Tuula Haapiainen

TOTEUTETTAVUUSSELVITYS SÄHKÖISEN ALLEKIRJOITUKSEN KÄYTTÖÖNOTOLLE
case
Kaakkois-Suomen Ammattikorkeakoulu Oy

Opinnäytetyö
Sähköinen asiointi ja arkistointi YAMK

Toukokuu 2016

MAMK
University of Applied Sciences

KUVAILULEHTI

MAMK University of Applied Sciences	**Opinnäytetyön päivämäärä** 7.5.2016
Tekijä(t) Tuula Haapiainen	**Koulutusohjelma ja suuntautuminen** **Sähköinen asiointi ja arkistointi**
Nimeke Toteutettavuusselvitys sähköisen allekirjoituksen käyttöönotolle – case Kaakkois-Suomen Ammattikorkeakoulu Oy	
Tiivistelmä Tämän opinnäytetyön tavoitteena oli pohtia sähköisen allekirjoituksen toteutettavuutta Kaakkois-Suomen Ammattikorkeakoulu Oy:ssä mahdollisimman laaja-alaisesti, alkaen yleisistä perusteista ja päätyen organisaation käytännön askeleisiin kohti sähköistä allekirjoitusta. Erityistä huomiota kiinnitettiin käyttöönoton kriittisiin kohtiin. Työ rajattiin organisaation johtamiseen ja tukipalveluihin. Tutkimusmateriaali kerättiin kyselytutkimuksella ja sitä täydennettiin asiantuntijahaastatteluilla. Lisäksi tehtiin tapaustutkimuksia Suomesta, Virosta ja Saksasta. Tutkimusmateriaalia tulkittiin loogisen lähestymistavan avulla. Sen pohjalta luotiin käytännön toteutusaskeleisiin johtava analyysikehikko, jonka pohjalta syntyi luonnostelma sähköisen allekirjoituksen käyttöönottoprojektille Kaakkois-Suomen Ammattikorkeakoulu Oy:ssä. Käyttöönottoon liittyvistä kriittisistä kohdista laadittiin riskianalyysi. Työn loppupäätelmänä todetaan, että valmiudet sähköisen allekirjoituksen käyttöönottoon Kaakkois-Suomen Ammattikorkeakoulu Oy:ssä ovat hyvällä tasolla, ja kiinteänä osana organisaation tiedonhallinnan kehittämistä sen käyttöönotto voidaan tehdä hyvin joustavasti ja kustannustehokkaasti. Myös ulkoiset tekijät, kuten lainsäädäntö ja julkisen vallan tuki, edistävät tätä kehitystä vahvasti. Ensimmäisiksi sovellusalueiksi kyselystä nousivat pöytäkirjojen tarkistaminen ja allekirjoitukset sekä päätökset. Kriittisiä kohtia olivat erityisesti aikataulujen viivästyminen ja käyttötuen organisointi.	
Asiasanat (avainsanat) Sähköinen allekirjoitus, sähköiset henkilökortit, sähköinen tunnistaminen, todentaminen, varmenteet	
Sivumäärä 47 s. + liitteet 12 s.	**Kieli** Suomi
Huomautus (huomautukset liitteistä)	
Ohjaavan opettajan nimi Mirja Loponen ja Anssi Jääskeläinen	**Opinnäytetyön toimeksiantaja** Kaakkois-Suomen Ammattikorkeakoulu Oy

DESCRIPTION

MAMK University of Applied Sciences	**Date of the master's thesis** 7 May 2016
Author(s) Tuula Haapiainen	**Degree programme and option** eServices and Digital Archiving

Name of the master's thesis

Feasibility study on the deployment of the electronic signature in the South-Eastern Finland University of Applied Sciences.

Abstract

The aim of this thesis was to discuss the feasibility of the electronic signature in the South-Eastern Finland University of Applied Sciences as broadly as possible, starting from the general principles and ending at practical steps on the way to electronic signature. Especially attention was paid to the introduction of critical control points. The thesis was limited to the management and support services.

The research material was collected by a questionnaire survey and supplemented with expert interviews. In addition, several case studies were make from Finland, Estonia and Germany. This material was interpreted through the logical framework approach. Based on it, an analysis framework was developed leading to the practical development steps. These steps constitute a draft for a deployment project of electronic signature in the South-Eastern Finland University of Applied Sciences.

The final conclusion of this thesis was that the starting point for the deployment of the electronic signature in the South-Eastern Finland University of Applied Sciences was good level. As integral part of the development of the knowledge management of the organisation the deployment can be made smoothly and in a cost-efficient way. Also external factors, like legislation and the support of the public authorities, promote strongly this development. The study emphasises that was first application areas could be inspecting and signing of the minutes of the meetings as well as decisions. Critical points were especially delays in timetables and organising user support.

Subject headings, (keywords)

Electronic signature, electronic identity cards, electronic identification, verification, certificates

Pages 47 p. + app. 12 p.	**Language** **Finnish**

Remarks, notes on appendices

Tutor Mirja Loponen and Anssi Jääskeläinen	**Master's thesis assigned by** South-Eastern Finland University of Applied Sciences Ltd

SISÄLTÖ

1 JOHDANTO

Opinnäytetyöni on toteutettavuusselvitys (eng. feasibility study) sähköisen allekirjoituksen käyttöönottamiseksi Kaakkois-Suomen Ammattikorkeakoulu Oy:ssä (myöhemmin Xamk). Sähköisen allekirjoituksen käyttöönottoa pohdin laaja-alaisesti organisaation eri toimintojen näkökulmasta: Millaisia valmisteluja ja valmiuksia tarvitaan organisaatiolta suunniteltaessa sähköisen allekirjoituksen käyttöönottoa? Miten ja millaisiin tehtäviin käyttöönoton suunnittelu on järkevää kohdentaa? Onko käyttöönotto toteutettavissa helposti ja lyhyellä aikataululla? Onko siirtyminen perinteisestä allekirjoituksesta sähköiseen toteutettavissa tarkoituksen mukaisella tavalla? Mitkä hyödyt sähköisen allekirjoituksen käyttöönotolla saavutetaan lyhyellä ja pitkällä aikavälillä?

Opinnäytetyöni toimeksiantajan, Kaakkois-Suomen Ammattikorkeakoulu Oy:n tavoitteena on fuusioitua tytäryhtiöidensä Kymenlaakson Ammattikorkeakoulu Oy:n ja Mikkelin Ammattikorkeakoulu Oy:n kanssa vuoden 2017 alussa. Kymenlaakson ammattikorkeakoulu toimii Kotkassa ja Kouvolassa, Mikkelin ammattikorkeakoulu Mikkelissä ja Savonlinnassa. Toimeksi saamani kehittämistehtävä ja samalla selvittäminen sähköisen allekirjoituksen käyttöönoton toteutusmahdollisuuksista ajoittuu samalle aikajanalle kuin tiedonhallintaratkaisun hankinta koko korkeakoulukokonaisuudelle. On perusteltua jo tässä vaiheessa selvittää sähköisen allekirjoituksen käyttöönoton edellytyksiä ja mahdollisia haasteita. Laatimani selvitys pohjautuu emoyhtiön Xamkin sekä tytäryhtiöiden Kymenlaakson ammattikorkeakoulun ja Mikkelin ammattikorkeakoulun esimiehille ja luottamushenkilöille kohdistamaani kyselyyn, asiantuntijahaastatteluihin sekä aiheesta julkaistuun kirjalliseen aineistoon.

Organisaatioilta edellytetään yhä enemmän uudistumista ja kehittymistä ja yhä laajempia kokonaisuuksia. Korkeakoulujen rakenteellisessa kehittämisessä, joka on yksi nykyisen hallituksen kärkihankkeista, ammattikorkeakoulujen uudistuksen tavoitteena on ”ammattikorkeakoulu, joka on kansainvälisesti arvostettu, itsenäinen ja vastuullinen

- osaajien kouluttaja
- alueellisen kilpailukyvyn rakentaja
- työelämän uudistaja
- innovaatioiden kehittäjä”

Uudistuksella pyritään itsenäisten, alueellisesti vahvojen koulutusrakenteiden synnyttämiseen, jossa uudella teknologialla ja innovaatioilla on suuri merkitys. Ammattikorkeakouluilta edellytetään myös uudistuksissa edellä käymistä. (Opetus- ja kulttuuriministeriö. AMK-uudistus 2011–2014.)

Tietoteknisestäkin näkökulmasta tarkasteltuna kehitys ja muutos työelämässä ja koulutusorganisaatioissa on ollut valtava lähes kolmenkymmenenkuuden vuoden työurani aikana. Työnantajani, Xamkin tytäryhtiö, Mikkelin Ammattikorkeakoulu Oy aloitti toimintansa 1.1.2009 useiden organisaatiomuutosten jatkona. Edeltäneet organisaatiot ja samalla työnantajani ovat olleet Mikkelin ammattikorkeakouluyhtymä vuosina 2001–2008, Mikkelin koulutusyhtymä vuosina 1995–2000, Mikkelin kaupungin ylläpitämä liiketalouden instituutti (aiemmin kauppaoppilaitos) vuosina 1980–1994. Kirjoituskoneella laadituista asiakirjoista tämän päivän sähköisiin asiakirjoihin ja sähköisen allekirjoituksen mahdollistavaan teknologiaan on vuosinakin mitattuna monen insinöörikoikan verran. Kehitys on edellyttänyt ja edellyttää edelleen myös oman asiantuntijuuden uudistamista ja kehittämistä. Toivon, että selvitykseni lopputulos vie tiedonhallinnan kehittämistä omalta osaltaan eteenpäin ja auttaa organisaation toimintojen virtaviivaistamista ja tehostamista entisestään.

”Asioita ei muuteta taistelemalla nykyisiä realiteetteja vastaan. Jos tahdot muutosta, rakenna uusi malli, joka vanhentaa nykyisen mallin.” - Keksijä Buckminster Fuller (1895–1983).

2 OPINNÄYTETYÖN TOTEUTUS

Tässä luvussa esittelen opinnäytetyöni tavoitteen, tutkimusongelmat ja rajauksen. Käsittelen myös tutkimus- ja aineistonkeruumenetelmää sekä niiden soveltuvuutta tähän opinnäytetyöhön. Luvun lopuksi käyn läpi opinnäytetyöni vaiheet.

2.1 Opinnäytetyön tavoite ja tutkimusongelmat

Tutkimuksellisen kehittämistyön lähtökohtana voi olla monia tarpeita kuten organisaation kehittämistarve tai halu muuttaa toimintatapaa. Tästä seuraa, että tutkimukselliseen kehittämistyöhön olennaisena osana sisältyy käytännön ongelmien ratkaisua, uusien

ajatusten ja käytänteiden luomista ja toteuttamista. Ominaista kehittämistyön päämäärille on kartoittaminen, kehittäminen ja ratkaisujen käyttöön ottaminen. (Ojasalo ym. 2009, 19.)

Opinnäytetyöni keskittyy sähköisen allekirjoituksen käyttöönoton toteutettavuuteen tulevassa Kymenlaakson ammattikorkeakoulun ja Mikkelin ammattikorkeakoulun fuusion myötä 1.1.2017 toiminnan aloittavassa Kaakkois-Suomen ammattikorkeakoulussa. Kymenlaakson Ammattikorkeakoulu Oy:n 2.6.2014 vuosille 2014–2016 hyväksymän strategian toimintalinjauksissa keskeisinä asioina ovat hyvät tieto- ja viestintäteknologiset valmiudet ja sähköisen asioinnin hyödyntäminen (Kyamk, 2014.) Digitaalisuus on vahvasti esillä myös jo Mikkelin Ammattikorkeakoulu Oy:n hallituksen 3.6.2013 hyväksymässä MAMK 2017 -strategiassa. (Mamk, 2013.)

Sähköisen arkistoinnin ja digipalvelujen yhtenä toimintalinjana on sähköisen tiedonhallinnan ja arkistoinnin kehittäminen. Xamkin hallituksen 23.9.2015 hyväksymässä Xamkin strategia 2022 ja visio vuoteen 2030, digitaalisen tiedonhallinta on nostettu yhdeksi digitaalisen talouden osaamisen kärjeksi. (Xamk, 2015.) Strategisistakin näkökohdista katsottuna digitaalinen tiedonhallinnan ja samalla sähköisen allekirjoituksen käyttöön ottaminen mahdollisimman monissa toiminnoissa, ja käyttöön oton edellyttämien asioiden selvittäminen on hyvinkin ajankohtaista. Tavoitteenani on tuottaa tietoa konkreettisen suunnittelun ja päätöksenteon tueksi.

Opinnäytetyöni tavoitteita ja tutkimusongelmia kuvaan kysymyksenasettelun kautta, joka koostuu yhdestä pääkysymyksestä ja sitä avaavista alakysymyksistä. Pääkysymys ja alakysymykset ovat taulukossa 1.

TAULUKKO 1. Opinnäytetyön kysymyksenasettelu

Pääkysymys
• Millä tavalla sähköinen allekirjoitus voidaan toteuttaa Xamkissa?
Alakysymykset
• Mikä on sähköinen allekirjoitus ja sen lainsäädännöllinen status? • Mitkä ovat yleiset perusteet sähköisen allekirjoituksen käyttöönottoon? • Mikä on sähköisen allekirjoituksen käyttöönoton tilanne tällä hetkellä kansallisesti ja kansainvälisesti? • Mitkä ovat oman organisaationi tekniset ja toiminnalliset valmiudet sähköisen allekirjoituksen käyttöönottoon? • Millaisia käytännön askeleita tarvitaan sähköisen allekirjoituksen käyttöönottoon? • Mitkä ovat kriittiset kohdat sähköisen allekirjoituksen käyttöönotossa Xamkissa?

Toteutettavuusselvitys määrittää kysymyksenasettelun rakenteen. Pää- ja alakysymyksien avulla tavoitteena on tuottaa konkreettisia tuloksia sähköisen allekirjoittamisen käyttöönotolle. Kysymysten asettelun kautta selvitetään myös toteutettavuuteen vaikuttavia taustatekijöitä.

Opinnäytetyöni on toteutettavuusselvitys. Pääpaino on siis soveltavassa tutkimuksessa, ja ei niinkään sähköisen allekirjoituksen teknisissä tai teoreettisissa kysymyksissä. Toki niidenkin pohdintaa sisältyy tähän tutkimukseen. Liitteessä 1 olevan peruskäsitteistön olen auki kirjoittanut tämän tutkimuksen tarkoitusperiä varten. Lisäksi työni rajautuu tutkimuskyselyn kautta organisaation johtamiseen ja tukipalveluihin. Tutkimuksen ulkopuolelle jää tässä yhteydessä varsinainen opetustoiminta.

2.2 Tutkimus- ja aineistonkeruumenetelmät

Opinnäytetyöni tutkimusote on konstruktiivinen. Ojasalon ym. (2009, 68) mukaan konstruktiivisessa tutkimuksessa voidaan käyttää hyvin monenlaisia menetelmiä, koska tavoitteena on saada yritykseen tai organisaatioon jotain uutta. Menetelmistä tyypillisimpiä ovat kysely ja haastattelu, joiden lisäksi kehittämistyössä oleellista on tuntea tulevien käyttäjien tarpeet.

Ojasalo ym. (2009, 66) toteaa, että ”konstruktiivinen tutkimus soveltuu hyvin lähestymistavaksi kun tehtävänä on luoda konkreettinen tuotos, esimerkiksi uusi tuote, järjestelmä, malli tai suunnitelma”. Tutkimuksen tuotoksena saadaan merkityksellinen ja käytännössä hyödynnettävä rakenne toimintatavan kehittämiselle. Kysymyksessä on siis lähestymistapa, jossa pyrkimyksenä ja tavoitteena on muuttaa organisaation toimintaa ja käytänteitä. Konstruktiivinen tutkimus sopii verrattomasti silloin, kun ongelmanratkaisun tueksi on oltava erityisen vahvasti myös teoreettista tietoa. Ojasalo ym. (2009, 66) mukaan on tärkeää, että toimeksiantaja sitoutuu kehittämistyöhön. Toimeksiantajan sitoutuminen kehittämiseen on merkittävä tekijä työn onnistumisen ja kehittämistyöhön osallistuvien työmotivaation kannalta.

Tässä toteutettavuusselvityksessä käytän aineistonkeruumenetelmänä kyselytutkimusta. Kyselytutkimuksella pyrin toisaalta kuvaamaan Xamkin sähköisen allekirjoituksen valmiuksia, ja toisaalta tunnistamaan mahdollisia kriittisiä alueita sähköisen allekirjoituksen käyttöönotossa. Lisäksi referoin ja analysoin aihealueeseen liittyvää tutkimustietoa ja haastattelen asiantuntijoita sekä omasta organisaatiostani että ulkopuolelta. Sovellan analysointiin loogisen viitekehyksen (eng. Logical Framework Approach) lähestymistapaa analyysikehikon avulla. Se mahdollistaa kerätyn tiedon pohjalta käytännönläheisen ja toteuttamisaskeleisiin ohjaavan toteutettavuusraportoinnin. Tällä tavoin tutkimuksen pohjalta syntyy jo kehys varsinaiselle käyttöönottoprojektille.

Tähän toteutettavuusselvitykseen loogisen viitekehyksen analyysikehikko sopii sen vuoksi erityisen hyvin, että se tarjoaa mahdollisuuden yhdistää tilanneanalyysin suunnitteluvaiheeseen. Näin toteutettavuusselvitys voidaan hyödyntää suoraan toteutussuunnitelman pohjaksi. Lähestymistapa myös korostetusti nostaa esiin toteutettavuuden kannalta kriittiset kohdat, jolloin toteutettavuutta voidaan arvioida realistisesti riski- ja tuotosanalyysein.

