LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

Opas: Digitaalinen maksaminen 2017

Vainikka, Kasper

LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

Opas: Digitaalinen maksaminen 2017

Kasper Vainikka
Liiketalouden koulutusohjelma
Opinnäytetyö
Toukokuu, 2017

Laurea-ammattikorkeakoulu **Tiivistelmä**
Liiketalouden koulutusohjelma
Tradenomi (AMK)

Kasper Vainikka

Opas: Digitaalinen maksaminen 2017

Vuosi 2017 Sivumäärä 58

Opinnäytetyön tavoitteena on tuottaa Turbiini yrityskiihdyttämölle opas, joka kuvaa digitaalisen maksamisen markkinaa Suomessa ja siihen vaikuttavia muutoksia. Työ on tehty kokoamalla digitaalisen maksamisen tietopaketti, jonka pohjalta on muodostettu opas. Opas on lähtökohtaisesti kirjoitettu henkilölle, joka suunnittelee liiketoimintaa maksamisen alalle. Opinnäytetyöhön ja oppaaseen on valikoitunut aiheita, jotka vaikuttavat tällä hetkellä käynnissä olevassa pankkiasioinnin murroksessa ja finanssialan sääntelyn kehityksessä.

Maksamisen markkinaa ovat viime vuosien aikana muokanneet esimerkiksi teknologian kehitys, ihmisten kulutuskäyttäytymisen muutos ja sääntelyn kehitys. Teknologian kehityksen myötä yrityksillä on mahdollisuus hyödyntää tietotekniikkaa helppokäyttöisten etäpalveluiden kehittämisessä. Uusien palveluiden myötä kuluttajakäyttäytyminen on muuttunut siten, että digipalveluiden tarve ja suosio on kasvanut. Kysyntään on vastattu kehittämällä uudenlaisia digipalveluita ja viime vuosien aikana myös mobiilimaksaminen on kasvattanut suosiotaan. Erilaisten digipalveluiden lisääntyessä Euroopan komissio on reagoinut muuttuneeseen markkinatilanteeseen säätämällä uuden maksupalveludirektiivin, jonka tavoitteena on mm. maksupalveluiden tarjonnan lisääntyminen ja turvallisemmat maksuratkaisut.

Opinnnäytetyön tietoperustana käytän erilaisia maksamisen markkinalla toimivien tahojen julkaisuja ja selvityksiä. Finanssialan jatkuvasta kehityksestä johtuen olen käyttänyt lähteinäni viime vuosien aikana julkaistuja teoksia. Digitaalisen maksamisen markkinaa rajatakseni olen käyttänyt maantieteellistä rajausta ja keskityn työssäni pääosin Suomessa käytössä oleviin maksamisen ratkaisuihin sekä Suomen lainsäädännön muutoksiin. Opinnäytetyön lopputuotoksena oleva opas on aloittelevalle yrittäjälle monipuolinen tietolähde, joka auttaa käsittämään tekijöitä, jotka liittyvät maksupalveluihin ja niiden toimintaan.

Asiasanat: Digitaalinen maksaminen, Maksamisen turvallisuus, Mobiilimaksaminen, Maksupalveludirektiivi, Biometriikka

Laurea University of Applied Sciences
Degree Programme in business Administration
Bachelor's Thesis

Abstract

Kasper Vainikka

A Guide Book: Digital Payments 2017

Year 2017 Pages 58

The main objective of this Bachelor's degree thesis was to create a guide book for Turbiini start-up accelerator about the payment industry. The guide will cover payment solutions that are currently available on the market and it will also explain forthcoming changes and trends that will have an impact on the industry. The guide is made by examining future main trends of the payment industry and generating brief texts from the wider report to the guide book.

The payment industry is under changes that are caused by for example changes in regulation, changes in customer behaviour and the development of technology. As a result of this, corporates and banks have a possibility to create entirely new and scalable digital services, which can improve their customer satisfaction. In banking, customer behaviour has shifted towards digital solutions and they have become very popular. Along with the trend few businesses have also established payment solutions for mobile devices. To keep up with the developing industry, regulators have introduced a revised payment service directive. The new directive aims to more secure and competitive payment industry and also takes new digital solutions and technical development into account.

The main sources for the thesis are research studies and white papers published by bodies involved in the payment industry. Because of the rapid changes in the industry, there has been used only recently published sources in the making of the thesis. In the market research there has been used geographical boundaries and focused on payment solutions available in Finland. As a result of the thesis, the composed guide book offers a good source of information related to payment solutions, future payment trends and the development of regulation.

Keywords: Digital payments, Payment security, Second Payment Service Directive, Mobile payments, Biometrics

Laki-, asetus- ja direktiiviluettelo

L617/2009. Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista.

Uusi maksupalveludirektiivi EU 2015/2366

Lyhennelmäluettelo

Euroopan keskuspankki, European Central Bank	EKP, ECB
Euroopan Pankkiviranomainen, European Bank Authority	EPV, EBA
Euroopan talousalue	ETA
Euroopan Unioni	EU
Regulatory technical Standards	RTS
Uusi maksupalveludirektiivi, Second Payment Service Directive	PSD2

Sisällys

1 Johdanto

Tämä on Laurea ammattikorkeakoulun tradenomikoulutuksen opinnäytetyö, joka on tehty yhteistyössä Turbiini yrityskiihdyttämön kanssa. Työn tarkoituksena on syventyä digitaalisen maksamisen markkinaan ja sen lähiaikojen kehitykseen pääsääntöisesti Suomessa. Euroopan Komissio on säätänyt uuden maksupalveludirektiivin, joka vaikuttaa maksamisen markkinoihin merkittävästi. Se muodostaa uusia liiketoimintamahdollisuuksia ja mahdollisesti muuttaa finanssialan perinteistä toimintaa. Työssä digitaalinen maksaminen rajataan koskemaan muita maksamisen tapoja kuin myymälöissä tapahtuvia käteis- tai maksukorttimaksuja. Termi sisältää maksukorteilla tapahtuvan verkkomaksamisen, mobiilimaksamisen, verkkopankissa maksamisen sekä kryptovaluutoilla (esimerkiksi Bitcoin) maksamisen.

Aiheen ajankohtaisuudesta johtuen työssä käytetään lähteinä suurimmaksi osaksi alan tutkimuksia sekä virkamiesten kirjoittamia selvityksiä ja raportteja. Kirjallisia lähteitä aiheesta ei ole laajasti vielä saatavilla. Finanssialan lähiaikojen muutokset tekevät aiheesta erittäin kiinnostavan.

Opinnäytetyö koostuu markkinaselvityksestä sekä oppaasta, joka on tehty Turbiini yrityskiihdyttämölle. Turbiini on Vantaalla sijaitseva yrityskiihdyttämö, jonka tavoitteena on tukea aloittavia Start-up yrityksiä. Turbiini tekee tiivistä yhteistyötä muiden pääkaupunkiseudulla toimivien yrityskiihdyttämöiden kanssa ja sen tavoitteena on auttaa yrittäjiä muodostamaan liikeideoista liiketoimintaa. Oppaan tarkoituksena on tarjota Turbiinille tiivis opas digitaalisesta maksamisesta ja siihen vaikuttavista tekijöistä. Opas on tehty kohderyhmälle, joka ajattelee liiketoiminnan rakentamista maksupalvelun tai jonkin muun finanssipalvelun muodossa. Oppaan sisältö ja aihealueet eivät ole kaikenkattavia vaan siihen on valikoitu aiheita, jotka ovat aloittelevan yrittäjän kannalta kaikkein olennaisimpia lähitulevaisuuden maksamisessa.

Opinnäytetyön tiedonkeruuvaiheessa on tehty taustahaastatteluja sekä vierailtu alan tapahtumissa. Haastateltavina ovat olleet Terhi Wathen Finanssivalvonnasta sekä Otso Manninen Suomen Pankista. Lisäksi tietoa on saatu keskusteluista alan asiantuntijoiden kanssa esimerkiksi maksamisen kyberturvallisuus-tapahtumassa. Kiitos vielä erikseen jokaiselle haastateltavalle tai muuten apua tarjonneelle taholle.

2 Taustaa

Ihmiskunnan historiassa on tehty kauppaa aikojen alusta lähtien. Yksinkertaisin kaupan muoto on ollut se, kun vaihdantaa on tehty kahden eri hyödykkeen, esimerkiksi riisin ja kankaan välillä. Jotta vaihdanta olisi helpompaa, on kehitetty rahaa, jonka avulla on voitu verrata kahden eri hyödykkeen arvoa. Rahana on historian aikana käytetty esimerkiksi arvometallista tehtyjä kolikoita, vekseleitä ja paperirahoja. Hyödykkeiden arvoa mittaava raha on mahdollistanut sujuvamman kaupankäynnin. (Herrmann 2013, 96 – 106.) Nykyään kaupankäynnissä maksaminen tapahtuu joko käteisrahan tai pankkitilillä olevan sähköisen rahan avulla. Pankkitilillä olevaa rahaa voi käyttää maksukorteilla, joita ovat sekä luotto- että pankkikortit. Korttimaksaminen rantautui Suomeen 1960-luvulla ja se on kehittynyt luottokunnan sekä pankkien ohjauksessa yhdeksi nykypäivän suosituimmista maksutavoista. Verkkokaupan yleistymisen myötä korttimaksaminen on levinnyt myös etäkaupan maksutavaksi. (Sommar 2011.) 2000-luvulla älypuhelinten kehityksen myötä myös maksamisen ratkaisut ovat siirtyneet mobiililaitteisiin. Suorituskykyiset tietoliikenneyhteydet, korttimaksaminen sekä pankkien kehittyneet digipalvelut ovat viime vuosien aikana vähentäneet käteisen rahan käyttöä. Uusien maksutapojen yleistyessä myös niitä koskeva lainsäädäntö kehittyy.

Uuden sääntelyn myötä maksamisen tavat voivat olla suurten muutosten edessä. Perinteisesti asiakkaiden tilejä hallinoivat pankit ovat olleet ainoa taho, jotka ovat voineet tarjota ihmisten henkilökohtaiseen taloudenhoitoon ja maksamiseen liittyviä palveluita. Perinteistä huolimatta alalle on 2000- ja etenkin 2010-luvulla synynyt erilaisia ”kolmannen sektorin” maksunvälittäjiä, jotka tällä hetkellä mahdollistavat transaktioiden tekemisen ilman luottokortteja. Tällaisista toimijoista esimerkkeinä toimii Trustly Ruotsissa, Sofort Saksassa ja iDeal Alankomaissa. Nämä kolmannen sektorin maksunvälittäjät pystyvät tarjoamaan uusia, jopa mullistavia palveluita, mutta myös keräämään mittavia määriä arkaluonteisia henkilötietoja, tarjoamaan uuden tavan rahanpesuun, terrorismin rahoittamiseen tai muuhun väärinkäyttöön. Koska kolmannen sektorin maksupalvelutarjoajat kantavat suurta vastuuta ja riskiä asiakkaidensa henkilötiedoista ja transaktioiden laillisuudesta, markkinoille halutaan selvemmät säännöt ja toimintatavat. Euroopan Unionin (EU) komissio on säätänyt uuden maksupalveludirektiivin, jonka myötä myös kolmannen sektorin maksupalvelutarjoajien laillinen asema sekä sen tuomat velvollisuudet selventyvät. EU:n jäsenmaiden pitää toimeenpanna uusi direktiivi paikalliseen lainsäädäntöön viimeistään tammikuussa 2018. (Valcke & Vandezande & Van De Velde 2015.)

Uuden maksupalveludirektiivin käyttöönoton jälkeen mahdollisuudet uudentyyppisille tilimaksamiseen perustuville maksamisen ratkaisuille ovat olemassa. Teknologian ja maksupalveluiden viimeaikojen kehitys on antanut suuntaa tulevalle: Danske Bankin Mobilepay toi ensimmäisenä Suomeen kuluttajien välisen mobiilimaksamisen. Mobilepayn vanavedessä myös OP:n

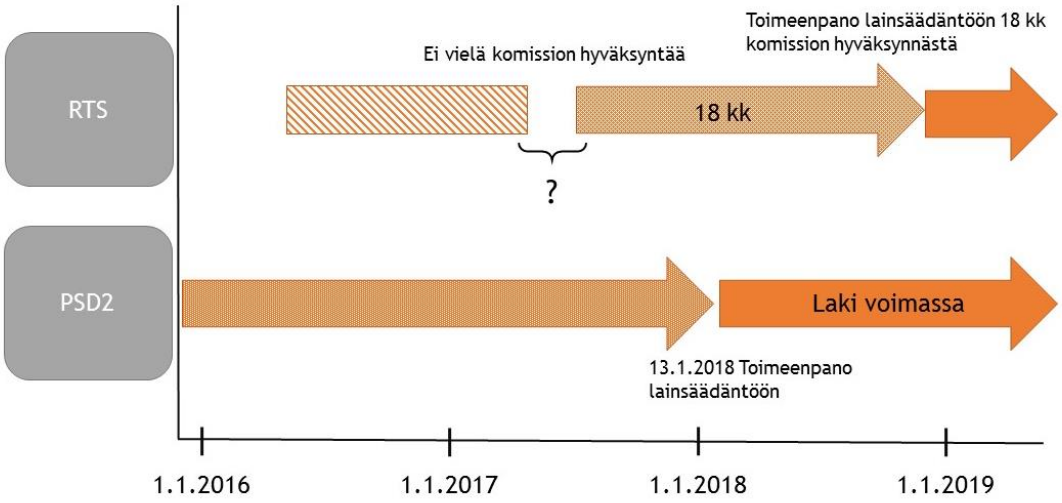
Pivo on tuonut mobiiliin aivan uudenlaisia palveluita maksamiseen ja henkilökohtaiseen taloudenhallintaan liittyen. Samalla Nordea on toiminut edelläkävijänä sähköisen tunnistamisen helpottamisessa tuomalla avainlukulistan mobiiliin muotoon tunnuslukusovelluksellaan. Uudet ja kansan keskuudessa suositut finanssialan sovellukset ovat kaikki nimenomaan mobiilisovelluksia. Mobiilisovellusten keskuudessa on yleistynyt myös niin sanottu sovellusmaksaminen, jossa käyttäjä tallentaa palveluun oman maksukorttinsa tiedot ja alkaa käyttää palvelua. Kun palvelua on käytetty ja on maksun aika, sovellus veloittaa automaattisesti maksun asiakkaan kortilta. Näin maksetaan jo useissa sovelluksissa, joista esimerkkeinä Easypark, Parkman, Uber ja Wolt. Kuten näissäkin sovelluksissa, nykyisin digitaalinen maksaminen perustuu suurilta osin maksukortteihin ja niiden kyttöön. Yksi suurimmista korttimaksamisen negatiivisista puolista on maksuvälinepetosten yleisyys. Maksuvälinepetokset ovat merkittävä digitaalisen maksamisen kenttää häiritsevä tekijä. Euroopan keskuspankin teettämän ”Fourth report on card fraud”-selvityksen (2015) mukaan etäkaupan korttiväärinkäytökset ovat tasaisesti lisääntyneet vuodesta 2010 vuoteen 2013. Kaikkien internetin kautta tehtyjen maksuvälinepetosten yhteenlaskettu summa euroalueella liikkeeseen lasketuilla korteilla oli vuonna 2013 958 miljoonaa euroa. Kun digitaalinen maksaminen ja korttien käyttömahdollisuudet eri kanavissa yleistyvät, on vaikea nähdä, että kansainvälinen maksuvälinerikollisuus ja niistä koituvat korvausmaksut vähenevät.

Euroopan Unionin säätämä uusi maksupalveludirektiivi mahdollistaa korttimaksamisen rinnalla myös toisenlaiset maksamisen tavat. Edellytyksenä uusille tilitieto- tai maksupalveluille on, että asiakkaalle tehdään vahva sähköinen tunnistaminen. Maksamisen tulevaisuuttaa käsittelevästä Suomen Pankin e-kirjasen (2016) teksteistä syntyy kuva, että direktiivin mahdollistamat uudet maksamisratkaisut otetaan laajasti käyttöön. Kirjasessa luodaan monen kirjoittajan toimesta kuva tulevaisuudesta, jossa maksutapahtuma perustuu maksajan tunnistamiseen, joka tapahtuu biometrisesti tai jotenkin muuten digitaalisesti siten, että siitä muodostuu näkymätön taustatoiminto. Moni kirjoittaja yhdistää tunnistamismenetelmien kehityksen mobiilimaksamisen sovellusten kehitykseen.

3 Uusi maksupalveludirektiivi PSD2

Euroopan Unionin komissio on säätänyt vuonna 2015 toisen maksupalveludirektiivin (PSD2), joka korvaa vuonna 2009 säädetyn edellisen direktiivin. Euromaiden pitää toimeenpanna uusi direktiivi omaan lainsäädäntöön 13.1.2018 mennessä. Uuden maksupalveludirektiivin kokonaisuuteen itse direktiivin (EU 2015/2366) lisäksi kuuluu Euroopan pankkiviranomaisen (EPV) säätämät direktiivin tekniset standardit (regulatory technical standards, RTS), jotka astuvat voimaan 18 kuukauden päästä siitä, kun EU:n komissio hyväksyy ne eli aikaisintaan loppuvuodesta 2018. (Kuvio 1) Direktiivin teknisissä standardeissa määritellään tarkasti maksamisen, tietoliikenneyhteyksien ja sähköiseen tunnistamiseen liittyvistä ehdoista. Hyvä esimerkki on

poikkeus maksupalvelun käyttäjän tunnistamisessa alle 30 euron suuruisissa maksuissa sekä pysäköintimaksuissa, minkä ansiosta pieniä transaktioita voidaan suoriittaa ilman asiakkaan tunnistamista (European Bank Authority 2017).



Kuvio 1: Uuden maksupalveludirektiivin ja sitä tarkentavien teknisten standardien voimaantulo

Uuden maksupalveludirektiivin yhtenä tavoitteena on avata maksumarkkinat uusille toimijoille. Maksumarkkinoiden avaamisella tavoitellaan kuluttajille mieleisiä asioita: palveluntarjoajien kilpailun lisäämistä, parempaa maksupalveluvalikoimaa ja kovempaa hintakilpailua. Yksi direktiivin muista tarkoituksista on yhteisten sääntöjen luonti maksupalvelumarkkinoille. Yhteisillä säännöillä tavoitellaan sitä, että EU-alueella tehdyt kansainväliset ja kotimaiset maksut olisivat kuluttajille helppoja, tehokkaita ja turvallisia. Uudelle maksupalveludirektiiville oli tarvetta, koska edellisessä direktiivissä ei oltu laajasti otettu huomioon verkko- ja mobiilimaksamisen yleistymistä ja niiden mahdollistamia innovaatioita. Direktiivin tärkein anti on turvallisuusvaatimusten määrittely itse maksulle, asiakkaan tunnistamiselle ja - maksutiedoille. Maksupalveluiden turvallisuusvaatimuksia tarvitaan etenkin petosten riskin pienentämiseksi. (Maksupalvelut EU:ssa 2016.)

