LAB University of Applied Sciences

Sähköisen allekirjoituksen lainvoimaisuus

LAB-ammattikorkeakoulu
Tradenomi (AMK), Liiketalous
2020
Maiju Uronen

Tiivistelmä

Tekijä(t)	Julkaisun laji	Valmistumisaika
Uronen, Maiju	Opinnäytetyö, AMK	2020
	Sivumäärä	
	28	

Työn nimi

Sähköisen allekirjoituksen lainvoimaisuus

Tutkinto

Tradenomi (AMK)

Ohjaavan opettajan nimi, titteli ja organisaatio

Kari Hämeenaho, juridiikan lehtori, LAB-ammattikorkeakoulu

Tiivistelmä

Tämän opinnäytetyön tarkoituksena oli tutkia sähköisen allekirjoituksen lainvoimaisuutta. Työn tarkoituksena oli selvittää, miten sähköisen allekirjoituksen lainvoimaisuus muodostuu sekä missä tilanteissa sähköinen allekirjoitus on lainvoimainen. Lisäksi työssä tutkittiin sähköisen allekirjoituksen eri muotoja ja niiden käyttömahdollisuuksia.

Opinnäytetyössä perehdyttiin sähköisen allekirjoituksen allekirjoitusprosessiin ja sähköisen tunnistamisen eri muotoihin. Sähköinen tunnistaminen voidaan tehdä vahvasti tai heikosti, jolloin tämä vaikuttaa sähköisen allekirjoituksen turvalliseen varmentamiseen.

Työssä perehdyttiin sähköistä allekirjoitusta koskevaan lainsäädäntöön sekä hallituksen esitöihin. Lainsäädäntö rajattiin koskemaan Suomea, koska tarkoituksena oli selvittää sähköisen allekirjoituksen lainvoimaisuus Suomessa. Työn keskeisiä lähteistä olivat laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista 617/2009 sekä Euroopan parlamentin ja neuvoston eIDAS-asetus (EU) N:o 910/2014. Opinnäytetyön tutkimusmenetelmänä oli oikeusdogmaattinen, koska tutkin sähköistä allekirjoitusta lain näkökulmasta.

Työn tuloksena selvisi, että sähköinen allekirjoitus on lainvoimainen ja yhtä sitova kuin perinteinen allekirjoitus. Lisäksi sähköinen allekirjoitus on turvallinen ja luotettava, jos se tehdään vahvalla tunnistamisella. Allekirjoituksen voi tehdä sähköisesti kaikissa tilanteissa, mutta rajoituksia sähköiselle allekirjoitukselle määritellään tunnistamisella. Heikolla tunnistamisella ei voida allekirjoittaa sähköisesti kaikkia asiakirjoja, mutta vahvalla tunnistamisella sähköinen allekirjoitus sopii kaikkiin tilanteisiin.

Asiasanat

sähköinen allekirjoitus, sähköinen tunnistaminen, varmenne

Abstract

Author(s)	Type of Publication	Published
Uronen, Maiju	Bacherlor's thesis	2020
	Number of Pages	
	28 pages	

Title of Publication

The legality of the electronic signature

Name of Degree

Bachelor of Business Administration

Name, title and organization of the supervising teacher

Mr Kari Hämeenaho, Senior Lecturer in Law, LAB University of Applied Sciences

Abstract

The purpose of this thesis was to study the legality of an electronic signature. The object of the work was to find out how the legality of an electronic signature is formed and in which situations the electronic signature is legal and valid. In addition, the work explored different forms and methods of electronic signatures and their use cases.

The thesis explored the electronic signature signing process and different forms of electronic authentication. Electronic authentication can be done strongly or weakly and this affects the security of the electronic signature.

The thesis explored the legislation on electronic signatures and the government's preliminary work on the subject. The legislation was limited to Finland, as the purpose was to determine the legality of electronic signatures in Finland. The main sources of work were the Act on Strong Electronic Identification and Electronic Trust Services 617/2009 and Regulation (EU) No 910/2014 of the European Parliament and of the Council. The research method of the thesis was forensic dogmatic, because I studied electronic signature from the point of view of law.

Result of the work is that an electronic signature is legal and as binding as a traditional signature. In addition, an electronic signature is secure and reliable if it is done with strong authentication. The signature can be made electronically in all situations, but the limitations of an electronic signature are defined by authentication level. With weak authentication it is not possible to electronically sign all documents as it is with strong authentication.

Keywords

electronic signature, electronic authentication, certificate

Sisällys

1 Johdanto 5
1.1 Työn tausta 5
1.2 Tavoite ja rajaukset 6
1.2.1 Tutkimuskysymykset 6
1.2.2 Keskeiset käsitteet 6
1.3 Tutkimusmenetelmä 7
1.4 Työn rakenne 8
2 Sähköinen allekirjoitus 9
2.1 Ajantasainen lainsäädäntö 10
2.2 Sähköisen allekirjoituksen lain historia 10
3 Sähköinen allekirjoitus käytännössä 13
3.1 Allekirjoitusprosessi 13
3.2 Sähköisen allekirjoituksen eri muodot 15
3.3 Sähköisen allekirjoituksen turvallisuus 16
3.3.1 Heikko tunnistautuminen 18
3.3.2 Vahva tunnistautuminen 18
3.4 Palveluntarjoajat 20
4 Sähköisen allekirjoituksen lainvoimaisuus eri käyttötilanteissa 21
5 Yhteenveto 23
Lähteet 26

1 Johdanto

Maailma digitalisoituu jatkuvasti ja myös asiakirjojen sähköinen allekirjoitus ja arkistointi lisääntyy. Työt siirtyvät jatkuvasti enemmän etätyöskentelyyn ja ihmiset liikkuvat paljon, jolloin etänä toimiva allekirjoituskin on kätevää. Sähköinen allekirjoitus helpottaa ja nopeuttaa monien dokumenttien allekirjoittamista ja näin ollen myös nopeuttaa asioiden käsittelyä. Ihmisten tietoisuus sähköisestä allekirjoituksesta on kuitenkin hyvin vähäistä, jolloin myös sen käyttö on jäänyt vähemmälle. Suurimmalle osalle ihmisistä kuitenkin sähköiset palvelut ovat jo tuttuja, kuten esimerkiksi verkkokaupat. Tilatessa tuotteita verkkokaupasta tilaaja kuitenkin tunnistautuu sähköisesti ja tilauksessa solmitaan kumpaakin sitova kauppakirja sähköisesti. Ihmiset eivät useinkaan yhdistä tällaista palvelua sähköiseen allekirjoitukseen, vaikka kyseessä onkin sähköisen allekirjoituksen kevyin muoto.

1.1 Työn tausta

Sähköisestä asioinnista ja arkistoinnista on tehty tutkimuksia ja opinnäytetöitä, mutta sähköisestä allekirjoituksesta pelkästään ei ole tehty kovinkaan paljon tutkimuksia, vaikka laki sähköisestä allekirjoituksesta (14/2003) tuli Suomessa voimaan jo vuonna 2003. Lain tarkoituksena on edistää sähköisten allekirjoitusten käyttöä (Laki sähköisistä allekirjoituksista 14/2003, 1 §).

Aihe oli jo alun perin kiinnostava ja ajankohtainen, mutta keväällä 2020 koronakriisin aikaan aihe nousi entistäkin suurempaan rooliin, koska monet yritykset siirtyivät työskentelemään etänä. Sähköisen allekirjoituksen käyttö kasvaa varmasti tämän kriisin aikana ja myös sen jälkeen suuresti. Hallituksen esityksessä vuonna 2009 todettiin sähköisten palveluiden ja sähköisen asioinnin kehityksen olleen hitaampaa kuin oli arvioitu (Hallituksen esitys Eduskunnalle laiksi vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista sekä eräiksi siihen liittyviksi laeiksi 36/2009, 1).

Pohjoisranta Burson-Marstellerin (2019) vuonna 2018 tekemässä kyselytutkimuksessa tutkittiin suomalaisten mielipiteitä liittyen sähköiseen allekirjoitukseen. Kyselyn perusteella suurin osa suomalaisista (64 %) ei pitänyt sähköistä allekirjoitusta laillisesti pätevänä, ellei tunnistusta tehty vahvasti, esimerkiksi pankkitunnuksilla tai mobiilivarmenteella. Kyselyyn vastanneista yli puolet (56 %) piti sähköistä allekirjoitusta vaivattomampana kuin perinteistä allekirjoitusta. Tästä huolimatta vain neljännes vastaajista (25 %) valitsisi sähköisen allekirjoituksen perinteisen allekirjoituksen sijaan. Kyselyn perusteella lain väärä tulkinta hidastaa sähköisen allekirjoituksen käyttämistä, koska harva tietää EU:n eIDAS-asetuksesta, joka säätelee sähköistä allekirjoitusta Suomessa.

1.2 Tavoite ja rajaukset

Opinnäytetyön tavoitteena on selvittää, mistä sähköisen allekirjoituksen lainvoimaisuus muodostuu, sekä missä tilanteissa sähköinen allekirjoitus on lainvoimainen. Työssä tutkitaan sähköisen allekirjoituksen eri muotoja ja niiden eri käyttömahdollisuuksia. Tavoitteena on lisätä tietoutta sähköisestä allekirjoituksesta ja sen lainvoimaisuudesta.

Opinnäytetyössä tutkitaan sähköistä allekirjoitusta yleisellä tasolla, eikä erityisesti yrityksen tai yksityishenkilön näkökulmasta. Työssä perehdytään sähköisen allekirjoituksen lainsäädäntöön ja siihen mitä laki määrittää lainvoimaisuudesta eri tilanteissa. Työssä avataan sähköisen allekirjoituksen tekniikkaa ja eri vaiheita, joita allekirjoitusprosessissa tapahtuu.

