kasvavasta… 2019) asetetaan kova tavoite: Operaattoreiden mukaan uudesta Mobiilivarmenteesta on määrä tulla asiakasmäärältään laajimmin käytetty tunnistusväline Suomessa. Vain aika näyttää, että toteutuuko tämä tavoite. Huomiota on kuitenkin syytä kiinnittää operaattoreiden sanavalintaan: **asiakasmäärältään** käytetyin. Operaattorit voisivat siis halutessaan laskea tähän lukuun mukaan vaikka kaikki SIM-kortit, joissa valmius Mobiilivarmenteen käyttöön on, vaikkei SIM-kortin haltija ominaisuutta käyttäisikään tai edes tietäisi siitä.

2.2.3 Kansalaisvarmenne ja muut menetelmät

Jokaisessa kirjoitushetkellä voimassa olevassa poliisin myöntämässä henkilökortissa on Digi- ja väestötietoviraston (ent. Väestörekisterikeskus) kansalaisvarmenne. Se tarkoittaa sitä, että henkilökortin sirulle on tallennettu kortinhaltijan perustietojen lisäksi Digi- ja väestötietoviraston myöntämät ja allekirjoittamat X.509-varmenteet (yksi tunnistautumiseen ja toinen sähköiseen allekirjoittamiseen) sekä sähköinen asiointitunnus (SATU), josta on kaavailtu henkilötunnuksen korvaajaa sähköisessä asioinnissa. (Digi- ja väestötietovirasto s.a.) Laissa väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista (21.8.2009/661) sähköisen asiointitunnuksen on määrätty koostuvan kahdeksasta satunnaisesti valitusta numerosta sekä tarkistusmerkistä. Huomionarvoista on, että sähköinen asiointitunnus ei kerro henkilön ikää tai sukupuolta. SATU siis viittaa tiettyyn henkilöön väestötietojärjestelmässä, mutta toisin kuin henkilötunnus, se ei itsessään paljasta mitään tietoja tunnuksenhaltijasta.

Henkilökortissa olevaa kansalaisvarmennetta voi käyttää vahvaan sähköiseen tunnistautumiseen sitä tukevissa palveluissa, eli toistaiseksi käytännössä vain

Suomi.fi-tunnistuksen kautta. Kansalaisvarmennetta käytettäessä tunnistautujan henkilöllisyyden takaajana on valtionhallinnon toimija yksityisen toimijan kuten pankin tai teleoperaattorin sijaan, eli tässä mielessä tunnistus voidaan mieltää käytössä olevista menetelmistä kaikkein luotettavimmaksi. Kansalaisvarmenteen vähäistä käyttöä selittänee ainakin se, että vaikka nykyaikainen henkilökortti onkin etäluettava NFC-tekniikkaa käyttäen, käytännössä kansalaisvarmenteen käyttö vaatii (ainakin vielä toistaiseksi) kortinlukulaitteen tai sen sisältävän tietokoneen hankkimista. Suomessa suurimmalla osalla kansalaisista ei ole kyseistä laitetta kotonaan. Jo vuonna 2008 Valtiontalouden tarkastusvirasto moitti silloista Väestörekisterikeskusta siitä, että tunnistusväline on sidottu loppukäyttäjän päätelaitteessa olevaan välineeseen (eli kortinlukijaan) ja että koko kansalaisvarmenne on toiminta-ajatukseltaan vanhentunut (Tunnistuspalveluiden kehittäminen… 2008). Lisäksi kansalaisvarmenteen käyttö ja käyttöönotto usein koetaan liian hankalaksi ja monimutkaiseksi (Timo Harakka tilasi henkilökortin ja yritti aktivoida yli tunnin… 2017).

Täysin tuulesta temmattuja väitteet kansalaisvarmenteen käytön hankaluudesta eivät myöskään oman kokemukseni mukaan ole. Osana tämän opinnäytetyön prosessia aktivoin omassa henkilökortissani olevan kansalaisvarmenteen. Aktivointi itsessään sujui kohtalaisen helposti Digi- ja väestötietoviraston verkkosivustolta ladattavan ohjelmiston avulla. Varmenteen käyttö vahvaan sähköiseen tunnistautumiseen oli kuitenkin erittäin kankeaa ja itselläni se lopulta onnistui ainoastaan Google Chrome -selaimella, vaikka esimerkiksi myös Firefox on virallisesti tuettujen selainten listalla. Koska henkilökorttiin on upotettu kaksi eri varmennetta, selain pyysi tunnistusprosessin aikana valitsemaan käytettävän varmenteen. Kyseinen valintadialogi käytti useita erittäin teknisiä termejä, ja luulen, että monella ns. peruskäyttäjällä sormi saattaa tässä vaiheessa mennä suuhun. Oikein toimiessaankin tunnistautuminen kansalaisvarmenteen avulla ei juurikaan ollut pankin tunnuslukusovelluksen käyttöä nopeampaa. Teknisesti näppäremmät käyttäjät todennäköisesti arvostavatkin enemmän käytännössä ilmaista, Digi- ja väestötietoviraston juurivarmenteella allekirjoitettua sertifikaattia (esimerkiksi sähköpostien salaamiseen), kuin itse mahdollisuutta vahvaan sähköiseen tunnistautumiseen sen avulla.

Todennäköisesti suurelta osin juuri edellä kuvattujen syiden takia myös kansalaisvarmenteen tulevaisuus on epävarma. Digi- ja väestötietovirasto on kaavaillut luopuvansa henkilökorttiin upotetusta kansalaisvarmenteesta ja korvaavansa sen ensisijaisesti älypuhelinsovelluksella, hieman pankkien tunnuslukusovellusten tapaan. Virallisia päätöksiä asiasta ei kirjoitushetkellä kuitenkaan vielä ole tehty. Kaukaiseen tulevaisuuteen on kaavailtu myös eräänlaista ”kansalaisen identiteettilompakkoa”. Se mahdollistaisi tunnistautujan hallita, että mitä tietojaan hän tunnistuksen vastaanottavalle palvelulle luovuttaa. Lisäksi ”lompakkoon” voisi tallentaa muitakin tietoja, kuten esimerkiksi ajokortti- tai aseluvatiedot. (Karkimo 2019.)

Henkilökortin lisäksi saatavilla on muitakin Digi- ja väestötietoviraston varmenteita sisältäviä henkilön tunnistusvälineitä. Näitä ovat erinäisten organisaatioiden työntekijöille myönnettävät organisaatiokortit sekä sosiaali- ja terveydenhuollon ammattihenkilöille myönnettävät ammattikortit. Edellä mainittuja voi käyttää vahvaan sähköisen tunnistautumiseen Suomi.fi-tunnistuksen kautta, mutta rajatun käyttöympäristönsä ja kohderyhmänsä takia nämä eivät ole tämän opinnäytetyön mielenkiinnon kohteena.

2.3 Sähköinen tunnistaminen muutosten keskellä

Edellä kuvattujen tunnistusmenetelmien ja -välineiden käyttö henkilöiden vahvaan sähköiseen tunnistamiseen luonnollisesti vaatii sopimuksen tekoa tunnistautujan identiteetin todentajan, eli esimerkiksi pankin tai teleoperaattorin, kanssa. Vielä muutama vuosi sitten ”tunnistusmarkkinat” olivat koko lailla suurten liikepankkien yhteisen TUPAS-tunnistuksen hallussa. TUPAS on lyhenne sanoista tunnistuspalvelu ja standardi. Tunnistautujan näkökulmasta TUPAS-tunnistautuminen alkoi valitsemalla oma pankki tunnistusta pyytävän toimijan palvelussa. Tunnistusta pyytävä toimija ohjasi tunnistautujan valitun pankin TUPAS-palveluun, jossa tunnistautuja kirjautui omilla pankkitunnuksillaan. Onnistuneen kirjautumisen jälkeen pankin TUPAS-palvelu myönsi käyttäjälle ns. TUPAS-tunnisteen, joka sisälsi käyttäjän tiedot. Tässä vaiheessa tunnistautuja pystyi vielä perumaan tunnistautumisen ja tietojensa siirtymisen tunnistusta pyytävän toimijan haltuun. Jos käyttäjä vahvisti haluavansa jatkaa,

TUPAS-palvelu ohjasi hänet takaisin tunnistusta pyytävään palveluun, joka sitten vastaanotti myönnetyn TUPAS-tunnisteen ja siten sai haltuunsa tarvitsemansa tiedot. (Finanssialan Keskusliitto 2013, 4.)

TUPAS oli monessakin mielessä ongelmallinen. Se oli suurten liikepankkien hallussa, eikä muilla tunnistusmenetelmillä tai -välineillä käytännössä ollut mahdollisuutta kilpailla sen kanssa. Kilpailun vähyyden vuoksi TUPAS-tunnistuksen käyttö oli käyttäjilleen myös kallista. Yksi tunnistustapahtuma saattoi pahimmillaan maksaa jopa 50 senttiä. Korkeaa hintaa kritisoivat myös julkishallinnon toimijat, joiden palveluihin saattaa tulla jopa tuhansia tunnistustapahtumia päivässä. (Lehto 2017.) Esimerkiksi Valtionvarainministeriön (Mitrunen, Salovaara ym. 2019, 24) mukaan jo vuonna 2018 Suomi.fi-tunnistus välitti 81,7 miljoonaa tunnistustapahtumaa vuodessa, jotka kaikkineen maksoivat valtiolle yli 4 miljoonaa euroa vuosittain.

Lisäksi vaikka TUPAS olikin pankkien yhteiskehittämä, tunnistusta pyytävän toimijan täytyi silti tehdä erillinen sopimus jokaisen pankin kanssa, joiden asiakkaita se halusi tunnistaa. Kaikilla toimijoilla ei välttämättä ollut resursseja tehdä sopimusta kaikkien pankkien kanssa, jolloin tiettyjen pankkien (yleensä pienempien) asiakkailla ei ollut lainkaan mahdollisuutta tunnistautua osaan palveluista.

2.3.1 Luottamusverkosto

Ratkaisuna TUPAS-tunnistuksen ongelmiin Liikenne- ja viestintäministeriö kehitti kansallisen Luottamusverkoston. Virallisesti se aloitti toimintansa jo vuonna 2017, mutta merkittävä toimija siitä tuli vasta vuoden 2019 aikana, jolloin se korvasi käytöstä poistuvan TUPAS-tunnistuksen. Luottamusverkosto perustuu tunnistusvälityksen palveluntarjoajiin (tästä eteenpäin palveluntarjoaja), jotka toimivat tunnistusvälineiden tarjoajien (pankkien ja teleoperaattoreiden) ja tunnistusta pyytävien toimijoiden välikätenä. (Jansson 2019.) Luottamusverkoston toimintaperiaatetta on kuvattu myös kuvassa 1.