Maksupalveluiden kilpailun lisäämiseksi uusi maksupalveludirektiivi tuo sääntelyn piiriin kaksi uutta toimijaa, joita tulevaisuudessa säännellään kolmannen sektorin maksunvälittäjinä. Kolmannen sektorin maksunvälittäjiä voi olla kahta eri luokkaa: maksupalvelutarjoajia tai tilitietopalvelutarjoajia. Maksupalvelutarjoaja on taho, joka ylläpitää maksun muodostamiseen rakennettua palvelua. Käyttäjä voi maksupalvelun kautta maksaa omalta tililtään ilman että hän käyttää verkkopankkiaan tai asioi muussa perinteisen pankin kanavassa. Maksupalveluntarjoaja voi myös perustaa maksuvälityksensä laskemalla liikkeelle maksukortteja tai muita fyysisiä maksuvälineitä. Toinen uusi toimija, tilitietopalveluntarjoaja tarjoaa palveluita,

joissa käyttäjä voi nähdä yhdessä paikassa kokonaiskuvan henkilökohtaisesta taloudellisesta tilanteestaan. Tilitietopalvelu voi esimerkiksi koota yhteen eri pankeista löytyvät tilit ja esittää ne asiakkaalle yhdellä näytöllä. Direktiivissä säädetään myös, että kolmannen sektorin palveluntarjoajilta vaaditaan ilmoittautumista viranomaiselle, minkä jälkeen he saavat luvan maksulaitoksena toimimiselle. Suomessa luvan maksupalvelun tarjonnalle antaa Finanssivalvonta. (Valcke 2015.)

Yksi uuden maksupalveludirektiivin suurimmista muutoksista on se, että perinteisten pankkien on mahdollistettava uusien maksupalvelutarjoajien toiminta muodostamalla tietoliikennemahdollisuus tahojen välille. Tulevaisuudessa perinteisten pankkien on asiakkaan niin valitessa lähetettävä hänen tilitietojaan kolmannelle osapuolelle, joka mahdollistaa maksun tai muun palvelun. (Valcke 2015.) Direktiivi tai sitä tarkentavat tekniset standardit eivät määrää yhtä tapaa tietoliikenneyhteyden muodostamiseen tilinhoitajapankin ja maksupalveluntarjoajan välille. Tämä johtaa siihen, että maksupalveluntarjoajan pitää jokaisen tilinhoitajapankin kanssa yksilöllisesti muodostaa tietoliikenneyhteydet. Se saattaa tulla erittäin kalliiksi ja viedä erittäin paljon aikaa liiketoiminnan aloitusvaiheessa.

Uusi maksupalveludirektiivi pyrkii myös parantamaan ja varmistamaan sähköisen kaupankäynnin turvallisuutta. Direktiivissä säädetään, että jokaisen maksupalveluita tarjoavan tahon on tunnistettava vahvasti palvelua käyttävä asiakas. Vahva sähköinen tunnistaminen vaaditaan, kun asiakas pyrkii digitaalisia kanavia pitkin katsomaan tilitietojaan, maksaa tililtään tai tekee jotain, minkä takia hän voi joutua maksuvälinepetoksen tai muun rikoksen uhriksi. Tällaisista rikoksista yleisimpiä ovat juuri maksuvälinepetos tai saatujen asiakastietojen pohjalta tehty identiteettivarkaus. (Valcke 2015.) Direktiivissä ja teknisissä standardeissa on kuitenkin säädetty poikkeus tapauksiin, joissa tapahtuman loppusumma on vähäinen tai haettavan tiedon riskitaso on pieni. On nähtävissä, että vahvan sähköisen tunnistamisen tekeminen on sidoksissa toimenpiteen luonteeseen ja riskiin. Direktiivin teknisissä standardeissa säädetään useita poikkeuksia, joiden takia transaktio tai toimenpide voidaan tehdä ilman täydellistä käyttäjän vahvaa sähköistä tunnistamista. Mobeyforumin raportissa (2015) todetaankin, että uuden sääntelyn myötä asiakkaan sähköisen tunnistamisen luonne hieman muuttuu. Sen sijaan että se tehtäisiin aina, tulevaisuudessa asiakkaan tunnistamiseen liitetään aina riskiajattelu. Jos toimenpiteen riskitaso on pieni (asiakkaan rahat ja tiedot ovat suurelta osin turvassa), ei vahvaa sähköistä tunnistamista ole tarpeen tehdä täydellisesti ja vastaavasti: kun suuri määrä asiakkaan varoja siirretään toiselle henkilölle, on vahva sähköinen tunnistaminen ensiarvoisen tärkeää.

Direktiivin teknisissä standardeissa säädetään myös, että uusien maksupalvelutarjoajien on luotettava pankkien tunnistusmenetelmiin eli käytännössä uutta maksupalvelua ei voi perus-

taa kehittämällä toisenlaista, käyttäjäystävällisempää tunnistusmenetelmää. RTS antaa pankeille kuitenkin vallan sopia uuden palveluntarjoajan kanssa erityisehdoista tunnistamisen teossa, mutta se ei välttämättä ole kannattavaa uudelle toimijalle. EPV:n luomat standardit sulkevat pois yhden suurimmista mahdollisista kilpailutekijöistä, joka uusilla maksupalvelutarjoajilla olisi voinut olla. (MePin 2017.)

4 Vahva sähköinen tunnistaminen

Uuden maksupalveludirektiivin voimaan astumisen jälkeen myös uudet palveluntarjoajat voivat tarjota sähköisiä finanssipalveluita. Joko maksu- tai tilitietopalvelun tarjoaminen vaatii kuitenkin asiakkaan vahvan tunnistamisen. Se on syy, miksi asiakkaan tunnistamista pitää myös käsitellä digitaalisen maksamisen yhteydessä. Vuoden 2017 maaliskuussa Suomessa lanseerattiin Siirto-maksujärjestelmä, joka ei perustu perinteisiin luotto- tai pankkikortteihin vaan asiakkaan vahvaan tunnistamiseen ja reaaliaikaiseen tilimaksamiseen.

Yksilön vahva sähköinen tunnistaminen on peruspilari sähköiselle asioinnille ja sähköisten palveluiden kehittymiselle. Vahvalla sähköisellä tunnistamisella tarkoitetaan yksittäisen henkilön tunnistamista sähköisiä menetelmiä hyväksikäyttäen. Vahvaa sähköistä tunnistamista tarvitaan, kun verkossa käytetään palveluita, joiden kautta voidaan maksaa tai tehdä oikeustoimia. Oikeustoimista hyvinä arkipäivän esimerkkeinä toimii erilaisten sopimusten solmiminen ja henkilökohtaisen talouden hoitaminen. Vahvaan sähköiseen tunnistautumiseen kehitetty palvelu perustuu erityisesti luottamukseen palveluntarjoajan ja käyttäjän välillä. Tunnistautujan pitää pystyä luottamaan palveluntarjoajan kykyyn hoitaa tietoturvaan ja yksityisyyden suojaan liittyvät haasteet. Palveluntarjoajan on taas luotettava siihen, että tunnistautuja on henkilö, joka tunnistautumisen perusteella väittää olevansa. (Innanen & Saarimäki 2012.)

Vahvaa sähköistä tunnistamista ei ole jokaisessa verkkopalvelussa pakko tehdä. Verkkopalvelua perustettaessa on suunniteltava, mitä kaikkea palvelussa voi tehdä. Kuluttajat ovatkin tottuneita käyttämään palveluita, joissa tunnistamisen taso on alhainen: tällaisia ovat esimerkiksi palvelut, joissa tunnistamista ei tehdä ollenkaan sekä palvelut, joissa käyttäjä saa itse määrittää oman käyttäjätunnus–salasana –yhdistelmänsä. Jos palvelu on luonteeltaan sellainen, ettei vaaraa taloudellisen vahingon tuottamisesta tai henkilötietojen vuotamisesta ole, ei vahvan tunnistamisen tekeminen ole asiaan kuuluvaa. Toiselta kantilta voitaisiin todeta, että tunnistamisen on tapahduttava vain, kun se on välttämätöntä. Tunnistusmenetelmien turvallisuudenkin kannalta on etu, ettei tunnistautumista tehdä jatkuvasti.

4.1 Tunnistusmenetelmän vaatimukset

Tunnistamismenetelmällä tarkoitetaan kokonaisuutta, jonka muodostavat tunnistautumisjärjestelmä sekä järjestelmän käyttäjän yksilöimiseksi tarvittavat tunnistautumisvälineet (salasanat, tunnukset, kortit ym). Tunnistautumismenetelmää käyttämällä voidaan vahvistaa käyttäjän henkilöllisyys ja siten antaa vahva pohja erilaisten oikeustoimien tekoon digitaalisessa ympäristössä. (Innanen & ym 2012.)

Sähköisestä tunnistamisesta on säädetty ”laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista”. Lain tavoitteena on luoda yhteiset pelisäännöt vahvan tunnistamisen palveluiden rakentamiseen sekä edistää palveluiden tarjontaa ja niiden käyttöä. Lain lähtökohtana on, että tunnistamispalveluita käyttävä kuluttaja pystyy luottamaan järjestelmän tietoturvaan ja yksityisyyden suojaan. (Viestintävirasto 2016a.)

Lain mukaan vahvan sähköisen tunnistamisen perustana on asiakkaan ensitunnistaminen, joka pitää tehdä ennen kuin tunnistamisvälineet hänelle myönnetään. Asiakas voi tehdä ensitunnistamisen henkilökohtaisesti tai sähköisesti. Henkilökohtaisesti asioitaessa asiakkaalla pitää olla viranomaisen myöntämä passi tai henkilökortti ja sen perusteella asiakkaalle voidaan myöntää sähköiset tunnistautumisvälineet. Jos joku muu taho on jo henkilökohtaisen tapaamisen perusteella myöntänyt asiakkaalle sähköiset tunnistautumisvälineet, voidaan niitä käyttää ensitunnistamiseen ja siten saada uudet sähköiset tunnukset uuden tarjoajan palveluun. Tällainen ensitunnistamisen ketjuuntuminen ei ole ongelmatonta. Jos sähköiset tunnistamisvälineet ovat väärissä käsissä, tunnistautuja voi pahimmassa tapauksessa perustaa asiakkuuden toiselle henkilölle ilman, että tunnistamisvälineiden oikea omistaja saa tietoonsa, että hänen kirjautumistietonsa ovat jonkun toisen henkilön hallussa.

Vahva sähköinen tunnistusmenetelmä koostuu itse tunnistamisjärjestelmästä ja tunnistautujalla olevista tunnistamisvälineistä. Menetelmässä on lain mukaan käytettävä vähintään kahta seuraavista todentamistekijöistä:

> ”1) tiedossa oloon perustuvaa todentamistekijää, jonka henkilön on osoitettava olevan tiedossaan;
> 2) hallussapitoon perustuvaa todentamistekijää, jonka henkilön on osoitettava olevan hallussaan;
> 3) luontaista todentamistekijää, joka perustuu johonkin luonnollisen henkilön fyysiseen ominaisuuteen.” (L617/2009)

Nykyisissä tunnistusmenetelmissä käytetään lähes poikkeuksetta tietoon – ja hallussaoloon perustuvaa todentamistekijää. Esimerkiksi verkkopankkitunnuksissa käyttäjätunnus ja salasana

ovat tietoon perustuvia todennustekijöitä ja tunnuslukulista on hallussaoloon perustuva tekijä. Nykyisissä vahvan sähköisen tunnistamisen palveluissa ei vielä käytetä biometriikkaa. Se on monen Suomen Pankin ”Miten maksamme 2020 luvulla?” –kirjasen (2016) kirjoittajan mielestä asia, joka tulee lähi vuosina muuttumaan.

4.2 Markkinoilla olevat vahvan sähköisen tunnistamisen menetelmät

On arvioitu, että pankkien myöntämillä verkkopankkitunnuksilla tehdään noin 99 prosenttia vahvan tunnistamisen tapahtumista (Innanen & ym 2012). Verkkopankkitunnusten lisäksi vahvaan tunnistamiseen on Suomessa olemassa väestörekisterikeskuksen kansalaisvarmenne ja teleyritysten tarjoamat mobiilivarmenteet (Viestintävirasto 2016a).

Pankit myöntävät asiakkailleen verkkopankkitunnuksia, joiden avulla asiakkaat voivat käyttää pankin tarjoamia verkkopalveluita ja asioida puhelinpalvelussa. Verkkopalveluissa asiakkaat voivat esimerkiksi hoitaa päivittäisiä raha-asioitaan, täyttää kortti-, ja lainahakemuksia ja allekirjoittaa sopimuksia. Verkkopankkitunnukset yksilöivät asiakkaan myös, kun hän asioi pankkien puhelinpalvelussa. Näin mahdollistetaan etäkanavia pitkin hoidettava asiakaspalvelu. Ilman asiakkaan vahvaa tunnistamista asiakkaan pankkiasioista ei voida puhua ja siten henkilökohtainen neuvonta etäkanavissa olisi erittäin vaikeaa.

Omien verkkopalveluiden lisäksi pankit tarjoavat yrityksille mahdollisuutta käyttää pankkitunnuksia asiakkaiden tunnistamiseen erilaisissa tilanteissa. Palvelua kutsutaan Tupas-palveluksi. Pankkien Tupas-tunnistuspalvelun avulla asiakas voi tunnistautua yritysten sähköisiin asiointikanaviin verkkopankkitunnuksia käyttäen. Palvelua tarvitaan verkkopalveluissa, joissa on nähtävillä luottamuksellisia tai taloudellisesti arvokkaita tietoja sekä niissä palveluissa, joissa tehdään sitovia oikeustoimia. Yritykset käyttävät Tupas-palvelua esimerkiksi asiakkaan tunnistamiseen ja erilaisten sopimusten allekirjoittamiseen. Tupas palvelussa asiakas tunnistautuu pankin sivuilla verkkopankkitunnuksillaan ja tunnistautumisen jälkeen pankki välittää yritykselle asiakkaan henkilöllisyyden. Tupas-palvelussa pankki huolehtii ainoastaan asiakkaan tunnistamisesta ja henkilötiedon välittämisestä kohdeyritykseen. Oikeustoimet, joita henkilö tekee yrityksen asiointipalvelussa ovat vain asiakkaan ja yrityksen välisiä. (Finannsialan Keskusliitto 2011.)

Verkkopankkitunnusten heikkous on niiden käytön hankaluus. Tunnistautujalla pitää tunnistautuessaan olla aina tunnuslukulista fyysisesti mukana. Verkkopankkitunnuksissa on myös paljon muistettavaa, sillä käyttäjän on muistettava käyttäjätunnus sekä oma henkilökohtainen salasanansa palvelua käytettäessä. Muistamisen paljous altistaa käyttäjän sille riskille, että hän kirjoittaa tunnuslukujaan muistiin ja tunnukset paljastuvat, kun muisitlappu tai tekstitiedosto joutuu vääriin käsiin. Pankit ovat kuitenkin luoneet tehokkaan järjestelmän, jonka

avulla kadonneet tunnukset saa helposti kuoletettua ja sen jälkeen käyttäjän ei tarvitse huolehtia siitä, jos joku yrittää vanhoja tunnuksia käyttää.

Nordea on ensimmäisenä pankkina Suomessa muodostanut tunnuslukukortittoman tavan Tupas-tunnistukseen. Nordea lanseerasi kesällä 2015 tunnuslukusovelluksen älypuhelimille. Se korvaa aikaisemman tunnuslukulistan ja tekee verkkopankkiin kirjautumisen ja maksujen maksamisesta paljon käyttäjäystävällisempää kuin aiemmin. Sovellus toimii kaikilla yleisillä käyttöjärjestelmillä (Windows, Android, iOS). Sovellus toimii 4-numeroisella PIN-koodilla ja tuolla koodilla käyttäjä kirjautuu verkkopankkiin ja vahvistaa maksuja. Kun sovellus on puhelimessa, on ensiarvoisen tärkeää, että pääsy puhelimeen on suojattu koodilla tai sormenjäljellä. Nordea on ensimmäisenä aurannut tietä verkkopankkitunnuksilla tehtävän tunnistamisen helpottamiseksi.

Verkkopankkitunnusten lisäksi Suomessa voi tunnistautua erilaisiin viranomaispalveluihin mobiili- tai kansalaisvarmennetta käyttäen. Pankkiasiointiin nämä tunnistusmenetelmät eivät kelpaa ja uuden maksupalveludirektiivin tuomat muutokset eivät muuta tätä asemaa. Uuden maksupalveludirektiivin mukaisesti tunnistaminen kolmannen tahon tekemissä maksupalveluissa pitää tapahtua samoilla tunnuksilla, joilla maksun voi tehdä oman pankin kautta. Suomessa täytyy silloin turvautua pankkien Tupas-tunnistautumiseen.

Mobiilivarmenne on sähköinen henkilöllisyystodistus, joka kytketään mobiililaitteen SIM-korttiin. Mobiilivarmennetta voi nykyisin käyttää sähköiseen tunnistautumiseen laajasti, mutta pankit eivät ole kelpuuttaneet sitä vielä pankkiasiointiin. Mobiilivarmenne toimii valitsemalla tunnistautumistavaksi mobiilivarmenteen. Sen jälkeen käyttäjä syöttää järjestelmään käyttäjätunnuksen (lähtökohtaisesti matkapuhelinnumero), jonka jälkeen puhelimeen avautuu tieto siirrettävistä tiedoista ja tunnistamisen kohteesta. Käyttäjä hyväksyy tunnistamisen itse valitulla PIN-koodilla ja koodin syöttämisen jälkeen SIM-kortti välittää tunnistamistiedon kohdesivustolle. (Sonera 2017.) Monella sivustolla ei ole erikseen ”tunnistaudu mobiilivarmenteella”-nappia, mutta mobiilivarmenteen käyttäjän on hyvä tiedostaa, että OP:n tunnistuspalvelun kautta voi tunnistautua myös mobiilivarmenteella. Tämän takia mobiilivarmennetta voi käyttää lähes kaikissa henkilön tunnistamista vaativissa verkkopalveluissa. Mobiilivarmenteen ovat luoneet teleoperaattorit Sonera, Elisa ja DNA. Kuluttaja voi aktivoida henkilökohtaisen mobiilivarmenteen suoraan oman operaattorinsa kautta.