Loogisen viitekehyksen lähestymistapa tutkimuksessani tiivistyy seuraaviin kysymyksiin:

- mitä halutaan saada aikaan?
- mitä toimintoja tarvitaan, jotta nämä tavoitteet voidaan saavuttaa?
- mitä resursseja tarvitaan tavoitteiden saavuttamiseen?
- mitkä ovat kriittiset kohdat?
- miten edistymistä mitataan?

Asioiden ennakointi ja kysymysten asettaminen ovat ehdottomasti niitä avainasioita, jotka mahdollistavat käytännön toteutuksen onnistumista parhaalla mahdollisella tavalla.

2.3 Aineistonkeruu ja raportointi

Tutkimukseen kertyi aineistoa hyvin runsaasti. Kirjallisuusaineistoa oli saatavilla hyvin, toteutettu kyselytutkimus tuotti myös rikkaan aineiston ja erityiskysymyksiin sain tarkennuksia asiantuntijahaastatteluilla. Tutkimusaineiston keruun aloitin korkeakoulu- ja yliopistokirjastojen tietokannoista ja käytin hyväkseni alan perusteosten lähdeviitteitä. Pyrin kokoamaan materiaalia Suomen lisäksi myös kansainvälisesti – lähinnä englannin ja saksan kielellä.

Kyselyn toteutin syys–lokakuussa 2015. Sen kohderyhmänä olivat Xamkin toimiva johto, luottamushenkilöt ja tukipalvelujen esimiehet sekä fuusioituvien yritysten, Mikkelin ammattikorkeakoulun ja Kymenlaakson ammattikorkeakoulun johto, esimiehet ja luottamushenkilöt. Kysely toteutettiin Webropol -verkkotyökalun avulla. Kysely koostui viidestätoista (15) monivalintakysymyksestä. Osaan kysymyksistä oli mahdollista valita useampi vastausvaihtoehto. Vastausprosentti oli hyvä ja tutkimusaineistoa kertyi uskottava määrä päätelmien tekoa varten.

Haastattelin tutkimusvaiheen aikana useita asiantuntijoita. Asiantuntijoilla testasin tiettyjä tutkimusolettamia (lähinnä sähköisen allekirjoituksen käyttöönoton kriittisiä kohtia) ja hain kokemusperäistä tietoa onnistuneista sähköisen allekirjoituksen soveltamistapauksista. Tutkimukseni lopputuloksena on toteutettavuusraportti. Se on konkreettinen toimintasuunnitelma pohjautuen loogisen viitekehyksen lähestymistapaan.

2.4 Opinnäytetyöprosessi

Kehittämistehtävän lopullinen toimeksianto allekirjoitettiin maaliskuussa 2015. Jo keväällä 2012 tutkimus- ja tiedonhankintaopintojakson aikana opinnäytetyöni aihealue, sähköinen allekirjoitus, hahmottui mielessäni, mutta tutkimuksen kohde oli tuolloin vielä hämärän peitossa. Tutkimusprosessi käynnistyi kuitenkin 8.9.2012, jolloin esittelin tutkimusteeman ensi kertaa suunnitelmaseminaarissa. Tutkimusteema, josta lähdin

liikkeelle, oli ”Sähköisen allekirjoituksen vaikutukset pöytäkirjojen tarkastuskäytänteisiin.” Seminaaripalaute rohkaisi työn jatkamiseen. Monista eri syistä johtuen opinnäytetyöni tekeminen pysähtyi suunnitelmaseminaarin jälkeen kokonaan pitkäksi ajaksi. Aihe oli tauon jälkeen entistä ajankohtaisempi eikä ollut menettänyt merkitystään. Tartuin aiheeseen uudelleen elokuussa 2014, jolloin tarkensin aiheeksi ”Kaakkois-Suomen Ammattikorkeakoulu Oy:n toimielinten pöytäkirjojen allekirjoitus sähköisesti: toteutettavuusselvitys.” Laadin viitekehyksen (taulukko 2), jonka mukaisesti päätin lähteä etenemään.

TAULUKKO 2. Opinnäytetyön viitekehys

1	Asianhallintajärjestelmän toiminnallisuus sähköisen allekirjoituksen mahdollistamisessa teknisesti ja tosiasiallisesti – kirjallisuus, haastattelu
2	Lainsäädännöllinen viitekehys – kirjallisuus • EU lainsäädäntö • kansallinen lainsäädäntö
3	Kirjallinen viitekehys • sähköinen allekirjoitus • sähköinen asiointi • sähköinen tunnistaminen
4	Käyttäjien valmiudet – kysely/haastattelututkimus • lomakekysely ja syventävät haastattelut • toimielinedustajat
5	Kokemukset muualta (Suomi, Eurooppa) – case-tutkimukset
6	Näiden pohjalta selvitetään, onko sähköisen allekirjoituksen käyttöönotto ko. käyttötilanteessa mahdollinen ja mitä toimenpiteitä se vaatisi? • kustannusvaikutukset (suorat ja välilliset)

Tämän jälkeen vielä kerran tarkistin tutkimuksen suuntaa ja tutkimussisältöä, ja pelkästään pöytäkirjojen allekirjoittamiseen kohdistuva tutkimus jäi pois. Viitekehyksen rakentamisen ja tutkimussisällön tarkennuttua tutkimuksen työnimeksi muotoutui SÄHKÖISEN ALLEKIRJOITUKSEN TOTEUTTAVUUSSELVITYS -case Kaak-

kois-Suomen Ammattikorkeakoulu Oy. Alustavien tutkimusongelmien määrittelyn jälkeen prosessi jatkui kirjallisuusaineiston keruulla. Näiden pohjalta tutkimus lopulta alkoi hahmottua, jonka jälkeen siirryin varsinaiseen tutkimusprosessiin.

Varsinainen tutkimusprosessini jakautui kolmeen vaiheeseen, joista ensimmäinen vaihe oli tutkimussuunnitelman täsmentäminen, kirjallisuusanalyysi ja käsitteistön määrittely. Toisessa tutkimusprosessin vaiheessa laadin ja toteutin kyselytutkimuksen. Kolmannessa vaiheessa purin kyselyn vastausaineiston taulukoiksi ja samaan vaiheeseen sisältyi myös analyysikehikon soveltaminen.

3 SÄHKÖINEN TUNNISTAMINEN JA ALLEKIRJOITUS

Sähköistä allekirjoitusta ja tunnistamista vien tässä tutkimuksessa eteenpäin kiinteänä käsiteparina. Pääpainoni on allekirjoituksen tarkoituksessa ja lainvoimaisuudessa, ei niinkään teknisessä toteutuksessa. Tosin tekninen toteutus on kiinteä osa sähköistä allekirjoitusta, mutta oma asiantuntemukseni ja mielenkiintoni on enemmän tekniikan soveltamisen puolella.

Englannin kielessä on käytössä käsitepari *digital signature* ja *electronic signature*, joista jälkimmäinen on nimenomaan lainsäädännön määrittelemä sähköinen allekirjoitus ja ensimmäinen tekninen allekirjoitustoimenpide. Tässä tutkimuksessa sähköisellä allekirjoituksella viitataan termiin *electronic signature*. Sähköisen tunnistamisen ja allekirjoituksen käsitteitä määrittelen tässä tutkimuksessa eurooppalaisen ja suomalaisen lainsäädännöllisen viitekehyksen mukaan. (Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista 7.8.2009/617, 5 §.)

3.1 Tunnistaminen

Tunnistamisella tässä tutkimuksessa tarkoitetaan juridisen henkilön yksilöimistä ja tunnisteen aitouden ja oikeellisuuden tunnistamista sähköistä menetelmää käyttämällä. Voutilaisen (2009, 244) mukaan sähköisen tunnistus suoritetaan tavalla, jolla palvelua käyttävä henkilö saadaan yksilöidyksi. Tunnistuksen yhteydessä tapahtuu myös henkilön todentaminen tietyksi henkilöksi. Todentaminen on menettely, jolla vastapuolelle varmistetaan tunnistuksessa esitettyjen tietojen paikkansa pitävyys.

Voutilainen (2009, 244–245) toteaa, että tunnistus voi tapahtua joko passiivisesti tai aktiivisesti. Passiiviseksi tunnistusta kutsutaan siinä tapauksessa, että tunnistus tapahtuu vertaamalla henkilön lomakkeella itsestään antamia tietoja esimerkiksi operatiivisista järjestelmistä saataviin tietoihin. Voutilainen (2009, 245) jatkaa toteamalla, että aktiivinen tunnistus tapahtuu siten, että tunnistus ja todennus toteutetaan yhtäaikaisesti useassa välineessä. Sähköisessä toimintaympäristössä tunnistus tapahtuu henkilön hallussa olevan tunnisteen avulla ja todentaminen muun muassa henkilön tiedossa olevan salasanan avulla. Käytössä olevia tunnistusmenetelmiä ovat

- käyttäjätunnukseen ja salasanaan perustuva tunnistus
- käyttäjätunnukseen ja salasanaan sekä avainlukulistaan tai aikaperusteiseen salasanaan pohjautuva tunnistus
- biometrinen tunnistus
- PKI -pohjainen tunnistus (Public Key Infrastructure).

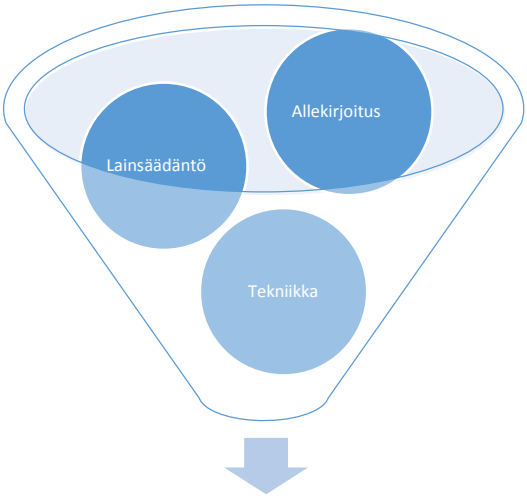
Aktiivinen tunnistus jakautuu edelleen kevyisiin ja vahvoihin tunnistusmenetelmiin. Näistä tunnistusmuodoista kevyt sähköinen tunnistaminen on käyttäjätunnukseen ja salasanaan perustuva, ilman varmennetta tai erillistä tunnistusvälinettä tapahtuva tunnistus ja todennus. (Voutilainen 2009, 245.) Vahvalla sähköisellä tunnistamisella tässä tutkimuksessa tarkoitetaan tunnistamista, joka perustuu

- salasanaan tai johonkin muuhun sellaiseen, minkä tunnistusvälineen haltija tietää
- sirukorttiin tai johonkin muuhun sellaiseen, mikä tunnistusvälineen haltijalla on hallussaan tai
- sormenjälkeen tai johonkin muuhun tunnistusvälineen haltijan yksilöivään ominaisuuteen.

Vahvan sähköisen tunnistamisen on perustuttava vähintään kahteen edellä luetelluista kolmesta vaihtoehdosta. (Laki vahvasta tunnistamisesta ja sähköisistä allekirjoituksista, 617/2009, 2 §.)

3.2 Sähköinen allekirjoitus

Sähköistä allekirjoitusta lähestyn suodattavan analyysikehikon (kuva 1) lävitse. Analyysikehikko tai analyyttinen kehys, joksi sitä englannin kielessä kutsutaan, auttaa tutkimusongelmien tarkastelua ja arviointia. (Analytic frame, Wikipedia, 2015.) Lähtökohtana on ollut omakätisen allekirjoituksen eri tarkoitusten, funktioiden määrittely. Näiden funktioiden täyttymistä sähköisissä allekirjoituksissa varmistetaan sekä lainsäädännön että teknisen kehittämisen kautta. Nykytilannetta ja kehittämisympäristöä kuvataan näiden parametrien avulla. Eli pelkistetysti nykytilan arviointini tarkoittaa sähköisen allekirjoituksen toteuttamisen lainsäädännöllisten ja teknisten valmiuksien arviointia ja niiden kykyä toteuttaa allekirjoituksen funktiota Xamkissa.



KUVA 1. Sähköisen allekirjoituksen analyysikehikko

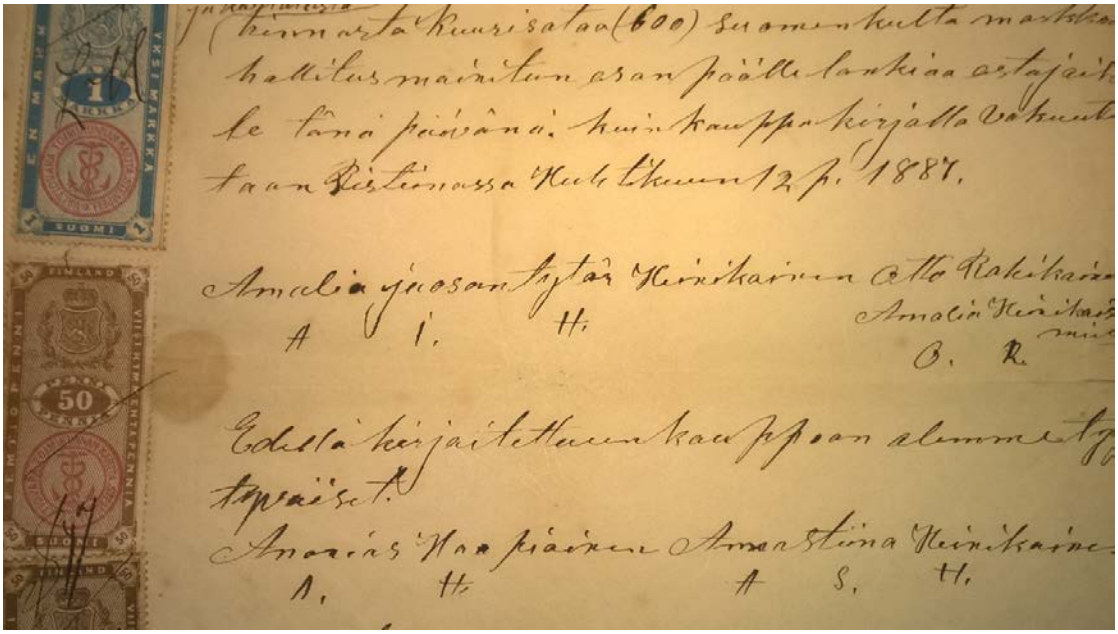
Sähköisellä allekirjoituksella tarkoitetaan tässä tutkimuksessa sähköiseen materiaaliin liitettyä dataa, jolla voidaan todentaa allekirjoittaja (identiteetti) ja allekirjoitettavan aineiston muuttumattomuus (integriteetti).

3.3 Allekirjoituksen tarkoitus ja tehtävät

Allekirjoituksesta todetaan että ”Allekirjoitus eli nimikirjoitus tai autografi on nimen kirjoitettu asu tai muu tunnistusmerkki, jonka henkilö kirjoittaa asiakirjaan todisteeksi henkilöllisyydestä ja tahdosta. Henkilökohtaiseen allekirjoitukseen käytetään yleensä omaa nimeä tai sen lyhennettä. Se toimii sinetin tavoin. Suomen kielessä nimikirjoitus

tarkoittaa jonkin henkilön nimeä hänen itsensä käsin kirjoittamana.” (Allekirjoitus. Wikipedia, 2015.)

Allekirjoittamista voidaan tarkastella monesta eri näkökulmasta ja merkityksestä. Tässä tutkimuksessa pääpaino on allekirjoituksen eri merkityksissä. Allekirjoitustapahtuma sinänsä voi olla arkinen, melkein huomaamaton, mutta joskus myös hyvin juhlallinen tapahtuma. Ennen kuin kirjoitustaito Suomessa yleistyi, käytettiin esim. sopimusten allekirjoituksena nimikirjoituksen sijasta puumerkkiä. Se koostui yleensä suorista kynällä tehdyistä piirroista, jotka voitiin helposti merkitä paperille. Kuvassa 2 oleva allekirjoitus on esimerkki oman sukuni asiakirjoista 1800-luvulta.



KUVA 2. Esimerkki allekirjoituksesta vuodelta 1887 (Haapiainen)

Allekirjoituksella tässä tutkimuksessa tarkoitetaan asiakirjaan liitettyä juridisen henkilön omakätistä nimikirjoitusta, jonka vain kyseinen henkilö on voinut tuottaa, osoituksena siitä, että teksti vastaa hänen tahtoaan.

Julkisoikeuden professori Tomi Voutilainen toteaa väitöskirjatutkimuksessaan ”ICT-oikeus sähköisessä hallinnossa - ICT oikeudelliset periaatteet ja sähköinen hallintomenettely” seuraavaa: ”Allekirjoituksen tarkoituksena on asiakirjan laatijan tai sopimusosapuolen tunnistaminen, jolla tarkoitetaan allekirjoittajan henkilöllisyyden varmistamista.” (Voutilainen 2009, 255.) Tällöin allekirjoituksella voidaan sanoa olevan tunnistusmerkitys.

Todennustarkoituksen allekirjoitus saa silloin kun tiedon alkuperä voidaan varmuudella todentaa tiettyyn henkilöön, joka on luonut tai lähettänyt tiedon. Edellä mainitun tarkoituksen perusteella allekirjoitus toimii viestinnällisessä merkityksessä, ja viestii asiakirjaa käsittelevälle siitä, kuka asiakirjan on laatinut tai hyväksynyt. Allekirjoituksen tehtävänä on osoittaa myös tietyn henkilön tahdon ilmaiseminen. Tämä tarkoittaa, että jälkikäteen asiakirjassa oleva tahdonilmaus tai toimi, esim. hyväksyntä, viranomaisen kannanotto tai päätös voidaan todentaa ja yhdistää kulloinkin kyseessä olevaan henkilöön. (Voutilainen 2009, 255.)