Opinnäytetyön teoreettinen viitekehys muodostuu lainsäädännöstä, esitöistä ja tieteellisistä artikkeleista, joissa käsitellään sähköistä allekirjoitusta ja sen lainvoimaisuutta. Työssä tutkitaan sähköisen allekirjoituksen lainvoimaisuutta Suomessa, joten aihe rajataan lainsäädäntöön, mikä koskee Suomea.

1.2.1 Tutkimuskysymykset

Opinnäytetyössä etsitään vastauksia sähköisen allekirjoituksen lainvoimaisuuteen sekä eri muotoihin ja niiden käyttömahdollisuuksiin. Työssä on yksi päätutkimuskysymys ja sen lisäksi kolme apukysymystä.

Työn päätutkimuskysymys on:

- Mistä sähköisen allekirjoituksen lainvoimaisuus muodostuu?

Päätutkimuskysymyksen lisäksi työssä on seuraavia apukysymyksiä:

- Mitä eri sähköisen allekirjoituksen muotoja on?
- Minkälaisiin käyttötarkoituksiin sähköisen allekirjoituksen eri muodot soveltuvat?
- Missä tilanteissa sähköinen allekirjoitus ei ole lainvoimainen?

1.2.2 Keskeiset käsitteet

Opinnäytetyön keskeiset käsitteet ovat seuraavat:

Ensitunnistaminen on tunnistusvälineen hakijan henkilöllisyyden todentamista tunnistusvälineen hankkimisen yhteydessä (Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista 617/2009, 2 §).

Mobiilivarmenne on puhelimen SIM-kortilla sijaitseva tunniste, sähköinen henkilöllisyystodistus (Mobiilivarmenne).

Sähköisellä allekirjoituksella tarkoitetaan sähköisessä muodossa olevaa tietoa, joka on liitetty muuhun sähköisessä muodossa olevaan tietoon ja jota käytetään allekirjoittamiseen ((EU) N:o 910/2014 Euroopan parlamentin ja neuvoston asetus sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta, 3 artikla).

Sähköisellä tunnistamisella tarkoitetaan prosessia, jossa henkilön henkilöllisyys todennetaan sähköisesti ((EU) N:o 910/2014, 3 artikla).

Tunnistuspalvelun tarjoaja on palveluntarjoaja, joka tarjoaa tunnistusvälityspalveluja tai tunnistusvälineitä (Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista 617/2009, 2 §).

Varmenteella tarkoitetaan sähköistä todistusta, joka todentaa henkilöllisyyden sekä sen lisäksi myös voi liittää luottamuspalvelun todentamistiedot luottamuspalvelun käyttäjään ja jota voidaan käyttää vahvassa sähköisessä tunnistamisessa (Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista 617/2009, 2 §).

1.3 Tutkimusmenetelmä

Opinnäytetyön tutkimusmenetelmä on lainoppi eli oikeusdogmatiikka, koska työssä perehdytään lainsäädäntöön ja sen tulkintaan. Oikeusdogmatiikka tulkitsee ja systematisoi voimassa olevaa lainsäädäntöä (Tieteen termipankki 2016). Systematisointi on voimassa olevan lainsäädännön järjestelmällistämistä, jotta tulkinta on ristiriidatonta (Wikisanakirja 2020).

Oikeusdogmatiikka on yksi oikeustieteen tutkimusmenetelmä. Oikeusdogmatiikka perustuu voimassa olevaan lainsäädäntöön ja sen tehtävänä on selvittää voimassa olevan oikeuden sisältö kulloinkin käsiteltävässä oikeusongelmassa. Oikeusdogmatiikka pyrkii antamaan vastauksen kysymykseen, kuinka todellisessa tilanteessa pitäisi toimia voimassa olevan oikeuden mukaan. Oikeusdogmatiikka on oikeusjärjestyksen sääntöjen tutkimista ja erityisesti sen tulkintaa. (Husa, Mutanen & Pohjolainen 2008, 20.)

Oikeustieteessä ei ole objektiivista totuutta vaan se on argumentaatiota eli punnittujen väitteiden ja perustelujen esittämistä (Husa ym. 2008, 13). Työssä hyödynnetään myös laadullisen tutkimuksen menetelmää joiltain osin, jotta aihetta saadaan tutkittua mahdollisimman kokonaisvaltaisesti. Kvalitatiivinen eli laadullinen tutkimus pyrkii tutkimaan kohdetta

mahdollisimman kokonaisvaltaisesti. Kvalitatiivisessa tutkimuksessa pyritään löytämään tai paljastamaan tosiasioita. (Hirsjärvi, Remes & Sajavaara 2009, 161.)

1.4 Työn rakenne

Ensimmäinen luku on johdanto, jossa kerrotaan taustaa työlle. Johdannossa kerrotaan työn tavoitteet ja tutkimuskysymykset, joihin etsitään vastauksia. Toisessa luvussa käsitellään sähköisen allekirjoituksen lainsäädäntöä. Luvussa esitellään ajantasainen lainsäädäntö sekä myös sähköisen allekirjoituksen lain historiaa. Kolmannessa luvussa perehdytään sähköiseen allekirjoitukseen käytännössä. Alaluvuissa tarkastellaan sähköisen allekirjoituksen eri muotoja ja tunnistamista. Lisäksi luvussa esitellään allekirjoitusprosessi ja kerrotaan sähköisen allekirjoituksen turvallisuudesta. Neljäs luku käsittelee sähköisen allekirjoituksen lainvoimaisuutta eri käyttötilanteissa. Luvussa esitellään eri käyttömahdollisuuksia ja vaatimuksia eri laeista. Viidennessä, eli viimeisessä luvussa on yhteenveto ja pohdinta.

2 Sähköinen allekirjoitus

Laissa sähköisistä allekirjoituksista (14/2003) määritelmä sähköiselle allekirjoitukselle 2 §:n mukaan on *sähköisessä muodossa olevaa tietoa, joka on liitetty tai joka loogisesti liittyy muuhun sähköiseen tietoon ja jota käytetään allekirjoittajan henkilöllisyyden todentamisen välineenä* (Laki sähköisistä allekirjoituksista 14/2003, 2 §). Sähköistä allekirjoitusta säätelee Suomessa niin kansallinen kuin myös EU-lainsäädäntö. Näitä lakeja on muutettu vuosien varrella. Sähköisen allekirjoituksen määritelmä ei ole muuttunut lakimuutosten myötä, vaan muutokset koskevat enemmän sähköistä tunnistamista ja varmenteita.

Sähköisellä allekirjoituksella tarkoitetaan yleisesti kaikkea digitaalisesta allekirjoituksesta aina hyväksyttyyn sähköiseen allekirjoitukseen. Sähköisessä allekirjoituksessa on eritasoisia allekirjoitusmuotoja, joita voidaan soveltaa erilaisissa tilanteissa. Nämä eri allekirjoitusmuodot on varmennettu eritasoisesti, jolloin voidaan puhua heikosti ja vahvasti varmennetuista sähköisistä allekirjoituksista. (Multisilta 2019a.)

Lainsäädäntö

Laki sähköisistä allekirjoituksista (14/2003) tuli voimaan Suomessa vuonna 2003. Vaikka laki on jo ollut voimassa lähes kaksikymmentä vuotta, on sähköisen allekirjoituksen käyttöönotto ollut hidasta. Laki sähköisistä allekirjoituksista pyrkii edistämään sähköisen allekirjoituksen käyttöä ja niihin liittyvien tuotteiden ja palveluiden tarjontaa. Lisäksi lain tarkoituksena on edistää sähköisen kaupankäynnin ja sähköisen asioinnin tietosuojaa ja tietoturvaa. (Laki sähköisistä allekirjoituksista 14/2003, 1 §.)

Suomessa sähköistä allekirjoitusta säätelee Euroopan parlamentin ja neuvoston eIDAS-asetus N:o 910/2014, jolla varmistetaan EU:n sisämarkkinoiden asianmukainen toiminta ja pyritään sähköisen tunnistamisen menetelmien ja luottamuspalvelujen tietoturvan riittävän korkeaan tasoon. Tämä asetus koskee jäsenvaltioiden ilmoittamia sähköisen tunnistamisen järjestelmiä ja unioniin sijoittuneita luottamuspalveluiden tarjoajia. ((EU) N:o 910/2014, 1 artikla.)

Sähköiseen allekirjoitukseen vaikuttavat myös muut kansalliset lait, kuten laki sähköisestä asioinnista viranomaistoiminnassa 13/2003, laki väestötietojärjestelmästä ja Digi- ja väestöviraston varmennepalveluista 661/2009 sekä tietosuojalaki 1050/2018. Näiden lisäksi monissa muissa laeissa säädellään sähköisen allekirjoituksen käytöstä.

2.1 Ajantasainen lainsäädäntö

Suomessa ajantasainen lainsäädäntö sähköisestä allekirjoituksesta koostuu kansallisista laeista sekä myös EU:n eIDAS asetuksesta. Kansallisista laeista tärkein sähköistä allekirjoitusta koskeva laki on laki vahvasta sähköisestä tunnistamisesta ja sähköisistä tunnistuspalveluista (617/2009). Tämä laki pitää sisällään säädökset sähköisestä allekirjoituksesta ja sähköisestä tunnistamisesta sekä tunnistuspalveluiden tarjoamisesta.