Väestörekisterikeskuksen myöntämä ja ylläpitämä kansalaisvarmenne on tällä hetkellä käytössä poliisin myöntämällä henkilökortilla. Kansalaisvarmennetta voi käyttää tunnistautumiseen, sähköpostien ja dokumenttien salaamiseen sekä sähköiseen allekirjoitukseen. (Väestörekisterikeskus) Jotta henkilökortilla olevaa sirua voi hyödyntää sähköisessä asioinnissa, käyttäjä tarvitsee kortinlukijan. Tunnistautuminen henkilökortilla tapahtuu syöttämällä sirukortti

lukijaan ja sen jälkeen syöttämällä oman tunnusluvun kohdesivustolle. Kun käyttäjä asioi tunnistautumista vaativalla sivustolla, pitää kortin olla koko ajan lukijassa. (Väestörekisterikeskus a)

4.3 Biometrinen tunnistaminen ja sen käyttö finanssipalveluissa

Biometrisellä tunnistamisella tarkoitetaan sitä, kun henkilö tunnistetaan käyttäen hyväksi ihmisen ainutlaatuisia piirteitä. Biometrisiä tunnisteita ovat esimerkiksi sormenjälki, silmän iiris, ääni, kasvot, kämmenkuva ja yksinkertaisimmillaan allekirjoitus. Biometriikan perusteella ihminen voidaan tunnistaa lähes varmasti, koska vain harvoilla yksilöillä on täysin identtiset biometriset tunnisteet. Turvallisesti toteutettuna biometriikan käyttö yksilöiden tunnistamisessa nopeuttaa tunnistamisprosessia ja parantaa sen laatua. Käyttäjän näkökulmasta biometriseen tunnistamiseen liitty monia positiivisia asioita: biometriikkaa ei voi unohtaa kotiin eikä sen muistamiseen tarvita ponnisteluja. Tämän takia biometristen tunnistusmenetelmien käyttö koetaan myös yksinkertaisemmaksi ja helpommaksi kuin salasanoilla tapahtuva tunnistautuminen. Uudet kehittyneet tunnistusmenetelmät mahdollistavat myös ihmisten automaattisen tunnistamisen esimerkiksi kasvojen, liikkumistavan tai äänen perusteella. Tällöin ihmisen ei tarvitse ”aktiivisesti tunnistautua” vaan tunnistautuminen siirtyy taustatoiminnoksi. (Tietosuojavaltuutetun Toimisto 2010.)

Erilaisten biometristen tunnisteiden käyttö on yleistynyt huimalla vauhdilla viimevuosina. On ennemminkin sääntö kuin poikkeus, että uudessa mobiililaitteessa on sormenjälkitunnistin ja sitä käyttämällä voi tunnistautua itse puhelimeen ja sen sisältämiin sovelluksiin. Erilaisten mobiilisovellusten kautta voi jo nyt maksaa ja tehdä mittavia hankintoja, joten mobiililaitteen turvallisuudesta on muodostunut merkittävä tekijä maksuvälineiden tietoturvassa.

Biometrisen tunnistamisen haasteisiin yhdistetään menetelmien huijaamisen mahdollisuus. Sormenjälkeen perustuvia järjestelmiä voidaan huijata sormenjälkijäljennöksillä, joita voidaan kameroiden kehityksen ansiosta muodostaa jopa pelkän valokuvan perusteella (Helsingin sanomat 2017). Ihmisen biometrisiä piirteitä ei voida vaihtaa, mutta niitä voidaan kerätä ja käyttää tunnistautumiseen ilman, että henkilö huomaa sitä. Tällainen identiteettivarkauden riski on olemassa varsinkin järjestelmissä, joissa ei käytetä muuta tunnistuskeinoa kuin biometriikkaa. Jotta väärinkäytön riski vähenee, suurta turvallisuustasoa vaativissa järjestelmissä pitäisi käyttää salasanoja tai turvakortteja biometrisen tunnistamisen ohella. Järjestelmän ylläpitäjän vastuulla on itse järjestelmän tietokannan turvallisuus. Jotta ihmisten biometriset mallinteet ovat turvassa mahdollisilta järjestelmään tunkeutujalta, mallinteet pitää salata. Järjestelmän rakentajan kannattaa myös harkita keskitetyn tietovaraston sijasta mallinteiden tallentamista johonkin käyttäjällä mukana olevaan asiaan. Tällaisia asioita voisivat olla älypuhelin, toimikortti tai henkilökortti. (Tietosuojavaltuutetun Toimisto 2010.)

Yhdeksi biomteriikkaa hydyntävien tunnistusjärjestelmien suurimmaksi uhaksi koetaan identiteettivarkaus, jota hyödynnetään taloudellisen edun saamiseksi. Identiteettivarkaus on mahdollinen, kun kolmannella taholla on hallussaan toisen henkilön biometrinen tunniste ja mahdollisesti myös muut järjestelmän vaatimat tunnusluvut. Taloudellisen haitan lisäksi identiteettivarkaus tekisi ihmisen biometrisen tunnisteen, esimerkiksi sormenjäljen, käyttämisen turvattomaksi tulevaisuudessa. Koska biometrisia tunnisteita ei voida ihmisessä muuttaa, on biometriikan tietoturvasta huolehtiminen erittäin tärkeää. Liikenne- ja viestintäministeriö kirjoittaakin, että pelkkään biometriseen käyttäjän tunnistamiseen perustuvien järjestelmien pitää olla sellaisia, että niiden väärinkäyttöön liittyvät riskit ovat vähäisiä eikä niiden huijaaminen ole siten houkuttelevaa. Tällaisia sovelluksia voisivat olla esimerkiksi auton istuimen säädöt ja kuntolaitteiden asetukset. Biometrisen tunnistamisen sovellusten yleistymistä estää kuitenkin se, ettei Suomen kansallisessa lainsäädännössä ole suoraan biotunnistamista käsittelevää kohtaa. Biometrisen tiedon käsittelyä ja säilyttämistä säädellään kuitenkin henkilötietolaissa ja laissa yksityisyyden suojasta työelämässä. (Liikenne- ja viestintäministeriö 2005.)

Tällä hetkellä älypuhelimet ja niissä toimivat sovellukset ovat ottaneet sormenjälkitunnistuksen laajaan käyttöön. Jos puhelin katoaa henkilölle, jolla on hallussaan myös pääkäyttäjän sormenjälki, voi puhelimen pankki- ja maksusovelluksissa tehdä merkittävää taloudellista vahinkoa laitteen omistajille. Kuluttajat ovat ottaneet sormenjälkitunnisteet laajaan käyttöön, mutta biometrisen tunnistautumisen riskeistä ei ole käyty julkisuudessa keskustelua muuten kuin yksittäisten lehtiartikkeleiden kautta.

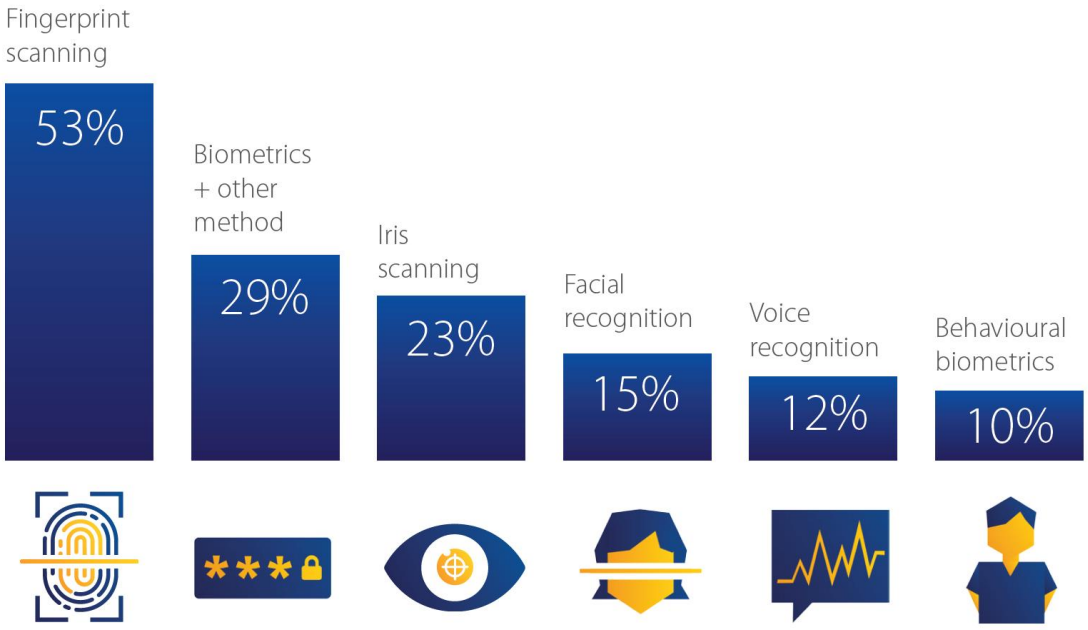
Jos biometrista tunnistamista käytetään korkeaa luottamusta vaativassa järjestelmässä, on ainoa tarpeeksi turvallinen ratkaisu käyttää sitä tunnusluvun tai fyysisen kortin tai laitteen ohessa. Yksin biometriseen tunnistamiseen perustuva maksujärjestelmä ei ole sen riskikäytön kannalta hyvä ratkaisu. (Liikenne- ja viestintäministeriö 2005.) Korkein turvataso maksamiseen saataisiin yhdistämällä fyysinen maksuväline (esim. kortti tai laite), biometriikkaa (sormenjälki) sekä tunnusluku. Tällöin maksuvälineen käyttäjä tunnistautuu kaikkia kolmea kriteeriä hyväksi käyttäen: jotain mitä käyttäjällä on, jotain mitä käyttäjä on ja jotain mitä käyttäjä tietää. Tällainen maksamisen tapa olisi kuitenkin melko hidas ja hankala käyttää.

Suomessa biometriikkaa (allekirjoitus poislukien) on käytetty pankkipalveluissa vain vähän aikaa, kun mobiililaitteet ovat viime vuosina mahdollistaneet sen. Maailmalla erilaisia biometriikka-kokeiluja on useita. Esimerkiksi Japanissa Citibankin asiakkaat ovat voineet nostaa rahaa automaatista vuodesta 2012 lähtien kädenkuvaan perustuvan tunnistamisen avulla ja Yhdysvalloissa USAA-pankin asiakkaat voivat valita käyttävätkö he mobiilisovelluksessaan sormenjälkeä, kasvontunnistusta vai äänen tunnistusta tunnistautumisen keinona. Pankit eivät ole olleet innostuneita kehittämään omia biometrisen tunnistamisen palveluita ennen kuin

älypuhelinten valmistajat toivat pankkipalvelut ja biometriset tunnistusmenetelmät asiakkaiden taskuihin. Biometriikan käytön ja mobiilipalveluiden lisääntyminen finanssisektorilla ovat sidoksissa toisiinsa ja ne myös tukevat toinen toisiaan. (Mobey Forum 2015.)

Suomessa voi tällä hetkellä käyttää biometriikkaa Nordean tunnuslukusovelluksessa, Danske Bankin Mobile Payssa ja mobiilipankissa sekä OP:n mobiilipankissa ja Pivossa. Biometriikan käyttäminen vaatii laitetta, jossa on sormenjälkitunnistin. Tällaisia ovat esimerkiksi uusimmat iPhonet ja useat uudet Android-käyttöjärjestelmän laitteet. Uskon, että muutaman vuoden sisällä Euroopassa ja etenkin Suomessa nähdään merkittävää kehitystä siinä, kuinka laajasti omia pankkipalveluitaan voi hoitaa biometriikan ja mobiilisovellusten avulla.

Liikenne- ja viestintäministeriön raportissa todetaan, että vuonna 2005 sormenjälkeen perustuvat tunnistusmenetelmät olivat kaikkein yleisimpiä. Raportin kirjoitushetkestä sen käyttö erilaisissa sovelluksissa on lisääntynyt reilusti. Visa on kesällä 2016 julkaissut kuluttajatutkimuksen, joka kartoitti Eurooppalaisten kuluttajien mielipiteitä biometrisen tunnistamisen käyttämisestä maksamisen yhteydessä. Tutkimuksen tulokset olivat selvät: 73 prosenttia kyselyn reilusta 14 000 vastaajasta olivat halukkaita käyttämään biometriikkaa yhtenä osana ennen transaktiota tapahtuvassa käyttäjän tunnistamisessa tunnusluvun tai jonkin fyysisen maksuvälineen rinnalla. Samainen tutkimus osoittaa, että maksettaessa kuluttajat käyttäisivät kaikkein mieluiten sormenjälkeä ja vasta toiseksi mieluiten tunnusluvun ja jonkin biometrisen menetelmän yhditelmää. Alla oleva kuva esittää kyselyn tuloksia. Tutkimuksen mukaan kuluttajat pitävät pelkkää sormenjälkeä tarpeeksi turvallisena henkilöllisyyden varmentamisen muotona eikä turvallisuutta lisäävää tunnuslukua välttämättä tarvittaisi. Tutkimuksesta paljastui myös, että kuluttajat pitävät sormenjälkitunnistamista paljon luotettavampana ja turvallisempana kuin tunnusluvuilla tapahtuvaa tunnistamista. (Kuvio 2) (Visa 2016.)



Kuvio 2: Kuluttajien mielestä kaikkein mieluisimmat biometrisen tunnistamisen tavat maksettaessa (Visa 2016.)

Sormenjäljellä tunnistaminen tapahtuu sormenjälkilukijalla ja siihen liitetyllä tunnistusohjelmistolla. Eri valmistajat tekevät tunnistimet eri materiaaleja ja algoritmejä käyttäen. Tunnistusohjelmistot etsivät yleensä lukijan tuottamasta kuvasta tyypillisiä sormenjälkeen liittyviä yksilöllisiä piirteitä ja vertaavat niitä ja niiden sijaintia älykortilla tai tietojärjestelmässä olevaan mallinteeseen. Jos sormenjälkilukijan ja tietokannassa olevan mallinteen tiedot ovat tarpeeksi yhtenevät, ilmoittaa järjestelmä, että tunnistautuja on sama henkilö kuin mallinteen antaja. Sormenjälkitunnistuksessa ei saada ikinä 100 prosentin vastaavuutta mallinteeseen vaan järjestelmissä on jokin ennalta määritelty raja, jonka avulla se tekee päätelmän sormenjäljen vastaavuudesta. (Liikenne- ja viestintäministeriö 2005.)

Kasvojen tunnistuksessa henkilön yksilöllisiä piirteitä erotellaan eri algoritmeja hyväksi käyttäen ja vertaamalla niitä jo järjestelmän muistissa olevaan mallinteeseen. Tällaisia mitattavia asioita ovat esimerkiksi silmien, nenän, leuan ja suun väliset geometriset suhteet. Kasvojentunnistuksen haasteisiin kuuluu esimerkiksi kuvan laatu (valaistus, kulma), silmälasit, hiukset ja muu karvoitus. Haasteita kohdataan varsinkin silloin, kun henkilö ei tiedä, että häntä kuvataan. (Liikenne- ja viestintäministeriö 2005.)

Iiristunnistuksessa järjestelmä ottaa silmästä kuvan kameralla ja laskee henkilön iiriksen yksilöllisestä kuvioinnista mallinteen, jota verrataan järjestelmän muistissa olevaan malliinteeseen. Koska jokaisen ihmisen iiriksessä oleva kuviointi on monimutkainen ja yksilöllinen, iiristunnistamista pidetään tarkkana ja luotettavana. Iiristunnistusjärjestelmien yleistymisen esteenä on niiden korkea hinta verrattuna muihin menetelmiin perustuviin järjestelmiin. (Liikenne- ja viestintäministeriö 2005.)

Puhujantunnistuksessa henkilön puhetapaa ja äänen intonaatiota verrataan järjestelmään aiemmin tallennettuihin näytteisiin. puhujantunnistusjärjestelmät hyödyntävät sitä, että ihmisillä on yksilöllinen puheääni, jonka ominaisista piirteistä ihmiset voidaan tunnistaa ”melko suurella varmuudella”. Kuitenkin tunnistamisen luotettavuus on puheeseen perustuvissa järjestelmissä heikompaa kuin sormenjälki- ja iiristunnistukseen perustuvissa järjestelmissä. (Liikenne- ja viestintäministeriö. 2005.)

5 Digitaalinen maksaminen 2017

Suomalaisilla on jo nyt erilaisia digitaalisia vaihtoehtoja maksamiseen. Erilaisia sovelluksia ja uusia palveluita on tullut markkinoille viime vuosien aikana useita. Verkkokaupoissa suomalaiset maksavat tilauksensa pääosin käyttäen maksukortteja tai verkkopankkipainikkeita. Markkinoilla on mobiilisovelluksia, joiden avulla perinteisiä maksukortteja voidaan muuttaa digitaaliseen muotoon ja näin niitä voidaan kätevästi hyödyntää mobiililaitteella maksettaessa. Monet uudet sovellukset helpottavat ja muuttavat myös verkkokaupassa maksamista. Useimmat maksamisen mobiilisovellukset ovat kuitenkin pankkisidonnaisia eli vain sovelluksen kehittäjäpankin asiakkaat pystyvät täysin käyttämään sovellusta. Tässä luvussa syvennytään digitaalisen maksamisen eri tapoihin ja muotoihin. Luvussa käsitellään pääosin Suomessa toimivia maksutapoja, mutta sen loppupuolella esitellään myös ulkomailla toimiva maksutapa, jonka leviäminen Suomeen on todennäköistä.

Maksukortit, verkkopankkipainikkeet ja laskujen maksaminen

Suomessa toimivat verkkokaupat tarjoavat kuluttajille useita erilaisia maksutapoja. Korttimaksu, verkkopankkipainikkeet, perinteinen lasku ja esimerkiksi osamaksu ovat kaikki yleisiä vaihtoehtoja. Verkkomaksuvälittäjä Klarnan julkaiseman tutkimuksen (2015) mukaan suomalaiset kuluttajat maksavat mieluiten (31 prosenttia) verkkokauppaostoksensa suoraveloituksena suoraan verkkopankkipainikkeen kautta ja toiseksi mieluiten (24 prosenttia) perinteistä laskua käyttäen. Muista Pohjoismaista poiketen korttimaksua käyttää ensisijaisesti vain 14 prosenttia suomalaisista. Muissa Pohjoismaissa korttimaksu oli kaikkein suosituin maksutapa kuluttajien keskuudessa. Tutkimuksessa tulee ilmi, että Suomi ja Ruotsi erottuvat selvästi suoraveloitusten suosiossa, sillä Tanskassa ja Norjassa vain pari prosenttia kuluttajista suosii

suoraveloituksia. Tanskassa ja Norjassa suositaan joko korttimaksuja tai koko ajan yleistyviä elektronisia lompakoita. Ne ovat ikään kuin pankkitilejä, joita ylläpitävät verkkomaksuihin erikoistuneet yritykset ja ihmiset voivat tilisiirroilla tallettaa niille katetta. Erilaiset mobiililompakot on suunniteltu tekemään verkkomaksaminen helpoksi ja turvalliseksi. (Klarna 2015.)