Todistemerkityksessä allekirjoitus on esimerkiksi oikeustoimitilanteissa tai lähetetyn asiakirjan todisteena, jos toinen osapuoli kiistää tapahtuman myöhemmässä vaiheessa. Allekirjoituksella asiakirja suljetaan, niin ettei siihen voida tehdä muutoksia muutoin kuin erikseen säädetyllä menettelyllä. Allekirjoituksella on erityisesti julkisen hallinnon päätöksenteossa julkisuusmerkitys, kun joudutaan arvioimaan asiakirjan julkisutta. Asianosaisten oikeuksiin tai niiden arviointiin voi allekirjoituksen ajankohdalla olla vaikutuksia. Tällöin puhutaan allekirjoituksen oikeusmerkityksestä. Yhtenä allekirjoituksen tehtävänä on vastuu, mikä tarkoittaa, että allekirjoituksella osoitetaan päätöksenteossa vastuussa olevat henkilöt. (Voutilainen 2009, 256.)

Voutilaisen mukaan (2009) allekirjoitus saa aikaan oletuksen asiakirjan laatijasta tai oikeustoimen tekijöistä, mutta se ei varmuudella todista allekirjoittajaa tai pelkästään sen perusteella ei voida henkilöä yksiselitteisesti tunnistaa. Allekirjoittajasta voidaan saada varmuus vasta jälkikäteen suoritettavilla toimenpiteillä. Yleisinä vaatimuksina allekirjoitukselle voidaan asettaa seuraavia tekijöitä:

- Allekirjoituksella pitää olla yhteys asiakirjan tai oikeustoimen sisältöön.
- Allekirjoitus pitää pystyä todentamaan helposti.
- Allekirjoituksen todentamisen pitää olla mahdollista niin kauan kuin asiakirjalla on merkitystä oikeudelliselta kannalta.
- Allekirjoituksen väärentämisen pitää olla vaikeaa ja toisaalta väärän allekirjoituksen todentamisen tulee olla mahdollista.
- Allekirjoituksen ja siihen liittyvien määritteiden perusteella pitää pystyä yksilöimään allekirjoittajien henkilöllisyys.

Sähköisen allekirjoituksen pitää pystyä vastaamaan näihin yleisiin allekirjoituksen vaatimuksiin saadakseen lainvoimaisuuden.

3.4 Sähköisen allekirjoituksen historia

Sähköisen allekirjoituksen historia alkaa 1950-luvulla Yhdysvalloissa puolustushallinnossa. Ensimmäisiä siviilipuolen kehittyneempiä sähköisiä allekirjoitusmenetelmiä otettiin käyttöön 1970-luvun loppupuolella, nämä myös Yhdysvalloissa. (Pfitzmann, Birgit, 1996.) Sähköisen allekirjoituksen perusteknologia kehittyi jo viime vuosisadalla Yhdysvalloissa. Vuonna 1977 Rivest, Shamir ja Adleman kehittivät MIT-laboratoriossa RSA-kryptaysjärjestelmän. Se mahdollisti dokumenttien allekirjoituksen. Goldwasser tutkimustiimeineen kehitti vuonna 1984 GRM-allekirjoitusmenetelmän, joka teki allekirjoituksista vaikeammin väärennettäviä. Samana vuonna Taher Elgamal kehitti nimeään kantavan allekirjoitusmenetelmän, jota NSA kehitti eteenpäin ja julkaisi 1991 oman kehitysversionsa tästä. (Gasser, 2009)

Sähköisen allekirjoituksen yleistyminen alkoi kuitenkin vasta 1990-luvulla internetin palveluiden kehittymisen kautta. Laajamittaiseen käyttöön sähköinen allekirjoitus on kuitenkin tullut vasta ihan viime vuosina. Lainsäädäntöön sähköinen allekirjoitus tuli 1990-luvulla. Ensimmäinen eurooppalainen direktiivi aiheeseen liittyen julkaistiin 1999. (Euroopan Parlamentin ja neuvoston direktiivi 1999/93/EY.)

3.5 Sähköisen allekirjoituksen lainsäädännöllinen ja tekninen viitekehys

Sähköisen allekirjoituksen yleistymiseen on vaadittu puhtaan teknisen kehityksen lisäksi mittavaa lainsäädännöllistä kehitystyötä. Ilman tätä sähköisellä allekirjoituksella ei voisi olla lainvoimaisuutta. Tässä tutkimuksessa lainsäädännöllisen viitekehyksen ymmärtäminen on teknistä viitekehystä tärkeämpi, koska kyseessä on nimenomaan soveltava tutkimus.

3.5.1 Lainsäädännöllinen viitekehys

Lainsäädännöllinen viitekehys mahdollistaa sähköisen allekirjoituksen laajamittaisen käytön. Mm. sähköisestä asioinnista viranomaistoiminnassa annetun lain 13/2003 perusteella kaikki julkisen hallinnon päätösasiakirjat voidaan allekirjoittaa sähköisesti. Näin on ollut itse asiassa jo vuodesta 1999 alkaen, jolloin Suomessa tuli voimaan laki sähköisestä asioinnista hallinnossa (kumottu 24.1.2003/13.)

Voutilainen nimeää viisi sähköisen hallinnon oikeudellista perusperiaatetta, jotka hyvin vahvasti ovat lainsäädännöllisen viitekehyksen sisällä. Nämä perusperiaatteet ovat sähköisen muodon syrjimättömyys, käytettävyys ja saavutettavuus, tietoturvallisuus, yhteensopivuus, todennettavuus ja läpinäkyvyys. (Voutilainen, 2012.)

Sähköisistä allekirjoituksista annetussa laissa 617/2009 on määritelty kolmentyyppisiä sähköisen allekirjoituksen muotoja: sähköinen allekirjoitus, kehittynyt sähköinen allekirjoitus ja laatuvarmenteeseen perustuva allekirjoitus. Sähköisellä allekirjoituksella lainsäädännöllisesti tarkoitetaan sähköisessä muodossa olevaa tietoa, joka on liitetty tai joka loogisesti liittyy muuhun sähköiseen tietoon ja jota käytetään allekirjoittajan henkilöllisyyden todentamisen välineenä. (Laki vahvasta sähköisestä tunnistamisesta ja allekirjoituksista, 2009/617, § 2, 9 k.)

Kehittyneellä sähköisellä allekirjoituksella lainsäädännöllisesti tarkoitetaan sähköistä allekirjoitusta,

- joka liittyy yksiselitteisesti sen allekirjoittajaan
- jolla voidaan yksilöidä allekirjoittaja
- joka on luotu menetelmällä, jonka allekirjoittaja voi pitää yksinomaisessa valvonnassaan
- ja joka on liitetty muuhun sähköiseen tietoon siten, että tiedon mahdolliset muutokset voidaan havaita. (Laki vahvasta sähköisestä tunnistamisesta ja allekirjoituksista, 2009/617, 2 § 10 k.)

Kolmas sähköisen allekirjoituksen muoto on laatuvarmenteeseen perustuva kehittynyt sähköinen allekirjoitus. Vahvasta sähköisestä tunnistamisesta ja allekirjoituksista annetussa laissa 2009/617, § 30 todetaan, että laatuvarmenteen tulee sisältää

- tieto siitä, että varmenne on laatuvarmenne

- tieto varmentajasta ja sen sijoittautumisvaltiosta
- allekirjoittajan nimi tai salanimi, josta ilmenee, että se on salanimi
- allekirjoituksen todentamistiedot, jotka vastaavat allekirjoittajan hallinnassa olevia allekirjoituksen luomistietoja
- laatuvarmenteen voimassaoloaika
- laatuvarmenteen yksilöivä tunnus
- varmentajan kehittynyt sähköinen allekirjoitus
- mahdolliset laatuvarmenteen käyttörajoitukset
- allekirjoittajaan liittyvät erityiset tiedot, jos ne ovat tarpeen laatuvarmenteen käyttötarkoituksen kannalta.

Tärkeä kannanotto sähköisen allekirjoitusten käyttöön julkishallinnossa on Valtion tilintarkastuslautakunnan kannanotto 1/2013. Siinä todetaan että tilintarkastajia velvoittava sääntely ei edellytä tilinpäätösmerkinnän ja tilintarkastuskertomuksen allekirjoittamista käsin. Kannanotossa kuitenkin todetaan, että sähköisessä allekirjoittamisessa on aiheellista noudattaa vahvaa sähköistä tunnistamista. (Valtion tilintarkastuslautakunta 2013, 1.)

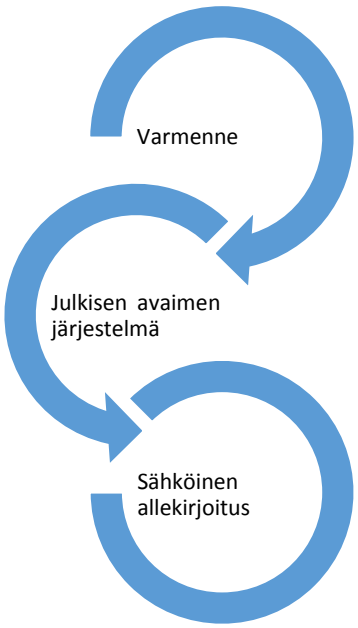
Sähköisen allekirjoituksen eurooppalainen lainsäädäntö on uusiutumassa. Vuoden 1999 sähköisen allekirjoituksen lainsäädäntö ollaan korvaamassa uudella eurooppalaisella asetuksella. Euroopan parlamentin ja neuvoston asetus (EU) N:o 910/2014, annettu 23 päivänä heinäkuuta 2014, sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta pyritään saattamaan lainvoimaiseksi EU:n laajuisesti heinäkuun alusta 2016. Lakimuutos vaikuttaa lähinnä tunnistus- ja varmennepalveluiden tuottajiin. Sähköistä allekirjoitusta uusi asetus tulee edistämään helpottamalla vahvan sähköisen tunnisteen luomista ja vähentämällä palveluntarjoajien luottamusverkostojen kautta tunnisteita.

3.5.2 Tekniset ratkaisut

Sähköisen allekirjoituksen yleistyneet tekniset ratkaisut pohjautuvat julkisen avaimen järjestelmään. Julkisen avaimen järjestelmällä tässä tutkimuksessa tarkoitetaan salausmenetelmää, jossa kullakin käyttäjällä on kaksi matemaattisesti toisiinsa liittyvää avainta: julkisessa hakemistossa julkaistava julkinen avain ja vain käyttäjän hallussa oleva yksityinen avain. Näistä avaimista syntyy ainutlaatuinen avainpari, joka teknisesti

yhdistetään allekirjoitettavaan materiaaliin. Matemaattisesti kyseessä on asymmetrinen kryptografinen laskutoimitus. (Digital Signature Standard 2013.)

Sähköinen allekirjoitus, johon tarvitaan varmenne, yhdistää allekirjoittajan identiteettitiedot julkiseen avaimeen (kuva 3). Sitä kautta tapahtuu henkilön tunnistaminen sekä allekirjoituksen todentaminen. Todentamisella tässä yhteydessä tarkoitetaan palvelun käyttäjän identiteetin ja allekirjoituksen aitouden varmistamista. Lainsäädännön edellyttämään sähköiseen allekirjoitukseen liittyy aina varmenne, jonka on tuottanut sertifioitu varmenteentuottaja (useimmiten Suomessa pankki).



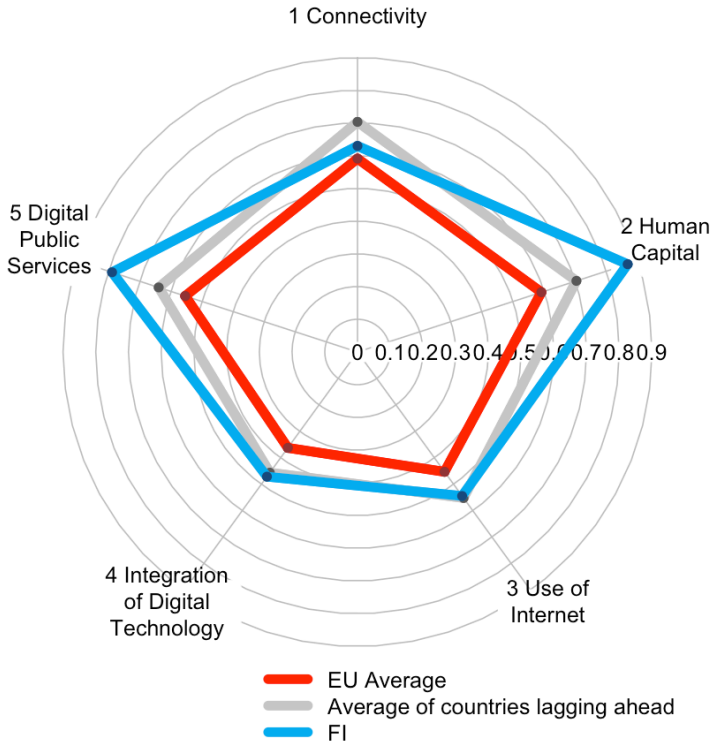
KUVA 3. Sähköisen allekirjoituksen tekninen toteutus

Erityistä huomiota sähköisen allekirjoitusten teknisissä ratkaisuissa olisi käytettävä allekirjoitusten arkistointiin. Tärkeää on allekirjoitusajankohdan tallentuminen todistettavasti, jotta vältetään jälkikäteen tehdyt väärennökset. Allekirjoitukset tapahtuvat aikaleimoilla, jotka vanhentuvat. Näin järjestelmiin on kehitettävä uusimismenetelmät. Lisäksi voimassaoleva lainsäädäntö mahdollistaa asianosaiselle oikeuden saada päätösasiakirjoista jäljennökset allekirjoitusvarmenteiden vanhenemisen jälkeen. (Laki sähköisestä asioinnista viranomaistoiminnassa, 2003/13, § 17.)

3.6 Sähköisen allekirjoituksen nykytilanne ja kehittämisympäristö

Sähköisen allekirjoitusten käyttöönoton mahdollistava lainsäädännöllinen viitekehys on olemassa ja tekniset valmiudet ovat hyvällä tasolla Suomessa. Siitä huolimatta käyttöönotto on verrattuna moniin kilpailijamaihin alhaisella tasolla. Tämä liittyy yleisemminkin sähköisten palveluiden hitaaseen käyttöönottoon maassamme. Suomessa tietoyhteiskuntakehitys on ollut enemmän tekniikka- kuin sisältövetoista. Tämä selittänee osittain nykytilannetta.

Vaikka Suomi ei ole ehkä enää tietoyhteiskuntakehityksen kärkimaita, niin EU:n laajuisessa vertailussa sijoitumme kuitenkin kärkipäähän (European Comission 2015). Ainoastaan yhteyksissä olemme kärkimaita selvästi jäljessä, joka selittyy hyvin pitkälle harvaanasutun maan haasteilla. (Kuva 4.)



KUVA 4. Suomen tietoyhteiskuntakehityksen tilanne (European Comission Digital Single Market)

Voutilainen (2015) toteaa yhdeksi sähköisen allekirjoituksen yleistymättömyyden syyksi sen, että Suomen hallintolaissa ei erityisesti määrätä sähköisen allekirjoituksen käytöstä.

Sähköisen allekirjoitusten käyttöönotto vaihtelee suuresti yhteiskunnan eri sektoreilla. Edistyneimmillään se on pankkisektorilla ja julkishallinnon puolella terveyspalveluissa sekä vero- ja lupahallinnossa. Koulutussektorilla sähköisen allekirjoituksen käyttö on vasta yleistymässä.

Viime vuosina kuitenkin sähköinen allekirjoitus on yleistynyt etenkin julkishallinnon palveluissa. Esimerkkinä voisi mainita verohallinnon yksityishenkilöille ja yrityksille tarjoamat palvelut. (www.vero.fi.) Tässä siirtymä paperisista veroilmoituksista sähköisiin on tapahtunut hyvin lyhyessä ajassa, muutamassa vuodessa. Toinen hyvä esimerkki on terveyspalveluiden sähköistyminen viime vuosina, uusimpana kansalaispalveluna sähköinen resepti. (www.kanta.fi.)

Sähköisten palveluiden kehittämistarve on yleisesti tunnustettu ja sitä tuetaan poliittisesti hyvin yksimielisesti. Nykyisen hallituksen hallitusohjelmaankin se on erityisenä painotuksena kirjattu. (Valtioneuvoston kanslia, 2015.) Tekniset järjestelmät ovat kehittyneitä ja lainsäädännöllinen viitekehys mahdollistaa sähköisten allekirjoitusten laajamittaisen käyttöönoton. Myös kokemukset allekirjoituspalveluiden käyttöönotosta ovat rohkaisevia. Kustannussäästöt ovat mittavia ja palveluiden luotettavuus ja laatu ovat kehittyneet.

Yksittäisen organisaation ottaessa käyttöön sähköistä allekirjoitusta seuraavia seikkoja tulee pohdittavaksi:

- missä organisaation prosesseissa tällä hetkellä tarvitaan omakätisiä allekirjoituksia?
- kuinka nämä käyttötilanteet voidaan sähköistää?
- mitä infrastruktuuriin, osaamiseen ja omaan sääntelyyn liittyviä toimenpiteitä tarvitaan käyttöönoton mahdollistamiseksi?
- mitkä ovat käyttäjätahojen valmiudet käyttöönottoon?
- mikä on saavutettava hyöty käyttöönotolla?