Merkittävin ero Luottamusverkoston ja TUPAS-tunnistuksen välillä on se, että tunnistusta pyytävän toimijan ei enää tarvitse tehdä erillistä sopimusta jokai-

sen tunnistusvälineen tarjoajan kanssa, vaan yksi sopimus valitun palveluntarjoajan kanssa riittää. Janssonin (2019) mukaan Suomessa Luottamusverkostoa koskevan lainsäädännön ja sääntelyn tavoitteena on ollut lisätä tunnistusmarkkinoiden kilpailua sekä sitä kautta edistää tunnistuspalveluiden yleistä saatavuutta ja kehitystä. Muissa EU:n jäsenvaltioissa ei Janssonin mukaan ole yhtä tiukkaa kansallista sääntelyä, sillä EU:n sisällä sähköistä tunnistamista säätelevä eIDAS-asetus ei sitä vaadi.

Kuva 1. Luottamusverkoston toimintaperiaate (Jansson 2019)

Lakia vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista koskevan muutossäädöksen (23.11.2018/1009) mukaan palveluntarjoajan on tehtävä toimintansa aloittamisesta kirjallinen ilmoitus Liikenne- ja viestintäministeriölle. Toisessa samaista lakia koskevassa muutossäädöksessä (29.3.2019/412) säädetään, että edellä mainitun ilmoituksen hyväksytysti tehneet palveluntarjoajat muodostavat Luottamusverkoston. TUPAS-siirtymäajan päättymisen jälkeen tunnistuspalveluja Suomessa tarjoavat ainoastaan Luottamusverkoston jäsenet. Kyberturvallisuuskeskus ylläpitää verkkosivuillaan ajantasaista listaa hyväksytyistä kaupallisista Luottamusverkoston palveluntarjoajista. (Kts. Kyberturvallisuuskeskus 2020b.) Kirjoitushetkellä listassa oli 17 palveluntarjoajaa.

Myös julkishallinnon käytössä oleva Suomi.fi-tunnistus on Luottamusverkoston jäsen ja palveluntarjoaja. Erona muihin palveluntarjoajiin on vain se, että palvelua ylläpitävä Digi- ja väestötietovirasto ei ole kaupallinen toimija, vaan tarjoaa palveluaan maksutta, mutta vain ja ainoastaan julkishallinnon toimijoiden käyttöön. Suomi.fi-tunnistuksesta ja sen mahdollisesta sopivuudesta opinnäytetyön toimeksiantajan käyttöön lisää myöhemmässä luvussa.

2.3.2 Palveluntarjoajat

Kyberturvallisuuskeskuksen hyväksyttyjen palveluntarjoajien listaa selatessa silmiin pistävää on se, että suurin osa niistä on edelleen pankkeja. Mukana on myös muutama teleoperaattori sekä muu yritys. Koko lista (kirjoitushetkellä) on tarkasteltavissa kuvassa 2.

Kuvasta 2 nähdään, että osa palveluntarjoajista mahdollistaa tunnistautumisen vain oman välineensä avulla. Esimerkiksi S-pankin tapauksessa tämä tarkoittaa sitä, että tunnistautua voivat vain S-pankin asiakkaat. Tämänkaltainen toiminta ei vastaa lainkaan opinnäytetyön toimeksiantajan vaatimuksia, joten tässä tapauksessa vain oman välineensä avulla tunnistautumista tukevat palveluntarjoajat voidaan saman tien hylätä sopivaa palveluntarjoajaa valittaessa.

Yksi sopivan palveluntarjoajan valintaan vaikuttava seikka ovat palveluntarjoajan tukemat rajapinnat. TUPAS-tunnistus tuki vain yhtä rajapintaa, eli ns. TUPAS-protokollaa. Tietoturvasyistä sen käyttö ei ole ollut sallittua enää missään muodossa 1.10.2019 alkaen (Kyberturvallisuuskeskus 2020a). Luottamusverkostossa palveluntarjoajat saavat sen sijaan itse valita tukemansa rajapinnat ja palvelunsa teknisen toteutuksen. Kuvasta 2 nähdään, että ehdottomasti suosituimmat rajapinnat ovat OpenID Connect (OIDC) sekä SAML 1.1/2.0 (Security Assertion Markup Language). Molemmat näistä ovat hyvin suosittuja kansainvälisestikin, joten niiden käyttöön varmasti löytyy laadukkaita ohjelmakirjastoja kaikille yleisimmille ohjelmointikielille.

		Välityspalvelu	Rajapinta asiointipalveluun
Checkout Finland Oy (Osa OP-Palvelut Oy:tä 31.3.2019 alkaen)		Muiden välineet	OIDC
NETS Branch Norway		Muiden välineet	OIDC, SAML 1.1
Signicat AS		Muiden välineet	OIDC, SAML 2.0
Aktia Pankki Oyj		Vain oma	OIDC, TUPAS (30.9.asti)
Danske Bank A/S		Oma ja muiden välineet	OIDC
Svenska Handelsbanken AB Suomen sivukonttori		Vain oma	OIDC, TUPAS (30.9.asti)
Nordea Bank Oyj		Oma ja muiden välineet	OIDC
Oma Säästöpankki Oyj		Vain oma	OIDC, TUPAS (30.9.asti)
OP-Palvelut Oy		Oma ja muiden välineet	OIDC, SAML 2.0 (rajoitetusti)
Pop Pankki –ryhmä		Vain oma	OIDC, TUPAS (30.9.asti)
S-Pankki Oy		Vain oma	OIDC
Säästöpankkiryhmä		Vain oma	OIDC, TUPAS (30.9.asti)
Ålandsbanken ABP		Vain oma	OIDC
DNA Oyj		mobiilivarmenne	OIDC, ETSI
Elisa Oyj		muiden välineet ja mobiilivarmenne	ETSI, TUPAS (30.9.asti)
Telia Finland Oyj		muiden välineet ja mobiilivarmenne	OIDC, SAML, ETSI (rajoitetusti)
Fujitsu Finland Oy		Muiden välineet	SAML2.0, ETSI, OIDC (alkaen 1.10.2019)

Kuva 2. Hyväksytyt kaupalliset Luottamusverkoston jäsenet, tilanne 7.5.2020 (Kyberturvallisuuskeskus 2020a)

Sopivaa palveluntarjoajaa valittaessa huomioon täytyy tietenkin ottaa myös palvelun hinta. Yleensä hinta koostuu kuukausimaksusta sekä jokaisesta tunnistustapahtumasta veloitettavasta erillisestä korvauksesta, eli niin sanotusta transaktiomaksusta. Laissa (Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista 12 c §) säädetään, että tunnistusvälineen tarjoaja saa veloittaa Luottamusverkoston jäseneltä yhdestä tunnistustapahtumasta korkeintaan kolme senttiä. Aiemmin yläraja oli 10 senttiä, joka sekin oli melko edullinen verrattuna TUPAS-tunnistuksen hintoihin (Lehto 2017; Mitrunen, Salovaara ym. 2019, 23). Hallituksen esityksen (HE 264/2018) mukaan tiukalta kuulostavan hintasääntelyn tavoitteena on kilpailun lisääminen markkinoilla ja siten *lisätä vahvan sähköisen tunnistamisen käyttöä ja volyymejä markkinoilla*.

3 VAHVA SÄHKÖINEN TUNNISTAMINEN YKSA-JÄRJESTELMÄSSÄ

Yksa on opinnäytetyön toimeksiantajan, Disec Oy:n, SaaS-palveluna (Software as a Service) tarjottava verkkopohjainen arkiston- ja kokoelmanhallintajärjestelmä, jonka tekninen toteutus perustuu pääasiassa Java-ohjelmointikieleen. Yksan käyttäjinä on niin kaupunginarkistoja, korkeakouluja, terveydenhuollon toimijoita kuin museoitakin. Yksi Yksan suurimmista vahvuuksista onkin sen helppo ja laaja kustomoitavuus. Moni Yksa-instanssin toimintaan ja käyttöliittymään liittyvistä asioista on säädettävissä XML-tyyppisen asetustiedoston kautta. Tämä mahdollistaa sen, että samasta ohjelmistosta voidaan pienellä vaivalla räätälöidä versio kaikkien näiden toimijoiden hyvin erilaisia käyttötarkoituksia varten.

Pääsääntöisesti arkistoon tai kokoelmaan tallennetut aineistot on tarkoitettu vain Yksa-instanssin omistavan asiakaan käyttöön ja siksi ne ovat kirjautumisen takana. Asiakkaan tarpeiden mukaan käyttöön voidaan ottaa kuitenkin ns. julkinen käyttöliittymä, joka mahdollistaa asiakkaan niin halutessa esimerkiksi aineiston selailun tietyin rajoituksin ilman kirjautumista. Yksaan on toteutettu myös verkkokauppatoiminnallisuus, joka tarjoaa käyttäjille mahdollisuuden sallia loppukäyttäjien (yleensä tavallisten kansalaisten) ostaa Yksassa olevien aineistojen käyttöoikeuksia. Yksa-järjestelmän toimintalogiikkaa on usein avattu kuvan 3 kaltaisella infografiikalla.

Kuva 3. Yksa-arkistonhallintajärjestelmän toimintaperiaatteen kuvaus (Disec Oy 2020)

3.1 Sähköisen tunnistamisen käyttötapaukset Yksa-järjestelmässä

Yksan käyttäjänhallinta perustuu käyttäjätileihin ja käyttöoikeuksien todentaminen tapahtuu LDAP-pohjaisella ratkaisulla. Jokaisella käyttäjällä on vähintään käyttäjätunnuksena toimiva sähköpostiosoite sekä salasana. Loppukäyttäjien käytössä oleville ns. asiakastileille kirjautuminen ja niiden rekisteröinti eivät kuitenkaan tapahdu LDAP-hakemistopalvelun kautta, vaan asiakastilit on tallennettu sovelluksen käyttämään dokumenttikantaan, Couchbaseen, sellaisenaan ja niiden käyttö käsitellään kokonaan Yksan sisällä.

Kirjoitushetkellä yhdelläkään toimeksiantajan asiakkaista ei vielä ole esittää täysin valmista käyttötapausta vahvan sähköisen tunnistamisen käytölle Yksassa. Erilaisia alustavia ajatuksia kuitenkin on, esimerkiksi osalla asiakkaista arkistoon saattaa olla tallennettu aineistoja, jotka eivät ole täysin salaisia, mutta joiden käyttö vaatii tutkimus- tai muun luvan. Tällä hetkellä asiakkaat eivät voi helposti hoitaa tällaisten aineistojen luovutusta luvan saaneiden käyttöön Yksan kautta, mikä on tietysti selkeä puute.