Finanssialan keskusliiton selvityksen (2015) mukaan kuluttajat maksavat päivittäisiä laskuja ensisijaisesti verkkopankissa tai e-laskulla (87 prosenttia vuonna 2015). Liiton mukaan kehitykseen ovat vaikuttaneet internetin ja verkkopankin käytön lisääntyminen. Pankit ovat tehneet verkkopankeista käyttäjäystävällisiä ja nykyisin lähes jokaisella pankilla on olemassa myös mobiilipankki-sovellus älypuhelimille. Mobiilipankkisovelluksia käytetään nykyään jopa enemmän kuin selaimen kautta avautuvaa verkkopankkia. Finanssiryhmä OP kertoi vuoden 2016 vuositiedotteessaan, että mobiilipankki on heillä kaikkein yleisin etäasioinnin muoto: ”keskimäärin OP-mobiilissa oli vuonna 2016 11,4 miljoonaa käyntiä kuukaudessa ja op.fi:ssä 10 miljoonaa”. (OP-Ryhmä 2017.)

Sovellus-maksaminen

Nykyään useissa mobiilisovelluksiin perustuvissa palveluissa maksaminen on upotettu palvelun taustalle eikä kuluttajan tarvitse sovellusta ja palvelua käyttäessään aktiivisesti maksaa missään palvelun vaiheessa. Tällainen niin kutsuttu sovellus-maksaminen on mahdollista, kun sovelluksen asentamisvaiheessa käyttäjä hyväksyy palvelun ehdot ja syöttää maksukortin tiedot sovelluksen käyttöön. Tällaisia mobiilisovellukseen perustuvia palveluita ovat esimerkiksi Spotify, Netflix, Viaplay, Uber, Wolt, Parkman ja Easypark. Easypark-pysäköintimaksupalvelu toimii yksinkertaisuudessaan niin, että kun käyttäjä pysäköi maksulliselle parkkialueelle, hän määrittää ensin sijaintinsa sovelluksen kartalta ja sen jälkeen arvioi pysäköinnin keston. Kun henkilö palaa autollensa, hän lopettaa pysäköinnin sovelluksesta. Viimeistään seuraavana päivänä parkkimaksu on veloitettu sovellukseen syötetyltä maksukortilta ja kuitti maksusta toimitetaan sähköpostiin. Käyttäjä ei siis ”aktiivisesti maksa” missään prosessin vaiheessa. Tällaiset palvelut perustuvat palveluntarjoajan ja käyttäjän väliseen luottamukseen ja ne ovat kovasti yleistymässä.

Mobiilimaksamisen sovellukset Suomessa

Pivo on OP:n kehittämä sovellus, jossa on henkilökohtaisen taloudenhallinnan lisäksi mahdollisuus tehdä maksuja kaupoissa ja henkilöiden välillä. Pivon taloudenhallinnan sovellusten käyttäminen ja kaupoissa maksaminen on mahdollista vain, jos käyttäjällä on OP:n maksukortti. Rahan lähettäminen yksityisten henkilöiden välillä ja maksujen vastaanottaminen on mahdollista kaikkien pankkien asiakkaille. Pivoon kirjaudutaan henkilökohtaisella tunnusluvulla,

jonka käyttäjä voi itse muodostaa ja uusia. Pivon käyttö aloitetaan vahvalla sähköisellä tunnistamisella, jonka jälkeen käyttäjä voi lisätä OP Visa mobiili-maksukorttinsa sovellukseen. Visa mobiili maksukortti ei ole millään tavalla yhdistettynä käyttäjän jo olemassa oleviin kortteihin ja sitä voi käyttää vain Pivossa maksamiseen. Kortti toimii tällä hetkellä vain Android-puhelimissa. Pivon avulla maksaminen perustuu NFC-siruun eli täysin samaan teknologiaan, jota käytetään lähimaksukorteissa. Pivon avulla voi tehdä lähimaksuja kauppojen kassalla ja ne näyttäytyvät kauppiaalle täysin samanlaisina kuin lähimaksuominaisuudella tehdyt korttiostot. Pivo oli Suomen ensimmäinen mobiilisovellus, jolla pystyi muuttamaan maksukorttinsa digitaaliseen muotoon mobiililaitteeseen ja maksaa sen avulla. (Pivolompakko 2016; OP-Ryhmä 2016.)

Mobile Pay on Danske Bankin kehittämä sovellus, joka alkuvaiheessa mahdollisti kaverilta kaverille maksamisen puhelinnumeron perusteella. Nykyään Mobile Pay:lla maksaminen on mahdollista myös kuluttajien ja yritysten välillä. Mobile Pay perustuu pohjimmiltaan korttimaksamiseen, mutta rekisteröitymisen jälkeen käyttäjän täytyy tietää vain vastaanottajan puhelinnumero rahan lähettämiseksi. Mobile Payn rekisteröitymisessä käyttäjä tunnistautuu verkkopankkitunnuksillaan, syöttää maksukorttinsa tiedot ja pankkitilinsä numeron. Rekisteröitymisen jälkeen käyttäjä voi lähettää ja vastaanottaa rahaa sekä maksaa ostoksiaan yritysten kassoilla, verkkokaupoissa ja sovelluksissa. Danske Bank on kehittänyt maksutavan, jossa kuluttajan ei tarvitse syöttää korttitietojaan eri järjestelmiin ja maksutapahtuma on lähes samanlainen ympäristöstä riippumatta. Kun Mobile Payhin on rekisteröidytty, sovellukseen kirjaudutaan joko käyttämällä itse määriteltyä suojakoodia tai Android-puhelinten sormenjälkitunnistuksen kautta. Sovelluksen kautta voi siirtää maksimissaan 500 euroa vuorokaudessa ja 15 000 euroa vuodessa. Nämä ovat ainoat turvallisuustekijät, joita sovelluksessa on. Jos käyttäjä hävittää puhelimensa, voi hän sulkea Mobile Pay:n Danske Bankin sulkupalvelusta ja asentaa sen uudestaan uuteen puhelimeensa. (Danske Bank 2017.)

Nordea Pay on mobiilisovellus, jonka avulla käyttäjä voi muuttaa Android-puhelimensa maksuvälineeksi. Sovellus asennetaan tunnistautumalla verkkopankkitunnuksilla, minkä jälkeen valitaan omista korteista se kortti, jota halutaan käyttää mobiilimaksamiseen. Kortin valinnan jälkeen käyttäjä luo itselleen tunnusluvun, jolla hän voi hyväksyä maksut maksettaessa. Kaupassa maksettaessa puhelin viedään maksulaitteen viereen, jonka jälkeen sovellus kysyy käyttäjän PIN-koodia. Koodin syöttämisen jälkeen puhelin pitää vielä viedä lähelle maksupäätettä ja puhelimen ruutu muuttuu vihreäksi maksun onnistumisen merkiksi. (Nordea 2017.)

OP:n, Nordean ja Danske Bankin omistama Automatia toi maaliskuussa 2017 markkinoille Suomen ensimmäisen tilisiirtoihin perustuvan mobiilimaksujärjestelmän. Pankit voivat Siirto-alustan avulla rakentaa omia sovelluksiaan, jotta heidän asiakkaat saavat reaaliaikaiset tilisiirtoihin ja puhelinumeroihin perustuvat maksut käyttöönsä. Järjestelmä on suunniteltu siten, että

sitä voi käyttää maksettaessa myymälän maksupäätteellä, kaverilta kaverille sekä verkkoympäristössä. Ensimmäisenä siirto-sovellusta tarjosi asiakkailleen Nordea. Automatian mukaan vastaavat sovellukset pitäisi tulla tarjolle myös OP:n, Aktian ja S-pankin asiakkaille. (Automatia 2016.) Suomen kolmesta suuresta pankista Danske Bank ei ainakaan alussa liity järjestelmään, koska heillä on Mobile Pay- järjestelmä, jossa on lähes vastaavat ominaisuudet. Kun jokin toinen pankki liittyy myös Siirtoon, sovellus on Suomessa toinen tilisiirtoihin perustuva järjestelmä, joka mahdollistaa reaaliaikaiset rahasiirrot pankkirajojen ylitse. Aiemmin Suomessa on toiminut pikasiirto.fi-palvelu, joka toimii realiajassa, mutta veloittaa rahan siirtämisestä palvelumaksuja lähes 3 prosenttia siirron arvosta. Siirto-sovelluksen käyttäminen on tällä hetkellä maksutonta. Siirron ehdottomiin vahvuuksiin kuuluu se, että jos se yleistyy, kuluttajan on mahdollista maksaa samalla sovelluksella riippumatta siitä asioiko hän myymälässä vai verkossa ja raha siirtyy tahojen välillä heti. (Nordea 2017a.) Ruotsissa vastaava tilinumeroon ja puhelinnumeroon perustuva tilisiirto– ja maksujärjestelmä on Swish ja sitä käyttää jo yli 5 miljoonaa ruotsalaista (GetSwish 2017).

Bitcoin

Bitcoin on virtuaalivaluutta, joka on tehty lohkoketjuteknologiaa hyödyntäen. Se mahdollistaa sen, ettei yksikään keskuspankki tai valtio hallitse kyseistä valuuttaa. Bitcoineilla voi tällä hetkellä maksaa useissa suomessa toimivissa verkkokaupoissa sekä joissain myymälöissä. Valuutalla maksaminen tapahtuu bittilompakoiden avulla. Bittilompakot ovat ”tilejä”, joihin voi tallettaa Bitcoineja ja niitä on kehitetty käytettäväksi tietokoneilla ja älypuhelimilla. Bitcoineja voi ostaa internetistä tai Bitcoin-automaatista ja hankintaprosessi on vastaava kuin valuutan vaihdossa. (Bittiraha 2015.) Bitcoinin ostovoima on viimeaikoina noussut paljon, mutta myös sen arvon suuria laskuja on historiassa nähty. Bitcoinin arvon heilahtelut ovat erittäin monen asian summa: sen epävirallinen status, Bitcoin-tekniikan kehitys, luottamusta vähentävät uutiset, arvopaperimarkkioniden tila ja mahdolliset hakkerointiyritykset vaikuttavat kaikki verkkovaluutan arvoon. Bitcoinilla on kuitenkin perinteiseen rahaan verrattuna monia hyötyjä: siirtokulut ovat pienet, siirrot ovat nopeita sekä koti- että ulkomaille maksettaessa, varat ovat turvassa tietokoneella tai mobiilisovelluksen pin-koodin takana sekä se, että siirrot tapahtuvat anonyymisti. Anonymiteetti on Bitcoinin ristiriitaisin ominaisuus. Sen takia sitä on jopa kutsuttu ”verkkokäteiseksi”. Euroopan komissio on ehdottanut, että sähköisen rahan vaihdantapalvelut, Bitcoin mukaan lukien, sisällytettäisiin rahanpesun ja terrorismin rahoituksen torjunnan sääntelyn piiriin. Tällöin virtuaalivaluuttojen anonyymiys ei olisi enää mahdollista. On myös tiedossa, että virtuaalivaluutat ovat olleet rikollisten käytössä ja anonyymiteetin rajoittaminen pyrkii pienentämään rikollisen käytön mahdollisuutta. (Valtiovarainministeriö 2017.)

Bitcoin perustuu lohkoketjuteknologiaan, joka tarkoittaa sitä, että keskitetyn palvelimen sijasta verkoston käyttäjät ylläpitävät ja päivittävät järjestelmää. Esimerkiksi Bitcoinissa jokainen sillä tehty transaktio tallentuu samanaikaisesti moneen verkostoon kuuluvaan tietokantaan. Ominaisuus on suuri turvallisuushyöty, koska järjestelmään hakkeroituja ei voi väärentää vain yhtä tietokantaa vaan, jos hän haluaa onnistua tietokannan väärentämisessä, pitää hänellä olla hallussaan suuri määrä järjestelmään kuuluvia koneita ja tiedostot pitää väärentää kaikkiin tietokantoihin samanaikaisesti. Tämä lohkoketjuteknologian ominaisuus tekee siitä turvallisen ja käytettävän omaisuuteen liittyviin ja muihin suurta luottamusta vaativiin sovelluksiin.

Moni ja trustly

Moni ja Trustly eivät ole Suomessa kovinkaan laajassa käytössä. Moni on juuri Suomessa aloittava MasterCardin verkossa toimiva maksuvälineen liikkeeseenlaskija. Moni-maksupalvelu koostuu maksukortista, tilistä ja Moni-sovelluksesta, jonka avulla voi tehdä tilisiirtoja ystäville tai yrityksille, pyytää lainaa, jakaa laskuja ja tarkkailla käyttäjän henkilökohtaista taloudellista tilannetta. Sovelluksen avulla kortille voi tallettaa haluamansa määrän rahaa, joka tekee kortista turvallisen käyttää. Kortin voi myös sulkea sovelluksen kautta, joka on myös turvallisuutta lisäävä ominaisuus. Moni ei ole vielä toiminnassa, mutta nettisivujen perusteella ei mene kauaa, kun kuluttajat voivat ryhtyä Monin asiakkaiksi. (Moni 2017.)

Trustly on Euroopassa laajasti toimiva verkkomaksujen mahdollistaja. Trustly on ruotsalainen maksulaitos ja se toimii 29 eri maassa. Trustlyn kautta tehdään yli 1,7 miljoonaa maksutapahtumaa joka kuukausi. (Trustly 2016.) Trustlyn toiminta on hyvin samanlaista, johon suomalaiset kuluttajat ovat jo tottuneet maksaessaan verkkopankkipainikkeilla. Kun asiakas valitsee verkkokaupassa maksutavaksi Trustlyn, valitsee hän seuraavaksi käyttämänsä pankin. Pankin valinnan jälkeen asiakas tunnistautuu palveluun pankkitunnuksillaan ja sen jälkeen valitsee tilin, jolta maksu veloitetaan. Kun tilivalinta on vahvistettu, asiakas palaa takaisin kauppiaan sivuille ja maksu on maksettu suoraan hänen pankkitililtään. (TrustlyOfficial 2013.) Suomessa Trustly on käytössä ainakin joidenkin nettikasinojen maksuliikenteen hoitajana.

Alipay

Alipay on kiinalaisen Alibaba groupin mobiilisovellus. Alipay yhdistää liikkeet, palvelut, verkkokaupat ja maksamisen yhteen sovellukseen, jonka kautta käyttäjä voi nähdä liikkeen sijainnin, elokuvan alkamisajan tai vaikkapa tilata ruokaa. Sovellusta voi käyttää normaalina maksuvälineenä, vaikka sillä on monia muitakin toimintoja. Tällä hetkellä sovelluksella on yli 450 miljoonaa käyttäjää, mikä on yli 5 prosenttia koko maailman väestöstä. (Alizila 2016.) Alipay hallitsee Kiinan maksamisen markkinoita ja tällä hetkellä Alipay on aloittanut levittäytymisen

Eurooppaan ja Yhdysvaltoihin. Suomeen Alipay on saapunut vuoden 2016 marraskuussa. Suomessa maksutapaa levittää ePassi ja tällä hetkellä sillä voi maksaa esimerkiksi Finnairin lennoilla, Helsinki-Vantaan lentoasemalla ja Lapissa kiinalaisten turistien suosimissa paikoissa. Kokonaisuudessaan reilu 200 suomalaista yritystä oli ottanut maksutavan käyttöön helmikuuhun 2017 mennessä. (Vänskä 2017.)

Apple Pay

Apple Pay on Applen oma maksamisen sovellus, joka toimii tällä hetkellä laajasti Amerikan mantereella Yhdysvalloissa ja Kanadassa, Euroopassa Iso-Britanniassa, Ranskassa, Sveitsissä, Venäjällä ja Espanjassa sekä muualla maailmassa Australiassa, Uudessa seelannissa, Singaporessa, Kiinasssa ja Japanissa. Apple Payn leviämistä hidastaa se, että Applen täytyy tehdä sopimus jokaisessa maassa paikallisten pankkien kanssa ennen kuin niiden asiakkaat voivat käyttää palvelua. Käyttäjällä pitää myös olla Applen valmistama älylaite käytössään: puhelin, kello, tabletti tai kannettava tietokone. (Apple 2016a.)

Apple Pay on maksutapa, jossa maksutapahtuma on asiakkaalle samanlainen riippumatta siitä tapahtuuko maksutapahtuma myymälässä, mobiilisovelluksessa tai verkkokaupassa. Käyttäjälle tämä on erittäin suuri askel, sillä aikaisemmin vastaavaa palvelua ei ole ollut saatavilla. Apple Pay näyttäytyy myyjälle normaalina korttimaksuna, vaikka se onkin tehty käyttäen älypuhelinta. Apple Pay toimii samaa tekniikkaa käyttäen kuin lähimaksukortti, jossa NFC-siru (Near Field Communication) antaa kortin tiedot maksupäätteelle. Applen puhelimiin on asennettu NFC-siru, joka on edellytys tekniikan toimimiselle. Koska puhelimessa on samaa tekniikkaa kuin maksukorteissa, kaikki edellytykset maksutavan käyttöönottoon Pohjoismaissakin on jo olemassa.

Apple Pay toimii seuraavasti: alussa käyttäjän täytyy lisätä maksukorttinsa tiedot Apple Pay:in. Se tapahtuu syöttämällä sovellukseen korttinumero, voimassaolopäivä ja CVC-koodi. Tietojen syöttämisen jälkeen pankki lähettää tekstiviestitse vahvistuskoodin ja koodin syöttämisen jälkeen Apple Paylla maksamisen voi aloittaa. Maksaminen kaupan maksupäätteellä tapahtuu siten, että käyttäjä pitää sormea sormenjälkiskannerin päällä ja vie kännykän maksupäätteen viereen. Maksutapahtuma etenee kuin lähimaksukortilla maksettaessa ja maksu veloittuu käyttäjän valitsemalta maksukortilta. Käyttäjä voi myös määrittää, ettei sormenjälkitunnistusta käytetä Apple Payssa, jolloin maksun vahvistaminen tapahtuu käyttämällä käyttäjän itse määrittämää koodia. Turvallisuuden näkökulmasta on erittäin hyvä, että Apple on pitänyt koodin toisena vahvistuskeinona sormenjäljen kanssa, koska milloin vain vaihdettavissa ja vain käyttäjän tiedossa oleva koodi on maksamisen turvallisuutta lisäävä vaihtoehto sormenjäljen ohella. Apple Pay on edelläkävijä myös maksutapahtumien turvallisuudessa. Sovellus ei tallenna eikä siten välitä suojaamattomia korttitietoja millekään taholle ja se tekee

siitä erittäin turvallisen. Esimerkiksi kaupassa maksettaessa maksupäätteeseen välittyvät käytetyn puhelimen yksilöllinen ID ja tapahtuman yksilöllinen koodi. Näiden tietojen avulla luottokorttiyhtiö pystyy yhdistämään transaktion oikeaan maksuvälineeseen ja veloittamaan tililtä tarvittavan summan. (Apple 2016b.)