Voutilainen (2012, 33) tuo ”Julkisen hallinnon asiakirjahallinnon lainsäädännön ja toiminnan uudistaminen” -selvitystyössään esimerkkinä esille, että pöytäkirjojen julkisekasituloprosessia ja tarkastusmenettelyitä voitaisiin keventää ja tehostaa sekä toiminnallisesti että teknisesti ilman lainsäädännöllisiä uudistuksia. Voutilainen toteaa, että toimie-

limien kokouspöytäkirjojen hallintajärjestelmää käytettäessä käyttäjien yksilöimisen tulee olla yksiselitteinen ja luotettava. Tunnistus pitää tapahtua luotettavasti ja kokoushallintajärjestelmää käyttävillä henkilöillä on oltava tehtävänsä mukaiset käyttöoikeudet.

Pöytäkirjojen tarkastuksen jälkeen ei tule olla mahdollisuutta muuttaa pöytäkirjan tietoja ilman, että muutetusta tiedosta jää jälki kyseessä olevaan asiakirjaan. Asia on ratkaistavissa ainakin kehittyneellä sähköisellä allekirjoituksella, jonka ominaisuuksien perusteella asiakirjaan mahdollisesti tehdyt muutokset on havaittavissa. Pöytäkirjojen tarkastustoiminnassa voidaan käyttää myös muita käytettävissä olevia sähköisiä henkilön yksilöimisen ja todentamisen muotoja. Esimerkiksi verkkopankkitunnuksilla tunnistettu pöytäkirjan tarkastaja voi hyväksyä pöytäkirjan sisällön järjestelmän ohjaamalla menettelyllä. Pöytäkirjojen tarkastukseen riittää myös käyttäjätunnukseen ja salasanaan perustuva henkilön tunnistus. (Voutilainen, 2012, 33.)

4 TAPAUSTUTKIMUKSIA TOIMIVISTA JÄRJESTELMISTÄ

Tutkimuksen kuluessa törmäsin useisiin sähköisen allekirjoituksen käyttökokemuksiin, joista valitsin neljä lähempää tarkastelua varten. Näihin liittyen kirjallisen tutkimisen lisäksi suoritin asiantuntijahaastatteluita.

4.1 Itä-Savon sairaanhoitopiiri

Itä-Savon sairaanhoitopiirin kuntayhtymä tarjoaa terveydenhoitopalveluita n. 45 000 asiakkaalle. Jäsenkuntia ovat: Enonkoski, Kerimäki, Punkaharju, Rantasalmi, Savonlinna ja Sulkava. Erikoissairaanhoito, perusterveydenhoito ja sosiaalihuolto on koottu yhden katto-organisaation alle. Organisaatiossa työskentelee n. 2 500 henkilöä

Itä-Savon sairaanhoitopiirillä on käytössään sähköisiä palveluita potilaan hoidossa, henkilöstöhallinnassa ja dokumenttienhallinnassa. Aiemmin kaikkien sähköisten järjestelmien tuottamat asiakirjat jouduttiin tulostamaan ja allekirjoittamaan käsin sekä myös arkistoimaan paperikopioina.

Sähköiseksi allekirjoitusmenetelmäksi sairaanhoitopiirissä valittiin toimikorttipohjainen järjestelmä. Toimikortissa on Väestörekisterikeskuksen myöntämä laatuvarmenne ja näin sillä voidaan tehdä vahva sähköinen allekirjoitus. Sähköistä allekirjoitusta voidaan käyttää kaikissa organisaation käyttämissä sähköisissä järjestelmissä. Sähköisesti allekirjoitetut asiakirjat arkistoidaan kansallisten sähköisten arkistointivaatimusten mukaiseen arkistointiratkaisuun.

Sähköisen allekirjoitusten myötä toiminta tehostui ja syntyi mittavia kustannussäästöjä. Asiakirjoja ei tarvitse enää tulostaa ja kierrättää organisaation sisällä. Lisäksi arkistointi tapahtuu automaattisesti arkistointisovelluksen avulla. Myös tietoturvallisuus parani palvelun kautta ja palveluprosessit nopeutuivat huomattavasti. Esimerkiksi reseptien lähettäminen valtakunnalliseen Reseptikeskukseen tapahtuu alle kahdessa minuutissa. (Avain Technologies Oy 2012.)

Sairanen (2015) toteaa, että kyseessä oli laaja, jo vuonna 2010 aloitettu hanke, joka eteni vaiheittain: ensimmäisessä vaiheessa käyttöön otettiin asianhallintaratkaisu, toisessa vaiheessa kehitettiin dokumenttien hallintaa ja kolmas vaihe eteni arkistoratkaisun käyttöön ottoon. Sairanen sanoo, että sähköisen allekirjoituksen käyttöönottoa suunnittelevan organisaation tulee kiinnittää riittävästi resursseja suunnitteluun. Hän pitää erityisen tärkeänä dokumenttien hallinnan suunnittelua. Sähköisen allekirjoituksen käyttöönotto edesauttaa sähköiseen pitkäaikaissäilytykseen siirtymistä. Perinteiseen päätearkistoon ei sen jälkeen kerry aineistoa. Ratkaisun hankinta yhdeltä toimijalta niin pitkälle kuin se on mahdollista, toteaa Sairanen.

4.2 HAKA-luottamusverkosto

HAKA-luottamusverkosto on kansallinen yliopistojen ja korkeakoulujen yhteinen käyttäjätunnistusjärjestelmä. Siinä on mukana tällä hetkellä 49 jäsenorganisaatiota ja loppukäyttäjiä on lähes 300 000. Haka-loppukäyttäjät, joita ovat sekä opiskelijat että henkilöstö, voivat käyttää kotiorganisaationsa käyttäjätunnuksia kirjautuessaan eri HAKA-jäsenorganisaatioiden palveluihin. HAKA on yhteensopiva myös muiden pohjoismaiden korkeakoulujen luottamusverkostojen kanssa, joten käyttäjätunnuksilla pääsee kirjautumaan myös pohjoismaisiin palveluihin.

Kukin jäsenorganisaatio vastaa käyttäjätietojen ylläpidosta ja henkilöllisyyden todentamisesta. Luottamusverkostossa mukana olevien palveluiden käyttäjätiedot saadaan suoraan niiden kotiorganisaatioista. Palveluissa yksityisyys on suojattu ja tietoturvallisuus varmistettu. (CSC – Tieteen tietotekniikan keskus Oy, 2014.) Myös Xamk on jäsenenä Haka-luottamusverkostossa (Väisänen, 2016).

4.3 Digi-ID Virossa

Viro on tullut tunnetuksi rohkeasta tietoyhteiskuntastrategiastaan ja nopeasta sähköisten palveluiden käyttöönotostaan. Yksi näistä palveluista on sähköiseen tunnistautumiseen liittyvät henkilökortit. Näitä on tällä hetkellä käytössä kolme erilaista:

- sähköinen henkilökortti;
- digi-ID ja
- mobiili- ID. (Estonian “chapter zero” for MoReq2. Version 2.0, 2012)

Digi-ID ja sähköinen henkilökortti molemmat mahdollistavat sähköisen allekirjoituksen. Digi-ID on digitaalinen identiteettikortti, jonka avulla voi tunnistautua digitaalisesti ja allekirjoittaa asiakirjoja. Sitä ei voi käyttää henkilön tunnistamiseen muuten, koska se ei sisällä valokuvaa tai muuta fyysistä tunnistetta. Sähköinen henkilökortti, joka toimii myös matkustusasiakirjana EU:n sisällä, sisältää kaksi varmennetta. Toinen näistä luo sähköisen identiteetin ja toinen mahdollistaa sähköisen allekirjoituksen. (Estonian “chapter zero” for MoReq2. Version 2.0, 2012)

Yksi digitaalisen identiteetin tunnistautumismuoto Virossa on mobiili-ID – kortti. Sitä voidaan käyttää sähköiseen tunnistautumiseen ja allekirjoitukseen matkapuhelimella. Mobiili ID-kortti pitää kuitenkin ennen käyttöönottoa varmentaa sähköisellä henkilökortilla. Mobiili-ID on helppokäyttöinen, koska se ei vaadi erillisiä kortin lukijoita tai tietokoneohjelmistoja. (Estonian “chapter zero” for MoReq2. Version 2.0, 2012)

Virossa monissa julkisissa palveluissa sähköinen tunnistautuminen on ollut vuodesta 2011 alkaen pakollinen. Myös kaikissa tiedonhallintajärjestelmissä, joita käytetään Virossa, sähköisen henkilökortin ja digi-ID:n käytön täytyy olla mahdollista. (Estonian “chapter zero” for MoReq2. Version 2.0, 2012) Sähköisen ID-kortin käyttö sähköiseen allekirjoitukseen on yleistynyt Virossa hyvin nopeasti. Tilastoituja digitaalisia allekirjoituksia oli huhtikuun alussa 2016 jo lähes 280 miljoonaa kappaletta. (Digi-ID Viro, 2016)

4.3 RUBcard - Bochum

Bochumin Ruhr-Universität Saksassa on ottanut käyttöön henkilöstölle ja opiskelijoille sekä vierailijoille yhteisen sähköisen tunnistamisen ja allekirjoituksen palvelun. Palvelu perustuu sirulliseen RUBcard toimikorttiin. Palveluun on yhdistetty useita ennen hajallaan olleita palveluita kirjastopalveluista aina lähiliikenteeseen saakka. Yhtenäisellä opiskelijoiden ja henkilöstön toimikortilla on haluttu myös korostaa yliopiston yhteisöllisyyttä. Toimikortti mahdollistaa sähköisen allekirjoittamisen ja toimii myös lähimaksuvälineenä (prepaid -maksukortti esim. kampusravintolassa).

RUBcard toimii yliopistoyhteisössä myös henkilökorttina. Siinä on neljä perustoiminnallisuutta.

- kirjastokortti
- kampuspalvelut (opiskelijapalvelut, kampushallinto ym.)
- lähiliikennekortti
- lähimaksukortti

Bochumin yliopisto on ollut edelläkävijä toimikorttien käytössä. Ensimmäinen korttijärjestelmä otettiin käyttöön jo vuonna 1997. Ensimmäinen korttiversio oli ainoastaan opiskelijoiden käyttöön ja sillä pyrittiin yksinkertaistamaan opiskelijoiden joka lukukausi tapahtuvaa sisään kirjautumista yliopistoon. Yli 30 000 opiskelijaa kirjautuu kaksi kertaa vuodessa yliopiston kirjoille. Kirjautumismenettely rasitti sekä henkilökuntaa että opiskelijoita. Älykortti mahdollisti kirjautumisen itsepalvelupäätteillä joustavasti. Saavutettu kustannushyöty oli mittava ja rohkaisi korttisovelluksen jatkokehittämistä. Henkilökunnan laajamittaiseen käyttöön toimikortti tuli vuonna 2009, jolloin siihen jo sisältyi sähköisen allekirjoituksen ominaisuus. Viranhaltijapäätöksissä sähköinen allekirjoitus otettiin ensisijaiseksi allekirjoitustavaksi 2011. (Ruhr-Universität Bochum, 2015.)

5 TOIMEKSIANTAJAN ESITTELY JA NYKYTILANTEEN KUVAUS

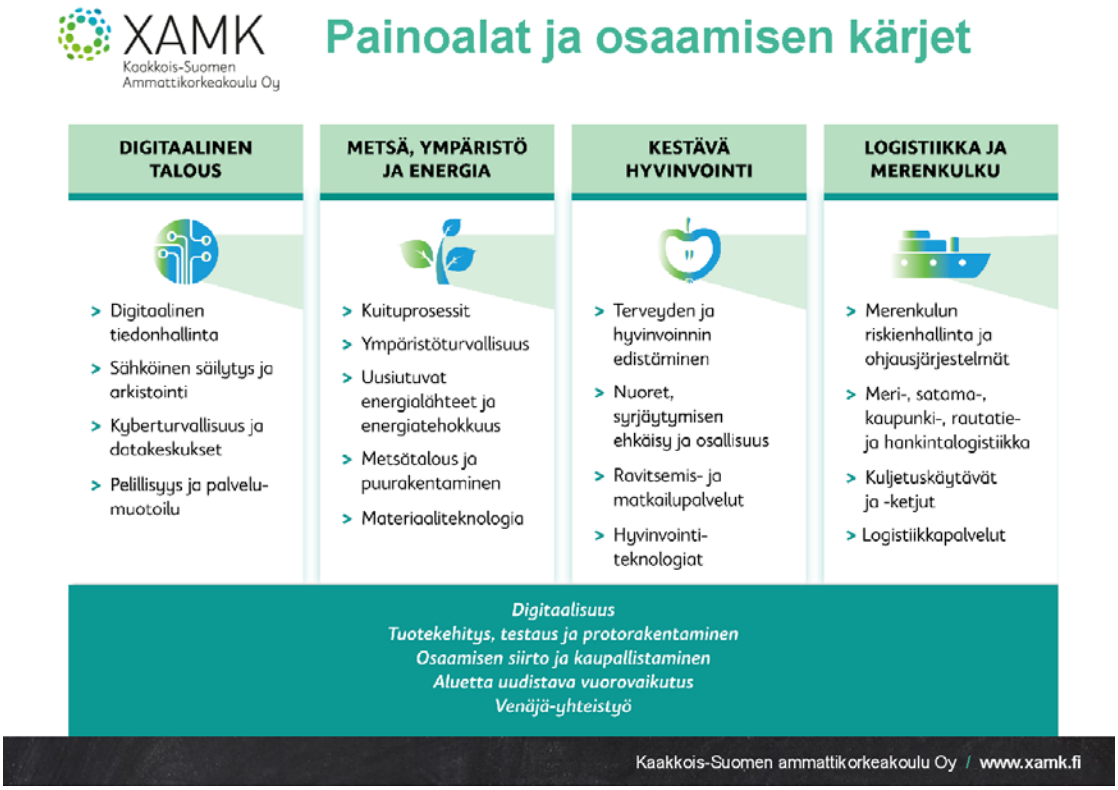
Kaakkois-Suomen Ammattikorkeakoulu Oy (Xamk) on Kymenlaakson ammattikorkeakoulun (Kyamk) ja Mikkelin ammattikorkeakoulun (Mamk) emoyhtiö. Kyamk ja Mamk toimivat tällä hetkellä erillisinä ja itsenäisinä oppilaitoksina, mutta yhdistyvät 1.1.2017 ja muodostavat Kaakkois-Suomen ammattikorkeakoulun, Xamkin. (Xamk 2016.)

5.1 Kaakkois-Suomen Ammattikorkeakoulu Oy (Xamk)

Kaakkois-Suomen Ammattikorkeakoulu Oy:n perustamissopimus allekirjoitettiin 24.1.2012. Sopimuksen myötä Suomeen syntyi ensimmäinen suomenkielinen yli maakunnallinen ammattikorkeakoulu (Mamk, 2012). Kymenlaakson ammattikorkeakoulun ja Mikkelin ammattikorkeakoulun välistä yhteistyötä kohti yhtä korkeakoulua on rakennettu vuodesta 2009. Kuvasta 5 voidaan nähdä Kyamkin ja Mamkin yhdentymisen polku.

KUVA 5. Yhdentymisen polku (Xamk, Kaakkois-Suomen Ammattikorkeakoulu Oy 2016)

Xamk Oy:n hallituksen 23.9.2015 hyväksymässä strategiassa todetaan, että ”digitaalisuus ei toistaiseksi ole lyönyt itseään läpi korkeakoulujen profiilitekijänä, mutta digitaalisuus kuuluu sekä Kymenlaakson että Etelä-Savon älykkään erikoistumisen kärkiin”. Kuvasta 6 voidaan todeta, että digitaalinen tiedonhallinta on yksi neljästä digitaalinen talous -painoalan osaamisen kärjistä.



KUVA 6. Xamkin painoalat ja osaamisen kärjet (Xamk, 2015)

Digitaalisen tiedonhallinnan kehittämisen tulee olla voimakkaasti esillä organisaation kaikilla osa-alueilla. Yhteiskunnan muutoksien aktiivinen seuraaminen, muutoksien ennakointi ja muutosketteryys ovat seikkoja, jotka toimivat myös digitaalisen tiedonhallinnan kehittämisessä. Digitaalisuus on Xamkin painoaloja läpäisevä periaate.

5.2 Nykytilanne

Xamkissa ollaan siirtymässä sähköiseen tiedonohjaukseen ja sähköiseen arkistointiin, mikä ensivaiheessa tarkoittaa asiakirjahallinnon kehittämistä. Vuoden 2015 aikana kilpailutettiin konsernin asianhallintajärjestelmä, jonka käyttöönotto alkaa vaiheittain vuoden 2016 aikana. Asianhallintajärjestelmän lisäksi hankintaan sisältyy tiedonohjausjärjestelmä sekä järjestelmä, joka mahdollistaa intran työtilojen integroinnin asianhallintaan. Xamkin tytäryhtiöissä Kymenlaakson Ammattikorkeakoulu Oy:ssä ja Mikkelin Ammattikorkeakoulu Oy:ssä on ollut käytössä eri asianhallintajärjestelmä. (Xamk. Ajankohtaista 2016.)