Hyväksytyllä sähköisellä allekirjoituksella ja käsin kirjoitetulla allekirjoituksella on lainsäädännön (eIDAS) mukaan samanlaiset oikeusvaikutukset. Eli nämä ovat täysin verrattaessa toisiinsa oikeudellisesti. Lisäksi Euroopan parlamentin ja neuvoston direktiivin N:o 910/2014 25 artiklassa sanotaan, että *sähköisen allekirjoituksen oikeusvaikutuksia ja käytettävyyttä todisteena oikeudellisissa menettelyissä ei voida kieltää pelkästään sillä perusteella, että se on sähköisessä muodossa tai ei täytä hyväksyttyjen sähköisten allekirjoitusten vaatimuksia*. Tämä siis tarkoittaa, että sähköinen allekirjoitus on laillisesti hyväksytty tapa allekirjoittaa. Lisäksi sähköisen allekirjoituksen muodolla ei ole väliä vaan kaikki ovat laillisesti yhtä sitovia allekirjoituksia. ((EU) 910/2014, 25 artikla.)

2.2 Sähköisen allekirjoituksen lain historia

Laki sähköisistä allekirjoituksista (14/2003) perustui Euroopan parlamentin ja neuvoston direktiiviin 1999/93/EY. Laki sähköisistä allekirjoituksista kohdistui ainoastaan sähköisiin allekirjoituksiin, joten Suomesta puuttui tuolloin lainsäädäntö, joka kohdistuu sähköiseen tunnistamiseen. Tämä lainsäädännön puuttuminen olikin syy, miksi laki sähköisistä allekirjoituksista kumottiin vuonna 2009. (HE 36/2009, 2.)

Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (617/2009) kumosi lain sähköisistä allekirjoituksista vuonna 2009. Lain 1 §:ssä määritellään, että *laissa säädetään vahvasta sähköisestä tunnistamisesta ja tunnistuspalveluiden tarjoamisesta palveluntarjoajille, yleisölle ja toisille tunnistuspalvelun tarjoajille* (Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista 617/2009, 1 §). Tässä uudessa laissa säädetään sähköisen allekirjoituksen lisäksi sähköisestä tunnistamisesta. Sähköiseen allekirjoitukseen ei uuden lain myötä tullut muutoksia vaan muutokset koskivat sähköistä tunnistamista. (HE 36/2009, 2.)

Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (617/2009) on voimassa oleva laki, mutta tähän on tehty muutoksia vuonna 2016. Lakimuutos oli tarpeellinen, koska Suomen lainsäädäntö tuli saada vastaamaan Euroopan parlamentin ja neuvoston uutta asetusta N:o 910/2014 sähköisestä tunnistamisesta ja sähköisiin

transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla (Hallituksen esitys eduskunnalle laiksi vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain muuttamisesta sekä eräiksi siihen liittyviksi laeiksi 74/2016, 5).

Vuoden 2016 muutokset laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista koskevat kansalaisien osalta tunnistamista. Vahvaa sähköistä tunnistamista ei voida enää vuoden 2019 alusta alkaen varmentaa niin, että esitunnistuksessa on käytetty pelkästään ajokorttia. Muutos tehtiin turvallisuussyistä, koska Suomessa ajokorttia myönnettäessä ei henkilöllisyyttä tarkasta enää viranomainen. Ajokortti ei ole enää todistus henkilöllisyydestä, vaan todistus ajo-oikeudesta. Vahvoja sähköisiä tunnistusvälineitä myönnetään paljon pankeissa. Pankit myöntävät tunnistusvälineet ajokortin perusteella, mutta tämä vaatii myös asiakkaalta lisätietoja. Muutoksen myötä pankit voivat esitunnistamisessa hyödyntää aikaisemman asiakassuhteen tietoja. (HE 74/2016, 6.)

Euroopan parlamentin ja neuvoston direktiivi 1999/93/EY kumottiin uudella N:o 910/2014 asetuksella (eIDAS), tämän uuden asetuksen tarkoitus on parantaa ja laajentaa 1999/93/EY direktiivin säännöksiä. Uuden eIDAS-asetuksen tavoitteena on poistaa esteet, jotka haittaavat jäsenvaltioiden sähköisen tunnistamisen menetelmien käyttöä yli rajojen. Direktiivi 1999/93/EY antoi pohjan uudelle eIDAS-asetukselle, jossa määritellään sähköisestä allekirjoituksesta ja sähköisestä tunnistamisesta. EU:n eIDAS-asetus koskee kaikkia EU:n jäsenvaltioita, jolloin kaikilla on samat säännöksen sähköiselle allekirjoitukselle. ((EU) N:o 910/2014.)

Uusi EU:n maksupalveludirektiivi (PSD2) tuli Suomessa voimaan asteittain vuosien 2018 ja 2019 aikana. PSD2-direktiivin tavoitteena on tehdä verkossa maksamisesta helpompaa ja turvallisempaa Euroopassa. PSD2-direktiivi muutti pankkien toimintaa esimerkiksi niin, että pankkien on mahdollistettava kolmansille palveluntarjoajille pääsy asiakkaan maksutileille. Lisäksi direktiivi pyrkii parantamaan maksamisen turvallisuutta määrittämällä uudet turvallisuusvaatimukset. Säädösten myötä maksaminen vahvalla tunnistamisella muuttui pakolliseksi ja pankkien tunnuslukulistat jäivät pois käytöstä, koska ne eivät täytä enää uuden direktiivin turvallisuusvaatimuksia. (Finanssivalvonta 2019.)

PSD2-direktiivi vahvisti vahvaa sähköistä tunnistamista, koska uusien vaatimusten mukaan henkilö tulee tunnistaa kahden tekijän varmennuksella. Tämä tarkoittaa, että asetuksessa on annettu kolme ehtoa vahvalle tunnistamiselle, joista kahden tulee täyttyä. PSD2-direktiivin (Euroopan parlamentin ja neuvoston direktiivi (EU) 2015/2366 maksupalveluista sisämarkkinoilla, direktiivien 2002/65/EY, 2009/110/EY ja 2013/36/EU ja asetuksen (EU) N:o 1093/2010 muuttamisesta sekä direktiivin 2007/64/EY kumoamisesta, 4 artikla) asettamat ehdot vahvalle tunnistamiselle ovat

- tieto, jotain minkä vain käyttäjä tietää esimerkiksi salasana tai PIN-koodi
- hallussapito, jotain mitä vain käyttäjällä on hallussaan esimerkiksi maksukortti, matkapuhelin tai tunnuslukulaite
- erityinen ominaisuus, jotain mitä käyttäjä on esimerkiksi sormenjälki tai kasvot.

Näistä kolmesta ehdosta tulee kahden täyttyä, jotta henkilö voidaan tunnistaa vahvasti. Vahvaa sähköistä tunnistamista käytetään niin maksutapahtuman yhteydessä kuin myös viranomaisten sähköisissä palveluissa, kuten Kela, poliisi ja verottaja. Vahvan sähköisen tunnistamisen avulla asioinnista ja verkkomaksamisesta tuli turvallisempaa, koska henkilön tulee tunnistautua vahvasti. Direktiivi antaa myös mahdollisuuden tehdä maksuja ilman vahvaa tunnistamista, jos maksu on vähäriskinen, esimerkiksi euromääräisesti pieni ostos. (Finanssivalvonta 2019.)

3 Sähköinen allekirjoitus käytännössä

Sähköisen allekirjoituksen etuja ovat sen nopea ja helppo tapa allekirjoittaa asiakirjoja, ajasta ja paikasta riippumattomuus sekä mahdollisuus säilyttää alkuperäistä allekirjoitettua asiakirjaa sähköisesti. Verrattuna tavalliseen käsin tehtävään allekirjoitukseen sähköinen allekirjoitus on todella nopeampi tapa. Tavallisessa allekirjoituksessa allekirjoitettava dokumentti tulostetaan ensin paperille, sitten lähetetään postilla allekirjoittajalle, joka allekirjoitettuaan jälleen lähettää dokumentin postilla takaisin lähettäjälle. Sähköisellä allekirjoituksella säästetään aikaa, kun dokumenttia ei tarvitse tulostaa ja lähetellä eteenpäin. (Eloluoto 2020.)