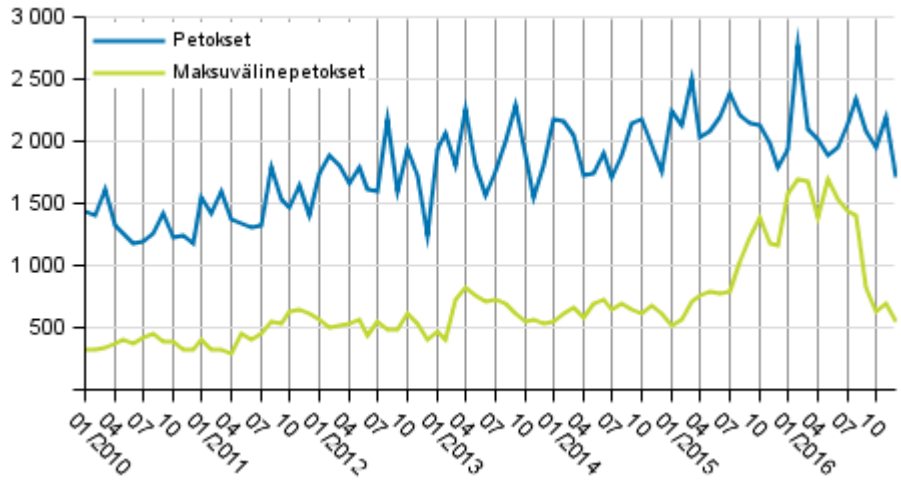
6 Digitaalisen maksamisen turvallisuus

Digitaalisen maksamisen turvallisuus on perinteisesti nähty omien maksukorttitietojen ja verkkopankkitunnusten suojelemisena. Viime vuosien kehitys mobiilisovelluksissa on tuonut maksuvälineet mobiililaitteisiin. Mobiilimaksaminen ja sen yleistyminen johtaa siihen, että maksamisen turvallisuudessa kasvava osa on myös mobiililaitteiden turvallisuutta.

Yleistäen voidaan todeta, että digitaalisessa maksamisessa on kyse henkilön pankkitilillä olevien varojen käytöstä. Maksu voidaan tehdä tilisiirtona tai jonkin maksuvälineen avustuksella, mutta perimmillään on kyse siitä, että tilin omistaja valtuuttaa maksun. Nykyään digitaalista maksamista hallitsevat korttimaksuihin perustuvat järjestelmät. Verkkomaksuissa maksukortin tiedot syötetään kauppiaan sivuille ja se, että kortti on aktiivinen ja käyttäjä syöttää oikeat luvut (korttinumero, voimassaoloaika ja cvc-koodi) järjestelmään on merkki siitä, että maksaja on korttin oikea käyttäjä ja tiliveloitus voidaan tehdä. Digitaalisen maksamisen turvallisuuteen liittyviä ongelmia on esitelty esimerkiksi maksuneuvoston työryhmän ”Maksamisen nykytila”-raportissa (2014). Raportissa esitellään eräs nykyajan maksamisen turvallisuushaaste: monissa verkossa tapahtuvissa ostotapahtumissa korttitiedot välitetään kryptaamattomina usean maksupalvelun tarjoajan arvoketjuun kuuluvan tahon kautta. Tämä johtaa siihen, että maksukorttien suojaamattomat tiedot tallentuvat usean eri tahon palvelimille ja raportin mukaan ”toistuvien” tietomurtojen kautta maksutiedot päätyvät kolmannen osapuolen tietoon. Tällainen korttitietojen vuotaminen rikollisten käsiin vaarantaa koko verkossa tapahtuvan korttimaksamisen luotettavuuden. (Maksuneuvoston työryhmä 1 2014.) Maksukorttien turvallisuudesta puhuttaessa on hyvä ottaa esille, että pankki- ja luottokortit kehitettiin alunperin maksuvälineiksi myymäläympäristöön.

Fyysisesti maksettaessa maksajan henkilöllisyyden varmentaminen on yksinkertaista. Valtio on luonut järjestelmän, jossa jokaiselle henkilölle on luovutettu henkilötunnus ja henkilöllisyyden todentaminen käy näyttämällä poliisilta saatua virallista henkilöllisyystodistusta. Digitaalisessa ympäristössä valtion tarjoama henkilöllisyyden todentamistapa perustuu poliisin myöntämään sirulliseen henkilökorttiin. Korttia voi tällä hetkellä käyttää vain valtion luomiin verkkopalveluihin, mutta sen käyttö on vähäistä. Digitaalisessa ympäristössä maksettaessa maksajan henkilöllisyyden todistaminen perustuu joko maksukorttitietojen ja verkkopankkitunnistuksen yhdistelmään tai vain pelkkiin maksukorttitietoihin.

Uuden maksupalveludirektiivin voimaantulon jälkeen maksamisen turvallisuutta on mahdollista parantaa. Kun tilimaksamisen mahdollisuudet kasvavat ja kuluttajien ei tarvitse aina käyttää maksukortteja, vähenee korttitietojen syöttäminen eri järjestelmiin. Korttitietojen pienempi määrä tekee mahdollisten väärinkäyttöjen todennäköisyyden pienemmäksi.



Kuvio 3: Petokset ja maksuvälinepetokset kuukausittain 2010-2016 (Tilastokeskus 2017.)

Yllä olevasta kuvasta (Kuvio 3) voi nähdä, että viimeisen kahden vuoden aikana maksuvälinepetokset ovat lisääntyneet Suomessa hurjaa vauhtia. Vuonna 2015 maksuvälinepetoksia tuli ilmi 10 900 kappaletta, mikä on 3 200 tapausta (40,8 prosenttia) enemmän kuin vuotta aiemmin (Tilastokeskus 2016). Vuonna 2016 maksuvälinepetoksia tuli ilmi 15 100 kappaletta, mikä on 4 200 tapausta (38,5 prosenttia) enemmän kuin vuonna 2015 (Tilastokeskus 2017). Maksuvälinepetosten määrän kasvu on yhteydessä digitaalisen korttimaksamisen suosioon. Mitä enemmän korttitietoja tietoverkoissa on, sitä houkuttelevampaa tietomurtojen tekeminen yritysten palvelimille on.

Koko eurolueella maksuvälinepetosten yhteenlaskettu summa oli vuonna 2013 1,44 miljardia euroa ja tuosta summasta 958 miljoonaa (kasvua 21 prosenttia vuodesta 2012) koostui verkon kautta tehdyistä maksuvälinepetoksista. Verkon kautta tehdyt maksuvälinepetokset ovat suuri syy siihen, minkä takia koko euromääräinen maksuvälinepetoksista saatu summa on kasvanut. (European Central Bank 2015.)

Maksukorttirikollisuus on yleensä kansainvälistä, järjestäytynyttä ja tuottoisuutensa vuoksi hyvin houkuttelevaa. Rikolliset saavat maksukorttien tietoja yrityksiin kohdistuvista tietomurroista, joita tehdään haittaohjelmilla, kuten viruksilla ja vakoiluohjelmilla. Haittaohjelma tallentaa tarvittavat korttitiedot ja sen jälkeen rikolliset voivat joko käyttää korttia hyväkseen itse tai myydä sen eteenpäin internetin kauppapaikoilla. Maksukorttirikollisten organisaa-

tioissa on yleensä selkeä työnjako: maksukorttitietojen hankinta, sen muuttaminen käyttökelpoiseksi, kortin väärinkäyttö ja rikoksen kautta saadun tavaran kuljettaminen on jaettu eri tahojen tehtäväksi. Yritysten tietoverkkoihin levitettävien haittaohjelmien avulla rikolliset voivat saada suuria määriä luottokorttitietoja ja/tai verkkopankkitunnuksia vähäisellä kiinnijäämisriskillä. (Yritysturvallisuuden kansallinen yhteistyöryhmä 2014.)

Tietomurrot ovat rikollisille tuottoisa tapa hankkia korttitietoja, kun taas murron kohteelle tietovuoto on erittäin vaikea asia. Tietoverkkorikokset ovat usein asianomistajarikoksia, joita yritykset eivät mielellään halua julkiseen ja pitkäkestoiseen tutkintaprosessiin. Vaikka ilmoitus mahdollisesta tietomurrosta saapuisi yritykseen poliisilta tai Viestintävirastolta, poliisi ei saa tutkia rikosta, ellei asianomistaja tee rikosilmoitusta ja vaadi rangaistusta rikoksen tekijälle. Suurinta osaa tietoverkkorikoksista ei havaita ollenkaan ja edellä mainitun syyn takia vielä pienemmästä osasta tehdään rikosilmoitus. EU-maiden poliisiorganisaatioiden yhteenliittymä Europol on rikollisuuden uhka-arviossaan todennut, että maksuvälinedataan kohdistuneita anastuksia koskevan ilmoitusvelvollisuuden puuttuminen lainsäädännöstä estää maksukorttirikollisuuden tutkintaa ja torjuntaa. ”Yritykset jättävät hallussaan olevaan tietoon kohdistuvat rikokset usein ilmoittamatta poliisille oman maineensa suojelemiseksi”, raportissa selvennetään. (Yritysturvallisuuden kansallinen yhteistyöryhmä 2014.)

> ”Keskuskauppakamarin ja Helsingin seudun kauppakamarin "Yritysten rikosturvallisuus 2012" -selvitystutkimuksen mukaan erityisesti suuret yritykset valikoituvat tietoverkkoon murtautumisen kohteeksi. Selvityksen mukaan neljässä kymmenestä (43 %:ssa) suuresta yrityksestä oli havaittu luvattomia yrityksiä päästä tietoverkkoon. Keskisuurista yrityksistä joka neljäs (24 %) ja pienistä yrityksistä vain joka viides ilmoitti murtautumisyrityksistä yrityksen tietoverkkoon. Pääsääntöisesti näistä selvitystutkimukseen vastanneiden yritysten havainnoista ei ole tehty poliisille rikosilmoitusta.” (Yritysturvallisuuden kansallinen yhteistyöryhmä 2014.)

Tietoverkkorikollisuudelta suojautumisessa yritysten on kiinnitettävä huomiota palveluita tuottavien alihankkijoiden tietoturvaan. Tietomurtoja tekevät tahot pyrkivät murtautumaan yrityksen verkkoon sieltä, missä tietoturva on heikoimillaan ja tällainen kohta löytyy usein alihankkijan tietoverkosta. (Yritysturvallisuuden kansallinen yhteistyöryhmä 2014.)

Esimerkkejä lähiaikojen suurista tietomurroista, joissa on saatu paljon käyttäjätietoja:

Kesäkuu 2016: Viime viikkoina on uutisoitu useista tietovuodoista, jotka koskevat tunnettuja verkkopalveluita kuten LinkedIn, Twitter, Tumblr ja MySpace. Käyttäjätietoja kaupataan pimeän verkon foorumeilla. (Viestintävirasto 2016b.)

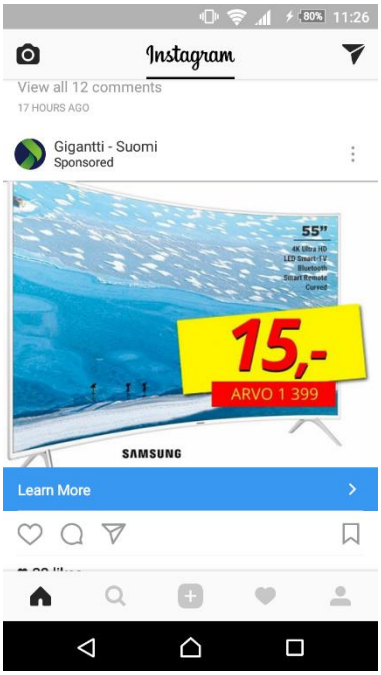
Tammikuu 2016 Hotels.com: Hotels.comin suomalaisasiakkaiden korttitietoja on joutunut verkkorikollisten käsiin, ja niillä on tehty maksuvälinepetoksia ympäri maailmaa. Lukumäärästä ei tietoa (Toivonen 2016.)

Huhtikuu 2011 Playstation Network: Sony on myös ilmoittanut, että joidenkin asiakkaiden luottokorttitiedot on onnistuttu varastamaan. Luottokorttitietoja on varastettu noin 12 700 käyttäjältä Euroopassa. Varkaat ovat päässeet myös tietokantaan, joka sisältää käyttäjien nimen, osoitteen, sähköpostiosoitteen, syntymäajan, puhelinnumeron ja käyttäjätunnuksen sekä salasanan tiivisteen. (Viestintävirasto 2011a.)

Marraskuu 2011 Steam: Valve Corporationin mukaan rikolliset ovat päässeet tietokantaan, joka sisältää asiakkaiden käyttäjätunnukset, salasanoista lasketut tiivisteet, tiedot palvelun kautta tehdyistä ostoksista, sähköpostiosoitteet, laskutusosoitteet ja salakirjoittamalla suojatut luottokorttitiedot. (Viestintävirasto 2011b.)

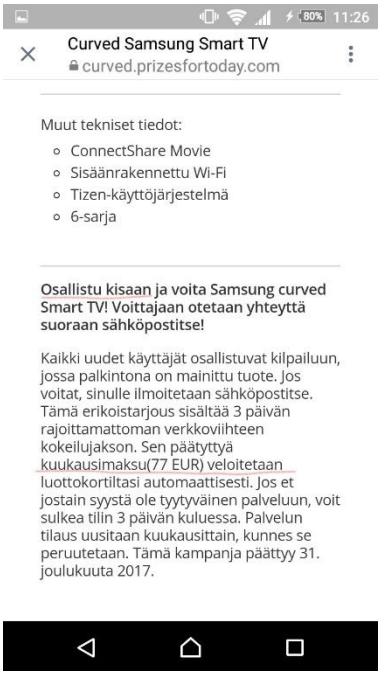
Yritysten tietoturvan lisäksi maksamisen ja oman talouden turvallisuuteen liittyy yksityishenkilöiden verkkoasiointitaidot. Viime vuosina verkkorikolliset ovat kohdistaneet yksittäisiin kuluttajiin mitä erikoisempia huijauksia, joiden motiiveina on saada tietoa ja rahaa hämmentyneiltä kuluttajilta. Ensimmäinen esimerkki tällaisesta huijauksesta on sähköpostiviesteinä levitettävät kampanjat, joissa yritetään saada kuluttaja syöttämään korttinumeroitaan, henkilötietojaan tai verkkopankkitunnuksiaan internettiin pystytetylle valesivustolle (Phishing). Toinen koko ajan yleistyvä huijaus on niin sanottu ”tilausansa”, jossa esimerkiksi laitetilauksen sijasta luottokorttinumeron syöttämisen jälkeen kuluttaja sitoutuukin kalliisiin kuukausiveloituksiin, jostain toisesta palvelusta.

Viestintäviraston ”Tietoturvan vuosi 2016”-raportin (2017) mukaan yllä mainituilla huijauksilla viedään suomalaisilta miljoonia euroja vuosittain. Selvityksen mukaan vuonna 2016 kaikkien suomalaisten liikepankkien nimissä lähetettiin kalasteluviestejä. Eniten niitä lähetettiin Danske Bankin nimissä. Liikepankkien lisäksi huijausviestejä lähetettiin mm. Postin, poliisin, verottajan ja verkkokauppojen nimissä, joten ongelma ei koske vain pankkeja vaan sitä voidaan pitää koko yhteiskunnan ongelmana. Alla (Kuvio 4, 5 ja 6) kirjoitushetkellä käynnissä ollut Gigantin nimissä Instagramissa leviävä ”tilausansa”, jossa taulutelevision ostamisen sijasta kuluttaja osallistuu arvontaan ja sitoutuu viihdepalvelun 3 päivän kokeilujaksoon, jonka jälkeen kuluttajan luottokortilta veloitetaan 77 euroa:



Kuvio 6: Tilausansa 1

Kuvio 5: Tilausansa 2



Kuvio 4: Tilausansa 3

7 Maksupalvelun tarjonta ja Finanssivalvonta

Sääntely on finanssialalla perinteisesti nähty vaatimuksina ja käskyinä, mutta kuten Heikki Kapanen ja Mikko Riikkinen kirjoituksissaan esittävät, sen tulevaisuus nähdään enemmänkin innovaation mahdollistajana ja rajojen selventäjänä. Molemmat myös kirjoittavat, että sääntelyn ylläpitäminen muuttuu paljon vuorovaikutteisemmaksi, joka sekin tukee uusien toimijoiden ja ketterien ratkaisujen saapumista markkinoille. (Suomen Pankki 2016.) Samaisessa teoksessa Anne Nisén ja Markku Koponen Finanssivalvonnasta kirjoittavat, että sääntelyn ja valvonnan olisi hyvä siirtyä maksamisen ohella kohti reaaliaikaisuutta. Tällä hetkellä sääntely on pitkälti reaktiivista eikä uusien toimijoiden luomia tilanteita pystytä aina ennakoimaan. Julkisuudessa finanssialalle povataankin erittäin laaja kirjo uusia palveluita ja on ennustettu, että kuluttajien asiakassuhde perinteisiin alan suuriin toimijoihin voi muuttua radikaalisti.

Maksupalveluita eli tilisiirtoja ja maksukorttimaksuja saa tarjota vain palveluntarjoaja, joka täyttää maksulaitoslaissa säädetyt edellytykset. Maksupalvelun tarjoaminen on luvanvaraista ja Suomessa luvan myöntää Finanssivalvonta. Maksupalveluita voi tarjota poikkeuksellisesti myös ilman toimilupaa, jos tietyt kriteerit palveluntarjoajan toiminnan laajuudessa täyttyvät. Ilman toimilupaa toimiminen vaatii kuitenkin ilmoituksen tekemisen ennen varsinaisen liiketoiminnan aloittamista. Ilmoituksen saatuaan Finanssivalvonta tarkistaa täyttääkö palveluntarjoaja laissa säädetyt edellytykset. Edellytykset ilman toimilupaa toimimiseen liittyvät esi-

merkiksi toteutettujen maksutapahtumien yhteismäärään, joka ei saa henkilön kohdalla ylittää keskimäärin 50 000 euroa vuodessa ja muun toimijan kohdalla keskimäärin 3 miljoonaa euroa kuukaudessa. Jos palveluntarjoaja on hakenut ja saanut toimiluvan maksulaitoksena toimimiseen, voi se tarjota maksupalveluitaan myös muissa Euroopan talousalueeseen (ETA) kuuluvissa maissa. Maksulaitoksen toimilupa on siis pakollinen, kun toiminta on laajempaa tai halutaan kansainvälistyä. (Finanssivalvonta 2014.)