Xamk uudistaa fuusion myötä myös opetuksen suunnittelun, hallinnon ja opintoasiainhallinnon toimintoja. Uudistustyötä vauhdittaa liittyminen PEPPI-konsortioon. Konsortiossa on mukana Xamkin lisäksi 12 ammattikorkeakoulua ja muutamia yliopistoja sekä 7 yritysjäsentä. Konsortioon liittyminen ja Peppi-järjestelmäkokonaisuuden käyttöönotto on Kaakkois-Suomen ammattikorkeakoulun strategiaa tukeva ratkaisu. Uusi järjestelmäkokonaisuus tulee tarjoamaan opiskelijoille ja henkilökunnalle monipuolisia sähköisiä palveluja. Uudesta järjestelmästä löytyvät jatkossa esimerkiksi opetussuunnitelmat, opetustarjonta, työjärjestykset, opintosuoritusrekisterit ja opintoihin ilmoittautuminen. Kokonaisuus mahdollistaa useista vanhoista erillisistä järjestelmistä luopumisen ja organisaatio voi tehostaa toimintojaan edellä mainituilla osa-alueilla.
(Xamk. Ajankohtaista 2016.)

Allekirjoitusmenettelyssä toimitaan vielä perinteiseen tapaan. Väisänen (2016) sanoo, että Xamkissa käytössä oleviin henkilöstö- ja taloushallinnon järjestelmiin tunnistaminen ja kirjautuminen tapahtuu järjestelmän omaan palveluun. Tunnistamista ei ole synkronoitu AD:n (Active Directory) käyttäjätietokantaan. Palvelun kautta tulevan käyttäjätunnuksen ja salasanan lisäksi järjestelmien käyttö edellyttää henkilön tehtävään perustuvia käyttöoikeuksia. Konsernin yhteisissä järjestelmissä AD on käytössä muun muassa verkko-oppimisympäristössä, työryhmäohjelmistossa (mm. sähköposti), pikaviestintäjärjestelmässä ja henkilöstön intranetissa.

5.3 Sähköisen allekirjoituksen tarve ja tarpeellisuus

Xamk toimii neljällä paikkakunnalla: Kotkassa, Kouvolassa, Mikkelissä ja Savonlinnassa. Jo pelkästään välimatkat edellyttävät toimintatapojen muutoksia, ja yksi tapa kehittää ja virtaviivaistaa toimintoja olisi sähköisen allekirjoituksen käyttöönottaminen. Yksi konkreettinen sähköisen allekirjoituksen soveltamiskohde on pöytäkirja, sen tarkistaminen ja allekirjoittaminen. Sähköisen allekirjoituksen valmiuksia kartoittavassa kyselytutkimuksessa tämän soveltamisalan sähköisen allekirjoituksen tarve nouseekin esille. Sähköisellä allekirjoituksen käyttöönottamisella voitaisiin osaltaan tehostaa asiakirjahallintaa. Asiakirjoja, kuten erilaisia organisaatiossa tehtäviä päätöksiä ei tarvitsisi tulostaa ja kierrättää allekirjoitettavaksi. Fuusion myötä tehtävien järjestelmäuudistusten ja strategiaa tukevien ratkaisujen avulla siirtyminen myös sähköiseen allekirjoitukseen tulisi olla Xamkin digitaalisen tiedonhallinnan kehittämisen kärjessä. Toki varmasti asiakirjoja allekirjoitetaan toisten osapuolien kanssa vielä jatkossakin käsin,

mutta oman organisaation sisällä ja organisaatiosta lähtevät asiakirjat voitaisiin allekirjoittaa sähköisesti.

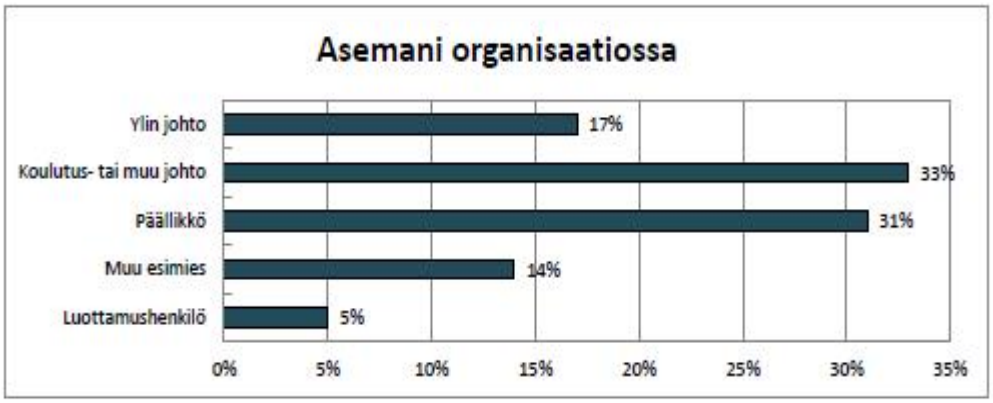
6 VALMIUDET SÄHKÖISEN ALLEKIRJOITUKSEN KÄYTTÖÖNOTOLLE

Sähköisen allekirjoituksen valmiuksia kartoitettiin kyselytutkimuksella. Kyselyn saatekirjeessä (liite 2) kerrottiin vastaajille kyselyn tarkoituksesta. Kyselytutkimus pohjautui kirjalliseen taustamateriaaliin ja valmisteltiin yhdessä organisaation asiantuntijoiden kanssa. Kyselyn tavoitteena oli selvittää sähköisen allekirjoituksen käyttöönoton valmiuksia potentiaalisessa käyttäjäryhmässä. Kysymyksillä kartoitettiin yleisiä tietoteknisiä valmiuksia, verkkoinfrastruktuuria, sähköisen allekirjoituksen tunnettuisuutta ja käyttöönottovalmiuksia. Kysely kohdistui nimenomaan Kaakkois-Suomen ammattikorkeakoulun organisaatioon ja sen tuloksilla ei haeta laajempaa soveltamisalaa.

Kysely toteutettiin Webropol-verkkotyökalun avulla. Liitteenä 3 oleva kysely koostui 15 monivalintakysymyksestä. Osaan kysymyksistä oli mahdollista valita useampi vastausvaihtoehto. Kysely lähetettiin vastaajille syyskuun lopussa 2015 ja vastausaikaa oli yksi viikko. Kyselyn kohderyhmänä oli potentiaalinen sähköisen allekirjoituksen käyttäjäjoukko Kaakkois-Suomen ammattikorkeakoulussa. Kysely lähetettiin kaiken kaikkiaan 86 vastaanottajalle, seuraavista kohderyhmistä:

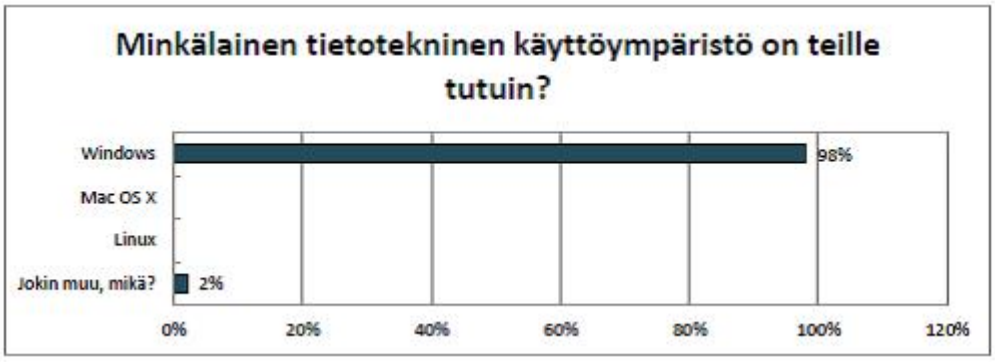
- luottamushenkilöt;
- ylin johto;
- koulutus- tai muu johto;
- päällikkö;
- muu esimies.

Kyselyyn vastasi lähes puolet vastaajista, 42 henkilöä. Kyselyyn vastanneiden jakauma kohderyhmittäin oli kuvassa 7 esitetyn jakauman mukainen.



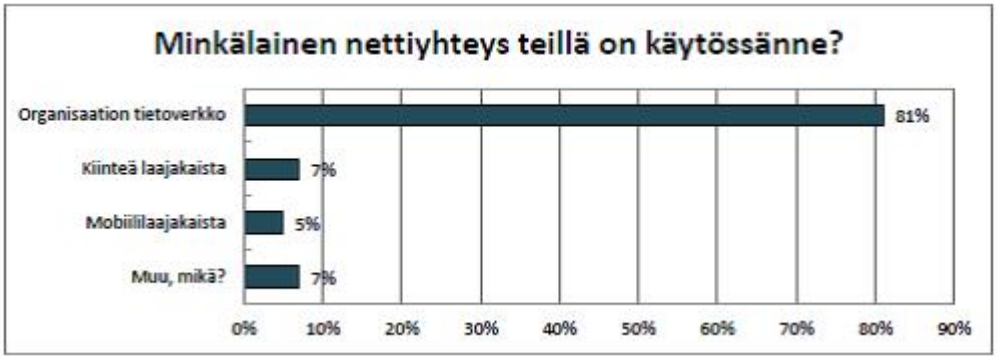
KUVA 7. Asemani organisaatiossa

Tietoteknisistä valmiuksista selviteltiin käyttöjärjestelmien ja nettiyhteyksien lisäksi tietoturvan ja verkkopalveluiden käyttöä. Kohderyhmän tietotekniset valmiudet ovat hyvällä tasolla. Kaikilla on tietokone ja nettiyhteys käytössään ja verkkopalveluiden käyttö on tuttua. Tietoteknisistä käyttöympäristöistä lähes kaikki käyttävät Windows-käyttöjärjestelmää (kuva 8).



KUVA 8. Tietotekninen käyttöympäristö

Kuvasta 9 voidaan nähdä, että lähes kaikilla kyselyyn vastanneilla on käytössään laaja-kaistatasoinen nettiyhteys, joko organisaationsa kautta tai yksityisesti.

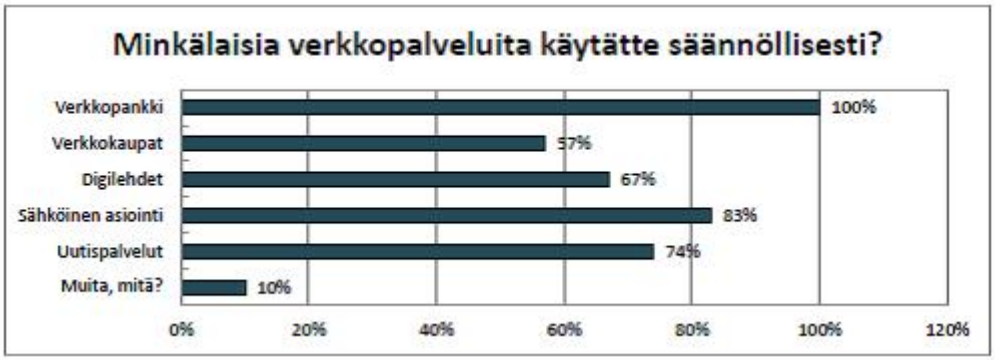


KUVA 9. Nettiyhteys

Kuva 10 havainnollistaa missä määrin tietoturvan suhteen vastaajat ovat valistuneita. Lähes kaikilla on käytössään palomuuri ja virustorjunta. Myös roskapostin käsittely on tuttua. Varmuuskopiointia harrastaa kuitenkin vain vajaa puolet vastaajista.

KUVA 10. Tietoturvaratkaisut

Kyselyyn vastanneet ovat aktiivisia verkkopalveluiden käyttäjiä (kuva 11). Kaikki käyttävät verkkopankkia ja sähköinen asiointi viranomaisten kanssa on tuttua suurimmalle osalle. Myös netin uutispalvelut ja digilehdet ovat tuttuja yli puolelle vastaajista.



KUVA 11. Verkkopalveluiden käyttö

Kyselyyn vastanneilla on jonkinlainen käsitys sähköisestä allekirjoituksesta (kuva 12) vaikkakaan eivät sitä käytännössä välttämättä tarvitsekaan. Useissa vastauksissa ihmeteltiinkin sitä, ettei sähköistä allekirjoitusta organisaatiossa vielä ole otettu laajemmin käyttöön. Sähköinen allekirjoitus oli käytännössä tuttu vain vähän yli kolmasosalle vastaajista.

KUVA 12. Sähköisen allekirjoituksen tunnettuus

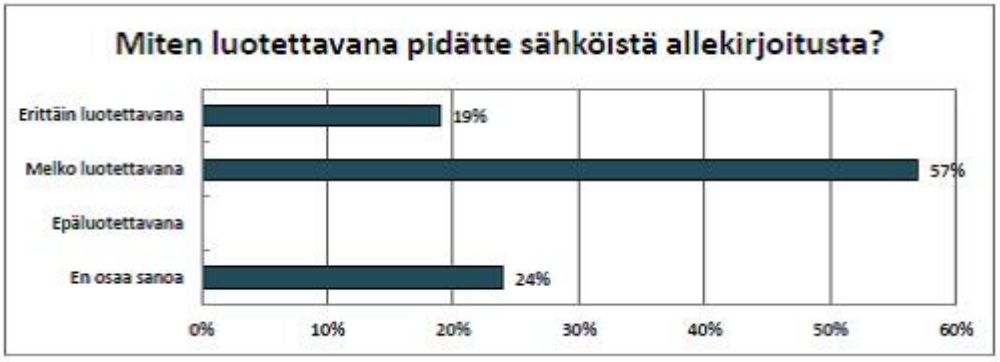
Verkkoasioinnissa käytettävistä tunnistamistavoista voidaan kuvasta 13 havaita, että kaikille oli tuttua käyttäjatunnuksen ja salasanan käyttö. Yli puolelle myös mobiilivarmenteen käyttö oli tuttua. Muista tunnistamistavoista kokemusta oli vain murto-osalla vastaajista.

KUVA 13. Verkkopalveluiden tunnistamistavat

Henkilökohtaisista varmenteista pankkitunnuksia olivat käyttäneet kaikki vastaajat. Kulunvalvontakorttia oli käyttänyt kolmasosa vastaajista. Sähköisen henkilökortin käyttö oli vähäistä (kuva 14).

KUVA 14. Henkilökohtaiset varmenteet

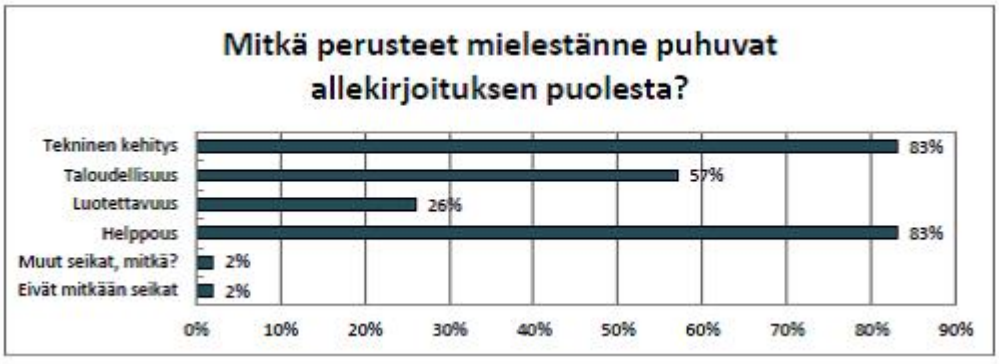
Sähköistä allekirjoitusta piti erittäin tai melko luotettavana 76 % vastaajista (kuva 15). Kukaan ei täysin kyseenalaistanut sähköisen allekirjoituksen luotettavuutta.



KUVA 15. Sähköisen allekirjoituksen luotettavuus

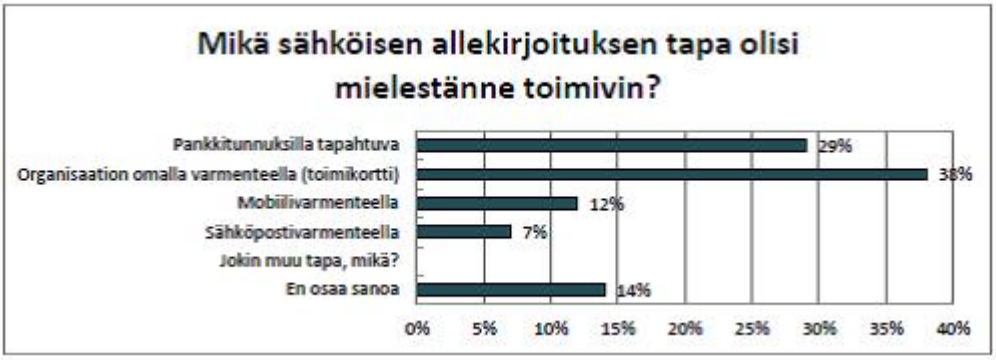
Kuva 16 osoittaa, että helppoutta ja teknistä kehitystä pidettiin merkittävimpinä seikkoina, jotka puhuvat sähköisen allekirjoituksen käyttöönoton puolesta. Myös taloudellisuutta piti merkittävänä reilusti yli puolet vastaajista.

Sähköisen allekirjoituksen toteutettavuudesta selvitettiin vastanneiden käsityksiä toimivista allekirjoituskäytännöistä, mahdollisista soveltamisalueista ja käyttöönoton tukipalveluiden tarpeesta. Suuri osa vastaajista toi tässä kysymysosiossa esiin myös tarpeen sähköisen allekirjoituksen mahdollisimman nopeasta käyttöönotosta.