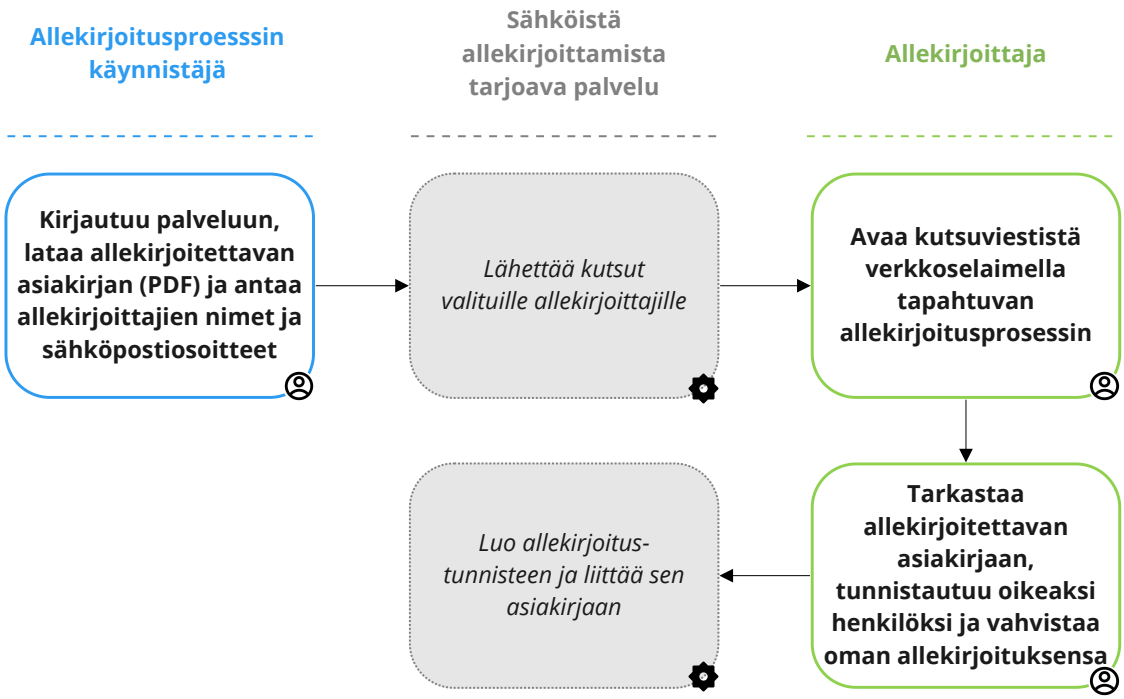
Sähköinen allekirjoitus on myös turvallinen tapa allekirjoittaa dokumentteja. Tavallisessa allekirjoitustilanteessa varmistetaan allekirjoittajan henkilöllisyystodistuksesta, että kyseessä on sama henkilö kuin allekirjoittaja. Sähköisessä allekirjoituksessa tämä hoituu allekirjoituksen yhteydessä, kun henkilö tunnistautuu sähköisesti esimerkiksi pankkitunnuksillaan. Sähköisessä tunnistamisessa ei myöskään tarvitse olla kenenkään ulkopuolisen henkilön tarkistamassa asiaa vaan tunnistautuminen hoituu kokonaan sähköisesti, jolloin henkilöiden ei tarvitse olla samanaikaisesti läsnä vaan allekirjoitus voidaan hoitaa kokonaan etänä. (Digi- ja väestötietovirasto a; Visma.)

Sähköinen allekirjoitus säästää myös paperia ja helpottaa arkistointia, koska allekirjoitettavaa dokumenttia ei tarvitse missään vaiheessa tulostaa paperille. Monet sähköisen allekirjoituksen palveluntarjoajat tarjoavat lisäksi sähköistä arkistointia, johon allekirjoitetut dokumentit saa arkistoitua. (Visma.) Sähköisesti allekirjoitettu ja sähköisesti arkistoitu asiakirja myös säilyy koneellisesti luettavissa, kun asiakirjaa ei tarvitse skannata missään välissä. Koneellisesti luettava asiakirja helpottaa dokumentin arkistoinnissa ja käsittelyssä. Dokumentin sisältöön voidaan esimerkiksi kohdistaa hakuja. (Digi- ja väestötietovirasto a.)

3.1 Allekirjoitusprosessi

Sähköisestä allekirjoitusprosessista on tehty vaivatonta, koska monet palveluntarjoajat ovat kehittäneet ohjelmansa helpottamaan ihmisten allekirjoittamista. Sähköisen allekirjoituksen voi tehdä palveluntarjoajan ohjelmalla tai myös ilman erinäistä ohjelmaa. Palveluntarjoajien ohjelmat ovat luotettava ja helppo tapa hoitaa koko allekirjoitusprosessi. Palveluntarjoajan vastuu määritellään EU:n eIDAS-asetuksen 13 artiklassa. Palveluntarjoaja on vastuussa luonnolliselle henkilölle tai oikeushenkilölle tahallaan tai tuottamuksesta aiheutetusta vahingosta, joka johtuu laissa säädettyjen velvollisuuksien laiminlyönnistä ((EU) 910/2014, 13 artikla).

Allekirjoitusprosessi on hyvin erilainen riippuen sähköisen allekirjoituksen muodosta. Yksinkertaisimmassa muodossa allekirjoitusprosessista jää henkilön tunnistus kokonaan pois, kun taas kehittyneessä ja hyväksytyssä allekirjoituksessa allekirjoittaja tunnistautuu ennen allekirjoittamista. Kuviossa 1 on kuvattu sähköisen allekirjoituksen allekirjoitusprosessi. Palveluntarjoajia allekirjoitusprosessiin on paljon, mutta heidän palvelunsa toimivat samoilla periaatteilla. Palveluun lisätään asiakirja, joka allekirjoitetaan ja varmennetaan.



Kuvio 1. Sähköisen allekirjoituksen allekirjoitusprosessi

Allekirjoitusprosessin käynnistäjä kirjautuu jonkin palveluntarjoajan ohjelmaan esimerkiksi käyttäjätunnuksella ja salasanalla. Ohjelmaan ladataan sähköinen asiakirja, johon allekirjoitukset on tarkoitus saada. Ohjelmaan ilmoitetaan kaikkien allekirjoittajien nimet ja esimerkiksi sähköpostiosoitteet, joihin ohjelma lähettää allekirjoituskutsut. Allekirjoittaja saa sähköpostiin kutsun, jossa on linkki palveluntarjoajan allekirjoitusprosessiin. Allekirjoittaja pääsee tutustumaan asiakirjaan ja tunnistautuu esimerkiksi pankkitunnuksilla oikeaksi henkilöksi sekä allekirjoittaa asiakirjan. Kun henkilö on allekirjoittanut asiakirjan, muodostaa palveluntarjoaja varmenteen, joka liittää henkilön allekirjoituksen allekirjoitettuun asiakirjaan niin, että se takaa allekirjoituksen oikeellisuuden sekä allekirjoitetun sisällön muuttumattomuuden. Kun kaikki pyynnön saaneet henkilöt ovat allekirjoittaneet asiakirjan, lähettää palvelu allekirjoitetun asiakirjan kaikille allekirjoittaneille henkilöille sekä myös allekirjoitusprosessin käynnistäjälle.

3.2 Sähköisen allekirjoituksen eri muodot

Sähköisellä allekirjoituksella on kolme eri tasoa, jotka on määritelty EU:n eIDAS-asetuksessa ((EU) N:o 910/2014). Eri tasoisia allekirjoituksia voidaan käyttää eri käyttötilanteissa. Toiset tilanteet vaativat allekirjoittajan vahvaa tunnistautumista ja toisissa riittää heikompi tunnistautuminen. Sähköisen allekirjoituksen kolme eri tasoa ovat

- sähköinen allekirjoitus
- kehittynyt sähköinen allekirjoitus
- hyväksytty sähköinen allekirjoitus.

Sähköisen allekirjoituksen määritelmä EU:n eIDAS-asetuksen 3 artiklassa on *sähköisessä muodossa olevaa tietoa, joka on liitetty tai joka loogisesti liittyy muuhun sähköisessä muodossa olevaan tietoon ja jota allekirjoittaja käyttää allekirjoittamiseen* ((EU) N:o 910/2014, 3 artikla). Tämä on sähköisen allekirjoituksen kevyin muoto, jossa allekirjoittaja ei tunnistaudu ennen allekirjoitusta.

Kehittynyt sähköinen allekirjoitus on sähköinen allekirjoitus, mikä yksilöi allekirjoittajan ja liittää allekirjoituksen allekirjoittajaan. Kehittynyt sähköinen allekirjoitus on luotu käyttäen sähköisen allekirjoituksen luontitietoja ja se on liitetty muuhun sähköiseen tietoon, kuten esimerkiksi sähköpostiviestiin, siten että tiedon mahdolliset muutokset voidaan havaita. Eli jos sähköistä asiakirjaa muutetaan jälkikäteen, niin aiemmin tehty sähköinen allekirjoitus ei enää täsmää muutetun asiakirjan sisällön kanssa. ((EU) 910/2014, 26 artikla; Kyberturvallisuuskeskus 2020a.) Kehittyneessä sähköisessä allekirjoituksessa allekirjoittaja tunnistautuu ennen allekirjoittamista esimerkiksi pankkitunnuksilla, jolloin voidaan varmentaa, että allekirjoittaja on oikea henkilö.

Hyväksytyn sähköisen allekirjoituksen määritelmä EU:n eIDAS-asetuksen 3 artiklassa on *kehittynyt sähköinen allekirjoitus, joka on luotu hyväksytyllä sähköisen allekirjoituksen luontivälineellä ja joka perustuu sähköisten allekirjoitusten hyväksyttyyn varmenteeseen*. ((EU) 910/2014, 3 artikla.) Hyväksytty allekirjoitus vastaa käsin kirjoitettua allekirjoitusta ((EU) 910/2014, 25 artikla). Hyväksytty sähköinen allekirjoitus on vahvin allekirjoituksen muoto, jossa henkilö tunnistautuu ennen allekirjoittamista esimerkiksi poliisin myöntämällä henkilökortilla.