Opinnäytetyön puitteissa toteutettavan prototyyppiversion ei ole tarkoitus olla täysin valmis toteutus jotakin tiettyä käyttötapausta tai tietyn tunnistusmenetelmän käyttöä varten, vaan pohja, jota voi myöhemmin laajentaa. Pitääksemme asiat yksinkertaisina, määritetään prototyyppiversiolle vain yksi pakollinen vaatimus:

> Yksa-instanssin julkiseen käyttöliittymään saapuva loppukäyttäjä voidaan tarvittaessa tunnistaa vahvasti. Tunnistamisen jälkeen jokin käyttäjän luotettavasti yksilöivä tieto on helposti myöhemmin mahdollisesti toteutettavien toiminnallisuuksien käytössä, se voidaan tallentaa tai esimerkiksi liittää olemassa olevan käyttäjän tietoihin.

3.2 Palveluntarjoajien vertailu ja sopivan valinta

Tässä vaiheessa opinnäytetyön prosessia oli aika tehdä vertailua eri palveluntarjoajien välillä. Tarkempaan tarkasteluun päädyin valitsemaan Suomi.fi-tunnistuksen sekä kaksi kaupallista palveluntarjoajaa. Ensiksi vertailemme näitä ja luvun lopuksi avaan hieman toimeksiantajan kanssa tehtyjä johtopäätöksiä sekä niiden perusteluja.

Mielestäni kaupallisten tunnistuspalvelujen markkinatilanne Suomessa on tällä hetkellä melko hyvä. Luottamusverkoston syntymisen sekä sitä seuranneen pankkien monopoliaseman purkautumisen myötä markkinoille on tullut paljon kaivattua kilpailua. Luottamusverkoston palveluntarjoajien toiminta on laissa tarkoin säädeltyä ja viranomaisten toimesta valvottua. Siispä minkä tahansa Luottamusverkostoon hyväksytyn palveluntarjoajan voi olettaa olevan sinällään luotettava ja sen perustoimintojen olevan kunnossa. Sopivaa palveluntarjoajaa valittaessa on omasta mielestäni hyvä kiinnittää huomiota ainakin palvelun hintaan, sen käyttöönoton ja ylläpidon helppouteen, kehittäjille suunnatun dokumentaation määrään ja laatuun sekä loppukäyttäjille tunnistuspalvelusta näkyvän osan käytettävyyteen, saavutettavuuteen sekä yleiseen graafiseen ilmeeseen.

Osana tämän opinnäytetyön prosessia tutustuin vähintään pintapuolisesti lähes kaikkiin Luottamusverkoston kaupallisiin palveluntarjoajiin. Kaupallisista palveluntarjoajista omasta mielestäni lupaavimmilta vaikuttivat Signicat AS:n Signicat Connect sekä OP Ryhmän Tunnistuksen välityspalvelu. Molemmat näistä ovat tunnettuja ja yleisesti käytettyjä ratkaisuja. Molemmat myös mahdollistavat tunnistamisen hyvin laajalla joukolla eri tunnistusvälineitä.

Signicat AS on vuonna 2007 perustettu norjalainen yritys, joka tarjoaa monenlaisia sähköisiä tunnistus- ja luottamuspalveluja Suomessa ja Euroopassa. Tässä yhteydessä olemme kiinnostuneita vain yrityksen Signicat Connect -tuotelinjasta, jonka pääominaisuus on henkilöiden sähköinen tunnistaminen. Palvelu mahdollistaa tunnistamisen hyvin laajalla joukolla erilaisia tunnistusvälineitä (niin heikkoja kuin vahvoja), mutta tässä yhteydessä tutustumme vain Luottamusverkoston alaiseen osaan niistä, eli käytännössä pankkitunnusten tai Mobiilivarmenteen avulla tapahtuvaan tunnistautumiseen. (Vahva tunnistaminen Signicat Connect -ratkaisulla s.a.)

Signicatin tarjoama dokumentaatio on omasta mielestäni laajahko ja ainakin pintapuolisin selattuna laadukas, joskin dokumentaatiosivuston navigaatiossa olisi parantamisen varaa. Pyydettäessä palvelua ja sen integraatiota Yksaan olisi mahdollista kokeilla testiympäristössä ennen tarjouspyynnön tai sopimusten tekemistä. Yksan ja tunnistuspalvelun välinen keskustelu tapahtuisi OIDC,

SAML 1.1 tai SAML 2.0 -protokollan välityksellä (Signicat AS 2019.) Tässä ratkaisussa varsinainen tunnistusvälineen valinta tapahtuu Signicatin omassa palvelussa ja käyttöliittymässä. Dokumentaation mukaan palvelun käyttöliittymää on kuitenkin mahdollista muokata vastaamaan kunkin asiakkaan tarpeita (Signicat AS s.a.).

OP Ryhmän tunnistuspalvelut kulkevat toiminimellä OP Tunnistuksen välityspalvelu. Myös OP:n palvelun tukema eri tunnistusvälineiden joukko on vähintäänkin tarpeeksi laaja, muttei kuitenkaan aivan Signicatin tasolla. Esimerkiksi ulkomaisia tunnistusvälineitä se ei tue lainkaan, mikä Yksan tapauksessa ei kuitenkaan mitä todennäköisimmin olekaan tarpeen. OP on valinnut palvelunsa rajapinnaksi OIDC:n. SAML-protokollaa palvelu ei tue. Tätäkin palvelua on mahdollista kokeilla etukäteen testiympäristössä, jota OP kutsuu Sandbox-ympäristöksi.

Yksassa OP:n ratkaisu voitaisiin ottaa käyttöön kahdella eri tavalla: Joko OP:n tarjoaman käyttöliittymän tai Yksaan upotetun käyttöliittymän avulla. (OP Tunnistuksen välityspalvelun palvelukuvaus 2019.) Ensiksi mainitussa vaihtoehdossa tunnistusprosessi tapahtuu siis kokonaan Signicatin tapaan palveluntarjoajan omassa verkkopalvelussa. Toinen, ja yleisesti tyylikkäämmäksi mielletty tapa olisi upottaa Yksan omaan käyttöliittymään ns. tunnistusnapit. Tässä toimintamallissa loppukäyttäjä valitsisi haluamansa tunnistusvälineen suoraan Yksan käyttöliittymästä. Tämänkaltainen ratkaisu on tyylikkäämpi ja monille tuttu TUPAS-tunnistuksen ajoilta, mutta luonnollisesti sen tekninen toteutus vaatisi suurempia muutoksia Yksaan. Aiemmin toteutetussa verkkokauppatoiminnallisuudessa kassalla olevat ns. maksunapit on tehty juuri tällä upotustyylillä. Maksunappien palveluntarjoajaksi valittu Checkout Finland on nykyään osa OP Ryhmää, joten tässä mielessä OP olisi luontainen valinta myös tunnistuspalvelujen tarjoajaksi.

Luottamusverkoston kaupalliset palveluntarjoajat eivät pääsääntöisesti kerro palvelujensa tarkkoja hintatietoja ennen yhteydenottoa tai tarjouspyynnön jättämistä ko. yritykseen. Kaikkien tunnetuimpien palveluntarjoajien hinta kuitenkin koostuu kolmesta eri osatekijästä: avaus-/käyttöönottomaksusta, kuukausimaksusta sekä transaktiomaksusta. Eräässä OP Ryhmän julkisesti saatavilla

olevassa yritysasiakkaiden hinnastossa (OP-Palveluhinnasto 2020) tunnistuksen välityspalvelun käyttöönottomaksun suuruudeksi on merkitty 160 euroa, kuukausimaksuksi 17 euroa ja transaktiomaksuksi 20 senttiä. Näistä viimeksi mainittu kuulostaa omasta mielestäni hieman hintavalta, ottaen huomioon sen, että lain mukaan palveluntarjoaja maksaa yhdestä tunnistustapahtumasta tunnistusvälineen tarjoajalle korkeintaan 3 senttiä. Lisäksi mahdollisen oman tunnistusvälineensä avulla suoritetuista tunnistustapahtumista palveluntarjoajan ei luonnollisesti tarvitse maksaa mitään.

3.2.1 Suomi.fi-tunnistus

Suomi.fi-tunnistus on Digi- ja väestötietoviraston kehittämä ja ylläpitämä vahvan sähköisen tunnistamisen palvelu, jota se tarjoaa maksutta julkishallinnon organisaatioiden käyttöön. Muihin Luottamusverkoston palveluntarjoajiin verrattuna Suomi.fi-tunnistus tukee laajinta joukkoa erilaisia suomalaisia tunnistusvälineitä. Kaikkien suomalaisten pankkien pankkitunnusten, Mobiilivarmenteen ja kansalaisvarmenteen lisäksi tuettujen tunnistusvälineiden listalla ovat myös Digi- ja väestötietoviraston myöntämät organisaatio- ja ammattikortit. Kuriositeettina mainittakoon myös se, että Suomi.fi-tunnistusta ollaan parhaillaan jatkokehittämässä niin, että myös muiden EU-maiden kansalaiset sekä ne suomalaiset, joilla on jonkin muun EU-maan myöntämä tunnistusväline, voisivat tunnistautua suomalaisiin asiointipalveluihin sen kautta. (Digi- ja väestötietovirasto 2019; Palvelun kuvaus s.a.)

Suomi.fi-tunnistuksen käyttöönotto edellyttää käyttöluvan sekä Väestötietojärjestelmään liittyvän tietoluvan hakemista ja saamista. Tietolupaa haettaessa tulee määritellä ja perustella ne tiedot, joita väestötietojärjestelmästä tarvitsee. Tietolupa voidaan myöntää suppeisiin, keskilaajoihin tai laajoihin henkilötietoihin. Suppeat tiedot sisältävät vain tunnistautujan henkilötunnuksen, mahdollisen sähköisen asiointitunnuksen (kun tunnistautuminen tapahtui kansalaisvarmenteen avulla) sekä rekisteröidyt viralliset nimet. Edellä mainittujen lisäksi keskilaajat tiedot sisältävät tunnistautujan asuinpaikan tiedot, sähköpostiosoitteen (jos tieto löytyy Väestötietojärjestelmästä) ja tiedon mahdollisesta turvakiellosta (joka voi estää asuinpaikan tietojen luovuttamisen). Laaja taso tarjoaa näiden lisäksi ainoastaan tiedon mahdollisesta Suomen kansalaisuu-

desta. (Digi- ja väestötietovirasto 2020.) Yksan käyttöön jo suppean tason tiedot mitä todennäköisimmin riittäisivät. Huomionarvoista on se, että ulkomaista tunnistusvälinettä käyttävästä tunnistautujasta toimitetaan aina samat tiedot riippumatta myönnetystä tietoluvasta.