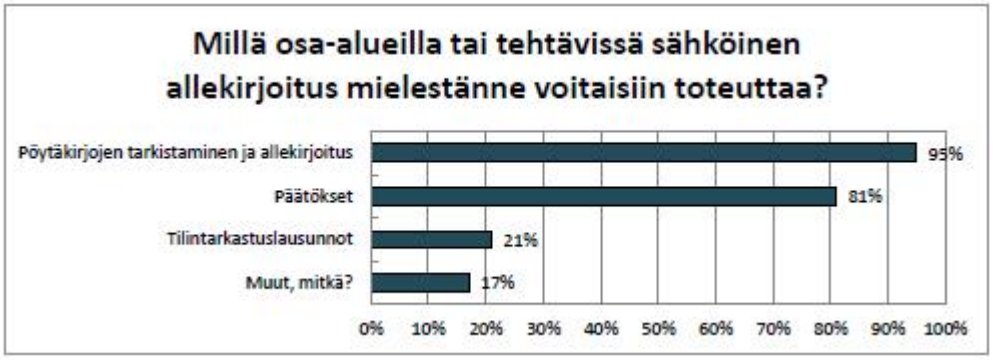
KUVA 16. Perusteet sähköiselle allekirjoitukselle

Sähköisen allekirjoituksen eri tavoista toimivimpana pidettiin organisaation omalla varmenteella tapahtuvaa allekirjoitusta. Myös pankkitunnuksilla tapahtuvaa allekirjoitusta piti toimivana lähes 30 % vastaajista (kuva 17).



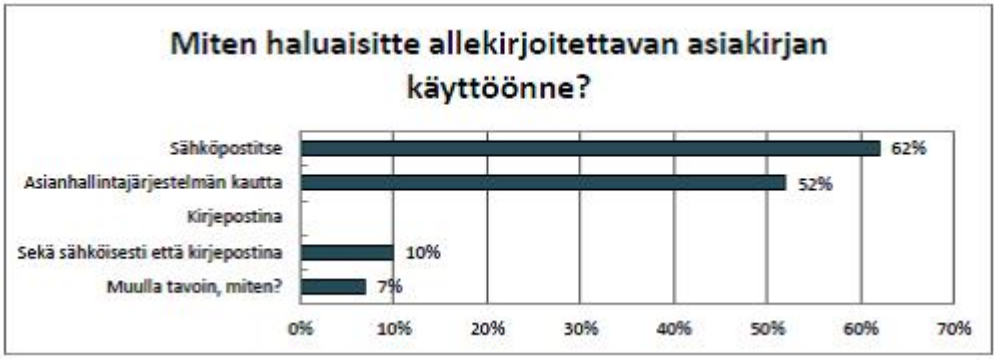
KUVA 17. Sähköisen allekirjoituksen tavat

Pöytäkirjojen tarkistamista ja allekirjoitusta sekä päätöksien allekirjoitusta pidettiin parhaimpina soveltamisalueina sähköiselle allekirjoitukselle (kuva 18). Myös tilintarkastuslausuntojen allekirjoitusta piti mahdollisena 21 % vastaajista.



KUVA 18. Sähköisen allekirjoituksen soveltamisalueet

Vastausten perusteella (kuva 19) suurin osa vastaajista haluaa allekirjoitettavan materiaalin käyttöönsä sähköisesti, joko sähköpostilla tai suoraan asianhallintajärjestelmän kautta. Vain 10 % vastaajista haluaa myös paperiversion materiaalista käyttöönsä.

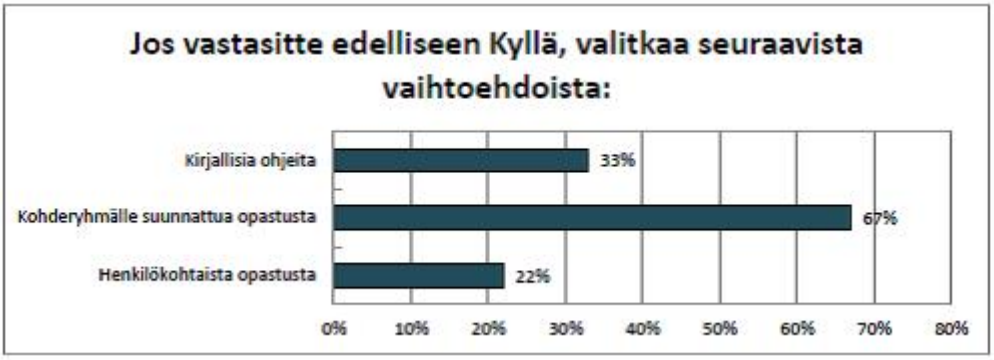


KUVA 19. Asiakirjojen toimitus

Selkeästi suurin osa (60 %) vastaajista tuntee tarvitsevansa apua sähköisen allekirjoituksen käyttöön (kuva 20). Vastaajista 21 % ei kokenut tarvitsevansa tukea sähköisen allekirjoitusta käyttöön otettaessa. Vajaa viidesosa vastaajista ei osannut sanoa tarvitsisivatko käyttöönottoon tukea.

KUVA 20. Käyttöönottotuen tarve

Parhaana käyttöönottotuen muotona pidetään kuvan 21 perusteella kohderyhmittäin tapahtuvaa opastusta. Merkittävä osa vastaajista kokee myös tarvitsevansa henkilökohtaista ohjausta ja kirjallisia ohjeita.



KUVA 21. Käyttöönottotuen muodot

Kyselyn perusteella sähköisen allekirjoituksen käyttöönoton valmiustaso on korkea ja mahdolliset soveltamisalueet ovat helposti määriteltävissä. Tavoitteena voi vain olla sähköisen allekirjoituksen mahdollisimman laaja soveltaminen läpi organisaation. Kyselyn pohjalta kaksi soveltamisalaa tulevat ensisijaisesti esille pöytäkirjojen tarkistaminen ja allekirjoitukset sekä päätökset.

7 KÄYTTÖÖNOTON SUUNNITELMA JA KRIITTISET KOHDAT

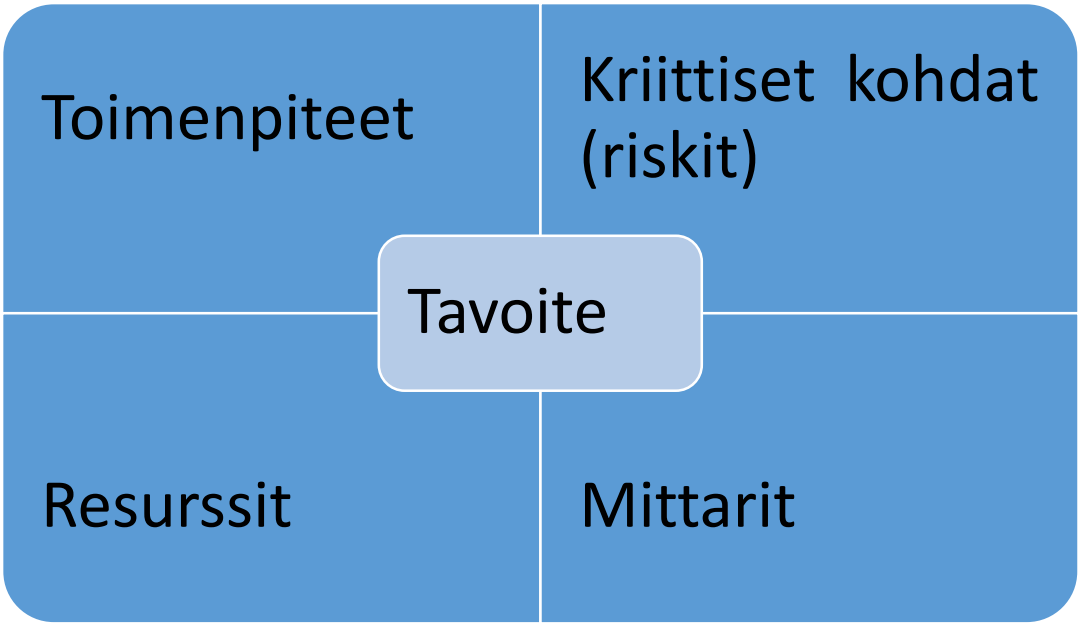
Sähköisen allekirjoituksen käyttöönottoa suunniteltaessa on tärkeää määrittää, minkätyyppinen sähköinen allekirjoitus kuhunkin käyttötilanteeseen sopii. Riittääkö yksinkertainen sähköinen allekirjoitus vai tarvitaanko vahvaan sähköiseen tunnistamiseen pohjautuvaa allekirjoitusta?

7.1 Looginen viitekehys

Looginen viitekehys (engl. Logical Framework Analysis/Approach, lyh. LFA) on alunperin kehitetty vuonna 1969 USA:ssa USAID:ssa (the United States Agency for International Development). Logical Framework Approach (LFA) on selkeä kehittämisprojektien suunnittelun, hallinnoin, raportoinnin ja arvioinnin ajattelutapa. Sen lähtökohtana on kokonaisvaltainen ja strategiseen ajatteluun perustuva ote, jossa tarkastelun kohteena on vaikuttavuus. Loogisen viitekehyksen lähestymistapa on hyvin tavoiteorientoitunut. LFA on tekniikka, jonka avulla identifioidaan ja analysoidaan esitettyä tilannetta sekä määritellään tavoitteet ja toimenpiteet, jotka tulisi toteuttaa esitetyn tilanteen parantamiseksi. Lähtökohtaisesti looginen viitekehys edistää sitoutumista, avoimuutta ja sen avulla ohjataan toiminnan tavoitteellisuutta. (Innokylä, 2012.)

Tässä kehittämistehtävässä käyttämäni looginen viitekehystaulukko on ennen kaikkea työväline, joka auttaa tässä tapauksessa sähköisen allekirjoituksen toteutussuunnitteluun liittyvien asioiden jäsentämisessä. Analyysivaiheessa olen koonnut toteutussuunnittelussa huomioitavat tavoitteet, tehtävät, resurssit, kriittiset kohdat ja mittarit. Näiden pohjalta on koottu konkreettinen matriisi.

Loogisen viitekehyksen matriisin (kuva 22) avulla selvitetään muun muassa seuraavaa: Mitkä ovat suunnitelman tavoitteet? Mitä toimintoja tarvitaan, jotta nämä tavoitteet voidaan saavuttaa? Mitä resursseja tarvitaan, jotta tavoitteet saavutetaan? Mitkä ovat kriittiset kohdat? Millä mittareilla tuloksia mitataan ja mistä lähteistä tietoa saadaan? Suunnittelun edistyttyä loogista viitekehystaulukkoa voidaan hyödyntää myös seurannan ja arvioinnin välineenä varsinkin siinä mainittujen indikaattoreiden eli mittareiden avulla.



KUVA 22. Loogisen viitekehyksen matriisi

Seuraavissa taulukoissa 3 – 9 on kuvattu tämän tutkimuksen tuloksena syntynyt loogi-nen viitekehys jaettuna seitsemään alatavoitteeseen:

- sähköisen allekirjoituksen käyttötilanteiden rajaus;
- tarvittavien teknisten ratkaisujen käyttöönotto;
- käyttäjäryhmien määrittely;
- käyttäjien kouluttaminen;
- turvallisuusmääräysten luominen;
- käyttötuen organisointi ja
- sähköisten allekirjoitusten arkistointi.

Taulukointi on vakiintunut tulosten esittämisen muoto loogisen viitekehyksen lähesty-mistavassa.

TAULUKKO 3. Sähköisen allekirjoituksen käyttötilanteiden rajaus

Toimenpiteet	**Resurssit**	**Kriittiset kohdat (riskit)**	**Mittarit**
1.1 Allekirjoitus-tilanteiden doku-mentointi	Projektin vetäjä Ohjaus-ryhmä	r1. Allekirjoitusti-lanteiden doku-mentointi viiväs-tyy	m1. Dokumentoidut mah-dolliset käyttötilanteet m2. Tarkennetut kuvaukset valituista käyttötilanteista

Toimenpiteet	Resurssit	Kriittiset kohdat (riskit)	Mittarit
1.2 Ensisijaisten käyttötilanteiden valitseminen 1.3. Valittujen käyttötilanteiden tarkennettu kuvaus		r2. Ensisijaisten käyttötilanteiden valinta epäonnistuu	

Käyttöönotossa ensimmäisessä vaiheessa on dokumentoitava kaikki ne mahdolliset allekirjoitustilanteet, joissa sähköinen allekirjoitus voidaan ottaa käyttöön. Näiden dokumentoitujen tapausten pohjalta valitaan ensisijaiset käyttötilanteet. Näistä tehdään tarkennetut kuvaukset.

TAULUKKO 4. Tarvittavien teknisten ratkaisujen käyttöönotto

Toimenpiteet	Resurssit	Kriittiset kohdat (riskit)	Mittarit
2.1. Käyttötilanteiden tekninen vaatimusmäärittely 2.2. Olemassa olevien järjestelmien valmiuksien kartoitus 2.3. Teknisen ratkaisun valinta 2.4. Teknisen ratkaisun testaus 2.5. Pilottikäyttötilanteet 2.6. Testauksen ja pilotoinnin kokemusten kerääminen	Projektin vetäjä Tekninen tiimi Ohjausryhmä	r3. Teknisen vaatimusmäärittelyn epäonnistuminen r4. Olemassa olevien teknisten järjestelmien sopimattomuus r5. Pilotoinnin epäonnistuminen r6. Lanseerauksen myöhästyminen	m3. Vaatimusmäärittelyraportti m4. Pilotointien määrä m5. Lanseerauksen näkyvyys

Toimenpiteet	Resurssit	Kriittiset kohdat (riskit)	Mittarit
2.7. Teknisen ratkaisun hienosäätö 2.8. Palvelun lanseeraus			

Valittujen käyttötilanteiden kuvausten pohjalta tehdään tekninen vaatimusmäärittely. Tämän määrittelyn pohjalta arvioidaan organisaatiossa käytössä olevien järjestelmien valmiudet ja valitaan tekninen ratkaisu näistä. Valittu ratkaisu testataan ja siirrytään sen jälkeen pilotointiin rajatulla käyttöryhmällä ja tilanteilla. Pilotoinnin kokemusten pohjalta tekninen ratkaisu hienosäädetään ja palvelu lanseerataan käyttöön.

TAULUKKO 5. Käyttäjäryhmien määrittely

Toimenpiteet	Resurssit	Kriittiset kohdat (riskit)	Mittarit
3.1. Potentiaalisten käyttäjien luettelointi 3.2. Käyttäjien valinta käyttötilanteiden mukaisesti 3.3. Käyttäjien oikeuksien määrittely 3.4. Käyttäjäkohtaisten profiilien luonti	Projektin vetäjä Ohjausryhmä Käyttäjäryhmät	r7. Käyttäjien muutosvastarinta r8. Käyttäjäoikeuksien määrittelyssä tulee ongelmia	m6. Käyttäjien ja ryhmien määrä m7. Käyttöoikeuksien eri luokat

Potentiaaliset allekirjoituspalvelun käyttäjät luetteloidaan ja valitaan näistä käyttötilanteittain allekirjoittajat. Näille käyttäjille määritellään eritasoisia oikeuksia. Oikeuksien pohjalta luodaan käyttäjäkohtaiset profiilit.

TAULUKKO 6. Käyttäjien kouluttaminen

Toimenpiteet	Resurssit	Kriittiset kohdat (riskit)	Mittarit
4.1. Koulutustarpeen selvittäminen 4.2. Koulutusohjelman ja materiaaleiden luominen 4.3. Yhteinen käyttökoulutus 4.4. Käyttäjäkohtainen valmennus	Projektin vetäjä Ohjausryhmä Käyttäjäryhmät Tekninen tiimi	r9. Koulutuksen epäonnistuminen r10. Henkilökohtaisen valmennuksen riittämättömyys	m8. Koulutusmateriaalit m9. Koulutettavien määrä m10. Valmennuksen määrä

Allekirjoituspalvelun käyttäjien koulutustarpeet selvitetään. Tulosten pohjalta laaditaan koulutusohjelma ja tarvittavat materiaalit. Järjestetään kaikille yhteistä käyttökoulutusta ja tarpeen mukaan käyttäjäkohtaista valmennusta.

TAULUKKO 7. Turvallisuusmääräysten luominen

Toimenpiteet	Resurssit	Kriittiset kohdat (riskit)	Mittarit
5.1. Turvallisuusmääräysten tarpeen analysointi 5.2. Turvallisuusmääräysten listaus 5.3. Epäkohtatilanteiden määrittely ja niihin liittyvät toimet 5.4. Turvallisuusmääräysten tiedottaminen	Projektin vetäjä Tekninen tiimi Ohjausryhmä	r11. Turvallisuusuhkien realisoituminen r12. Turvallisuusmääräysten riittämättömyys	m11. Turvallisuusmääräykset m12. Tiedotusmateriaali

Allekirjoituspalvelun turvallisuusnäkökohdat selvitetään ja analysoidaan turvallisuusmääräysten tarve. Tarvittavat määräykset listataan ja niihin liittyvät epäkohtatilanteet

määritellään. Epäkohtiin liittyvät korjaustoimenpiteet kirjataan ja tiedotetaan turvallisuusmääräykset kohderyhmille, eli palvelun käyttäjille.

TAULUKKO 8. Käyttötuen organisointi

Toimenpiteet	Resurssit	Kriittiset kohdat (riskit)	Mittarit
6.1. Käyttötuen eri muotojen kartoitus 6.2. Sähköisen käyttötuen luominen 6.3. Henkilökohtaisen käyttötuen organisointi	Projektin vetäjä Tekninen tiimi Ohjausryhmä	r13. Käyttötuen saavutettavuus	m13. Käyttötukimateriaali m14. Tukihenkilöverkosto

Kartoitetaan sähköisen allekirjoituksen käyttöön liittyvän käyttötuen muodot. Luodaan sähköinen käyttötukipalvelu ja organisoidaan henkilökohtainen käyttötuki. Käyttötuen saatavuuteen ja saavutettavuuteen kiinnitetään erityistä huomiota.