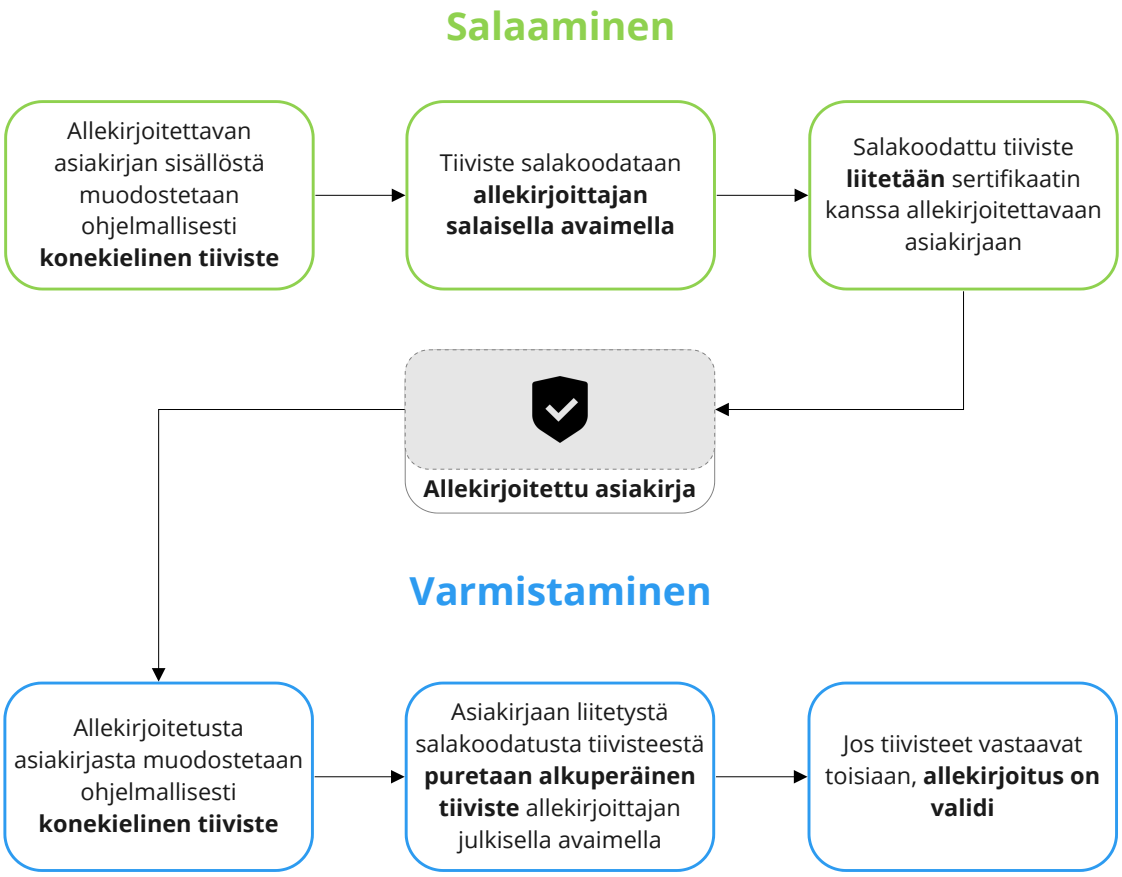
Eroa hyväksytyllä ja kehittyneellä sähköisellä allekirjoituksella on tunnistautumisen vahvuus. Hyväksytyssä sähköisessä allekirjoituksessa vaaditaan hyväksytty varmenne, kun kehittyneessä sähköisessä allekirjoituksessa riittää tunnistamiseen esimerkiksi pankkitunnukset. Digi- ja väestötietovirasto on Suomen ainoa hyväksytyn sähköisen

allekirjoitusvarmenteen tarjoaja. Heidän myöntämiään henkilövarmenteita voidaan käyttää hyväksyttyyn sähköiseen allekirjoitukseen. (Digi- ja väestötietovirasto b.)

3.3 Sähköisen allekirjoituksen turvallisuus

Visma Solutionsin markkinoinnissa työskentelevä Kerttu Multisilta (2019b) kertoo blogissaan, että sähköinen allekirjoitus on käsin kirjoitettua allekirjoitusta huomattavasti turvallisempi, koska se jättää jälkeensä digitaalisen jäljen eli audit trailin. Tämän audit trailin avulla allekirjoitetun asiakirjan alkuperäisyys ja eheys on jälkikäteen todistettavissa. Näin sähköisesti allekirjoitetusta dokumentista pystyy näkemään jälkikäteen, että kuka, missä ja milloin on allekirjoituksen tehnyt. Dokumenttia ei myöskään pysty jälkikäteen muuttamaan huomaamatta. (Visma.)

Kuviossa 2 on kuvattu sähköisen allekirjoituksen salaamisen ja varmentamisen tekninen toteutus. Sähköisen allekirjoituksen salaaminen ja varmentaminen perustuvat julkisen avaimen menetelmään, jolla varmennetaan allekirjoittaja ja dokumentin muuttumattomuus. Sähköisessä allekirjoituksessa allekirjoittaja ei suoranaisesti allekirjoita dokumenttia, vaan allekirjoitus tapahtuu teknisesti esimerkiksi klikkaamalla ohjelman valikosta kohtaa allekirjoita. (Hallituksen esitys eduskunnalle laeiksi sähköisistä allekirjoituksista ja viestintähallinnosta annetun lain 2 §:n muuttamisesta 197/2001, 1.)



Kuvio 2. Sähköisen allekirjoittamisen salaaminen ja varmentaminen

Salaaminen

Kuviossa 2 teknisesti sähköinen allekirjoitus muodostetaan laskemalla tiiviste allekirjoitettavasta dokumentista. Tiiviste saadaan aikaan dokumentista tiivistefunktiolla, joka tiivistää dokumentin sisällön eräänlaiseksi koodiksi. Tiiviste salataan allekirjoittajan yksityisellä avaimella, jolloin syntyy salattu tiiviste. Sertifikaatti pitää sisällään julkisen avaimen, jolloin tämä julkinen avain ja salattu tiiviste liitetään allekirjoitettavaan dokumenttiin. Julkisen avaimen avulla saadaan salattu tiiviste auki. Sertifikaatilla ja salatulla tiivisteellä pystytään jälkikäteen varmistamaan dokumentin muuttumattomuus ja aitous. (HE 197/2001, 1.)

Varmentaminen

Kuviossa 2 on kuvattu myös sähköisen allekirjoituksen varmentaminen. Allekirjoitettu dokumentti voidaan purkaa allekirjoittajan yksityisen avaimen ja julkisen avaimen avulla. Yksityisestä sekä julkisesta avaimesta lasketaan tiivisteet, joita verrataan toisiinsa. Jos nämä tiivisteet vastaavat toisiaan niin allekirjoittaja on varmennettu sekä myös dokumentin sisältö on pysynyt muuttumattomana. (HE 197/2001, 1.)

Allekirjoituksen yksityistä avainta käytetään sähköisen allekirjoituksen tekemiseen ja julkista avainta käytetään sähköisen allekirjoituksen tarkistamiseen. Hyväksytyssä sähköisessä allekirjoituksessa käytetään kumpaakin, yksityistä sekä julkista avainta. (Digi- ja väestötietovirasto b.)

3.3.1 Heikko tunnistautuminen

Heikossa tunnistautumisessa allekirjoittajan henkilöllisyyttä ei varmisteta sähköisesti. Kyseessä on sähköisen allekirjoituksen yksinkertaisin muoto, jossa henkilö allekirjoittaa sähköisen dokumentin esimerkiksi hiiren tai sormen avulla. Allekirjoituksen yhteydessä henkilö ei vahvista henkilöllisyyttään millään virallisella varmenteella. Tämä muoto sopiikin parhaiten esimerkiksi yrityksen sisäisiin allekirjoituksiin ja tilanteisiin, jossa osapuolet tuntevat entuudestaan. (Multisilta 2019a.) Heikkoa tunnistautumista käytetään esimerkiksi verkkokaupoissa ja sosiaalisen median palveluissa, joissa käyttäjän tunnistaminen perustuu esimerkiksi käyttäjätunnukseen ja salasanaan, sekä käyttäjän itse antamiin henkilötietoihin. (HE 74/20016, 2.)

Heikko tunnistautuminen toimii myös tilanteissa, jossa allekirjoituksia tarvitaan eripuolilta maailmaa, sillä kaikkialla maailmassa ei ole käytössä samoja vahvoja tunnistusmenetelmiä kuin Suomessa. Euroopan Unionin alueella sähköistä allekirjoitusta sääntelee EU:n eIDAS-asetus, ja EU:n sisällä voidaan tunnistautua vahvasti. EU:n ulkopuolella ei kaikissa maissa ole samaa vahvaa tunnistautumista, jolla sähköinen allekirjoitus voidaan tehdä, joten silloin sähköisen allekirjoituksen yksinkertaisin muoto sopii allekirjoittamiseen, koska siinä ei tunnistauduta vahvasti. Allekirjoittaminen ilman vahvaa tunnistautumista on juridisesti yhtä sitova kuin vahvasti tunnistautuneella. (Multisilta 2019a.)