Vaikka palvelun käyttö ja käyttöönotto onkin maksutonta, jokainen organisaatio luonnollisesti itse vastaa käyttöönoton vaatimista muutoksista omiin palveluihinsa sekä niiden kustannuksista. Palvelun käyttöönottoa helpottamaan on saatavilla testiympäristö. (Digi- ja väestötietovirasto 2019.)

Suomi.fi-tunnistus on laajasti käytössä käytännössä kaikilla julkishallinnon organisaatioilla. Eikä ihme, sillä kaupallisten toimijoiden on hyvin hankala kilpailla ilmaista palvelua vastaan. Myös tämän opinnäytetyön toimeksiantaja on luonnollisesti kiinnostunut maksuttomasta vaihtoehdosta, mutta kaupallisena toimijana heillä ei ole mahdollisuutta suoraan saada palvelun käyttöoikeutta itselleen. Sen sijaan Yksan käyttäjinä on useita organisaatioita, joille palvelun käyttöoikeus myönnettäisiin. Tässä toteutusmallissa Yksaan rakennettaisiin mahdollisuus käyttää Suomi.fi-tunnistuksen rajapintoja, mutta tunnistuspalvelun käyttö- ja tietoluvat haettaisiin asiakasorganisaatioille, ei toimeksiantajalle. Tämänkaltaisessa järjestelyssä haasteeksi saattaisi muodostua se, että luvat olisi haettava jokaiselle tunnistusta käyttävälle asiakasorganisaatiolle erikseen.

3.2.2 Johtopäätökset

Tässä vaiheessa opinnäytetyön prosessia oli aika kääntyä toimeksiantajan puoleen ja tehdä päätöksiä prototyyppiversion toteutuksen suhteen. Koska toistaiseksi mahdollinen tarve loppukäyttäjien vahvaan sähköiseen tunnistamiseen on vasta muutamilla toimeksiantajan asiakkaista, tulimme siihen johtopäätökseen, että toimeksiantajan ei vielä ole taloudellisesti kannattavaa ostaa palvelua miltään kaupallisista palveluntarjoajista. Sen sijaan lähdemme nyt toteuttamaan Yksaan mahdollisuutta käyttää Suomi.fi-tunnistuksen rajapintaa. Ominaisuus tulee luonnollisesti toteuttaa niin, että se on myöhemmin helppo ottaa käyttöön missä tahansa Yksa-instanssissa.

Suomi.fi-tunnistuksen rajapinta käyttää SAML 2.0 -protokollaa, jota myös useat kaupalliset palveluntarjoajat tukevat. Tämä tarkoittaa sitä, että toteuttamalla nyt Yksaan tuen Suomi.fi-tunnistuksen käytölle, lähes huomaamatta toteutamme samalla valmiuden pienin muutoksin käyttää muitakin palveluntarjoajia, mikäli tarvetta sille myöhemmin ilmenee.

4 TOTEUTUS YKSA-JÄRJESTELMÄSSÄ

Suomi.fi-tunnistuksen käyttöönotto tuotantoympäristössä vaatii käyttö- ja tietoluvan hakemista ja saamista. Kuten edellisessä luvussa totesimme, luvat tulee hakea kullekin asiakasorganisaatiolle, ei toimeksiantajalle. Jo ennen lupien hakemista ja/tai saamista on kuitenkin mahdollista liittyä kaikille avoimeen Suomi.fi-tunnistuksen testiympäristöön, jonka avulla tunnistusprosessia ja Yksaan tehtäviä muutoksia voi helposti testata kehitystyön aikana. (Suomi.fi-tunnistus: Käyttöönoton vaiheet s.a.).

Suomi.fi-tunnistuksen testiympäristöä vasten testaaminen tullaan tekemään toimeksiantajan stage- eli testauspalvelimella. Kehitystyön aikana omassa sovelluskehitysympäristössäni käytän Node.js-pohjaista erittäin kevyttä SAML 2.0 tunnistustietojen tarjoajaa (*identity provider*, tästä eteenpäin käytetään yleisesti tunnettua lyhennettä IdP), jonka asetukset konfiguroin vastaamaan mahdollisimman paljon oikeaa Suomi.fi-tunnistuksen käyttöympäristöä.

4.1 Suomi.fi-tunnistuksen testiympäristö ja asiointipalvelun metatiedot

Kaikkien organisaatioille tarkoitettujen Suomi.fi-palvelujen hallinta tapahtuu keskitetysti Palveluhallinta-sivustolla osoitteessa https://palveluhallinta.suomi.fi. Organisaation tulee rekisteröityä ja kirjautua Palveluhallintaan, jonka jälkeen sen tulee täyttää Suomi.fi-tunnistuksen käyttö- ja tietolupalupahakemus ja hyväksyä palvelun käyttöehdot. (Suomi.fi-tunnistus: Käyttöönoton vaiheet s.a.) Useilla organisaatioilla saattaa jo valmiiksi olla tunnukset ko. palveluun.

Testiympäristöön liittyminen tapahtuu toimittamalla asiointipalvelun (eli Yksan) SAML 2.0 -standardin mukaiset metatiedot Palveluhallinnan kautta. Organisaatio voi Palveluhallinnan kautta antaa palvelukohtaisia käyttöoikeuksia

organisaation ulkopuolisille tahoille, esimerkiksi juuri näiden metatietojen toimittamista varten (Mikä on Palveluhallinnan käyttäjähallinta? 2019). Metatietojen lähettämisen jälkeen tunnistuspalvelun ylläpito tarkastaa toimitetut tiedot ja lisää asiointipalvelun testiympäristöön, jonka jälkeen sen käyttö voi alkaa. Samat metatiedot (pienin muutoksin) toimitetaan myöhemmin tuotantokäyttöä varten, mutta testausvaiheessa kaikkien tietojen ei tarvitse olla oikeita ja SAML-sanomien allekirjoittamiseen (josta lisää alempana) käytettävä varmenne voi olla itse allekirjoitettu. (Suomi.fi-tunnistus: Testiympäristöön liittyminen s.a.)

Asiointipalvelun metatiedot ovat SAML 2.0 -standardin mukaisesti XML-muotoiset ja niiden juurielementtinä on md:EntityDescriptor-elementti. Sen alla olevilla lapsielementeillä määritetään muun muassa asiointipalvelun kuvaus ja yhteystiedot sekä tunnistautujasta pyydettävät tiedot. (Kaikkia tietoluvan sallimia tietoja ei siis välttämättä tarvitse pyytää.) Tässä suhteessa Suomi.fi-tunnistus toimii hieman yleisestä käytännöstä poiketen. Yleensä SAML-protokollaa käytettäessä tunnistautujasta pyydettävät tiedot määritetään jokaisessa tunnistuspyynnössä erikseen, ei asiointipalvelun metatiedoissa.

Kaikkia metatiedoissa olevia elementtejä en käy tässä läpi, vaan nostan esille vain muutamia, omasta mielestäni erityisen huomionarvoisia kohtia. Tunnistuspalvelun dokumentaatiossa on kaikki pakolliset elementit sisältävä mallipohja, jota itsekin hyödynsin. (Kts. Asiointipalvelun metatiedot 2020.)

Hyväksytyt tunnistusvälineet määritetään mdattr:EntityAttributes-elementissä FinnishAuthMethod-nimisessä SAML-attribuutissa. Asiointipalvelu voi esimerkiksi halutessaan määrittää, että tunnistautuminen on mahdollista vain korkean varmuustason tunnistusvälineillä. Käytännössä tämänkaltainen määrittely on kuitenkin hyvin harvinaista, sillä se rajoittaa merkittävästi käytettävissä olevien tunnistusvälineiden määrää. Testiympäristöä varten käyttöön voi määrittää myös testitunnistusvälineen, joka helpottaa kehitystyön aikaista testaamista huomattavasti mahdollistamalla ”tunnistautumisen” testihenkilönä nappia painamalla ilman oikeaa tunnistusvälinettä.

Samaisen elementin sisällä määritetään muutama muukin tunnistuspalvelun toimintaan vaikuttava asetus, kuten ulkomaisten (eIDAS-) tunnistusvälineiden

tuki. Pääsääntöisesti on syytä käyttää asetusta ”full”, jolloin tunnistautuminen kaikilla Suomi.fi-tunnistuksen tukemilla ulkomaisilla tunnistusvälineillä on mahdollista. Asiointipalvelun on kuitenkin otettava huomioon se, että eIDAS-tunnistusvälinettä käyttävillä ei välttämättä ole suomalaista henkilötunnusta ja että osa eIDAS-tunnistusvälinettä käyttävien tunnistustiedoista on tunnistusvastauksessa eri kentässä kuin vastaava tietue suomalaista tunnistusvälinettä käyttävillä. (Asiointipalvelun metatiedot 2020.)

Tässä vaiheessa on tärkeää ymmärtää se, että kaikki tunnistustapahtuman aikainen verkkoliikenne asiointi- ja tunnistuspalvelun välillä tapahtuu käyttäjän verkkoselaimen välityksellä. Tämän vuoksi tunnistuspalvelu ei suoraan voi luottaa vastaanottamaansa dataan, vaan asiointipalvelun on allekirjoitettava jokainen tunnistuspalveluun lähetettävä pyyntö omalla varmenteellaan. Kyseisen varmenteen julkinen avain kuvataan metatiedoissa kuvan 4 osoittamalla tavalla. Testiympäristössä voi käyttää itse allekirjoitettua varmennetta, mutta tuotantokäytössä varmenteen olisi hyvä olla jonkin tunnetun varmentajan (*Certificate Authority*) allekirjoittama. Lisäksi vaikka asiointipalvelun metatiedoissa kuvataan ainoastaan varmenteen julkinen avain, Suomi.fi-tunnistuksen ylläpito ei suosittele käytettäväksi samaa varmennetta kuin asiointipalvelun TLS-liikenteen salaamiseen. (Asiointipalvelun metatiedot 2020.)

```
<md:SPSSODescriptor AuthnRequestsSigned="true" WantAssertionsSigned="true"
    <md:KeyDescriptor>
        <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
            <ds:X509Data>
                <ds:X509Certificate>
                    [Sertifikaatin base64-enkoodattu julkinen avain tähän]
                </ds:X509Certificate>
            </ds:X509Data>
        </ds:KeyInfo>
    </md:KeyDescriptor>
    ...
</md:SPSSODescriptor>
```