Ilman toimilupaa toimivaksi maksupalvelutarjoajaksi rekisteröityminen on laaja projekti. Ilmoitus pitää tehdä vasta juuri ennen kuin liiketoiminta aloitetaan ja rekisteröitymisessä voi kulua yrityksen näkökulmasta paljon aikaa. Kun dokumentit ovat ”täydelliset” ja Finanssivalvonta on ne saanut, tarkistaa alan valvoja ne ja sen jälkeen hyväksyttää, hylkää tai pyytää täydentämään ilmoitusta. Kun dokumentit toimitetaan valvojalle, voi prosessissa kulua puolikin vuotta ennen päätöstä. Kokonaisuudessaan ilmoituksen tekeminen on erittäin aikaa vievä projekti. Valvojalle tehtävässä ilmoituksessa pitää olla seuraavat selvitykset: liiketoimintasuunnitelma, selvitys luonnollisista henkilöistä, jotka osallistuvat maksupalvelun tarjoamiseen ja vastaavat siitä, selvitys mahdollisista oikeushenkilöistä (muista yrityksistä), jotka ovat osallisena palvelun tarjoamisessa, selvitys asiakasvarojen suojaamisesta, selvitys asiakkaan tunnistamis- ja tuntemismenetelmistä sekä yhteistiedot kommunikointiin Finanssivalvonnan kanssa. Liiketoimintasuunnitelmassa maksupalvelun kokonaistoimintaa pitää kuvailla monesta eri näkökulmasta. Suunnitelmassa pitää olla kuvaus siitä, kuinka palvelu asiakkaalle näyttäytyy, selvitys palvelun turvallisuusrajoista ja tietokantojen turvallisuudesta, kuvaus ulkoistetuista toiminnoista sekä selvitys yrityksen palvelinten ja järjestelmien maantieteellisestä sijainnista. Liiketoimintasuunnitelmassa pitää myös olla tiedot liiketoiminnan suunnitellusta laajuudesta, toiminnan tavoitteista ja asiakaskunnan määrän kehittymisestä. Henkilöiden ja palvelun tuottamiseen liittyvien tahojen luotettavuuden arviointi perustuu Maksulaitoslain vaatimukseen siitä, että maksupalvelua tarjoavan henkilön on oltava luotettava. Luotettavuus selvitykset on tehtävä yhtiön hallituksen jäsenistä, toimitusjohtajasta ja mahdollisista yksittäisten liiketoiminta-alueiden johtajista. Selvityksissä pitää olla otteet liiketoimintakieltorekisteristä, holhousasioiden rekisteristä sekä ulosottorekisteristä. Asiakasvarojen suojaamisselvityksessä maksupalvelun toimintaa pitää kuvata siten, että Finanssivalvonta saa selvän kuvan siitä kuinka on estetty asiakkaiden varojen mahdollinen sotkeutuminen tai häviäminen maksutapahtuman tilisiirtoketjussa. Selvityksessä asiakkaan tunnistamis- ja tuntemismenetelmistä yrityksen pitää kertoa niistä toimista, joiden avulla se varmistuu asiakkaan oikeasta henkilöllisyydestä ja hänen normaalista asiointitavasta. Asiakkaan tunnistamisella ja tuntemisella pyritään estämään rahanpesu ja terrorismin rahoittaminen. Yleensä asiakkaan tuntemistietoihin kerätään tietoja tavanomaisen tilin käytön määrästä, summasta ja laadusta. (Finanssivalvonta 2016.)

Maksulaitoksen toimiluvan hakeminen on vielä laajempi projekti kuin yrityksen ilmoittaminen ilman toimilupaa toimivaksi. Maksulaitoksen toimiluvan hakemuksessa käsitellään osittain samoja asioita kuin yllä mainitussa ilmoituksessa, mutta jokainen osa-alue käydään lävitse paljon perusteellisemmin. Esimerkiksi henkilöselvitysessä käydään yritys lävitse johtoa, johtamisjärjestelmää, henkilöstöä sekä tilintarkastajia myöden. Osa-alueita, joita yllä olevassa ilmoituksessa ei ollut, ovat maksulaitoksen omiin varoihin ja taloudelliseen tilanteeseen, sisäiseen valvontaan sekä riskienhallintaan liittyvät selvitykset. Maksulaitoksen toimilupaa haettaessa sen tekijä joutuu selvittämään perinpohjaisesti toimintaa useasta eri näkökulmasta. (Finanssivalvonta 2016.)

Maksupalvelun tarjoajan pitää raportoida liiketoiminnastaan Finanssivalvonnalle myös tilivuoden aikana. Jatkuvan raportoinnin laajuuden määrittää se onko taho saanut maksulaitoksen aseman vai toimiiko se ilman maksulaitoksen toimilupaa. Ilman toimilupaa toimittaessa tilivuoden aikainen raportointi on hieman kevyempää. Raportointiin sisältyvät tiedot yrityksen johtohenkilöistä, heidän ammattitaidostaan sekä soveltuvuudesta tehtävään, merkittävän toiminnan ulkoistamisesta ja maksutapahtumien yhteismäärästä. Maksulaitoksen toimiluvan saanut taho on näiden tietojen lisäksi velvollinen raportoimaan operatiivisista riskeistä, asiakasriskeistä, omistajamuutkosista, luotoista ja erääntyneistä saamisista, yrityksen omista varoista ja vakavaraisuudesta sekä tilinpäätökseen ja kirjanpitoon perustuvista valvontatiedoista. (Finanssivalvonta 2016.)

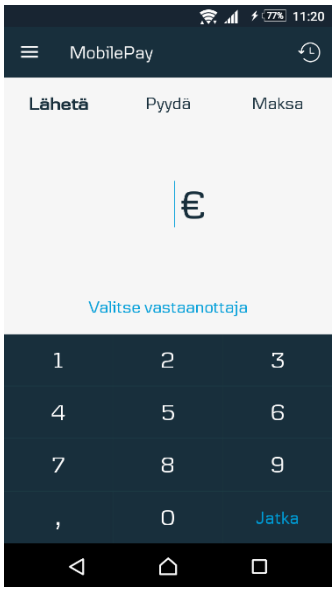
Toimintaa aloittavia yrityksiä ja startupeja auttaakseen Finanssivalvonta on avannut Innovaatio Helpdesk- palvelun, jonka tarkoitus on auttaa ja opastaa alalle pyrkijöitä. Innovaatiohelpdeskissä Finanssivalvonnan asiantuntijat nostavat esille asioita, joita yrittäjät eivät välttämättä ole vielä ajatelleetkaan. Palvelun pääasiallinen tarkoitus on auttaa yrityksiä ja samalla parantaa dialogia Finanssivalvojan ja yritysten välillä. Innovaatio Helpdesk on maksuton palvelu ja se on auki useampana päivänä viikossa. Palvelusta saa asiantuntijoilta vastauksia sähköpostin, puheluiden, tapaamisten tai jopa Skypen kautta. Se on alan uudelle toimijalle paras tapa saada neuvoa ja kontakti Finanssivalvontaan. (Finanssivalvonta 2017.) Haastattelin yhtä Helpdesk-palvelun käyttäjää ja hänellä oli erittäin positiivinen mielikuva palvelusta. Palvelun parhaimmaksi puoliksi hän nosti asiantuntijoiden kattavan määrän, erinomaisen yhteydenpidon ja mukana olleiden asenteen. Palveluun hakeutuvan kannattaa valmistautua rakentamalla ytimekkään esityksen aiotusta liiketoiminnasta sekä varautumalla vastaamaan tiukkoihin ja haastaviin kysymyksiin. Palvelusta saa palautetta, jolla on arvoa. (Matikainen 2017.)

8 Maksupalvelun kilpailutekijät

Jotta uudet toimijat onnistuisivat uuden maksupalvelun kehittämisessä, on hyvä miettiä sen ominaisuuksia: mitä tarvitaan, että uusi maksamisen tapa yleistyy ja voittaa vanhat? Tällä

hetkellä korttimaksaminen on kaikkein suosituin maksamisen muoto. Sillä on sekä hyviä että huonoja puolia. Hyviin puoliin kuuluu se, että kortit käyvät maksuvälineenä mailmanlaajuisesti ja niiden käyttäminen on helppoa, mutta huonoihin puoliin kuuluu, että niiden käyttämisestä veloitetaan kauppiailta ja maksukorteilla on selviä turvallisuushaasteita.

Koska maksukortit ovat kuluttajilla laajasti käytössä, on uuden maksupalvelun oltava parempi, turvallisempi tai käytettävämpi kuin perinteinen kortti. Korttimaksamisen voi päihittää muodostamalla mobiilimaksutavan, jossa on jokin lisäarvoa tuottava ominaisuus, jota maksukortilla ei ole. Tällä hetkellä kuluttajat ottavat innoissaan käyttöön pankkiasiointiin liittyviä mobiilisovelluksia, joten maksamisen vienti mobiiliin on järkevää. Mobiilisovelluksista voi tehdä palvelumuotoilun keinoilla erittäin käytettävän ja se on maksupalvelun yksi ehdoton kilpailutekijä. Palvelun käyttäjäkokemuksen on oltava huippuluokkaa. Mobiilisovelluksen kokonaiskäyttäjäkokemus rakentuu sovelluksen toiminnoista, toimintalogiikasta, käytettävyydestä, visualisuudesta ja sisällöstä. Käyttäjäkokemus on paljon laajempi asia kuin pelkkä sovelluksen käytettävyys, sillä siihen vaikuttavat laajasti kuluttajien mielissä palveluun liittyvät eri tekijät. Käyttäjäkokemukseen kannattaa panostaa, koska sillä on selvä vaikutus liiketoimintaan. Käyttäjäkokemukseen panostavilla yrityksillä on korkea asiakastyytyväisyys, asiakkaat ovat sitoutuneita, käyttäjät viettävät palvelussa enemmän aikaa ja kaikki tämä johtaa palvelun menestymiseen. Parhaat käyttäjäkokemuksen parantamiseksi tehtävät ratkaisut saavat monimutkaiset asiat näyttäytymään erittäin yksinkertaisina ja ymmärrettävinä. (Nichols & Chesnut 2014, 9-15, 19.) Maksupalveluiden käyttäjäkokemuksissa korostuvat käytön helppous, sovelluksen desing sekä sisällön selkeys. Esimerkiksi Mobilepayssa sisältöä ei ole paljoa ja sovellus on varsinkin maksua tehdessä erittäin yksinkertainen käyttää. Sovelluksessa käytetään myös visuaalisia kuvakkeita, jotka ovat mieluisia silmälle. (Kuvio 7)



Kuvio 7: Mobile Payn käyttöliittymä

Toinen mahdollinen kilpailutekijä on maksutavan pankkiriippumattomuus. Tällä hetkellä maksukortit ja jotkin pankkien sovellukset ovat tarjolla vain kehittäjäpankin asiakkaille. Jos uuden maksupalvelun haluaa laajaan käyttöön markkinoilla, on hyvä suunnitella se niin, että kaikkien pankkien asiakkaat voivat liittyä sen käyttäjiksi. Kolmas käyttäjiin liittyvä kilpailutekijä on maksuvälineen turvallisuus. Tällä hetkellä korttimaksamisen turvallisuus digitaalisessa ympäristössä on hieman kyseenalaista. Uusi maksupalveludirektiivi mahdollistaa maksajan vahvaan sähköiseen tunnistamiseen perustuvat maksutavat ja yksi maksupalvelun kehittäjän mahdollisuuksista on ohittaa fyysiset maksukortit ja perustaa maksujärjestelmä tunnistamisen varaan. Tällöin maksamisen turvallisuuden muodostavat käyttäjien tunnistusvälineet ja niihin liittyvät heikkoudet.

Myyjät ja kauppiaat katsovat maksutavan valintaa hieman eri kulmasta: tällä hetkellä luottokorttiyhtiöt Visa ja Master Card perivät kuluja pankki- ja luottokorteilla tehdyistä ostoksista. Jotta uusi maksupalvelu olisi myös kauppiaille kiinnostava vaihtoehto, olisi hyvä jos myyjien ja kauppiaiden kulut olisivat alhaisempia kuin korttimaksuissa. Toinen maksupalvelun etu kauppiaan näkökulmasta olisi se, ettei kassajärjestelmään tarvitsisi tehdä suuria toimenpiteitä ja järjestelmän integrointi olisi helppoa.

Viimeinen ja yksi tärkeimmistä uuden maksupalvelun kilpailueduista on sen toimintaympäristön laajuus. Se, että maksupalvelu toimisi verkkokaupoissa, kaverilta kaverille sekä kivijalkakaupoissa maksettaessa, loisi pohjan palvelun menestykselle. Sekä asiakkaan että myyjän näkökulmasta olisi mahtavaa, jos sama turvallinen maksutapa toimisi monikanavaisessa ympäristössä.

9 Yhteenveto ja johtopäätökset

Yksi Euroopan Unionin säätämän uuden maksupalveludirektiivin tavoitteista on maksupalveluiden kilpailun lisääminen. Tulevaisuus näyttää päästäänkö tavoitteeseen, mutta lähtökohdat uusien palveluiden kehittämiselle ovat olemassa. Kuitenkin yksi merkittävä uusien maksupalveluiden syntymistä hidastava tekijä on vaikea alalle tulo. Kun maksupalvelutarjoaja aloittaa toimintaansa, tarvitsee se jo alussa huomattavan määrän resursseja sääntelyn voittamiseen ja erilaisten turvallisten tietojärjestelmien ja tietoliikenneyhteyksien rakentamiseen.

Maksaminen on siirtymässä lähiaikoina mobiililaitteisiin, joiden kehitys on viimeisten vuosien aikana ollut huimaa. Koska mobiililaitteissa on paljon tietoja käyttäjästä ja sillä voidaan tehdä mitä erilaisempia asioita, on niihin tulevaisuudessa odotettavissa erilaisia käyttäjän

tunnistamiseen liittyviä tekijöitä. Biometristen tunnisteiden määrän lisääntyminen ja käyttäytymiseen perustuvien biometristen järjestelmän yleistyminen luovat tekniset mahdollisuudet reaaliaikaiseen käyttäjän oikeallisuuden seurantaan. Mobiililaitteiden kehitys luo mahdollisuuksia uuden tekniikan käyttöön ja edesauttaa turvallisuutta maksamisen sovelluksissa.

Digitaalisen maksamisen turvallisuus on yhdistelmä käyttäjän maksuvälineisiin liittyvää tilannetajua, yritysten ja niiden alihankkijoiden järjestelmien tietoturvaa. Maksuvälinepetokset ovat nykyajan verkkorikollisille tuottoisa vapaa-ajanviete. Rikolliset saavat maksuvälineiden tietoja suoraan kuluttajilta kalasteluviestien avulla tai yritysten suojaamattomista tietokannoista verkkoa pitkin tehtävien hyökkäysten kautta. Maksutietoja voi myös ostaa suoraan Torverkossa toimivilta kauppapaikoilta, joista suomalaisena esimerkkinä toimii Silkkitie.

Mobiilimaksamisen sovellukset voivat hyvin toteutettuna parantaa maksamisen turvallisuutta. Esimerkiksi Apple Pay ei säilytä eikä maksettaessa välitä koko korttinumeroa millään palvelimella. Maksupalvelut, joissa turvallisuustekijät on otettu vakavasti huomioon ovat tulevaisuutta. Ilman turvallisuutta ei todennäköisesti ole asiakkaitakaan, koska loppujen lopuksi maksamisen ratkaisut ovat tasapainoilua järjestelmän käytettävyyden ja turvallisuuden välillä.

Siirto -maksujärjestelmän siivittämänä digitaalinen maksaminen on Suomessa siirtymässä reaaliaikaan. Nopeat tietoliikenneyhteydet mahdollistavat varojen nopean siirtymisen maksajan ja saajan välillä. Tilimaksamiseen perustuvat järjestelmät luovat painetta asiakkaan vahvan sähköisen tunnistamisen eli Suomessa suurimmaksi osaksi pankkien verkkopankkitunnusten kehitykselle. Nordean tunnuslukusovellus on edelläkävijä tällä saralla. Minulla on vahva usko, että lähitulevaisuudessa muutkin finanssialan toimijat alkavat kehittää käytännöllisempiä vahvan tunnistamisen järjestelmiä.

Maksamisen palvelun liiketoiminta on suurten käyttäjämäärien (high volume) ja matalien katteiden (low value) varassa. Koska alalla ei ole mahdollista periä korkeita katteita kuluttajilta tai yrittäjiltä, on laaja käyttäjäryhmä edellytys palvelun menestymiselle. Laajan käyttäjäryhmän houkutteleminen palveluun, maksupalvelun kehittäminen, tietoliikenneyhteyksien rakentaminen ja tietoverkkojen suojaaminen vaativat niin paljon resursseja jo ennen varsinaisen liiketoiminnan aloittamista, etten usko, että start-up:maiset pienet toimijat onnistuvat suosittuja maksamisen palveluita lähiaikoina rakentamaan. Uusi maksupalveludirektiivi mahdollistaa uuden liiketoiminnan, mutta sen aloittaminen vaatii valtavasti resursseja. Tällöin mahdollisuus on auki lähinnä suurilla jo toisella alalla toimivilla yrityksillä.

Opinnäytetyössä tutkituista aiheista on kirjoitettu tiiviit tekstit Turbiini-yrityskiihdyttämölle tuotettuun oppaaseen. Opas on lähtökohtaisesti kirjoitettu henkilölle, joka on kiinnostunut

liiketoiminnan rakentamisesta maksamisen markkinoille. Oppaassa on käsitelty muun muassa sääntelyn kehitystä, markkinoilla jo olevia maksamisen ratkaisuja, maksamisen markkinoilla havaittavia kehityssuuntia sekä toimiluvan hakuprosessia. Oppaan tekstit on pyritty pitämään helposti ymmärrettävinä, minkä takia yksityiskohdissa ei mennä kovinkaan tarkalle tasolle. Oppaan tarkoituksena on tarjota lukijalleen perustietoa ja uusia ajatuksia, minkä jälkeen lukija voi syventyä oppaan aiheisiin tarkemmin opinnäytetyön tekstiosion tai muun materiaalin kautta. Toivon, että oppaan tekstit herättäisivät innovaation kipinän sekä ajatuksia lähitulevaisuuden maksamisen ratkaisuista.

Lähteet

Kirjalliset lähteet

Chesnut, D. & Wiley, N. 2014. UX for Dummies. 1. Painos. John Wiley & Sons.

Herrmann, U. 2013. Pääoman voitto – Kasvun, rahan ja kriisien historia. Helsinki: Into Kustannus.

Kontkanen, E. 2015 Pankkitoiminnan käsikirja. 4. uudistetun painoksen lisäpainos. Vantaa: Hansaprint.

Innanen, A. & Saarimäki, J. 2012. Internetoikeus. 2., uudistettu painos. Porvoo: Bookwell.