3.3.2 Vahva tunnistautuminen

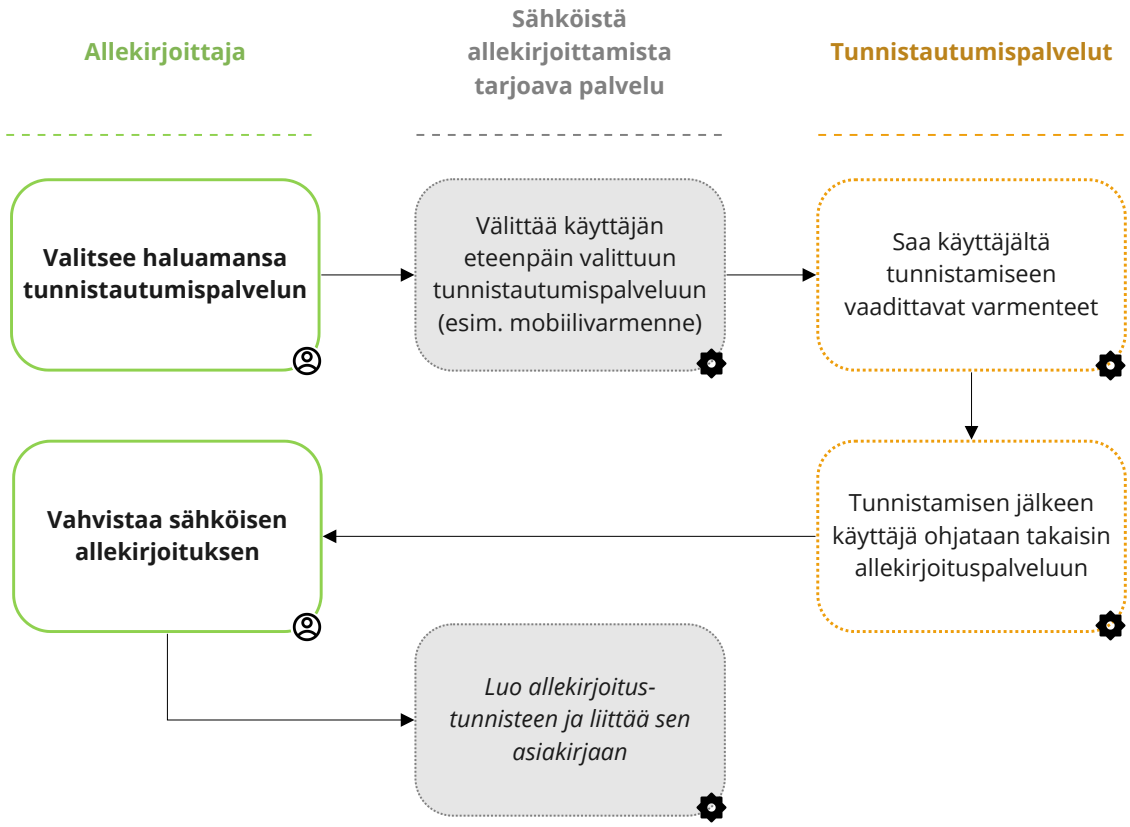
Sähköisen allekirjoituksen muodot kehittynyt ja hyväksytty allekirjoitus vaativat aina vahvan tunnistautumisen. Vahva eli kaksivaiheinen tunnistautuminen on juridisesti sitova tapa allekirjoittaa dokumentteja ((EU) N:o 910/2014, 25 artikla). Vahvassa tunnistautumisessa vahvistetaan henkilöllisyys aina allekirjoituksen yhteydessä.

Vahvalla tunnistautumisella tarkoitetaan henkilön henkilöllisyyden todentamista sähköisesti. Vahvalla tunnistautumisella kuluttajat vahvistavat henkilöllisyytensä eri sähköisissä palveluissa ja sähköisten asiointipalveluiden tarjoajat tunnistavat asiakkaansa. (Kyberturvallisuuskeskus 2020b.)

Vahvoja sähköisiä tunnistuspalveluita ovat

- pankkien verkkopankkitunnukset
- mobiilivarmenne
- kansalaisvarmenne poliisin myöntämällä henkilökortilla.

Kuviossa 3 on kuvattu esimerkki vahvasta sähköisestä tunnistautumisesta. Monessa tapauksessa allekirjoittaja itse valitsee, kuinka hän haluaa tunnistautua allekirjoituksen yhteydessä. Sähköisen allekirjoituksen palveluntarjoaja tarjoaa monia eri tunnistautumisvaihtoehtoja, esimerkiksi pankkien verkkopankkitunnukset tai mobiilivarmenne, joista allekirjoittaja valitsee haluamansa. Allekirjoittajan valinnan perusteella hänet ohjataan tekemään tunnistautuminen valitsemassaan tunnistuspalvelussa, jonka jälkeen hänet ohjataan takaisin sähköisen allekirjoituksen prosessiin, jossa hän vahvistaa sähköisen allekirjoituksensa. Palveluntarjoaja huolehtii allekirjoituksen salaamisesta luomalla allekirjoitustunnisteen ja liittämällä sen asiakirjaan.



Kuvio 3. Vahva sähköinen tunnistautuminen

Vahva tunnistautuminen on rinnastettavissa henkilöllisyystodistuksen esittämiseen. Kuten tavallisessa allekirjoitustilanteessa pyydetään allekirjoittajalta henkilöllisyystodistus, jolla todennetaan allekirjoittajan henkilöllisyys oikeaksi. Vahva tunnistautuminen tekee tämän

saman sähköisessä muodossa, kun henkilöllisyys varmennetaan jollakin tunnistuspalvelulla. (Multisilta 2019a.)

3.4 Palveluntarjoajat

Palveluntarjoajia sähköisille allekirjoituspalveluille on niin kaupallisia toimijoita kuin myös valtiohallinnon yhteisen ratkaisun toimittaja Digi- ja väestötietovirasto. Kaupallisissa allekirjoituspalveluissa tunnistaudutaan esimerkiksi verkkopankkitunnuksilla ja mobiilivarmenteella, kun taas Digi- ja väestötietoviraston ratkaisussa allekirjoittaminen tapahtuu sirullisella organisaatiokortilla ja sirullisella henkilökortilla. (Eloluoto 2020.)

EU:n asetuksessa ((EU) N:o 910/2014) säädellään palveluntarjoajien toimintaa koko EU:n laajuisesti. Palveluntarjoajien tarjoamia luottamuspalveluita ovat asetuksen mukaan sähköinen allekirjoitus, sähköiset leimat, sähköisten allekirjoitusten ja leimojen validointi- ja säilyttämispalvelut, sähköiset aikaleimat, sähköiset rekisteröidyt jakelupalvelut sekä verkkosivujen todentamisen varmennepalvelut. (HE 74/2016, 4.) Lainsäädäntö sääntelee myös tunnistuspalveluiden tarjoamisesta sekä myöntämisestä. Tunnistuspalveluita tarjoavat esimerkiksi pankit ja teleyritykset. Suomessa Liikenne- ja viestintävirasto ylläpitää julkista rekisteriä Suomessa toimivista tunnistuspalveluiden tarjoajista ja niiden palveluista, sekä myös valvoo palveluntarjoajia. Liikenne- ja viestintävirastolle tulee tehdä ilmoitus ennen toiminnan aloittamista ja virasto hyväksyy toiminnan, jos se täyttää laissa annetut vaatimukset. (Kyberturvallisuuskeskus 2020a.)

4 Sähköisen allekirjoituksen lainvoimaisuus eri käyttötilanteissa

Sähköistä allekirjoitusta voidaan käyttää monien eri dokumenttien allekirjoitukseen, kuten esimerkiksi erilaiset sopimukset, pöytäkirjat ja kauppakirjat. EU:n eIDAS-asetuksen 25 artiklan mukaan sähköisen allekirjoituksen oikeusvaikutuksia ja käytettävyyttä todisteena ei voida kieltää pelkästään sen perusteella, että se on sähköisessä muodossa tai että se ei täytä hyväksyttyjen allekirjoitusten vaatimuksia. Näin ollen sähköistä allekirjoitusta voidaan käyttää lähes kaikissa tilanteissa, joissa tavallistakin allekirjoitusta, ellei muussa laissa toisin määrätä. ((EU) N:o 910/2014, 25 artikla.)

Esimerkiksi työsopimuslain (55/2001) 3 §:ssä määritellään suoraan, että työsopimus voidaan tehdä sähköisesti. Työsopimuksen voi allekirjoittaa sähköisesti esimerkiksi pankkitunnuksilla, jolloin allekirjoittajan henkilöllisyys varmistetaan, tai allekirjoituksen voi myös tehdä esimerkiksi sähköpostitse, jossa henkilö piirtää sähköiseen dokumenttiin allekirjoituksensa hiiren avulla. Kumpikin näistä on yhtä lainvoimaisia ja sitovia.

Toisessa esimerkissä laki määrittää vaatimuksia sähköiselle allekirjoitukselle seuraavasti: päätösasiakirja voidaan allekirjoittaa sähköisesti, mutta viranomaisen on allekirjoitettava asiakirja eIDAS-asetuksessa määrittelyllä kehittyneellä sähköisellä allekirjoituksella tai muuten sellaisella tavalla, että asiakirjan alkuperäisyydestä ja eheydestä voidaan varmistua (Laki sähköisestä asioinnista viranomaistoiminnassa 13/2003, 16 §). Alkuperäisyydellä tarkoitetaan allekirjoittajan henkilöllisyyden tunnistamista ja eheydellä asiakirjan muuttumattomuutta (Eloluoto 2020). Päätösasiakirjaa ei voida allekirjoittaa sähköisen allekirjoituksen kevyimmällä muodolla, jossa allekirjoittaja ei tunnistaudu vahvasti ennen allekirjoitusta.

Laissa sähköisestä asioinnista viranomaistoiminnassa (13/2003) säädetään 9 §:ssä, että viranomaiselle voidaan toimittaa hakemuksia ja ilmoituksia kirjallisesti sekä myös sähköisesti. Sähköisessä asiakirjassa voi olla sähköinen allekirjoitus, mutta sitä ei vaadita, jos asiakirjassa on tiedot lähettäjästä eikä asiakirjan alkuperäisyyttä tai eheyttä ole syytä epäillä. (Niemi 2020.)

Maakaaren 2 luvun 1 §:ssä säädetään kiinteistön kaupasta. Kiinteistön kauppakirjat voidaan allekirjoittaa sähköisesti, kun tunnistaudutaan vahvasti ja käytetään Maanmittauslaitoksen kiinteistövaihdannan palvelua. Kiinteistökaupoissa tunnistautumisen voi tehdä esimerkiksi pankkitunnuksilla tai mobiilivarmenteella.