Kuva 4. Käytettävän varmenteen kuvaaminen asiointipalvelun metatiedoissa

Elementeissä md:AssertionConsumerService ja md:SingleLogoutService tulee määritellä tunnistusvastausten ja uloskirjautumisen paluuosoitteet kuvan 5 kaltaisesti. Nämä ovat ne URL-osoitteet, joihin Suomi.fi-tunnistus käyttäjän tunnistusprosessin jälkeen ohjaa ja johon se lähettää uloskirjautumispyynnöt. Osoitteiden muotoa ei juurikaan ole rajoitettu, ainoastaan HTTPS-protokollan

käyttö on pakollista. (Asiointipalvelun metatiedot 2020.) Paluuosoitteiden vaihto jälkikäteen vaatii uusien metatietojen toimittamista, joten niiden oikeellisuus on syytä varmistaa useaan otteeseen ennen metatietojen lähettämistä Suomi.fi-tunnistuksen ylläpidon tarkastettavaksi. Toimeksiantajan käyttöympäristössä vastaanotettujen SAML-sanomien käsittely tapahtuu Yksan ja julkisen verkon välissä olevassa pääsynhallintajärjestelmässä. Pääsynhallintajärjestelmästä ja sen roolista lisää alempana, mutta jo tässä vaiheessa on tärkeää asettaa metatietoihin pääsynhallintajärjestelmän kannalta oikeat paluuosoitteet.

```
<md:AssertionConsumerService
    Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
    Location="https://am.disec.fi/nidp/saml2/spassertion_consumer"
    index="1"
    isDefault="true" />
<md:SingleLogoutService
    Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
    Location="https://am.disec.fi/nidp/saml2/spslo"
    ResponseLocation="https://am.disec.fi/nidp/saml2/spslo_return" />
```

Kuva 5. Paluuosoitteiden määrittely

4.2 SAML-tunnistustapahtuman kulku

Ennen ohjelmointityön aloittamista käydään tunnistustapahtuman kulku alusta loppuun teoriatasolla läpi. Tunnistusprosessi alkaa, kun loppukäyttäjä on verkkoselaimellaan Yksan julkisessa käyttöliittymässä ja ilmaisee haluavansa tunnistautua. Tämä voi tapahtua esimerkiksi nappia tai linkkiä painamalla.

Yksan ja julkisen verkon välissä on Micro Focusen NetIQ Access Manager -pääsynhallintajärjestelmä, jonka läpi kaikki liikenne Yksaan kulkee. Pääsynhallintajärjestelmä vastaa muiden tehtäviensä ohella myös SAML-sanomien muodostamisesta ja muusta käsittelemisestä. Siispä Yksan näkökulmasta tunnistusprosessi aloitetaan ohjaamalla käyttäjä sellaiseen reittiin (URL-osoitteeseen), joka on pääsynhallintajärjestelmässä merkitty suojatuksi reitiksi niin, että siihen siirtyminen edellyttää autentikointia määrätyn IdP:n kautta.

Kun käyttäjä pyrkii suojattuun reittiin ja ko. käyttäjää ei ole aktiivisen istunnon aikana vielä autentikoitu, uudelleenohjaa järjestelmä hänet käytössä olevan IdP:n metatiedoissa määriteltyyn URL-osoitteeseen HTTP-pyynnöllä (yleensä

HTTP POST), jonka mukana lähetetään base64-enkoodattu SAML 2.0 -standardin mukainen AuthnRequest, eli tunnistuspyyntö.

Useimmat tunnistustietojen tarjoajat, Suomi.fi-tunnistus mukaan lukien, eivät hyväksy tunnistuspyyntöjä, ellei niitä ole allekirjoitettu asiointipalvelun metatiedoissa kuvatulla varmenteella. Tässä kohden on syytä uudelleen painottaa sitä, että tunnistusprosessin aikana kaikki verkkoliikenne Yksan, pääsynhallintajärjestelmän sekä IdP:n välillä tapahtuu käyttäjän selaimen välityksellä. Yksa tai pääsynhallintajärjestelmä ei siis missään vaiheessa tee suoraa pyyntöä tunnistustietojen tarjoajan palveluun.

Suomi.fi-tunnistus ja osa muistakin palveluntarjoajista tukevat ns. kertakirjautumista (*single sign-on*, SSO). Suomi.fi-tunnistusta käytettäessä se tarkoittaa sitä, että loppukäyttäjän tarvitsee selainistuntonsa aikana tunnistautua tunnistusvälinettä käyttäen vain kerran, vaikka hän käyttäisi useita eri toisistaan riippumattomia asiointipalveluja. Yksan näkökulmasta jokainen tunnistustapahtuma kuitenkin aina vahvistetaan samalla tavalla IdP:n kautta. Suomi.fi-tunnistuksen kertakirjautumisistunto on voimassa 32 minuuttia, mutta jokainen asiointipalvelu saa itse päättää oman palvelunsa istunnon voimassaoloajan.

Jos Suomi.fi-tunnistus ei vielä ole tunnistanut käyttäjää aktiivisen istunnon aikana (eli kyseessä ei ole kertakirjautuminen), pyytää se käyttäjää valitsemaan haluamansa tunnistusvälineen, jonka jälkeen käyttäjä ohjataan kyseisen tunnistusvälineen omaan palveluun, joka taas vuorostaan oman prosessinsa jälkeen ohjaa käyttäjän takaisin Suomi.fi:n palveluun.

Kun Suomi.fi-tunnistus on vahvistanut käyttäjän henkilöllisyyden (joko tunnistusvälineen tai kertakirjautumisistunnon perusteella) ohjaa se käyttäjän takaisin asiointipalveluun metatiedoissa määriteltyyn paluuosoitteeseen. Pyynnön mukana on SAML-standardin mukainen tunnistusvastaus, joka myös sisältää tunnistautujasta pyydetyt tiedot (SAML-termeillä attribuutit), jos tunnistustapahtuma oli onnistunut.

4.3 Tunnistustapahtuman käynnistys ja käyttäjän ohjaus tunnistuspalveluun

Access Manager -pääsynhallintajärjestelmä huolehtii siis monista tunnistustapahtuman kulkuun liittyvistä vaiheista. En tässä opinnäytetyössä käy läpi kaikkia Access Managerin eri asetusten ja ominaisuuksien konfigurointia kovinkaan tarkasti. Perusajatus on kuitenkin melko yksinkertainen. Määritin pääsynhallintajärjestelmän asetuksiin uuden suojatun reitin (esimerkiksi /Yksa4/auth/suomiFI), johon yhdistämisen ehtona on, että asetuksissa määritetty IdP (tässä tapauksessa Suomi.fi-tunnistus tai paikallisen kehitysympäristön testi-IdP) autentikoi käyttäjän. Pääsynhallintajärjestelmä parsii vastaanottamastaan SAML-tunnistusvastauksesta tunnistautujan tiedot automaattisesti. Vasta tämän jälkeen se sallii pääsyn ko. suojattuun reittiin ja ohjaa käyttäjän selaimen Yksaan.

Konfiguroin pääsynhallintajärjestelmän niin, että se välittää parsimansa tiedot Yksalle kustomoiduissa otsakkeissa (*header*) HTTP-pyynnön mukana. Näin Yksan on helppo vastaanottaa tiedot tietoturvallisesti. Asiaan perehtymättömän korvaan tämän kaltaisten tietojen lähettäminen HTTP-otsakkeissa saattaa kuulostaa hieman erikoiselta. Itse ainakaan en ollut tällaisesta käytännöstä aiemmin kuullut. Kyseessä on kuitenkin melko yleisesti käytetty tapa, sillä ainoa muu vaihtoehto tietojen välittämiseksi HTTP GET -pyynnön mukana olisi käyttää URL-parametrejä, jotka taas näkyvät selaimen osoiterivillä ja saattavat tallentua selaimen selaushistoriaan.

Yksassa tiettyyn reittiin tulevien HTTP-pyyntöjen vastaanottamiseen, käsittelyyn ja niihin vastaamiseen käytetään Stripes Frameworkin ActionBeaneja. Yleisesti yhtä toiminnallisuutta varten kirjoitetaan yksi Stripesin ActionBeania laajentava Java-luokka. Nyt luomaani luokkaa tullaan siis käyttämään kaikissa vahvaan sähköiseen tunnistamiseen liittyvissä toiminnallisuuksissa. Kyseisen Java-luokan runko ennen varsinaisten toiminnallisuuksien lisäämistä näytti kuvan 6 kaltaiselta.

```java
@UrlBinding("/auth/{$event}/{org}")
public class eIdentificationController extends YksaBaseActionBean {
    final Logger logger = LogManager.getLogger(eIdentificationController.class);

    private final UserService userService;
    private final CustomerRepository customerRepository;

    private String org;

    @Inject
    public eIdentificationController(final UserService userService,
                                     final CustomerRepository customerRepository) {
        this.userService = userService;
        this.customerRepository = customerRepository;
    }

    @DefaultHandler
    public Resolution notFound() {
        return this.forwardTo(NOT_FOUND_JSP);
    }

    @HandlesEvent("suomiFI")
    public Resolution suomiFIAuth() {
        // TODO
    }

    public String getOrg() {
        return org;
    }
    public void setOrg(final String org) {
        this.org = org;
    }
}
```

Kuva 6. eIdentificationController-luokan runko

Yksan HTML-sivut parsitaan kokoon JSP (JavaServer Pages) -tekniikalla. Tunnistustapahtuman aloittavan napin lisääminen käyttöliittymään oli siis yksinkertaista. Prototyyppiä varten lisäsin Yksan julkisen käyttöliittymän etusivulle linkin edellä kuvattuun suojattuun reittiin ja tyylittelin linkin Yksan valmiiden tyyliluokkien avulla. Yksinkertaisimmillaan tunnistustapahtuman aloittavan linkin lisääminen tapahtui kuvan 7 kaltaisesti.

```
<s:link
    beanclass="fi.mamk.yksa.stripes._public.eIdentificationController"
    event="suomiFI"
    class="btn btn--primary">
    <fmt:message key="identification.start"/>
</s:link>
```

Kuva 7. Linkin lisääminen Stripes Frameworkin avulla

4.4 Tunnistustietojen vastaanotto

Seuraava haaste oli vastaanottaa pääsynhallintajärjestelmän Yksalle lähettämät tiedot. Kehitystyötä, testaamista ja myös mahdollista vianmääritystä helpottamaan kirjoitin yksinkertaisen JSP-sivun, joka tulostaa näkyviin kaikki pyynnön mukana tulleet otsakkeet. Aluksi laitoin luomani ActionBeanin vastaamaan kaikkiin sille tuleviin pyyntöihin parsimalla kyseisen JSP:n näkyviin. Se olikin hyödyllistä, sillä heti ensimmäisen onnistuneen tunnistustapahtuman jälkeen nähtävissä oli ongelma: IdP:n palauttamat tiedot tulivat kyllä perille, mutta tietojen merkistökoodaus oli täysin väärä, sillä esimerkiksi skandinaaviset merkit, kuten Ä ja Ö, eivät näkyneet oikein, kuten kuvasta 8 on selvästi nähtävissä.