Sähköiset lähteet

Alizila. 2016. What is Alipay?. Viitattu 10.3.2017. https://www.youtube.com/watch?v=t5ElQaVjQZE

Apple. 2016a. Apple Pay participating banks in Europe. Viitattu 28.2.2017. https://support.apple.com/fi-fi/ht206637

Apple. 2016b. Apple Pay security and privacy overview. Viitattu 28.2.2017. https://support.apple.com/en-us/HT203027

Automatia. 2016. Kännykkämaksaminen helpottuu – Suomalaispankkien omistama Automatia tuo markkinoille avoimen mobiilimaksujärjestelmän. Viitattu 3.3.2017. https://siirto.fi/kannykkamaksaminen-helpottuu/

Bittiraha. 2015. Bitcoin Käsikirja. Viitattu 11.3.2017. https://bittiraha.fi/bitcoin-kasikirja-2-painos.pdf

Danske Bank. 2017. MobilePay. Viitattu 20.2.2017. http://www.mobilepay.fi/fi-fi/Pages/mobilepay.aspx

European Bank Authority. 2017. Final Report on Draft RTS on SCA and CSC. Viitattu 6.3.2017. https://www.eba.europa.eu/documents/10180/1761863/Final+draft+RTS+on+SCA+and+CSC+under+PSD2+%28EBA-RTS-2017-02%29.pdf

European Central Bank. 2015. Fourth report on card fraud. Viitattu 17.2.2017. https://www.ecb.europa.eu/pub/pdf/other/4th_card_fraud_report.en.pdf

Finanssivalvonta. 2017. Tarvitseeko innovaatio toimiluvan?. Viitattu 6.3.2017. http://www.finanssivalvonta.fi/fi/Toimiluvat/Innovaatio/Pages/Default.aspx

Finanssivalvonta. 2016. Määräykset ja ohjeet 8/2016 Maksulaitokset ja maksupalvelua ilman toimilupaa tarjoavat henkilöt. Viitattu 2.3.2017. http://www.finanssivalvonta.fi/fi/Saantely/Maarayskokoelma/Uusi/Documents/2016_08.M1.pdf

Finanssivalvonta. 2014. Maksupalvelun tarjoajat. Viitattu 2.3.2017. http://www.finanssivalvonta.fi/fi/Finanssiasiakas/Palveluntarjoajat/Maksupalvelu/Pages/Default.aspx

GetSwish. 2017. Vem blev Swish-användare nr 5 000 000?. Viitattu 6.3.2017. https://www.getswish.se/vad-roligt-att-det-blev-jag/

Helsingin Sanomat. 2017. Japanilaiset tutkijat varoittavat: Älä näytä rauhanmerkkiä sosiaalisessa mediassa. Viitattu 7.3.2017. http://www.hs.fi/talous/art-2000005047823.html

Klarna. 2015. Verkkokaupan trendit Pohjoismaissa 2015. Viitattu 3.3.2017. https://www.klarna.com/download_file/view_inline/1463

Liikenne- ja viestintäministeriö. 2005. Biometrisen tunnistamisen tietoturvallisuus ja yksityisyyden suoja. Viitattu 1.2.2017. http://urn.fi/URN:ISBN:952-201-458-3

Maksuneuvoston työryhmä 1. 2014. Maksamisen nykytila ja trendit. Viitattu 14.2.2017. https://www.suomenpankki.fi/globalassets/fi/raha-ja-maksaminen/maksujarjestelmat/suomen-pankki-katalystina-maksuneuvosto/maksamisen_nykytila_ja_trendit_lyhennetty.pdf

Maksupalvelut EU:ssa. 2016. Viitattu 23.3.2017. http://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=URISERV:2404020302_1&from=EN&isLegissum=true

MePin. 2017. Webinar: PSD2 + Strong Customer Authentication - Key findings from the EBA's RTS final draft. Viitattu 29.3.2017. https://www.youtube.com/watch?v=kvWmfo5lfC0&feature=youtu.be

Mobey Forum. 2015. Biometrics in payments: Touching convenience. Viitattu 8.3.2017. http://mobeyforumorg.virtualserver26.hosting.fi/w/download/2015-Nov-Mobey-forum-White-paper-Biometrics-in-payments_Touching-Convenience.pdf

Moni. 2017. Maksukorttien taskukokoinen monitoimityökalu. https://moni.fi/ominaisuudet/

Nordea. 2017. Nordea Pay. Viitattu 27.2.2017. https://www.nordea.fi/henkiloasiakkaat/paivittaiset-raha-asiat/internet-mobiili-ja-puhelinpalvelut/nordea-pay.html#tab=Nordea-Pay

Nordea. 2017a. Siirto. Viitattu 3.3.2017. https://www.nordea.fi/henkiloasiakkaat/paivittaiset-raha-asiat/internet-mobiili-ja-puhelinpalvelut/siirto.html#faq=Usein-kysyttya-Siirrosta+172863&tab=Kysymyksia-ja-vastauksia

OP-Ryhmä. 2016. OP-Visa Debit Mobiili. Viitattu 20.2.2017. https://www.op.fi/op/henkiloasiakkaat/kortit/maksukortit/op-visa-debit-mobiili?id=12906&srcpl=8

OP-Ryhmä. 2017. Keskeiset tapahtumat. Viitattu 3.3.2017. https://op-year2016.fi/op-ryhma/keskeiset-tapahtumat

Pivolompakko. 2016. Usein kysyttyä. Viitattu 20.2.2017. https://pivolompakko.fi/faq.html

Sommar, H. 2011. Rahat kortilla. Viitattu 23.4.2017. http://yle.fi/aihe/artikkeli/2010/06/10/rahat-kortilla

Sonera. Sonera ID. Viitattu 18.2.2017. https://www.sonera.fi/media/13a202c4fbf4faae9f304a228a7fd1ec00c889cc/13a202c4fbf4faae9f304a228a7fd1ec00c889cc.pdf

Suomen Pankki. 2016. Millä tavoin maksamme 2020-luvulla? Näkökulmia tulevaisuuden maksamisratkaisuihin. Viitattu 1.2.2017. https://www.suomenpankki.fi/globalassets/fi/raha-ja-maksaminen/maksujarjestelmat/suomen-pankki-katalystina-maksuneuvosto/maksuneuvoston_e_kirjanen_2016.pdf

Tietosuojavaltuutetun toimisto. 2010. Biometrinen tunnistus, mikä se on?. Viitattu 1.2.2017. http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/6JfqPiEON/Biometrinen_tunnistus_mika_se_on.pdf

Tilastokeskus. 2016. Petosten ja maksuvälinepetosten määrä lisääntyi vuonna 2015. Viitattu 14.2.2017. http://www.stat.fi/til/rpk/2015/04/rpk_2015_04_2016-01-19_tie_001_fi.html

Tilastokeskus. 2017. Tietoon tulleiden seksuaalirikoksien määrä kasvussa. Viitattu 14.2.2017. http://www.stat.fi/til/rpk/2016/04/rpk_2016_04_2017-01-19_tie_001_fi.html

Toivonen, T. 2016. Suositun Hotels.comin tietoturvassa aukko? KRP: Sadan suomalaisen korttitiedot viety varauksen jälkeen. Viitattu 23.3.2017. http://yle.fi/uutiset/3-8598203

Trustly. 2016. Shop and pay from your bank account. Viitattu 28.3.2017. https://trustly.com/en/

TrustlyOfficial. 2013. Trustly - Direct bank e-payments. Viitattu 5.4.2017. https://www.youtube.com/watch?v=o7iHhMb3hzY

Valtiovarainministeriö. 2016. Terrorismin rahoituksen torjuntaa tehostetaan. Viitattu 16.3.2017. http://vm.fi/artikkeli/-/asset_publisher/terrorismin-rahoituksen-torjunta

Valcke, P. Vandezande, N. Van De Velde, N. 2015. The evolution of third party payment providers and cryptocurrencies under the EU's upcoming PSD2 and AMLD4. Viitattu 12.2.2017. http://www.swiftinstitute.org/wp-content/uploads/2015/09/SIWP-No-2015-001-AML-Risks-of-the-Third-Party-Payment-Providers_FINAL.pdf

Viestintävirasto. 2017. Tietoturvan vuosi 2016. Viitattu 4.3.2017. https://www.viestintavirasto.fi/attachments/tietoturva/Tietoturvan-vuosi_2016_ViVi_29-11-2017_L.pdf

Viestintävirasto. 2016a. Vahva sähköinen tunnistaminen, sähköinen allekirjoitus ja varmenne. Viitattu 15.2.2017. https://www.viestintavirasto.fi/kyberturvallisuus/sahkoinentunnistaminenjaallekirjoitus.html

Viestintävirasto. 2016b. Viimeaikaiset tietovuodot koskevat satoja miljoonia käyttäjiä. Viitattu 23.3.2017. https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2016/06/ttn201606131227.html

Viestintävirasto. 2011a. Sony PlayStation Network -käyttäjien tietoja varastettu tietomurron seurauksena. Viitattu 23.3.2017. https://www.viestintavirasto.fi/kyberturvallisuus/varoitukset/2011/varoitus-2011-01.html

Viestintävirasto. 2011b. Tietomurto Steam-verkkokauppaan. Viitattu 23.3.2017. https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2011/11/ttn201111111108.html

Väestörekisterikeskus. Kansalaisvarmenne. Viitattu 6.3.2017. http://vrk.fi/kansalaisvarmenne

Väestörekisterikeskus a. Tunnistautuminen varmennekortilla. Viitattu 6.3.2017. https://www.suomi.fi/suomifi/suomi/asioi_verkossa/sahkoinen_tunnistus_ja_allekirjoitus/tunnistautuminen_varmennekortilla/index.html

Vänskä, H. 2017. "Suomi on saanut paljon huomiota Kiinassa Alipayn mobiilin maksamisen festivaaleilla". Viitattu 10.3.2017. http://www.kauppalehti.fi/uutiset/kiinalaisen-mobiilimaksuyhtion-maihinnousu-etenee-suomessa/2rFzY6Xj

Yritysturvallisuuden kansallinen yhteistyöryhmä. 2014. Yrityksiin kohdistuvan ja niitä hyödyntävän rikollisuuden tilannekatsaus nro 15. Viitattu 16.2.2017. https://www.finnsecurity.fi/application/files/2114/8473/2301/140520_tilannekuva_kevat_2014.pdf

Julkaisemattomat lähteet

Haastattelu Terhi Wathen, Finanssivalvonta

Haastattelu Otso Manninen, Suomen Pankki

Haastattelu Tim Matikainen, Laskit

Maksamisen kyberturvallisuus- tilaisuus:
Vesa Hietanen, turvallisuusasiantuntija, S-Pankki
Ville Elenius, vanhempi rikoskonstaapeli, Keskusrikospoliisin kyberrikostorjuntakeskuksesta

Kuviot

Liitteet

Digitaalinen maksaminen 2017

-

Opas maksamisen markkinoiden tilasta ja tulevista muutoksista

Kasper Vainikka

2017

Turbiini
YRITYSKIIHDYTTÄMÖ

LAUREA
AMMATTIKORKEAKOULU

Sisällys

Alkusanat

Opas on osa Laurea ammattikorkeakoulun opinnäytetyötä ja sen tavoitteena on tarjota lukijalle tiivis tietopaketti maksamisen markkinoiden tilasta ja tulevista muutoksista. Oppaan tekstit ovat täydessä laajuudessa luettavissa opinnäytetyöni tietopaketista.

Opas ei ole täydellinen otos suomalaisesta digitaalisen maksamisesta, mutta siinä pyritään luomaan kattava kuva nykyisistä trendeistä ja markkinaan vaikuttavista tekijöistä.

Taustaa

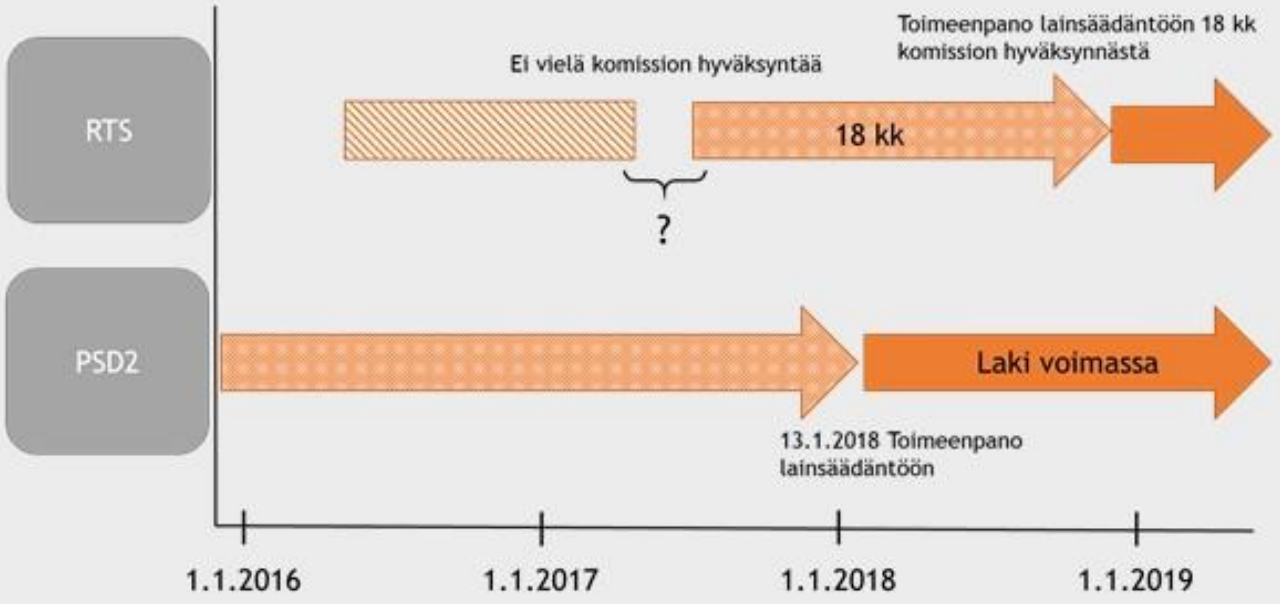
Digitaalinen maksaminen ja sen mahdollistavat palvelut ovat alan uuden sääntelyn takia suurten muutosten edessä. Uusi maksupalveludirektiivi mahdollistaa uusien maksupalvelutarjoajien toiminnan alalla ja pakottaa perinteiset pankit tarjoamaan tarvittavat asiakastiedot maksun suorittamiseksi. Tuore lainsäädäntö luo mahdollisuuden täysin uuden toimialan muodostumiselle.

Jo muutaman viime vuoden kehitys on luonut pohjan maksamisen palveluiden tulevaisuuden kehitykselle: mobiililaitteiden määrä lisääntyy jatkuvasti ja samalla erilaiset omaa taloudenhallintaa helpottavat sovellukset ovat keränneet suosiota. Hyvä esimerkki on Danske Bankin Mobile Pay, joka toi ensimmäisenä Suomeen kuluttajien välisen mobiilimaksamisen. Siinä vanavedessä myös OP:n Pivo on tuonut mobiiliin aivan uudenlaisia palveluita maksamiseen ja henkilökohtaiseen taloudenhallintaan liittyen. Samalla Nordea on toiminut edelläkävijänä sähköisen tunnistamisen helpottamisessa tuomalla avainlukulistan mobiiliin muotoon.

Kun digitaalisen maksamisen määrä kasvaa, on kasvanut myös digitaalinen maksuvälinerikollisuus. Viimeisin virallinen Euroopan keskuspankin julkaisema luku maksuvälinepetosten euromääräisestä yhteissummasta antaa kuvaa alan massiivisuudesta. Kaikkien internetin kautta tehtyjen maksuvälinepetosten yhteenlaskettu summa euroalueella liikkeeseen lasketuilla korteilla oli vuonna 2013 958 miljoonaa euroa. Verkkorikollisuus on viimevuosien aikana kasvanut selvästi, joten se on merkittävä digitaalisen maksamisen markkinaa varjostava tekijä.

Uusi maksupalveludirektiivi PSD2

Euroopan Unionin komissio on säätänyt vuonna 2015 toisen maksupalveludirektiivin (Second Payment Service Directive, PSD2), joka korvaa vuonna 2009 säädetyn edellisen direktiivin. Euromaiden pitää toimeenpanna uusi direktiivi omaan lainsäädäntöön 13.1.2018 mennessä. Uuden maksupalveludirektiivin kokonaisuuteen itse direktiivin (EU 2015/2366) lisäksi kuuluu Euroopan pankkiviranomaisen (European Bank Authority, EBA) säätämät direktiivin tekniset standardit (Regulatory technical standards, RTS), jotka tulevat voimaan myöhemmin kuin itse direktiivi. Voimaantulo:



Uuden maksupalveludirektiivin tavoitteina on maksupalvelumarkkinoiden avaaminen uusille toimijoille alan kilpailun ja kuluttajien valinnanvaran lisäämiseksi, yhteisten sääntöjen luominen markkinalle ja maksupalvelumarkkinan kehittämistä siten, että toimijoiden oikeudet ja velvollisuudet ovat selkeät.

Maksupalvelujen kilpailun lisäämiseksi uusi maksupalveludirektiivi tuo sääntelyn piiriin kaksi uutta toimijaa: maksupalvelu- ja tilitietopalveluntarjoajan. Maksupalveluntarjoaja voi myös perustaa maksuvälityksensä laskemalla liikkeelle maksukortteja tai muita fyysisiä maksuvälineitä. Uusien palveluntarjoajien toiminta mahdollistetaan niin, että perinteisten pankkien on mahdollistettava tietoliikenneyhteydet tahojen välille. Perinteisten pankkien on siis jaettava asiakastietoja kolmannelle osapuolelle mikäli asiakas näin haluaa. Uudet toimijat:

- PSP (Payment Service Provider) eli maksupalvelutarjoaja
    - Asiakas voi maksupalvelutarjoajan kautta käyttää toisen tahon hallinnoimaa pankkitiliä
- AISP (Account Information Service Provider) eli tilitietopalveluntarjoaja
    - Asiakas voi palvelun kautta nähdä pankkitiliensä saldot yhdestä paikasta, vaikka tilejä olisi useammassa eri pankissa

Jotta uudet palveluntarjoajat voivat tarjota palveluitaan, heidän on tunnistettava asiakas käyttäen samaa menetelmää, jolla asiakas voisi tehdä toimenpiteen oman tilinhoitajapankkinsa kautta. Suomessa uusien toimijoiden on siis tunnistettava asiakkaansa pankkien verkkopankkitunnuksilla. Uusi maksupalveludirektiivi mahdollistaa kuitenkin vähäriskisten toimenpiteiden teon kevyemmällä tunnistamisella.

Vahva sähköinen tunnistaminen

Uuden maksupalveludirektiivin voimaan astumisen jälkeen myös uudet palveluntarjoajat voivat tarjota sähköisiä finanssipalveluja. Joko maksupalvelun tai tilitietopalvelun tarjoaminen vaatii kuitenkin asiakkaan vahvan tunnistamisen. Vuoden 2017 maaliskuussa Suomessa lanseerattiin ensimmäinen maksujärjestelmä, joka ei perustu perinteisiin luotto- tai pankkikortteihin vaan asiakkaan vahvaan tunnistamiseen ja reaaliaikaiseen tilimaksamiseen. Uuden maksupalveludirektiivin mukaisesti tunnistaminen kolmannen tahon tekemissä maksupalveluissa pitää tapahtua samoilla tunnuksilla, joilla maksun voi tehdä oman pankin kautta. Tällöin Suomessa tunnistamisessa pitää käyttää verkkopankkitunnuksia.