Sähköisen allekirjoituksen kevyintä muotoa on helppo ja nopea käyttää esimerkiksi yhdistystoiminnassa. Hallituksen kokousten pöytäkirjat voidaan allekirjoittaa sähköisesti. Yhdistysten pöytäkirjoille ei ole laissa määrätty tiettyjä määrämuotoja, joten nämä voidaan tehdä

ja allekirjoittaa sähköisesti. Tämä myös helpottaa pöytäkirjojen arkistointia sähköisesti, kun ne ovat valmiiksi sähköisessä muodossa.

Rajoitukset

Hyväksyttyä tai kehittynyttä sähköistä allekirjoitusta ei voida tehdä, jos allekirjoittajalla ei ole pankkitunnuksia, mobiilivarmennetta tai henkilökorttia. Sähköisen allekirjoituksen yksinkertaisimmassa muodossa ei tarvitse tunnistautua, joten allekirjoitus onnistuu myös ilman vahvaa tunnistamista. Sähköisen allekirjoituksen yksinkertaisimmassa muodossa allekirjoittajaa ei tunnisteta ja varmenneta millään tavoin, joten tämä allekirjoitusmuoto ei sovi kaikkiin tilanteisiin.

Hyväksytyn sähköisen allekirjoituksen käyttö on Suomessa hyvin vähäistä ja sitä vaaditaankin vain terveydenhuollossa. Esimerkiksi sosiaali- ja terveyspalveluissa potilaan lääkemääräykset toimitetaan sähköisesti. Nämä voi allekirjoittaa ainoastaan hyväksytyllä sähköisellä allekirjoituksella. (Visma 2019.) Suomessa yleisesti käytetään kehittynyttä sähköistä allekirjoitusta asiakirjojen allekirjoittamiseen. Kehittyneessä allekirjoituksessa tunnistaudutaan pankkitunnuksilla, henkilökortilla tai mobiilivarmenteella. Kehittynyttä sähköistä allekirjoitusta voi käyttää lähes joka tilanteessa, mutta terveydenhuollossa tulee käyttää joissakin tilanteissa hyväksyttyä sähköistä allekirjoitusta. (Heinola.)

Rajoituksia sähköiselle allekirjoitukselle on hyvin vähän, sillä kaikki asiakirjat pystytään pitkälti luomaan sekä allekirjoittamaan sähköisesti, joissakin tapauksissa tulee kuitenkin käyttää erillistä sähköistä palvelua, esimerkiksi kiinteistökaupoissa. Rajoituksia sähköiselle allekirjoitukselle syntyy eri käyttötilanteissa, joissa vaaditaan eri tasoisia tunnistamisia. Joissakin tilanteissa vaaditaan allekirjoittajalta vahvaa tunnistamista, jotta voidaan olla varmoja allekirjoittajan henkilöllisyydestä.

5 Yhteenveto

Opinnäytetyön tarkoituksena oli selvittää, mistä sähköisen allekirjoituksen lainvoimaisuus muodostuu ja missä tilanteissa sähköinen allekirjoitus on lainvoimainen. Lisäksi työssä tutkittiin sähköisen allekirjoituksen eri muotoja ja niiden käyttömahdollisuuksia. Työssä tutustuttiin kansalliseen ja EU:n lainsäädäntöön, jossa määritellään sähköisestä allekirjoituksesta. Lainsäädännön lisäksi opinnäytetyössä tutustuttiin sähköisen allekirjoituksen palveluntarjoajiin ja erilaisiin artikkeleihin. Kirjallisuutta työssä en pystynyt hyödyntämään, koska sähköisestä allekirjoituksesta ei löydy ajantasaista kirjallisuutta.

Opinnäytetyötä aloittaessa sähköinen allekirjoitus oli monille ehkä hiukan vieras käsite, mutta moni on varmasti tutustunut sähköiseen allekirjoitukseen vuoden 2020 aikana. Koronan aikana monet siirtyivät etätöihin, jolloin myös sähköisestä allekirjoituksesta tuli monille arkipäivää. Etätöiden myötä sähköisestä allekirjoituksesta tuli monille tuttu ja tämä oli varmasti myös sysäys sähköisen allekirjoituksen käyttöönotolle monissa yrityksissä.

Sähköisen allekirjoituksen lainvoimaisuus muodostuu pitkälti EU:n asetuksesta (eIDAS), jonka perusteella on säädetty Suomen kansallinen lainsäädäntö sähköisestä allekirjoituksesta. Teknisesti sähköisen allekirjoituksen lainvoimaisuus muodostuu eri tasoisesta tunnistamisesta allekirjoitusta tehdessä. Sähköinen allekirjoitus on yhtä lailla lainvoimainen kuin myös perinteinen kynällä paperille tehty allekirjoitus. Vaikka sähköisessä allekirjoituksessa on kolme eri muotoa, niin kaikki näistä ovat lainvoimaisia ja sitovia.

Sähköisen allekirjoituksen eri muotoja käytetään eri käyttötilanteissa, sillä henkilön tunnistautuminen on eri tasoista. Tilanteissa, joissa täytyy olla täysin varma allekirjoittajan henkilöllisyydestä, ei voida käyttää sähköisen allekirjoituksen yksinkertaisinta muotoa, koska tässä allekirjoittajan henkilöllisyyttä ei varmenneta. Hyväksytyllä sähköisellä allekirjoituksella pystyy laillisesti allekirjoittamaan kaiken sähköisesti, koska tässä allekirjoituksen muodossa allekirjoittajan henkilöllisyys on varmennettu vahvasti ja lisäksi allekirjoitus on tehty hyväksytyllä varmenteella. Hyväksyttyä sähköistä allekirjoitusta vaaditaan Suomessa vain harvoissa tapauksissa, kuten esimerkiksi terveydenhuollossa terveydenhuollon ammattilaisilta.

Yleisempi ja myös riittävä sähköisen allekirjoituksen muoto on kehittynyt sähköinen allekirjoitus, jossa tunnistatumiseen riittää esimerkiksi pankkitunnukset. Suomessa lähes kaikki vahvalla sähköisellä tunnistamisella tehdyt allekirjoitukset ovat kehittyneitä sähköisiä allekirjoituksia. Tämä on Suomessa yleinen ja turvallinen tapa tehdä sähköisiä allekirjoituksia.

Tunnistuspalveluidentarjoajia ovat esimerkiksi pankit, jotka tarjoavat pankkitunnuksia asiakkailleen. Meillä Suomessa on luotettava pankkijärjestelmä ja ihmiset pitävät

pankkitunnuksia luotettavana tapana tunnistautua palveluissa. Tämä vahvistaa myös sähköisen allekirjoituksen luotettavuutta, kun allekirjoituksen yhteydessä tunnistaudutaan pankkitunnuksilla. On myös tilanteita, joissa esimerkiksi yrityksen henkilökunta ei halua käyttää omia henkilökohtaisia pankkitunnuksiaan työasioiden hoitamiseen, kuten sähköiseen allekirjoitukseen. Tavallisessa allekirjoituksessa henkilö kuitenkin henkilökohtaisesti allekirjoittaa asiakirjan, joka on lain näkökulmasta sama, kuin henkilö olisi allekirjoittanut asiakirjan sähköisesti. Työnantaja voi ratkaista ongelman esimerkiksi hakemalla kaikille työntekijöilleen mobiilivarmenteen, joilla työntekijät voivat asioida sähköisesti. Tämä mobiilivarmenne voidaan liittää esimerkiksi työntekijöiden työpuhelinnumeroon, jolloin työntekijät voivat käyttää mobiilivarmennetta töissä.

Sähköisen allekirjoituksen rajoituksia ei lain puolesta ole, mutta esimerkiksi ikäihmisille sähköinen allekirjoitus ei ole välttämättä helppoa tehdä. Jos henkilöllä ei ole osaamista sähköisistä palveluista, niin voi myös sähköinen allekirjoitus olla liian vaativaa. Lisäksi rajoituksena vahvalle sähköiselle allekirjoitukselle on se, että henkilöllä ei ole pankkitunnuksia, mobiilivarmennetta tai henkilökorttia. Ilman vahvaa tunnistautumista ei voi monia sähköisiä allekirjoituksia tehdä, koska usein allekirjoituksen yhteydessä vaaditaan vahvaa tunnistautumista. Sähköisen allekirjoituksen ilman vahvaa tunnistamista voi tehdä myös ilman pankkitunnuksia, mobiilivarmennetta tai henkilökortti, mutta näissä allekirjoittajaa ei tunnisteta, jolloin tämä ei sovi joka tilanteeseen. Sähköisen allekirjoituksen rinnalla olisikin hyvä toistaiseksi säilyttää perinteinen allekirjoituksen muoto, jotta kaikki ihmiset pystyisivät allekirjoituksia pätevästi tekemään.

Sähköisen allekirjoituksen hyötyjä on sen turvallisuus ja jäljitettävyys jälkikäteen. Sähköisessä allekirjoituksessa käytetään vahvaa sähköistä tunnistamista, jonka ansiosta allekirjoittaja voidaan luotettavasti tunnistaa oikeaksi henkilöksi. Vahvassa tunnistamisessa henkilön tulee tunnistautua esimerkiksi pankkitunnuksilla, joka on esimerkiksi pelkkää henkilötunnusta luotettavampi tapa tunnistautua. Henkilötunnus on helposti saatavissa monille identiteettivarkaille, toisin kuin pankkitunnukset, joihin nykyään vaaditaan uuden EU:n maksupalveludirektiivin (PSD2) myötä tietoturvallisempia tapoja kuin ennen. Vahvalla tunnistamisella tehty allekirjoitus pystytään myös jälkikäteen tarkistamaan, ettei dokumenttiin ole tehty muutoksia sekä nähdään ketkä kaikki ovat sähköisesti allekirjoittaneet dokumentin. Vahvaa sähköistä tunnistamista tullaan varmasti hyödyntämään tulevaisuudessa enemmänkin, koska se on turvallisempi tapa tunnistaa henkilö kuin pelkkä henkilötunnus.