SAML 2.0 tunnistustapaht

Jatka

auth-otsakkeet

Otsakkeen nimi	Otsakkeen arvo
auth_personidentifier	null
auth_familyname	null
auth_foreignpersonidentifier	null
auth_firstname	Matti Sakari
auth_sn	MeikÃ¤lÃ¤inen
auth_givenname	Matti
auth_nationalidentificationnumber	010181-900C
auth_electronicidentificationnumber	null

Kuva 8. Osa pääsynhallintajärjestelmän Yksalle lähettämistä otsakkeista

Ongelma johtui siitä, että pääsynhallintajärjestelmä muuttaa parsimansa tiedot käyttämään ISO-8859-1-merkistökoodausta HTTP-otsakkeiden tietueina lähettämistä varten, mutta ilmeisesti joko Yksan käyttämä Apache Tomcat -palvelin tai Stripes Framework lukee otsakkeet sisäisesti UTF-8-merkistökoodausta käyttäen. RFC 7230 -standardin mukaan otsakkeen tietue saisi sisältää vain ASCII-merkkejä (eli ei esimerkiksi lainkaan skandinaavisia merkkejä), mutta kuten web-kehityksen maailmassa yleisesti, tämäkin standardi on vain yksi monien joukossa.

Tässä tapauksessa ongelma oli helppo korjata kuvan 9 kaltaisella Java-koodilla. Kuvassa riveillä 1 ja 2 luetaan käyttäjän etunimen mahdollisesti sisältävien otsakkeiden tiedot omiin muuttujiinsa. Jos pyynnön mukana ei tullut jotakin otsaketta, saa sitä vastaava muuttuja arvon null. Muut tiedot luetaan täsmälleen samalla tavalla, etunimeä käytetään tässä vain esimerkkinä. Olin konfiguroinut pääsynhallintajärjestelmän niin, että suomalaista tunnistusvälinettä käyttävän tunnistautujan etunimi sijaitsi otsakkeessa auth_givenname ja eIDAS-tunnistautujan taas otsakkeessa auth_FirstName. Selvyyden vuoksi kunkin otsakkeen nimen loppuosa vastaa suoraan Suomi.fi-tunnistuksen tunnistusvastauksen attribuutin nimeä. Aiemmin kustomoitujen otsakkeiden nimien tuli standardin mukaan alkaa merkkijonolla X- (Kirjain X ja yhdysmerkki). Tästä käytännöstä on kuitenkin myöhemmin luovuttu. (RFC 6648.)

Kuvan 9 riviltä 3 alkaen käytän Javan Stream-luokan metodeja luettujen arvojen käsittelyyn. Ehdottomasti merkityksellisin kohta löytyy riviltä 6, jossa map-metodin avulla muutan otsakkeesta luetun arvon uudeksi String-olioksi (eli käytännössä tekstiksi) käyttäen String-luokan muodostimesta (*constructor*) kuormitettua versiota, joka hyväksyy ensimmäisenä parametrinä taulukon tavuja ja toisena parametrinä merkistökoodauksen, jota käyttäen String-olion tekstisisältö annetuista tavuista muodostetaan. Tämän myötä merkistökoodausongelma oli ratkaistu.

```
1  final String givenName = getContext().getRequest().getHeader("auth_givenname");
2  final String firstName = getContext().getRequest().getHeader("auth_FirstName");
3  final String firstnameToUse = Stream.of(givenName, firstName)
4      .filter(StringUtils::isNotBlank)
5      .findFirst()
6      .map(s -> new String(s.getBytes(StandardCharsets.ISO_8859_1), StandardCharsets.UTF_8))
7      .orElseThrow(RuntimeException::new);
```

Kuva 9. Tietojen lukeminen otsakkeista ja merkistökoodauksen korjaaminen

Päätimme yhdessä toimeksiantajan kanssa, että prototyyppiversio loisi uuden asiakastilin (eli tietokantaan tallennetun Customer-olion) jokaiselle uudelle tunnistautujalle. Jos sama henkilö tunnistautuu myöhemmin uudelleen, hänet tulisi kirjata sisään aiemmin luodulle asiakastilille. Tämän toteuttaminen luonnollisesti vaati, että tunnistautunut käyttäjä oli jotenkin voitava yksilöidä niin, että samalle henkilölle ei jokaisen tunnistautumisen yhteydessä luotaisi uutta asiakastiliä. Suomi.fi-tunnistuksen palauttamista attribuuteista tämän yksilöinnin

voi tehdä henkilötunnuksen, sähköisen asiointitunnuksen, ulkomaisen henkilön tunnisteen tai eIDAS-tunnistautujan tunnisteen avulla. Jo suppea tietolupa riittää kaikkien edellä mainittujen tietojen saamiseen Suomi.fi-tunnistuksesta.

Henkilötunnus ja myös muut yksilöivät tunnisteet ovat henkilötietoja, joiden tallentamisen ja säilyttämisen kanssa tulee aina olla ehdottoman tarkkana. Jo alusta asti oli selvää, että henkilötunnusta tai muuta yksilöivää tunnistetta ei voi tallentaa Yksan tietokantaan selkokielisenä. Eräs vaihtoehto olisi ollut salakirjoittaa tunniste jollakin sopivalla salakirjoitusfunkttiolla. Tajusimme kuitenkin toimeksiantajan kanssa, että tällä hetkellä pöydällä olevissa vahvan sähköisen tunnistamisen käyttötapauksista yksilöivää tunnistetta ei itsessään tunnistuksen jälkeen tarvita mihinkään. Sitä ei esimerkiksi ole tarkoitus näyttää käyttöliittymässä tai missään Yksan generoimista asiakirjoista. Siispä tietoturvan kannalta paras ratkaisu oli laskea tunnisteesta sopivalla tiivistefunktiolla ns. tarkistussumma tai tiiviste, aivan kuten normaalin asiakastilin salasanallekin tehdään.

Toteutuksessani tämä tarkistussumma lasketaan jokaisen onnistuneen tunnistustapahtuman jälkeen ja jos tietokannasta jo löytyy asiakastili vastaavalla tarkistussummalla, käytetään sitä uuden luomisen sijaan. Käytettäväksi tiivistefunktioksi valitsin SHA-512-tiivistefunktion. Se on varmasti riittävän järeä nyt ja myös tulevaisuudessa, jotta törmäyksen mahdollisuus on hyväksyttävän pieni. Tiivistefunktioista puhuttaessa törmäys (tai konflikti) tarkoittaa tilannetta, jossa kaksi eri syötettä palauttavat saman tarkistussumman (Kyberturvallisuuskeskus 2020c).

Yksilöivät tunnisteet sisältävät ainoastaan ASCII-merkkejä, joten merkistökoodauksen muuttamisesta ei niiden yhteydessä tarvinnut välittää. Sen sijaan käytin kuvan 10 kaltaisesti Apache Commons Lang -ohjelmakirjastosta löytyvän DigestUtils-luokan funktiota sha512Hex tunnisteen muuttamiseksi tarkistussummaksi. Kuvasta 10 on hyvä huomata myös tunnisteiden käyttöjärjestys. Ensisijaisesti toteutukseni yrittää käyttää tunnisteena henkilötunnusta. Sen puuttuessa (tai ollessa tyhjä) yrittää se käyttää ulkomaisen henkilön tai eIDAS-tunnistautujan tunnistetta. Toteutuksessani sähköistä asiointitunnusta käytetään yksilöimiseen vasta viimeisenä vaihtoehtona. Tämä sen vuoksi, että se

on mukana Suomi.fi-tunnistuksen tunnistusvastauksessa vain, jos tunnistusvälineenä käytettiin kansalaisvarmennetta. Jos sähköistä asiointitunnusta käytettäisiin ensisijaisena yksilöivänä tunnisteena, tunnistautujaa ei seuraavalla kerralla pystyttäisi liittämään aiemmin luotuun asiakastiliin, jos tunnistautuja silloin käyttäisikin jotakin muuta tunnistusvälinettä.

```
final String identifierToUse = Stream.of(
    nationalIdentificationNumber, foreignPersonIdentifier, personIdentifier, electronicIdentificationNumber
).filter(StringUtils::isNotBlank)
.findFirst()
.map(DigestUtils::sha512Hex)
.orElseThrow(RuntimeException::new);
```

Kuva 10. Yksilöivän tunnisteen tarkistussumaan laskeminen

Viimeiset vaiheet vastaanotettujen tunnistustietojen käsittelyssä ovat mahdollisesti jo olemassa olevan asiakastilin hakeminen tietokannasta, tarvittaessa uuden tilin luominen ja tallentaminen sekä asiakastilin tietojen lisääminen istunnon tietoihin. Nämä toimet suorittava lyhyt ohjelmakoodi on nähtävissä kuvassa 11. Yksassa tietokantaan tallennettuihin Customer-olioihin pääsee käsiksi CustomerRepository-luokan ilmentymän kautta. Laajensin ko. luokkaa lisäämällä siihen findByIdentiferHash-funktion, joka hyväksyy parametrinä aiemmin generoidun tarkistussumman ja etsii sen perusteella olemassa olevaa asiakastiliä tietokannasta. Jos sellainen löytyy, käytetään sitä uuden tilin luomisen sijaan.

Koska Yksan käyttämä tietokanta, Couchbase, on dokumenttitietokanta (eikä perinteinen relaatiotietokanta), se ei kaikissa tilanteissa suoriudu erityisen tehokkaasti yksittäisen dokumentin etsimisestä suuresta tietomassasta. Suorituskykyongelmien välttämiseksi SQL-kyselyn muotoon tulee kiinnittää erityistä huomiota ja hyödyntää siinä Couchbasen tarjoamia suorituskykyä parantavia ominaisuuksia kuten indeksejä ja näkymiä (*view*). Vaihtoehtoisesti aiemmin tallennetun Customer-olion etsimiseen tietyn kentän arvon perusteella voi Yksassa käyttää Solr-hakumoottoria, jonne asiakastilit jo alusta saakka on Yksassa automaattisesti indeksoitu. Prototyyppiversion toteutuksessa suorituskyvyllä ei kuitenkaan vielä ole kovin suurta merkitystä, mutta asia oli hyvä tiedostaa ja pitää mielessä jo tässä vaiheessa.