Tunnistusmenetelmän pitää lain mukaan koostua vähintään kahteen seuraavista tekijöistä:

1) tiedossa oloon perustuvaa todentamistekijää, jonka henkilön on osoitettava olevan tiedossaan;

2) hallussapitoon perustuvaa todentamistekijää, jonka henkilön on osoitettava olevan hallussaan;

3) luontaista todentamistekijää, joka perustuu johonkin luonnollisen henkilön fyysiseen ominaisuuteen.

Verkkopankkitunnuksissa käyttäjätunnus ja salasana ovat tietoon perustuvia todennustekijöitä ja tunnuslukulista on hallussa oloon perustuva tekijä. Nykyisissä vahvan sähköisen tunnistamisen palveluissa ei vielä käytetä biometriikkaa.

Kun reaaliaikaisen tilimaksamisen mahdollisuudet kasvavat uskon, että perinteiset pankit kehittävät vahvan tunnistamisen menetelmiään, jotta tilimaksamisen edut saadaan täysmääräisesti käyttöön. Biometriikan käyttöönotto tunnistamismenetelmissä parantaisi menetelmien käyttäjäystävällisyyttä.

Digitaalisen maksamisen tavat 2017

Maksukortit, verkkopankkitunnukset ja laskujen maksaminen

Valtaosa suomalaisten verkossa tekemistä ostoksista maksetaan joko verkkopankkipainikkeiden tai maksukorttien kautta. Perinteisiä laskuja maksetaan paljon e-laskuina ja verkkopankki-sovellusten (tietokone/mobiili) kautta. Verkkopankin käyttö on siirtynyt tietokoneelta mobiililaitteisiin. Esimerkiksi OP:n verkkopankkia käytettiin vuonna 2016 paljon enemmän mobiililaitteilla kuin tietokoneella.

Sovellusmaksaminen

Mobiilisovelluksiin perustuvissa palveluissa maksaminen on upotettu palvelun taustalle eikä kuluttajan tarvitse sovellusta ja palvelua käyttäessään aktiivisesti maksaa missään palvelun vaiheessa. Tällaisissa sovelluksissa käyttäjä syöttää maksukortin tiedot sovellukseen rekisteröitymisvaiheessa. Esimerkkipalveluita ovat Spotify, Netflix, Viaplay, Uber, Wolt, Parkman ja Easypark.

Mobiilimaksamisen sovellukset

OP Pivo, Danske Bankin Mobile Pay sekä Nordean Nordea Pay ja Siirto ovat mobiilimaksamisen tien auraajia Suomessa. Pivo, Mobile Pay ja Nordea Pay mahdollistavat älypuhelimella maksamisen muuttamalla maksukortin digitaaliseen muotoon. Nordean Siirto-sovellus perustuu asiakkaan tunnistamiseen ja reaaliaikaiseen tilimaksamiseen. Mobiilimaksusovelluksilla on ollut suuri vaikutus vertaismaksamisessa eli "kaverimaksamisessa". Nykyään on suosittua käteismaksun sijasta siirtää rahaa Mobile Pay:n tai Pivon kaltaisten sovellusten kautta. Vuoden 2017 maaliskuusta lähtien Pivon ja Mobile Pay:n kautta pystyi maksamaan liikkeiden lisäksi myös verkkokaupoissa. Verkkokauppojen maksuratkaisuja kehittävä Checkout Finland lisäsi sovellukset maksutavakseen, minkä jälkeen sovelluksilla voi maksaa yli 2500 verkkokaupan kassalla.

Bitcoin lompakot

Virtuaalivaluutta, jonka etuihin kuuluvat siirtojen nopeus, edullisuus, turvallisuus ja vielä tällä hetkellä anonyymiys. Valuutalla voi maksaa mobiili- ja tietokoneelle kehitettyjen lompakoiden avulla verkkokaupoissa, myymälöissä ja muille käyttäjille. Bitcoin on rakennettu lohkoketjuteknologiaa hyväksikäyttäen, mikä mahdollistaa sen, ettei yksikään valtiollinen taho tai pankki hallitse valuuttaa. Anonyymiteettinsä vuoksi valuutta yhdistetään verkkorikollisuuteen eikä yksikään valtio tai muu taho ole vielä hyväksynyt sitä viralliseksi rahaksi.

Trustly

Euroopassa toimiva tilipohjaisten verkkomaksujen mahdollistaja. Trustly toimii 29 eri maassa ja sen kautta tehdään yli 1,7 miljoonaa maksutapahtumaa joka kuukausi. Trustly toimii Suomessa etenkin nettikasinojen rahansiirroissa.

Moni

Suomessa aloittava MasterCardin verkostossa toimiva maksuvälineen liikkeeseenlaskija. Moni-palvelu koostuu maksukortista, tilistä ja mobiilisovelluksesta, jonka avulla voi tehdä tilisiirtoja, pyytää lainaa, jakaa laskuja ja tarkastella taloudellista tilaansa.

Alipay

Alipay on etenkin kiinalaisturistien Suomessa käyttämä digitaalisen maksamisen sovellus. Alipayta käyttää Kiinassa yli 450 miljoonaa ihmistä. Vuoden 2016 loppupuolella Alipayn Euroopan valloitus saavutti Suomen, jossa se otettiin käyttöön kiinalaisturistien suosimilla alueilla: Helsinki-Vantaan lentokentällä ja monissa Lapin matkailukohteissa.

Apple Pay

Maksusovellus, jonka avulla Applen älylaitteesta voi tehdä maksuvälineen. Sovellusta ei voi vielä käyttää Suomessa, mutta Euroopassa sitä käytetään jo Iso-Britanniassa, Ranskassa, Sveitsissä, Venäjällä ja Espanjassa. Apple Pay on maksu-sovellus, joka on suunniteltu mahdollisimman turvalliseksi ja helppokäyttöiseksi.

Maksamisen turvallisuus

Digitaalisen maksamisen turvallisuus on erittäin monen asian summa. Turvalliseen maksamiseen liittyvät olennaisesti kuluttajan verkkoasiointitaidot, fyysisen maksukortin käsittelytaito, kuluttajan mobiililaitteen turvallisuus sekä verkossa toimivien yritysten tietojärjestelmien turvallisuus. Erilaisten mobiilisovellusten kautta voi jo nyt maksaa ja tehdä mittavia hankintoja, joten mobiililaitteen turvallisuudesta on muodostunut merkittävä tekijä maksuvälineiden tietoturvassa. Verkko- ja maksuvälinerikolliset vievät suomalaisilta kuluttajilta miljoonia vuosittain.

Kun digitaaliset palvelut, maksaminen ja ihmisen henkilökohtaiset tiedot keskittyvät tulevaisuudessa mitä enemmän yhteen laitteeseen, älypuhelimeen, on sen turvallisuudesta huolehtiminen yksilön kannalta ensiarvoisen tärkeää. Älypuhelimen suojaaminen tunnusluvuilla tai sormenjäljellä on turvallisen asioinnin kannalta erittäin tärkeää.

Toinen merkittävä maksamisen turvallisuuden tekijä on kalasteluviestien ja verkkokauppaa haittaavien tilausansojen määrän lisääntyminen. Kalasteluviestien kautta yritetään saada luottokorttinumeroita sekä verkkopankkitunnuksia ja niiden avulla rikolliset saavat taloudellista hyötyä. Tilausansoilla kuluttaja huijataan mukaan palveluun jonkin vedätyksen kautta ja luottokorttia veloitetaan palvelun hinnaston mukaisesti.

Merkittävin nykyistä netissä tapahtuvaa korttimaksamista haittaava tekijä on verkkorikollisuus, jossa yritysten tietokannoista haetaan murtautumalla asiakkaiden korttinumeroita ja sen jälkeen niitä joko käytetään tai myydään muille väärinkäyttäjille Tor-verkon kauppapaikoilla. Digitaalisen kaupankäynnin määrän lisääntyessä verkkorikollisuuden määrä on myös kasvanut.

Maksamisen trendit

Älypuhelimet ovat yleistyneet 2010-luvulla ja myös maksamisen palvelut ovat siirtymässä mobiiliin. Vuonna 2016 Suomessa on otettu mobiilimaksamisen ensiaskeleet, kun Pivo ja Nordea Pay mahdollistivat maksukortin muuttamisen mobiililaitteessa toimivaan muotoon. Vuoden 2017 alusta myös Mobile Pay-sovelluksen kautta voi maksaa verkkokaupoissa ja kauppojen kassoilla. Kiinassa Alipay-maksutapaa käyttää yli 450 miljoonaa henkilöä ja 60% sen kautta tehdyistä transaktioista on tehty mobiililaitteella. Merkit viittaavat, että mobiilimaksamisesta on muodostumassa yksi maksamisen päätavoista.

Toinen vuoden 2017 muuttuva asia on maksamisen reaaliaikaistuminen. Maaliskuussa lanseeratun Siirto-maksujärjestelmän avulla maksut liikkuvat kotimaisten pankkien välillä reaaliajassa. Reaaliaikaisuus helpottaa digitaalista kaupankäyntiä, kun rahat siirtyvät heti, tavaratkin voivat vaihtaa omistajaa.

Älypuhelinten yleistymisen myötä myös niiden mahdollistamat biometrisen tunnistamisen ratkaisut saavat enemmän käyttäjiä. Tällä hetkellä sormenjälkitunnistus on yleisin biometrisen tunnistamisen muoto, mutta erilaiset käyttäjän käyttäytymistä seuraavat (behavioral biometrics) ratkaisut eivät ole pois suljettuja tulevaisuudessa. Kun maksamisen ratkaisut ja biometriikka kohtaavat älypuhelimissa, muodostuu biometriasta normaali osa maksun vahvistamisessa.

Viimeisenä merkittävänä trendinä pidän virtuaalivaluuttojen yleistymistä kaupankäynnissä. Euroopan Komissio on säätämässä asetusta, jonka ansiosta anonyymit sähköiset valuutat olisivat historiaa. Anonyymiyden poistumisen jälkeen virtuaalivaluuttojen asema paranee ja sen hyötyjä ryhdytään hyödyntämään laajasti.

Biometriikka

Erilaisten biometristen tunnisteiden käyttö on yleistynyt viimevuosina huimaa vauhtia. On lähes sääntö kuin poikkeus, että uudessa mobiililaitteessa on sormenjälkitunnistin ja sitä käyttämällä voi tunnistautua itse puhelimeen ja sen sisältämiin sovelluksiin. Visan teettämän tutkimuksen mukaan kuluttajat ovat valmiita biometrian käyttöön ja kaikkein mieluiten kuluttajat käyttäisivät sormenjälkitunnistusta maksun vahvistamisessa. Tutkimuksen mukaan kuluttajat pitävät sormenjälkeä tunnuslukua parempana vahvistamisen keinona, sillä se on nopeampi ja turvallisempi. Biometriikan suurimpana uhkana pidetään biometristen väärennösten mahdollisuutta. Jos jonkun sormenjälki kopioidaan, voidaan sitä käyttää tunnistautumiseen ilman, että henkilö huomaa. Biometrian yleistymisen myötä identiteettivarkauksien muodot lisääntyvät.

Sormenjälki

Tunnistautuminen tapahtuu sormenjälkilukijalla ja tunnistusohjelmistolla.
Tunnistusohjelmisto vertaa lukijan tuottamaa kuvaa tietokannassa olevaan mallinteeseen ja jos jälkien yksilölliset piirteet ovat tarpeeksi samanlaiset, järjestelmä kertoo tunnistautujan olevan sama henkilö mallinteen antajan kanssa. Sormenjälkitunnistuksessa ei saada ikinä 100% vastaavuutta mallinteeseen.

Kasvojen tunnistus

Kasvojen yksilöllisiä piirteitä erotellaan ja verrataan järjestelmän muistissa jo olevaan mallinteeseen. Mitattavia asioita ovat esim. silmien, nenän, leuan ja suun väliset geometriset suhteet. Kasvojentunnistusta voidaan käyttää myös ilman, että kohde huomaa tunnistamisen.

Iiristunnistus

Jokaisen ihmisen iiriksessä oleva kuviointi on monimutkainen ja yksilöllinen.
Iiristunnistuksessa silmästä otetaan kuva ja sitä verrataan järjestelmässä jo olevaan mallinteeseeen. Iiristunnistamista pidetään tarkkana ja luotettavana.

Maksupalvelu ja Finanssivalvonta

Maksupalvelun tarjonta on luvanvaraista eli jos yritys tahtoo palvelua tarjota, täytyy sillä olla viranomaisen myöntämä toimilupa. Suomessa maksupalvelun toimilupia myöntää Finanssivalvonta. Finanssivalvonta myös valvoo maksupalvelutarjoajien toimintaa ja sen lain määräämien edellytysten täyttymistä. Maksupalvelutarjoajan toimintaa rajoittaa Suomessa useampi laki, joista tärkeimpinä maksulaitoslaki, maksupalvelulaki ja laki rahanpesun ja terrorismin rahoittamisen estämisestä ja selvittämisestä.

Maksupalveluntarjoaja voi Suomessa toimia kahdella eri tavalla: hakemalla Finanssivalvonnalta maksulaitoksen toimiluvan tai ilmoittautumalla Finanssivalvonnalle ilman toimilupaa toimivaksi maksupalveluksi. Joko maksulaitoksen toimilupa tai ilmoitus ilman toimilupaa toimimisesta pitää olla tehtynä ennen varsinaisen liiketoiminnan aloittamista.

Maksupalvelun tarjoajan pitää raportoida toiminnastaan Finanssivalvonnalle myös normaalin tilivuoden aikana. Ilman toimilupaa toimittaessa tilivuoden aikainen raportointi on hieman kevyempää. Raportointiin sisältyvät tiedot yrityksen johtohenkilöistä, heidän ammattitaidostaan sekä soveltuvuudesta tehtävään, merkittävän toiminnan ulkoistamisesta ja maksutapahtumien yhteismäärästä. Maksulaitoksen toimiluvan saanut taho on näiden tietojen lisäksi velvollinen raportoimaan operatiivisista riskeistä, asiakasriskeistä, omistajamuutkosista, luotoista ja erääntyneistä saamisista, yrityksen omista varoista ja vakavaraisuudesta sekä tilinpäätökseen ja kirjanpitoon perustuvista valvontatiedoista.

Maksulaitoksen toimiluvan hakeminen vai ilman toimilupaa toimimisesta ilmoittaminen?

1 Liiketoimintaa suunnitellessa ja rakennettaessa kannattaa ottaa yhteys Finanssivalvonnan Innovaatio-Helpdesk-palveluun. Palvelun kautta voi saada arvokkaita kommentteja ja vastauksia askarruttaviin kysymyksiin.

2 Päätös siitä haetaanko maksulaitoksen toimilupaa vai ilmoitetaanko toiminnasta ilman toimilupaa. Kuinka laajaa toiminta on? Toimitaanko kansainvälisesti vai vain Suomessa? Päätös vaikuttaa merkittävästi haku/ilmoitusprosessiin.

3 **Ilmoitus ilman toimilupaa toimimisesta**

- Toimintaa vain Suomessa ja transaktioita keskimäärin alle 50 000€ vuodessa/hlö

Sisältö:

- Perusteellinen liiketoimintasuunnitelma
- Selvitykset avainhenkilöistä ja muista olennaisista oikeushenkilöistä
- Selvitys asiakasvarojen käsittelystä ja suojaamisesta
- Selvitys käytettävistä tunnistusmenetelmistä
- Selvitys asiakkaan tuntemiseen liittyvistä toimenpiteistä
- Yhteystiedot kommunikointiin

3 **Hakemus maksulaitoksen toimiluvasta**

- Mahdollistaa toiminnan Euroopan talousalueen (ETA) maissa
- Hakemusprosessi tarkempi ja perus-teellisempi kuin viereisessä ilmoituksessa

Sisältö:

- Perusteellinen liiketoimintasuunnitelma
- Selvitykset avainhenkilöistä ja muista olennaisista oikeushenkilöistä
- Selvitys asiakasvarojen käsittelystä ja suojaamisesta
- Selvitys käytettävistä tunnistusmenetelmistä
- Selvitys asiakkaan tuntemiseen liittyvistä toimenpiteistä
- Omat varat ja taloudellinen tilanne
- Sisäinen valvonta
- Riskien hallinta
- Yhteystiedot kommunikointiin

4 Tarvittavien lisäselvitysten tekeminen ja kommenttien huomiointi.

5 Finanssivalvonta hyväksyy tai hylkää ilmoituksen tai hakemuksen toimiluvasta.

Hakemusprosessi on erittäin yksilöllinen jokaisen yrityksen kohdalla ja läpimenoaika riippuu liiketoiminnan ja hakemuksen laadusta.

Lisätietoja

Mielenkiintoisia seurattavia aiheita ja julkaisuja:

Suomen Pankin maksufoorumi ja maksuneuvosto:
Maksufoorumi on vuosittain järjestettävä tilaisuus, jonka tarkoituksena on edistää maksamisen markkinoita Suomessa tuomalla yhteen tilaisuuteen alan tärkeimmät osaajat. Maksuneuvosto on asiantuntijaryhmä, joka tuottaa tutkimuksia ja julkaisuja aiheesta.
https://www.suomenpankki.fi/fi/raha-ja-maksaminen/maksujarjestelmat/maksufoorumi/

Mobey Forum:
Voittoa tavoittelematon finanssialan teknologista kehitystä seuraava taho, joka julkaisee tutkimuksia ja raportteja ajankohtaisista aiheista. Mobey Forum koostuu kansainvälisissä pankeissa työskentelevistä asiantuntijoista. www.mobeyforum.org

Euroopan keskuspankki, SecuRe Pay:
Euroopan keskuspankin turvalliseen kuluttajamaksamiseen keskittyvä yhteenliittymä. Osallistujat jakavat tietoa maksumarkkinoista ja sen ajankohtaisista asioista. Julkaisee raportteja ja tilastoja ETA-alueen markkinasta. www.ecb.europa.eu > hae SecuRe Pay

EU Komission uusi tietosuoja-asetus:
Komissio on säätänyt päivitetyn tietosuoja-asetuksen, jonka soveltaminen alkaa 25.5.2018. Uusi asetus tuo henkilötietojen käsittelyn digiaikaan ja sen tavoitteena on määrittää tarkemmin yritysten velvollisuuksista henkilötietojen käsittelyssä ja säilömisessä.
Lisätietoja: tietosuoja.fi > EU:n tietosuojauudistus

Turbiini

YRITYSKIIHDYTTÄMÖ

LAUREA

AMMATTIKORKEAKOULU