TAULUKKO 9. Sähköisten allekirjoitusten arkistointi

Toimenpiteet	Resurssit	Kriittiset kohdat (riskit)	Mittarit
7.1. Sähköisen allekirjoituksen arkistointivaatimusten kartoitus 7.2. Sähköisen arkistoinnin ratkaisut allekirjoituksiin 7.3. Organisaatiovarmenteen kehittäminen allekirjoitusten pitkäaikaissäilytykseen	Projektin vetäjä Arkistovastaava Ohjausryhmä	r14. Sähköisten allekirjoitusten arkistointiin ei löydy kestävää ratkaisua	m15. Sähköisten allekirjoitusten arkistointiratkaisu m16. Allekirjoitusten pitkäaikaissäilytykseen organisaatiovarmenne

Ensiksi kartoitetaan lainsäädännöstä ja käytännöistä sähköisen allekirjoituksen arkistointivaatimukset. Olemassa olevat sähköisen arkistoinnin ratkaisut allekirjoitusten arkistointiin selvitetään. Allekirjoitusten pitkäaikaissäilytyksen vaatima organisaatiovarmenne kehitetään.

7.2 Kriittiset kohdat

Sähköisen allekirjoituksen käyttöönoton osalta kriittisiä kohtia on käyty läpi asiantuntijahaastatteluissa ja tapaustutkimuksissa. Esitän kriittiset kohdat tässä riskianalyysin muodossa. Kriittiset kohdat ovat ristiintaulukoitavissa loogisen viitekehyksen kanssa. Tämän vuoksi ne on esitetty taulukkomuodossa, jotta ne ovat ymmärrettävissä oikeassa yhteydessään. Riskien todennäköisyyttä olen arvioinut kolmiportaisesti:

- +++ hyvin todennäköinen
- ++ todennäköinen
- + ei kovin todennäköinen

Taulukko 10 sisältää neljätoista kohdetta, joissa riski tässä tutkimuksessa on tunnistettu. Todennäköisyysarvion lisäksi on arvioitu vaikutuksia, esitetty toimia sekä riskien minimoimisen että seurannan kannalta.

TAULUKKO 10. Riskianalyysi

Riski	**Todennäköisyys**	**Vaikutus**	**Toimet riskin minimoimiseksi**	**Seuranta**
r1. Allekirjoitustilanteiden dokumentointi viivästyy	+++	Käyttöönottoprojekti myöhästyy	Riittävä resursointi ja henkilöstön sitouttaminen	Projektiaikataulun seuraaminen
r2. Ensisijaisten käyttötilanteiden valinta epäonnistuu	++	Projekti viivästyy ja joudutaan alkupisteeseen, kustannukset nousevat	Käyttötilanteiden pohdinta ohjausryhmässä ja verifiointi asiantuntijoilla, riittävä	Käyttötilanteiden määrän rajoittaminen projekti-

Riski	Todennäköisyys	Vaikutus	Toimet riskin minimoimiseksi	Seuranta
			rajaus, korkeintaan kaksi ensisijaista käyttötilannetta	suunnitelman mukaisesti
r3. Teknisen vaatimusmäärittelyn epäonnistuminen	+	Projekti ei etene käyttöönottoon, käyttöönotto epäonnistuu	Teknisen tuen riittävyyden varmistaminen, käyttötilanteiden pelkistäminen	Teknisen raportoinnin seuranta
r4. Olemassa olevien teknisten järjestelmien sopimattomuus	+	Projekti viivästyy tai jopa peruuntuu	Olemassa olevien teknisten järjestelmien ennakkoarviointi järjestelmätoimittajien kanssa	Järjestelmätoimittajien kanssa jatkuva tilannepäivitys
r5. Pilotoinnin epäonnistuminen	++	Projekti viivästyy, pilotoinnit joudutaan toistamaan	Pilottikohteiden tarkka määrittely, pilottien tarkka rajaus määrällisesti ja ajallisesti	Pilottikohteiden raportointi
r6. Lanseerauksen myöhästyminen	+++	Projekti viivästyy	Lanseerauksen hyvä ennakkovalmistelu ja ajoittaminen	Projektiaikataulun seuraaminen
r7. Käyttäjien muutosvastarinta	+	Käyttöönotto vaikeutuu ja mahdollisesti viivästyy	Käyttäjäryhmien oikea-ai-	Käyttäjien osal-

Riski	Todennäköisyys	Vaikutus	Toimet riskin minimoimiseksi	Seuranta
			kainen tiedottaminen ja sitouttaminen	listuminen pilotteihin
r8. Käyttäjäoikeuksien määrittelyssä tulee ongelmia	+	Käyttöönotto viivästyy, kustannukset nousevat	Käyttäjäoikeuksien määrittely aloitetaan ajoissa ja pohjautuu olemassa oleviin järjestelmiin	Käyttäjäoikeusmäärittelyt osana teknistä raportointia
r9. Koulutuksen epäonnistuminen	++	Käyttöönotto hankaloituu ja järjestelmä toimii vajaasti	Koulutuksen hyvä suunnittelu ja riittävä koulutusaika	Koulutussuunnitelmat ja osallistujapalaute
r10. Henkilökohtaisen valmennuksen riittämättömyys	++	Käyttäjät eivät osaa käyttää palvelua ja käyttöönotto hankaloituu	Henkilökohtaisen valmennustarpeen arviointi oikealle tasolle	Valmennuspalaute
r11. Turvallisuusuhkien realisoituminen	+	Palvelu voidaan joutua sulkemaan kunnes turvallisuusaukot selvitetään ja korjataan	Turvallisuusuhkien ennakointi ja uhkatilanteiden välitön raportointi	Turvallisuusraportointi
r12. Turvallisuusmääräysten riittämättömyys	+	Palvelua ei voida ottaa	Turvallisuusmääräysten tes-	Turvallisuusraportointi

Riski	Todennäköisyys	Vaikutus	Toimet riskin minimoimiseksi	Seuranta
		käyttöön turvallisuusuhkien vuoksi	taus asiantuntijoilla ja vertaisanalyysit	
r13. Käyttötuen saavutettavuus	+++	Käyttäjät eivät saa apua käyttötilanteissa ja palvelun käyttö vaikeutuu, lisää muutosvastarintaa	Käyttötuen määrän arviointi riittävälle tasolle. Tukihenkilöverkoston luominen ja sen koulutus.	Käyttäjäpalaute
r14. Sähköisten allekirjoitusten arkistointiin ei löydy kestävää ratkaisua	++	Asiakirjojen arkistointiin joudutaan luomaan uusia ratkaisuja. Lisää kustannuksia	Olemassa olevien arkistointikäytänteiden selvittäminen ja soveltaminen.	Arkistonmuodostusseuranta

Riskianalyysi nostaa esille hyvin todennäköisinä riskeinä allekirjoitustilanteiden viivästymisen, sähköisen allekirjoituksen lanseerauksen myöhästymisen sekä käyttötuen saavutettavuuden. Riskianalyysin perustana ovat loogisessa viitekehyksessä esitetyille toimenpiteille ennakoidut kriittiset kohdat. Jokaiselle riskille on analyysissa esitetty myös toimet riskin minimoimiseksi. Seurannan avulla arvioidaan riskien toteutumista.

8 POHDINTA

Tässä pohdintaosiossa arvioin tutkimukseni käytettävyyttä sekä organisaationi puitteissa että laajemminkin. Lisäksi nostan esille uusia tutkimusaihioita, joita tutkimuspro-

sessin aikana nousi esille. Samalla arvioin tutkimukseni toteutusta ja sen pohjalta sähköisen allekirjoituksen mahdollista käyttöönottoprosessia organisaatiossani. Liitteessä esitän rungon mahdolliselle käyttöönottoprojektille.

Tutkimukseni tavoitteena oli tilaajan toimeksiannosta selvittää sähköisen allekirjoituksen käyttöönoton toteutettavuutta Kaakkois-Suomen ammattikorkeakoulu Oy:ssä (Xamk). Pyrkimyksenä oli lähestyä aihetta mahdollisimman konkreetilla tasolla organisaationi arkisen toiminnan puitteissa. Sen vuoksi lähestymistavaksi valittiin myös suoraan mahdollista käyttöönottoprojektia tukeva looginen viitekehys.

Mielestäni tutkimus antaa selkeän viestin siitä, että sähköisen allekirjoituksen käyttöönotolle organisaatiossa ei ole suuria esteitä. Pikemminkin niin, että sen käyttöönotto on hyvin luonteva osa organisaation kehittämistä. Myös ulkoiset tekijät, kuten lainsäädäntö ja julkisen vallan tuki, tukevat tätä kehitystä vahvasti. Tutkimuksen käytettävyyttä lisää myös se, että sen toteutuksessa on ollut mukana lähes koko organisaation toimiva johto.

Tutkimus tarkastelee käyttöönoton toteutettavuutta kriittisesti. Useita kriittisiä kohtia nousee esille, mutta niille kaikille löytyy myös toimivat ratkaisut, jotka organisaatio pystyy toteuttamaan kustannustehokkaasti. Kaiken kaikkiaan sähköisen allekirjoituksen käyttöönoton teknisiin ratkaisuihin ei vaadita suuria taloudellisia investointeja. Tekniikat ja käyttösovellukset löytyvät jo komponentteina olemassa olevista järjestelmistä organisaation tiedonhallinnassa. Loogisen viitekehyksen pohjalta organisaatio voi luoda hyvin helposti käyttöönottoprojektin. Mahdolliselle käyttöönottoprojektille olen laatinut tutkimukseni liitteessä olevan 4 suunnitelmarungon, jonka avulla voi asiaa lähteä suunnittelemaan eteenpäin.

Tutkimukseni on rajattu omaan organisaatiooni. Siitä huolimatta tutkimusmenetelmää voidaan soveltaa hyvin monenlaisissa organisaatioissa. Tutkimuksessa on tuotu myös esiin laajempaa sähköisen allekirjoituksen viitekehystä, jolle lienee käyttöä laajemminkin. Oletettavasti sähköinen allekirjoitus yleistyy lähivuosina, joten käyttöönottoprojekteja tulee olemaan runsaasti. Ne toivottavasti pystyvät hyötymään tämän tutkimuksen menetelmistä ja johtopäätöksistä.

Tutkimukseni aikana yksi vaikeimmista asioista oli aihealueen rajaaminen. Sähköiselle allekirjoitukselle olisi hyvin laajasti käyttökohteita organisaatiomme sisällä, joiden tutkiminen olisi ollut mielenkiintoista, mutta se ei ollut tämän tutkimuksen puitteissa mahdollista eikä tarkoituksenmukaista.

Yksi selkeistä jatkotutkimuksen aiheista on opiskelijapalveluissa sähköisen allekirjoituksen soveltaminen. Sitä voidaan soveltaa hyvin samalla tapaa kuin saksalaisessa tapaustutkimuksessani Bochumin yliopistossa opiskelijoiden rekisteröinnissä. Mutta sitä voitaisiin soveltaa myös opiskelija-arvioinnissa aina tutkintotodistuksiin saakka.

Lisäksi olisi mielenkiintoista toteuttaa osana sähköisen allekirjoituksen käyttöönottoprojektia käyttäjälähtöinen seurantatutkimus. Sen voisi hyvin integroida käyttäjätukeen ja kerätä tietoa myös suoraan käyttöönotettavasta allekirjoitussovelluksesta. Tällä seurantatutkimuksella pystyttäisiin tukemaan sähköisen allekirjoituksen laajamittaisempaa käyttöönottoa organisaatiossa.

LÄHTEET

Allekirjoitus. WWW-dokumentti. https://fi.wikipedia.org/wiki/Allekirjoitus. Muokattu 14.12.2015. Luettu 9.3.2016.

Analytic_frame. WWW-dokumentti. https://en.wikipedia.org/wiki/Analytic_frame. Muokattu 10.8.2015. Luettu 23.10.2015.

Avain Technologies Oy 2012. Itä-Savon sairaanhoitopiiri siirtyi palvelukeskeiseen sähköiseen toimintamalliin. 2012. WWW-dokumentti. http://www.avaintec.com/wp-content/uploads/2012/08/Avain_Case_ISSHP_FI.pdf. Ei päivitystietoa. Luettu 21.8.2015.

CSC – Tieteen tietotekniikan keskus Oy 2015. WWW-dokumentti. https://www.csc.fi/-/haka-kayttajatunnistusjarjestel-1. Päivitetty 7.5.2014. Luettu 21.8.2015.

Digi-ID Viro 2016. WWW-dokumentti. www.id.ee. Luettu 10.4.2016.

Digital Signature Standard 2013. PDF-dokumentti. Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8900 Issued July 2013. https://oag.ca.gov/sites/all/files/agweb/pdfs/erds1/fips pub_07_ 2013.pdf). Luettu 2.2.2016.

Estonian “chapter zero” for MoReq2. PDF-dokumentti. Implementation of the MoReq2 Model Requirements for the Management of Electronic Records in Estonia (Estonian “chapter zero” for MoReq2) Version 2.0, 2012, Ministry of Economic Affairs and Communication. https://www.mkm.ee/sites/default/files/estonian_et_-_chapter_0_english.pdf. Luettu 10.4.2016.

Euroopan Parlamentin ja neuvoston direktiivi 1999/93/EY. PDF-dokumentti http://eur-lex.europa.eu/LexUriServ/. Luettu 12.2.2016.

European Comission 2015. Digital Single Market. WWW-dokumentti. https://ec.europa.eu/digital-agenda/en/scoreboard/finland. Ei päivitystietoa. Luettu 12.2.2016.

Evifin Oy 2016. WWW -dokumentti. http://www.evifin.fi/toimikortinlukijat.php. Ei päivitystietoa. Luettu 27.4.2016.

Gasser, Oliver. Elektronische Signaturen. 2009. PDF -dokumentti. https://www7.in.tum.de/um/courses/seminar/krypto/SS09/gasser/ausarbeitung.pdf. Ei päivitystietoa. Luettu 12.2.2016.

Haapiainen, Tuula. Valokuva. Asiakirjan allekirjoitus. Henkilökohtainen arkisto.

INNO-kylä. Logical Framework Approach. WWW-dokumentti. https://www.inno-kyla.fi/web/malli111677. Luotu 21.11.2012. Muokattu 29.5.2013. Luettu 23.10.2015.

Kansallinen terveysarkisto, Kanta, 2016. WWW-dokumentti. http://www.kanta.fi/fi /palvelut. Ei päivitystietoa. Luettu 14.2.2016.

Kyamk 2014. Kymenlaakson ammattikorkeakoulun strategia 2014 - 2016. WWW-dokumentti. http://www.kyamk.fi/folders/Files/Strategia%202014-2016/index.html. Ei päivitystietoa. Luettu 12.3.2016.

Laki sähköiestä asioinnista viranomaistoiminnassa. 24.1.2003/13.

Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista 7.8.2009/617.

Mamk 2012. WWW-dokumentti. http://www.mamk.fi/ajankohtaista/tiedotteet/101/0/kaakkois-suomen_ammattikorkeakoulu_oy_n_perustamissopimus_allekirjoitettiin. Ei päivitystietoa. Luettu 10.3.2016.

Mamk 2013. Mikkelin ammattikorkeakoulun strategia. WWW-dokumentti. http://www.mamk.fi/instancedata/prime_product_julkaisu/mamk/embeds/mamkwwwstructure/20831_Mamk_2017_strategia_low.pdf. Ei päivitystietoa. Luettu 10.3.2016.

Ojasalo, Katri; Moilanen, Teemu & Ritalahti Jarmo 2009. Kehittämistyön menetelmät. Uudenlaista osaamista liiketoimintaan. WSOYpro Oy, s. 19, 66-68.

Opetus- ja kulttuuriministeriö. AMK-uudistus 2011-2014. WWW-dokumentti. http://www.mnedu.fi/OPM/Koulutus/ammattikorkeakoulutus/ammattikorkeakoulu_uudistus/index.html. Ei päivitystietoa. Luettu 9.3.2016.

Pfitzmann, Birgit. Digital Signature Schemes. General Framework and Fail-Stop Signatures. Lecture Notes in Computer Science, Vol. 1100, Springer-Verlag, Berlin Heidelberg New York, 1996. http://download.springer.com/static/pdf/. PDF-dokumentti. Ei päivitystietoa. Luettu 22.8.2015.

Ruhr-Universität Bochum. WWW-dokumentti. http://www2.uv.ruhr-uni-bochum.de/it-services/rubcard/index.html.de. Letzte Änderung 7.8.2015. Luettu 21.8.2015.

Sairanen, Matti 2015. Haastattelu 18.3.2015. Terveystarkastaja. Itä-Savon sairaanhoitopiiri.

Valtioneuvoston kanslia, 2015. Ratkaisujen Suomi Pääministeri Juha Sipilän hallituksen strateginen ohjelma 29.5.2015. http://valtioneuvosto.fi/documents/10184/1427398 /Ratkaisujen+Suomi_FIYHDISTETTY_netti.pdf/. Hallituksen julkaisusarja 10/2015. Edita Prima, 2015.

Valtion tilintarkastuslautakunta. 2013. Kannanotto 1/2013, 5.2.2013. Tilintarkastajien sähköisistä allekirjoituksista. WWW-dokumentti. https://www.tem.fi/files/36089/VALA_kannanotto_2013.pdf. Ei päivitystietoa. Luettu 19.4.2015.

VERO, 2016. WWW-dokumentti. http://www.vero.fi/fi-FI/Asioi_verkossa. Ei päivitystietoa. Luettu 14.2.2016.

Voutilainen, Tomi 2015. Haastattelu 20.4.2015. Julkisoikeuden, sähköisen hallinnon ja informaatio-oikeuden professori, HTT Itä-Suomen yliopisto.