Lopuksi asiakastilin tiedot lisätään istunnon tietoihin, jonka jälkeen sisäänkirjautuminen on suoritettu ja käyttäjä voidaan ohjata takaisin julkisen käyttöliittymän etusivulle. Customer-olion kaikkia tietoja ei Yksassa suoraan lisätä istunnon tietoihin, vaan käytetään UserService-luokasta löytyvää funktiota copyCustomerProperties, joka palauttaa istunnon tietoihin tallennettavaksi sopivan User-olion. Kyseinen funktio huolehtii muun muassa siitä, että ylimääräisiä tietoja, kuten salasanan tiivistettä, ei koskaan ole istunnon tiedoissa. Tämä on tärkeää jo tietoturvankin kannalta. Lisäsin User-olioon totuusarvomuuttujan (*boolean*) requiresIDPLogout, jota siis nimensä mukaisesti tullaan hyödyntämään uloskirjautumisen yhteydessä.

```
final Optional<Customer> pointerToCustomer = customerRepository.findByIdentifierHash(identifierToUse);
if (pointerToCustomer.isPresent()) {
    customer = pointerToCustomer.get();
} else {
    final Customer newCustomer = new Customer();
    newCustomer.setFirstName(firstnameToUse);
    newCustomer.setLastName(surnameToUse);
    newCustomer.setAuthenticatedBy("SuomiFI");
    newCustomer.setIdentifierHash(identifierToUse);
    customer = customerRepository.save(newCustomer);
}

final User customerUser = this.userService.copyCustomerProperties(customer);
customerUser.setFederatedLogin(true);
customerUser.setRequiresIDPLogout(true);
super.getContext().setUser(customerUser);
```

Kuva 11. Asiakastilin hakeminen tietokannasta, uuden luominen tarvittaessa sekä tilin tietojen lisääminen istunnon tietoihin

4.5 Muut käyttötapaukset

Tunnistuspyynnön lähettämisen ja sitä seuraavan tunnistusvastauksen vastaanottamisen lisäksi jokaisen Suomi.fi-tunnistusta käyttävän palvelun on tuettava uloskirjautumiseen liittyviä pyyntöjä ja vastauksia. (Tekninen rajapintakuvaus 2020.) Kertakirjautumiseen kuuluu se, että jos tunnistautunut käyttäjä ilmaisee haluavansa kirjautua ulos Yksasta, pyyntö tulee välittää myös IdP:lle, joka puolestaan automaattisesti lähettää uloskirjautumispyynnön muihin asiointipalveluihin, joihin käyttäjä on saman kertakirjautumisistunnon aikana tunnistautunut. Tämän on luonnollisesti toimittava myös toisinpäin, eli Yksan on kyettävä ottamaan vastaan IdP:n lähettämä uloskirjautumispyyntö ja toteutettava se.

Pääsynhallintajärjestelmä hoitaa tämänkin osuuden suurelta osin automaattisesti. Melkeinpä ainut Yksaan vaadittava muutos oli tehtävä käyttöliittymän

uloskirjautumisnappiin. Tähän saakka se oli toiminut niin, että jos käytössä oli asiakastili, napin painaminen ohjasi Yksan omaan tapahtumankäsittelijään, joka yksinkertaisesti vain poisti asiakastilin tiedot istunnon tiedoista ja ohjasi tämän jälkeen selaimen takaisin julkisen käyttöliittymän etusivulle. Tähän saakka uloskirjautumisnappi ohjasi selaimen pääsynhallintajärjestelmän uloskirjautumisosoitteeseen vain, jos LDAP-todennuksella autentikoitu istunto (eli normaali käyttäjätili, ei asiakastili) oli aktiivinen. Laajensin tätä logiikkaa niin, että nyt nappi ohjaa kyseiseen uloskirjautumisosoitteeseen myös silloin, kun istuntoon on tallennettu tieto aktiivisesti istunnosta IdP:n kanssa eli User-olion requiresIDPLogout-kenttä on asetettu totuusarvoon ’tosi’ (*true*).

5 PÄÄTÄNTÖ

Opinnäytetyössä päästiin sille asetettuihin tavoitteisiin. Teoriaosuudesta tuli laajahko ja siinä käsitellään kaikki ne asiat, joista toimeksiantajan kanssa opinnäytetyön aloituksen yhteydessä sovittiin ja myös kaikki ne asiat, joita itse suunnittelin siinä käsitteleväni. Uskoisin, että tästä opinnäytetyöstä on hyötyä toimeksiantajalle nyt ja myös tulevaisuudessa, kun se lähtee suunnittelemaan ja toteuttamaan vahvan sähköisen tunnistamisen käyttöönottoa palvelutuotannossaan.

TUPAS-tunnistuksen vuoden 2019 aikana korvannut Luottamusverkosto on edelleen kohtalaisen uusi asia. Sen vuoksi siitä oli tietyissä tapauksissa haasteellista löytää luotettavaa tietoa. Monet kaupallisista Luottamusverkoston palveluntarjoajista eivät myöskään kerro palvelujensa tarkkoja yksityiskohtia tai edes hintatietoja julkisesti ilman yhteydenottoa kyseiseen palveluntarjoajaan. Tämä teki palveluntarjoajien vertailemisesta haastavaa, joskin olisin tarvittaessa voinut olla yhteydessä suoraan palveluntarjoajiin kysymysteni kanssa.

Opinnäytetyön prosessin aikana prototyyppiversion toteutuksen tavoitteet, vaatimukset sekä toteutustapa tarkentuivat useaan otteeseen. Alkuperäisessä suunnitelmassa prototyyppiversion toteutus oli pitkälti sidottu erään tietyn asiakkaan käyttötapaukseen. Suunnitelmat kyseisen asiakkaan kanssa kuitenkin muuttuivat juuri kun prototyyppiversiota oli alettu toteuttaa. Vaikka itselläni

meinasi tässä vaiheessa iskeä epäusko koko työn valmistumisen suhteen, raporttiin tai prototyyppiversioon tämä vaikutti jälkikäteen katsottuna todella vähän.

Suunnitelmia laatiessani olin siinä käsityksessä, että prototyyppiversion toteuttaminen tulisi vaatimaan paljon enemmän ohjelmointityötä, kuin se lopulta sitten vaati. En etukäteen tiennyt, että Access Manager -pääsynhallintajärjestelmä hoitaisi niin monia asioita lähes automaattisesti ja ilman yhtäkään koodiriviä. Opinnäytetyön kannalta tämä oli sekä hyvä, että huono asia. Pääsynhallintajärjestelmän hoitaessa suuren osan ”raskaasta työstä”, pystyin raportoinnissa paremmin keskittymään juuri vain haluamiini teknisiin yksityiskohtiin. Jos nyt aloittaisin opinnäytetyön tekemisen kokonaan alusta, suunnittelisin kuitenkin prototyyppiversion toteutuksen paremmin yhdessä toimeksiantajan kanssa siten, että työhön saataisiin suurempi käytännön ohjelmointiosuus.

Prototyyppiversion toteutuksen raportoinnissa otan hyvin vähän kantaa pääsynhallintajärjestelmän yksityiskohtiin tai sen asetusten konfiguroimiseen. Tämä oli tietoinen valinta, jonka tein kahdesta eri syystä: Ensiksi, tietoturvallisuuden kannalta kaikkia pääsynhallintajärjestelmän käyttöön ja asetuksiin liittyviä asioita ei tämän kaltaisessa julkisessa työssä olisi voinut kokonaisuudessaan käsitellä. Lisäksi toimeksiantajalle on samaan aikaan valmistumassa toinen opinnäytetyö, jossa pääsynhallintajärjestelmään ja sen toimintaan paneudutaan tarkemmin, enkä halunnut, että vahingossa käsittelisimme töissämme täsmälleen samoja aiheita.

Vuoden 2020 aikana maailmalla ja Suomessakin riehunut koronaviruspandemia ei onneksi vaikuttanut merkittävästi opinnäytetyön edistymiseen tai aikataulussa pysymiseen. Myös toimeksiantajayrityksessä jouduttiin siirtymään välillä kokonaan etätyöskentelyyn, mikä luonnollisesti hieman vaikeutti yhteistyötä toimeksiantajan kanssa. IT-alalla etätyön tekeminen on tänä päivänä kuitenkin jo normi ja lähes kaikilla on siitä kokemusta, joten suurempaa ongelmaa ei tästäkään asiasta onneksi syntynyt.

Kaikkinensa koen, että opinnäytetyöprosessi oli pääpiirteissään onnistunut ja myös itselleni positiivinen kokemus. Aihe oli alusta saakka minua kiinnostava

ja se varmasti auttoi pitämään motivaation ylhäällä loppuun saakka. Koen olevani melko huono kirjoittamaan opinnäytetyön vaatimaa tieteellistä tekstiä, mutta oman tasoni huomioiden onnistuin mielestäni kohtuullisesti. Toivon, että tämän opinnäytetyön eteen tekemästäni työstä on hyötyä niin itselleni, toimeksiantajalle kuin täysin ulkopuolisillekin lukijoille.

LÄHTEET

Asiointipalvelun metatiedot. 2020. Digi- ja väestötietovirasto. WWW-dokumentti. Päivitetty 26.8.2020. Saatavissa: https://palveluhallinta.suomi.fi/fi/tuki/artikkelit/590adae814bbb10001966f53 [viitattu 15.9.2020].

Digi- ja väestötietovirasto. 2019. Suomi.fi-tunnistus organisaatioille. WWW-dokumentti. Päivitetty 30.12.2019. Saatavissa: https://www.suomi.fi/palvelut/suomi-fi-tunnistus-organisaatioille-digi-ja-vaestotietovirasto/1870170e-ea0f-40d6-b3fb-6d2ddc478065 [viitattu 6.7.2020].

Digi- ja väestötietovirasto. 2020. Tunnistetusta käyttäjästä välitettävät attribuutit. WWW-dokumentti. Päivitetty 18.5.2020. Saatavissa: https://palveluhallinta.suomi.fi/fi/tuki/artikkelit/590ad07b14bbb10001966f50 [viitattu 29.8.2020].

Digi- ja väestötietovirasto. s.a. Kansalaisvarmenne ja sähköinen henkilöllisyys. WWW-dokumentti. Saatavissa: https://dvv.fi/kansalaisvarmenne-ja-sahkoinen-henkilollisyys [viitattu 13.5.2020].

Finanssialan Keskusliitto. 2013. Pankkien Tupas-tunnistuspalvelun tunnistusperiaatteet V2.0c 2.12.2013. PDF-dokumentti. Saatavissa: https://www.finanssiala.fi/maksujenvalitys/dokumentit/Tupas_tunnistusperiaatteet_v20c.pdf [viitattu 17.5.2020].

Finanssialan keskusliitto. 2014. Hallituksen esitys eduskunnalle laiksi vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain muuttamisesta. Lausunto. Saatavissa: https://www.finanssiala.fi/lausunnot/HE_vahva_sahkoinen_tunnistaminen_ja_sahkoiset_allekirjoituksset_03122014.pdf [viitattu 28.7.2020].

HE 264/2018. Hallituksen esitys eduskunnalle laiksi vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain muuttamisesta ja väliaikaisesta muuttamisesta.