Oma oppiminen

Opinnäytetyön aikana olen perehtynyt sähköisen allekirjoituksen lainsäädäntöön ja moniin artikkeleihin, joista opin lähdekritiikkiä ja tiedon analysoimista. Työni alussa tiesin

sähköisestä allekirjoituksesta hyvin vähän, vaikka olin itse kirjoittanut muutamia asiakirjoja jo sähköisesti. Työn edetessä oli hienoa huomata oma oppiminen aiheesta, kuten esimerkiksi, että sähköisiä allekirjoituksia voi tehdä todella monella eri tavalla. Opinnäytetyö opetti minulle ajanhallintaa, koska kirjoitin työni kokonaan työn ohella, jolloin vapaa-aika tuli suunnitella niin, että työ edistyy.

Ymmärrän paremmin ihmisten ennakkoluuloja sähköistä allekirjoitusta kohtaan, työn ansioista itse tiedän nyt sähköisen allekirjoituksen lainvoimaisuuden ja turvallisuuden. Tietoa sähköisestä allekirjoituksesta olisi hyvä tuoda ihmisten tietoisuuteen, jotta ihmiset luottaisivat prosessiin ja uskaltaisivat ottaa sähköisen allekirjoituksen käyttöön, koska sähköinen allekirjoitus on nopeampi ja luotettavampi tapa allekirjoittaa dokumentteja, kuin tavallinen käsin tehtävä allekirjoitus.

Opinnäytetyön kirjoittaminen oli itselle pitkä prosessi. Aiheenvalintaa hiottiin pitkään ja lopulta aihe saatiin muodostumaan lainsäädännön ympärille. Aiheena sähköinen allekirjoitus kiinnosti itseä, mutta tiesin aiheesta hyvin vähän. Opinnäytetyön alku tuntui siis hyvin haastavalta, sillä aihe sekä tutkimusmenetelmä olivat itselle vieraita. Työn edetessä tutustuin lainsäädäntöön sekä moniin artikkeleihin, joista aiheen teoreettinen viitekehys muodostui. Työn rajaaminen piti muistaa koko työn ajan, koska aihe lähti hyvin helposti leviämään liian laajaksi.

Sähköisestä allekirjoituksesta saa tehtyä monia opinnäytetöitä monesta eri näkökulmasta. Aiheesta on tehty hyvin vähän opinnäytetöitä, joten aiheena tämä on loistava ja tarpeellinen. Oma työni aiheesta oli hyvin yleisellä tasolla, jossa ei perehdytty syvemmin aiheeseen, vaan tutkittiin eri lainsäädäntöjä ja niiden vaikutuksia sähköiseen allekirjoitukseen. Aiheeseen voi perehtyä hyvin monelta eri suunnalta, kuten esimerkiksi yrityksen kannalta tai yksityishenkilön kannalta, näin aiheesta saa kirjoitettua monia erilaisia opinnäytetöitä. Ajankohtainen opinnäytetyön aihe on myös vahva sähköinen tunnistaminen, koska tämän käyttö tulee varmasti tulevaisuudessa kasvamaan.

Lähteet

Digi- ja väestötietovirasto a. Sähköisen allekirjoituksen hyödyt. Viitattu 31.10.2020. Saatavissa https://dvv.fi/sahkoisen-allekirjoituksen-hyodyt

Digi- ja väestötietovirasto b. Hyväksytty varmenne. Viitattu 30.10.2020. Saatavissa https://dvv.fi/hyvaksytty-varmenne

Eloluoto, H. 2020. Sähköinen allekirjoitus – nopea ja luotettava tapa varmentaa asiakirjoja. Viitattu 7.10.2020. Saatavissa https://www.suomidigi.fi/artikkelit/sahkoinen-allekirjoitus-nopea-ja-luotettava-tapa-varmentaa-asiakirjoja

(EU) 2015/2366 Euroopan parlamentin ja neuvoston direktiivi maksupalveluista sisämarkkinoilla, direktiivien 2002/65/EY, 2009/110/EY ja 2013/36/EU ja asetuksen (EU) N:o 1093/2010 muuttamisesta sekä direktiivin 2007/64/EY kumoamisesta. Saatavissa https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A32015L2366

(EU) N:o 910/2014 Euroopan parlamentin ja neuvoston asetus sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta. Saatavissa https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A32014R0910

Finanssivalvonta 2019. PSD2 muutti maksamista. Viitattu 11.11.2020. Saatavissa https://www.finanssivalvonta.fi/kuluttajansuoja/kysymyksia-ja-vastauksia/maksupalvelut/psd2--toinen-maksupalveludirektiivi/

HE 36/2009 Hallituksen esitys Eduskunnalle laiksi vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista sekä eräiksi siihen liittyviksi laeiksi. Saatavissa https://www.finlex.fi/fi/esitykset/he/2009/20090036

HE 74/2016 Hallituksen esitys eduskunnalle laiksi vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain muuttamisesta sekä eräiksi siihen liittyviksi laeiksi. Saatavissa https://finlex.fi/fi/esitykset/he/2016/20160074

HE 197/2001 Hallituksen esitys eduskunnalle laeiksi sähköisistä allekirjoituksista ja viestintähallinnosta annetun lain 2 §:n muuttamisesta. Saatavissa https://www.finlex.fi/fi/esitykset/he/2001/20010197

Heinola, J. Canon. Kuinka hyödyntää sähköistä allekirjoitusta? Viitattu 12.11.2020. Saatavissa https://www.canon.fi/business/insights/articles/kuinka-hyodyntaa-sahkoista-allekirjoitusta/

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2009. Tutki ja kirjoita. 15 uud. p. Helsinki: Tammi.

Husa, J., Mutanen, A. & Pohjolainen, T. 2008. Kirjoitetaan juridiikkaa. 2. uud. p. Helsinki: Talentum.

Kyberturvallisuuskeskus 2020a. Sähköinen allekirjoitus ja muut eIDAS-palvelut. Viitattu 5.10.2020. Saatavissa https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/sahkoinen-allekirjoitus-ja-muut-eidas-palvelut

Kyberturvallisuuskeskus 2020b. Sähköinen tunnistaminen. Viitattu 5.10.2020. Saatavissa https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/sahkoinen-tunnistaminen

Laki sähköisestä asioinnista viranomaistoiminnassa 24.1.2003/13. Saatavissa https://www.finlex.fi/fi/laki/ajantasa/2003/20030013

Laki sähköisistä allekirjoituksista 14/2003. Saatavissa https://www.finlex.fi/fi/laki/alkup/2003/20030014

Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista 7.8.2009/617. Saatavissa https://www.finlex.fi/fi/laki/ajantasa/2009/20090617

Maakaari 12.4.1995/540. Saatavissa https://finlex.fi/fi/laki/ajantasa/1995/19950540

Mobiilivarmenne. Mikä ihmeen mobiilivarmenne? Viitattu 8.10.2020. Saatavissa https://mobiilivarmenne.fi/2017/10/23/mika-ihmeen-mobiilivarmenne/

Multisilta, K. 2019a. Visma. Sähköinen tunnistautuminen: Kevyen ja vahvan tunnistautumisen lyhyt oppimäärä. Blogi 26.9.2019. Viitattu 31.10.2020. Saatavissa https://vismasign.fi/blog/sahkoinen-tunnistautuminen/

Multisilta, K. 2019b. Visma. Sähköisen allekirjoituksen turvallisuus – Digitaalinen jälki ei valehtele. Blogi 21.11.2019. Viitattu 31.10.2020. Saatavissa https://vismasign.fi/blog/sahkoisen-allekirjoituksen-turvallisuus/

Niemi, K. 2020. Sähköisistä allekirjoituksista. Maanmittauslaitos. Viitattu 7.11.2020. Saatavissa https://www.maanmittauslaitos.fi/sites/maanmittauslaitos.fi/files/attachments/2020/04/Sähköinen%20allekirjoittaminen_Niemi.pdf

Pohjoisranta Burson-Marsteller 2019. Sähköinen allekirjoitus leviää Suomessa hitaasti, koska valtaosa tulkitsee lakia väärin. Viitattu 3.10.2020. Saatavissa https://news.cision.com/fi/pohjoisranta-bcw-oy/r/sahkoinen-allekirjoitus-leviaa-suomessa-hitaasti--koska-valtaosa-tulkitsee-lakia-vaarin,c2741134

Tieteen termipankki 2016. Oikeustiede. Viitattu 14.11.2020. Saatavissa https://tieteentermipankki.fi/wiki/Oikeustiede:oikeustieteellinen_tutkimus/laajempi_kuvaus

Työsopimuslaki 26.1.2001/55. Saatavissa https://www.finlex.fi/fi/laki/ajantasa/2001/20010055

Visma. Sähköinen allekirjoittaminen. Mikä on sähköinen allekirjoitus? Ohjeet ja oppaat. Viitattu 4.10.2020. Saatavissa https://vismasign.fi/ohjeet/mika-on-sahkoinen-allekirjoitus/

Visma 2019. Usein kysytyt kysymykset sähköisestä allekirjoittamisesta. Viitattu 3.10.2020. Saatavissa https://vismasign.fi/blog/usein-kysytyt-kysymykset/

Wikisanakirja 2020. Systematisoida. Viitattu 14.11.2020. Saatavissa https://fi.wiktionary.org/wiki/systematisoida