Voutilainen, Tomi 2009. ICT-oikeus sähköisessä hallinnossa – ICT oikeudelliset periaatteet ja sähköinen hallintomenettely. Helsinki. Edita Prima Oy, s. 255-261.

Voutilainen, Tomi 2012. Julkisen hallinnon asiakirjahallinnon lainsäädännön ja toiminnan uudistaminen. Selvitystyö Mikkelin ammattikorkeakoululle. ”Sähköisten palveluiden soveltavan tutkimuksen rakenteet” –hanke. Pdf-dokumentti. http://www.mamk.fi/instancedata. Ei päivitystietoa. Luettu 14.3.2016.

Voutilainen, Tomi 2012. Sähköisen hallinnon oikeudelliset perusteet. Luentomateriaali 12.-13.12.2012. Verkkojulkaisu. Luettu 19.4.2015.

Väisänen Jari 2016. Haastattelu 29.3.2016. Järjestelmäpäällikkö. Xamk.

Xamk 2015. http://www.xamk.fi/fi. Kaakkois-Suomen Ammattikorkeakoulu Oy:n strategia. PDF-dokumentti. Ei päivitystietoa. Luettu 10.3.2016.

Xamk 2016. Ajankohtaista 2016. WWW-dokumentti. http://www.xamk.fi/fi/Ajankohtaista/2016). Luettu 20.4.2016.

Xamk 2016. Kaakkois-Suomen Ammattikorkeakoulu. Tietoa yhteistyöstä. WWW-dokumentti. http://www.xamk.fi/fi/Tietoa%20yhteisty%C3%B6st%C3%A4. Luettu 10.3.2016.

Xamk 2016. Kasva vahvaksi. Grow strong. WWW-dokumentti. http://www.kyamkmamk.fi/fi. Luettu 10.3.2016.

Allekirjoitus:
Allekirjoitus eli nimikirjoitus tai autografi on nimen kirjoitettu asu tai muu tunnistusmerkki, jonka henkilö kirjoittaa asiakirjaan todisteeksi henkilöllisyydestä ja tahdosta. Henkilökohtaiseen allekirjoitukseen käytetään yleensä omaa nimeä tai sen lyhennettä. Se toimii sinetin tavoin. Suomen kielessä nimikirjoitus tarkoittaa jonkin henkilön nimeä hänen itsensä käsin kirjoittamana.

Julkisen avaimen järjestelmä (PKI):
Julkisen avaimen järjestelmällä on salausmenetelmä, jossa kullakin käyttäjällä on kaksi matemaattisesti toisiinsa liittyvää avainta: julkisessa hakemistossa julkaistava julkinen avain ja vain käyttäjän hallussa oleva yksityinen avain.

Sähköinen allekirjoitus:
Sähköinen allekirjoitus on sähköiseen materiaaliin liitettyä dataa, jolla voidaan todentaa allekirjoittaja (identiteetti) ja allekirjoitettavan aineiston muuttumattomuus (integriteetti).

Todentaminen:
Todentamisella tarkoitetaan palvelun käyttäjän identiteetin ja allekirjoituksen aitouden varmentamista. Tämä voidaan tehdä jonkun seuraavan perusteella:

- jotain, jonka vain tämä käyttäjä tietää (salasana, PIN-koodi, salausavain)
- jotain, joka on vain tämän käyttäjän fyysinen ominaisuus (biotunnistus, esimerkiksi sormenjälki)
- jotain, jonka vain tämä käyttäjä omistaa (henkilötodistus)
- jotain, jonka vain tämä käyttäjä osaa

Toimikortti
Sirukortti (eli älykortti eli toimikortti) on muovinen kortti, joka sisältää mikrosirun (Evifin Oy.)

Tunnistaminen:
Tunnistamisella tarkoitetaan juridisen henkilön yksilöimistä ja tunnisteen aitouden ja oikeellisuuden tunnistamista sähköistä menetelmää käyttämällä.

Vahva sähköinen tunnistaminen:
Vahvalla sähköisellä tunnistamisella tässä tutkimuksessa tarkoitetaan tunnistamista, joka perustuu vähintään kahteen seuraavasta kolmesta vaihtoehdosta:
a) salasanaan tai johonkin muuhun sellaiseen, mitä tunnistusvälineen haltija tietää; b) sirukorttiin tai johonkin muuhun sellaiseen, mitä tunnistusvälineen haltijalla on hallussaan; tai c) sormenjälkeen tai johonkin muuhun tunnistusvälineen haltijan yksilöivään ominaisuuteen (Laki vahvasta tunnistamisesta ja sähköisistä allekirjoituksista, 617/2009.)

Varmenne:
Varmenteella tässä tutkimuksessa tarkoitetaan sähköistä todistetta, joka todentaa juridisen henkilöllisyyden ja liittää allekirjoituksen todentamistiedot allekirjoittajaan.

LIITE 2.

Kyselyn saate

Hyvä vastaanottaja!

Suoritan ylempää ammattikorkeakoulututkintoa Mikkelin ammattikorkeakoulun Sähkö- ja informaatiotekniikan laitoksella Sähköinen asiointi- ja arkistointi -koulutusohjelmassa. Opinnäytetyönäni on selvittää sähköisen allekirjoituksen käyttöönoton edellytyksiä ja mahdollisuuksia. Työni toimeksiantajana on Kaakkois-Suomen Ammattikorkeakoulu Oy.

Ohessa on linkki kyselyyn, jossa pyydän teiltä vastauksia muutamiin asiaa koskeviin kysymyksiin. Vastaaminen on ehdottoman luottamuksellista eikä missään vaiheessa yksittäinen vastaus nouse selvityksessäni esiin.

Toivon, että teiltä löytyisi hetki aikaa tämän kehittämiskyselyn vastaamiseen 21.9.2015 mennessä. Jos teillä on aiheeseen liittyen kysyttävää, vastaan mielelläni kysymyksiinne. Mikäli teillä ei ole mahdollisuutta vastata webropol –kyselyyn, ottakaa myös siinä tapauksessa yhteyttä minuun, tuula.haapiainen@mamk.fi, niin toimitan kysymykset teille postitse. Tällöinkin voitte myös vastata nimettömänä ja palauttaa vastauksenne palautuskirjekuoressa.

Linkki kyselyyn: https://www.webropolsurveys.com

Ystävällisin terveisin

Tuula Haapiainen

Sähköinen allekirjoitus

Tämän kyselyn tarkoituksena on kartoittaa sähköisen allekirjoituksen käyttöönoton edellytyksiä Kaakkois-Suomen Ammattikorkeakoulu Oy:ssä (myöh. Xamk). Kysely on suunnattu Kyamkissa, Mamkissa ja Xamkissa esimiesasemassa toimiville sekä luottamushenkilöille. Vastaamalla kyselyyn annatte oman näkemyksenne sähköisen allekirjoituksen käyttöönoton edellytyksistä ja mahdollisuuksista. Vastaaminen on ehdottoman luottamuksellista eikä missään vaiheessa yksittäinen vastaus nouse selvityksessäni esiin.

1. Asemani organisaatiossa *

- ◯ Ylin johto
- ◯ Koulutus- tai muu johto
- ◯ Päällikkö
- ◯ Muu esimies
- ◯ Luottamushenkilö

2. Minkälainen tietotekninen käyttöympäristö on teille tutuin?

- ◯ Windows
- ◯ Mac OS X
- ◯ Linux

Jokin muu, mikä?

- ◯ _____

3. Minkälainen nettiyhteys teillä on käytössänne?

- ◯ Organisaation tietoverkko
- ◯ Kiinteä laajakaista

○ Mobiililaajakaista

Muu, mikä?

○ _____

4. Mitkä seuraavista tietoturvaratkaisuista verkkoasioinnissa teillä on tällä hetkellä käytössänne?

☐ Palomuuri ja virustorjunta

☐ Roskapostisuodatin

☐ Varmuuskopiointi

Muu tietoturva, mikä

☐ _____

☐ En osaa sanoa

5. Minkälaisia verkkopalveluita käytätte säännöllisesti?

☐ Verkkopankki

☐ Verkkokaupat

☐ Digilehdet

☐ Sähköinen asiointi

☐ Uutispalvelut

Muita, mitä?

☐ _____

6. Onko sähköinen allekirjoitus teille tuttu asia käytännössä?

○ Kyllä

○ Ei

○ En osaa sanoa

7. Mitkä seuraavista verkkopalveluiden tunnistamisen vaihtoehdoista ovat teille tuttuja?

- ☐ Käyttäjätunnus ja salasana
- ☐ Mobiilivarmenne
- ☐ Sähköinen henkilökortti
- ☐ Toimikortti
- ☐ Tupas

8. Minkälaisia henkilökohtaisia varmenteita käytätte nykyään?

- ☐ Pankkitunnuksia
- ☐ Sähköistä henkilökorttia
- ☐ Kulunvalvontakorttia

Jotakin muuta, mitä?

- ☐ _____

9. Miten luotettavana pidätte sähköistä allekirjoitusta?

- ○ Erittäin luotettavana
- ○ Melko luotettavana
- ○ Epäluotettavana
- ○ En osaa sanoa

10. Mitkä perusteet mielestänne puhuvat allekirjoituksen puolesta?

- ☐ Tekninen kehitys
- ☐ Taloudellisuus
- ☐ Luotettavuus
- ☐ Helppous

Muut seikat, mitkä?

- ☐ _____

☐ Eivät mitkään seikat

11. Millä osa-alueilla tai tehtävissä sähköinen allekirjoitus mielestänne voitaisiin toteuttaa?

☐ Pöytäkirjojen tarkistaminen ja allekirjoitus
☐ Päätökset
☐ Tilintarkastuslausunnot
Muut, mitkä?
☐ _____

12. Mikä sähköisen allekirjoituksen tapa olisi mielestänne toimivin?

○ Pankkitunnuksilla tapahtuva
○ Organisaation omalla varmenteella (toimikortti)
○ Mobiilivarmenteella
○ Sähköpostivarmenteella
Jokin muu tapa, mikä?
○ _____
○ En osaa sanoa

13. Miten haluaisitte allekirjoitettavan asiakirjan käyttöönne?

☐ Sähköpostitse
☐ Asianhallintajärjestelmän kautta
☐ Kirjepostina
☐ Sekä sähköisesti että kirjepostina
Muulla tavoin, miten?
☐ _____

14. Jos sähköinen allekirjoitus otettaisiin käyttöön nyt, tarvitsisitteko käyttöönottoon tukea?

- ○ Kyllä
- ○ En
- ○ En osaa sanoa

15. Jos vastasitte edelliseen Kyllä, valitkaa seuraavista vaihtoehdoista:

- ☐ Kirjallisia ohjeita
- ☐ Kohderyhmälle suunnattua opastusta
- ☐ Henkilökohtaista opastusta

16. Kertokaa aiheeseen liittyviä ajatuksianne:

_____

_____

_____

Projektin tavoite

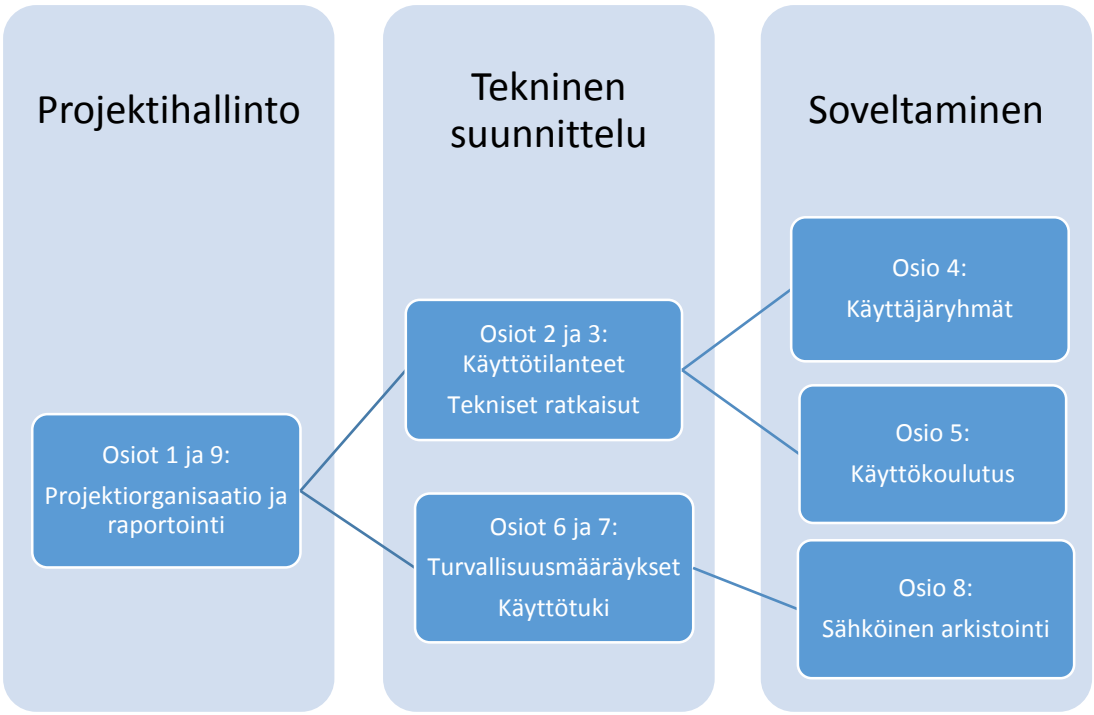
Tavoitteena on ottaa käyttöön sähköinen allekirjoitus Xamkin hallinnossa ja myöhemmin laajentaa myös muille tehtäväalueille.

Kohderyhmä

Kohderyhmänä on ensi vaiheessa Xamkin johto ja myöhemmin muu henkilökunta ja opiskelijat.

Osiot

Projekti koostuu yhdeksästä (9) osiosta, jotka linkittyvät toisiinsa sekä sisällöllisesti että kronologisesti.



1. Projektiorganisaation luominen

Projektiin nimetään päällikkö ja ohjausryhmä. Lisäksi perustetaan tekninen ja viestinnällinen projekti-/tukiryhmä.

2. Sähköisen allekirjoituksen käyttötilanteiden rajaus

Mahdolliset allekirjoitustilanteet dokumentoidaan ja valitaan näistä ensisijaiset käyttötilanteet. Näistä valituista käyttötilanteista tehdään tarkemmat kuvaukset.

3. Tarvittavien teknisten ratkaisujen käyttöönotto

Valittujen käyttötilanteiden kuvausten pohjalta tehdään tekninen vaatimusmäärittely. Vaatimusmäärittelyn avulla kartoitetaan organisaation olemassa olevien tietojärjestelmien valmiudet. Sähköisen allekirjoituksen tekniseksi ratkaisuksi valitaan kartoitusten pohjalta yksi tai useampia vaihtoehtoja. Tekniset ratkaisut testataan ja pilotoidaan. Testien ja pilotoinnin kokemukset raportoidaan. Raporttien pohjalta tekniset ratkaisut hienosäädetään. Sen jälkeen palvelu on lanseeraukseen valmis.

4. Käyttäjäryhmien määrittely

Valittujen allekirjoitustilanteiden pohjalta luetteloitaan kaikki kyseeseen tulevat käyttäjät. Jokaiseen käyttötilanteeseen nimetään omat käyttäjäryhmät. Käyttöoikeudet määritellään käyttäjäryhmittäin. Luodaan käyttäjäkohtaiset profiilit.

5. Käyttäjien kouluttaminen

Selvitetään käyttäjien sähköisen allekirjoituksen valmiustaso ja koulutustarpeet. Laaditaan koulutusohjelma ja tarvittava koulutusmateriaali. Järjestetään kaikille yhteinen käyttökoulutus ja sen jälkeen käyttäjäkohtainen valmennus.

6. Turvallisuusmääräysten luominen

Määritetään turvallisuusmääräysten tarpeet. Listataan kriittiset turvallisuusnäkökohdat ja niihin liittyvät turvamääräykset. Määritellään mahdolliset epäkohtatilanteet ja luodaan niihin vastaavat toimintamallit. Tiedotetaan turvallisuusmääräyksistä kohderyhmille.

7. Käyttötuen organisointi

Kartoitetaan käyttötuen mahdolliset muodot. Luodaan sähköinen käyttötukimateriaali ja palvelumalli. Organisoidaan tukihenkilöverkoston avulla henkilökohtainen käyttötuki.

8. Sähköisten allekirjoitusten arkistointi

Kartoitetaan sähköisen allekirjoituksen arkistointivaatimukset. Näiden vaatimusten pohjalta haetaan käytössä olevia sähköisen arkistoinnin ratkaisuja, joissa sähköisen allekirjoitusten arkistointivaatimukset toteutuvat. Kehitetään organisaatiovarmennetta, joka mahdollistaa sähköisten allekirjoitusten pitkäaikaissäilytyksen.

9. Projekti tulosten raportointi ja levittäminen

Käyttöönottoprojektin tuloksia kerätään koko projektin ajan. Niistä tiedotetaan hankkeeseen osallistuville prosessin aikana ja organisaation ulkopuolella projektin viestintäryhmän määrittelemällä tavalla. Projektin tuloksista tehdään materiaalia myös laajempaan levitykseen. Projektin pohjalta tehdään levitettävä toimintamalli, joka mahdollistaa sähköisen allekirjoituksen käyttöönoton omassa organisaatiossa laajemmin, ja joka on levitettävissä myös muihin organisaatioihin.

Projektiaikataulu

Projektin kesto on 12 kk. Projekti on pilotointihanke, joka voi jatkua uusilla laajennusprojekteilla. Projektiosioittain aikataulu on esitetty alla olevassa kuvassa.