Karkimo, A. 2019. Tähänkö loppuu pankkien rahastus? – ”Valtiolta mobiilisovellus tai usb-tikku tunnistautumista varten”. Tivi. Verkkolehti. Päivitetty 8.3.2019. Saatavissa: https://www.tivi.fi/uutiset/tahanko-loppuu-pankkien-rahastus-valtiolta-mobiilisovellus-tai-usb-tikku-tunnistautumista-varten/768d7f08-632a-3188-9f7e-e8878c139f89 [viitattu 13.5.2020].

Komission täytäntöönpanoasetus (EU) 2015/1502.

Kyberturvallisuuskeskus. 2020a. Sähköinen tunnistaminen. WWW-dokumentti. Päivitetty 31.3.2020. Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/sahkoinen-tunnistaminen [viitattu 7.5.2020].

Kyberturvallisuuskeskus. 2020b. Toimijat, rajapinnat ja kontaktitiedot. PowerPoint-dia. Päivitetty 26.5.2020. Saatavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Luottamusverkostotoimijat_rajapinnat_ja_kontaktitiedot_PPT_taulukot.PPTX [viitattu 26.5.2020].

Kyberturvallisuuskeskus. 2020c. SHA-1-tiivistefunktio on lopullisesti murrettu. WWW-dokumentti. Päivitetty 14.1.2020. Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/sha-1-tiivistefunktio-lopullisesti-murrettu [viitattu 27.10.2020].

Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista 7.8.2009/617.

Laki väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista 21.8.2009/661.

Lehtiniitty, M. 2019. Mobiilivarmenne uudistuu ensi vuonna – luvassa entistä monipuolisempi ja helppokäyttöisempi palvelu. Mobiili.fi. Uutisartikkeli. Päivitetty 4.11.2019. Saatavissa: https://mobiili.fi/2019/11/04/mobiilivarmenne-uudistuu-ensi-vuonna-luvassa-entista-monipuolisempi-ja-helppokayttoisempi-palvelu/ [viitattu 12.5.2020].

Lehto, T. 2017. Nettitunnistautumiseen viimein kilpailua – "Hinnat tähän asti pöyristyttäviä Tekniikka&Talous. Uutisartikkeli. Päivitetty 13.2.2017. Saatavissa: https://www.tekniikkatalous.fi/uutiset/nettitunnistautumiseen-viimein-kilpailua-hinnat-tahan-asti-poyristyttavia/636e1256-d50f-3f64-b0eb-761b12df04fd [viitattu 16.5.2020].

Metsola, A. 2018. Mitä vahva sähköinen tunnistaminen tarkoittaa? FiCom ry. WWW-dokumentti. Päivitetty 10.10.2018. Saatavissa: https://www.ficom.fi/ajankohtaista/uutiset/mit%C3%A4-vahva-s%C3%A4hk%C3%B6inen-tunnistaminen-tarkoittaa [viitattu 7.5.2020].

Mikä on Palveluhallinnan käyttäjähallinta? 2019. Digi- ja väestötietovirasto. WWW-dokumentti. Päivitetty 8.12.2019. Saatavissa: https://palveluhallinta.suomi.fi/fi/tuki/ukk/5b38d5bf243f34001cb00f7f [viitattu 30.8.2020].

Mitrunen, J., Salovaara, T. & Viskari, J. 2019. Sähköinen tunnistaminen: Selvitys nykytilasta sekä kehittämistarpeista. Valtionvarainministeriön julkaisuja 2019:20. Helsinki: Valtionvarainministeriö. PDF-dokumentti. Saatavissa: http://urn.fi/URN:ISBN:978-952-367-000-6 [viitattu 11.5.2020].

Niiranen, P. 2019. Verkkopankkiin ei pääse pian pelkällä pahvilapulla - Turvallisuus kasvaa, mutta perinteinen tunnuslukulista ei vielä katoa. Yle. Uutisartikkeli. Päivitetty 30.7.2019. Saatavissa: https://yle.fi/uutiset/3-10897752 [viitattu 9.5.2020].

Nordea Bank Oyj. s.a. Pankkitunnukset. WWW-dokumentti. Saatavissa: https://www.nordea.fi/henkiloasiakkaat/palvelumme/verkko-mobiilipalvelut/pankkitunnukset.html [viitattu 12.5.2020].

OP Tunnistuksen välityspalvelun palvelukuvaus. 2019. OP Ryhmä. PDF-dokumentti. Päivitetty 12.4.2019. Saatavissa: https://www.op.fi/documents/20556/29157067/OP+Tunnistuksen+v%C3%A4lityspalvelun+palvelukuvaus/76279386-e714-184e-e059-c1134d68d1f3 [viitattu 2.8.2020]

OP-Palveluhinnasto. 2020. Rantasalmen Osuuspankki. PDF-dokumentti. Saatavissa: https://www.op.fi/documents/276934/32253890/FI-Yritysasiakkaat/ce59527c-7aeb-098e-2c77-136eb91821d6 [viitattu 28.8.2020].

Palomaa, A. 2016. Maksuhäiriömerkintä ei enää estä verkkopankkitunnusten saamista. Yle. Uutisartikkeli. Päivitetty 8.5.2017. Saatavissa: https://yle.fi/uutiset/3-9364251 [viitattu 11.5.2020].

Palvelun kuvaus. s.a. Digi- ja väestötietovirasto. WWW-dokumentti. Saatavissa: https://palveluhallinta.suomi.fi/fi/sivut/tunnistus/palvelukuvaus/palvelunkuvaus [viitattu 21.9.2020].

RFC 6648. 2012. Deprecating ”X-”.

RFC 7230. 2014. Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing.

Signicat AS. 2017. Authentication. WWW-dokumentti. Päivitetty 20.11.2017. Saatavissa: https://developer.signicat.com/documentation/authentication/ [viitattu 11.8.2020].

Signicat AS. s.a. Finnish Bank eIDs (FTN). WWW-dokumentti. Saatavissa: https://developer.signicat.com/id-methods/finnish-bank-eids-ftn/ [viitattu 11.8.2020].

Suomi.fi-tunnistus: Käyttöönoton vaiheet. s.a. Digi- ja väestötietovirasto. WWW-dokumentti. Saatavissa: https://palveluhallinta.suomi.fi/fi/sivut/tunnistus/kayttoonotto/kayttoonoton-vaiheet [viitattu 29.8.2020].

Suomi.fi-tunnistus: Testiympäristöön liittyminen. s.a. Digi- ja väestötietovirasto. WWW-dokumentti. Saatavissa: https://palveluhallinta.suomi.fi/fi/sivut/tunnistus/kayttoonotto/asiakastestiymparisto [viitattu 30.8.2020].

Tekninen rajapintakuvaus. 2020. Digi- ja väestötietovirasto. WWW-dokumentti. Päivitetty: 20.8.2020 Saatavissa: https://palveluhallinta.suomi.fi/fi/sivut/tunnistus/kayttoonotto/asiakastestiymparisto [viitattu 30.8.2020].

Timo Harakka tilasi henkilökortin ja yritti aktivoida yli tunnin – ”Käyttöohjeenkin on kirjoittanut itse Franz Kafka”. 2017. Uusi Suomi. Verkkolehti. Päivitetty 26.7.2017. Saatavissa: https://www.uusisuomi.fi/uutiset/timo-harakka-tilasi-henkilokortin-ja-yritti-aktivoida-yli-tunnin-kayttoohjeenkin-on-kirjoittanut-itse-franz-kafka/3921c71c-0e41-3d7d-8e2e-67b7fee05977 [viitattu 13.5.2020].

Tunnistuspalveluiden kehittäminen ja käyttö julkisessa hallinnossa. 2008. Valtiontalouden tarkastusviraston toiminnantarkastuskertomukset 161/2008. Helsinki: Edita Prima Oy. PDF-dokumentti. Saatavissa: https://www.vtv.fi/app/uploads/2018/07/03111900/tunnistuspalvelut-161-2008.pdf [viitattu 4.7.2020].

Vahva tunnistaminen Signicat Connect -ratkaisulla. s.a. Signicat AS. WWW-dokumentti. Saatavissa: https://www.signicat.com/fi/palvelut/vahva-tunnistaminen/ [viitattu 2.8.2020].

Vauhdilla kasvavasta kännykkätunnistuksesta entistä monipuolisempaa: DNA, Elisa ja Telia sopivat uudistetun Mobiilivarmenteen kehittämisestä. 2019. Lehdistötiedote. Saatavissa: https://mobiilivarmenne.fi/2019/11/04/vauhdilla-kasvavasta-kannykkatunnistuksesta-entista-monipuolisempaa-dna-elisa-ja-telia-sopivat-uudistetun-mobiilivarmenteen-kehittamisesta/ [viitattu 30.8.2020].

KUVALUETTELO

Kuva 1. Luottamusverkoston toimintaperiaate. Jansson, P. 2019. Luottamusverkosto, TUPAS ja tunnistamisen muutokset. Finanssiala ry. WWW-dokumentti. Päivitetty 11.2.2019. Saatavissa: https://www.finanssiala.fi/uutismajakka/Sivut/Luottamusverkosto,-TUPAS-ja-tunnistamisen-muutokset.aspx [viitattu 23.5.2020].

Kuva 2. Hyväksytyt kaupalliset Luottamusverkoston jäsenet, tilanne 7.5.2020. Kyberturvallisuuskeskus. 2020a. Sähköinen tunnistaminen. WWW-dokumentti. Päivitetty 31.3.2020. Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/sahkoinen-tunnistaminen [viitattu 7.5.2020].

Kuva 3. Yksa-arkistonhallintajärjestelmän toimintaperiaatteen kuvaus. Disec Oy. 2020. Yksa-arkistonhallintajärjestelmä. PowerPoint-dia. Saatavissa: https://disec.fi/arkistopalvelut/ [viitattu 27.10.2020].

Kuva 4. Käytettävän varmenteen kuvaaminen asiointipalvelun metatiedoissa. Kuvakaappaus.

Kuva 5. Paluuosoitteiden määrittely. Kuvakaappaus.

Kuva 6. eIdentificationController-luokan runko. Kuvakaappaus.

Kuva 7. Linkin lisääminen Stripes Frameworkin avulla. Kuvakaappaus.

Kuva 8. Osa pääsynhallintajärjestelmän Yksalle lähettämistä otsakkeista. Kuvakaappaus.

Kuva 9. Tietojen lukeminen otsakkeista ja merkistökoodauksen korjaaminen. Kuvakaappaus.

Kuva 10. Yksilöivän tunnisteen tarkistussumman laskeminen. Kuvakaappaus.

Kuva 11. Asiakastilin hakeminen tietokannasta, uuden luominen tarvittaessa sekä tilin tietojen lisääminen istunnon tietoihin. Kuvakaappaus.