Kai Korhonen

PSD2 ja sen vaikutukset verkkomaksamisen tietoturvaan ja liiketoimintamalleihin

Tietotekniikan pro gradu -tutkielma

27. syyskuuta 2016

Jyväskylän yliopisto

Tietotekniikan laitos

Tekijä: Kai Korhonen

Yhteystiedot: kaivkorhonen@gmail.com

Ohjaajat: Timo Hämäläinen

Työn nimi: PSD2 ja sen vaikutukset verkkomaksamisen tietoturvaan ja liiketoimintamalleihin

Title in English: PSD2 and its effects on web payment security and business models

Työ: Pro gradu -tutkielma

Suuntautumisvaihtoehto: Ohjelmisto- ja tietoliikennetekniikka

Sivumäärä: 60 + 0

Tiivistelmä: Verkkomaksujen ympärille on kehittynyt viimeisen vuosikymmenen aikana kokonainen toimiala, jossa liikutellaan paljon arkaluonteisia tietoja, ja jossa tietoturva on yksi avainsanoista. Alan toimijoita säädellään maan sisäisten laitosten lisäksi EU:n maksupalveludirektiivein, joista järjestyksessä toinen otetaan jäsenmaiden lainsäädäntöön vuoden 2017 alkuun mennessä. Muiden asioiden ohella se pakottaa pankit avaamaan ohjelmointirajapinnat, jotka antavat kolmansille osapuolille mahdollisuuden käyttää verkkokauppojen asiakkaiden pankkitunnuksia pankkimaksujen käynnistämiseen.

Toinen maksupalveludirektiivi tuo mukanaan tietoturvaongelmia, joita ei ole kovin tarkasti tutkittu. Tässä työssä tehdään kirjallisuuskatsaus verkkomaksamisen tietoturvasta, minkä lisäksi tutkitaan toista maksupalveludirektiiviä ja sen vaikutuksia verkkomaksamisen tietoturvaan. Työssä tarjotaan myös tietoturvallinen tapa toteuttaa toisen maksupalveludirektiivin mahdollistamia maksutapoja.

Avainsanat: Verkkomaksaminen, tietoturva, tietoturvallisuus, maksupalveludirektiivi, toinen maksupalveludirektiivi,

Abstract: Web payments have created a whole industry around them in the last decade where sensitive data is moved around and where security is one of the key concepts. On top of internal facilities, members of the EU are regulated by EU directives of which the second will be taken to legislation by the start of year 2017. It forces the banks to open interfaces that allow third parties to use web shop customers banking credentials in order to initiate payments.

Second directive on payment services brings up a set of web security hazards that have yet to be studied. In this thesis a literature review is made on web payment security. I will also study the second directive on payment services and its effects on web payment security and present a secure way to implement a payment service that makes use of the directive.
Keywords: Web-payment, cyber security, payment service provider, directive on payment services, second directive on payment services

Sisältö

Termistö

AISP	Account Information Service Provider
API	Application Programming Interface
ASPSP	Account Servicing Payment Service provider
BEAST	Browser Exploit Against SSL/TLS
CBC	Cipher Block Chaining
cPSP	Collective Payment Service Provider
CSS	Cascading Style Sheet
EBA	European Banking Authority
EU	Euroopan Unioni
Jonosalaus	Stream cipher
Kuljetuskerros	Transport Layer
Lohkosalaus	Block cipher
MiTM	Man in The Middle
NIST	National Institute of Standards and Technology
Nollatyyli	Null Style
OWASP	Open Web Application Security Project
PISP	Payment Initiation Service Provider
POODLE	Padding Oracle On Downgraded Legacy Encryption
PSD	Directive on Payment Services
PSP	Payment Service Provider
REST	Representational State Transfer
RTS	Regulatory Technical Standards

RSA	Rivest, Shamir ja Adleman
Tiiviste	Fingerprint
TLS	Transport Layer Security
TLSHP	Transport Layer Security Handshake Protocol
TLSRP	Transport Layer Security Record Protocol
TPP	Third Party Provider
Tyyppisekoitushyökkäys	Type confusion attack
Sanomatiiviste	Hash
SHA	Secure Hash Algorithm
SOAP	Simply Object Access Protocol
Sormenjälkilaskenta	Authcode calculation
SSL	Secure Socket Layer
SSL-kättely	Secure Socket Layer Handshake
SSLAP	Secure Socket Layer Alert Protocol
SSLCP	Secure Socket Layer Cipher Protocol
SSLHP	Secure Socket Layer Handshake Protocol
SSLRP	Secure Socket Layer Record Protocol
XS2A	Access to Account

1 Johdanto

Tämä pro gradu -työ käsittelee toisen maksupalveludirektiivin vaikutuksia verkkomaksamisen tietoturvaan verkkomaksupalvelun tarjoajan näkökulmasta katsottuna. Verkkomaksupalvelun tarjoajan tehtävä on muun muassa tarjota turvallista tiedonsiirtoa verkkokauppojen ja rahoituslaitosten välillä. Toimialalla, jossa käsiteltävät tiedot liittyvät usein yksityishenkilöihin ja rahaan, sääntely on tarkkaa ja velvoitteet myös tietoturvan suhteen tiukat. Suomessa sääntelyä hoitavan Finanssivalvonnan lisäksi toimintaa säädellään Euroopan Unionin asettamilla maksupalveludirektiiveillä, joista ensimmäinen maksupalveludirektiivi otettiin Suomessa käyttöön 1.11.2009. Toisesta maksupalveludirektiivistä on annettu EU-direktiivi vuoden 2015 lopussa, ja se otetaan EU:n jäsenmaiden lainsäädäntöihin vuoden 2017 loppuun mennessä.

Toisen maksupalveludirektiivin suurin muutos on kolmansien osapuolien lupa käsitellä kuluttajien pankkitunnuksia verkkomaksua suoritettaessa. Aiemmin asiakas on ohjattu pankin verkkopalveluun suorittamaan maksu omilla verkkopankkitunnuksillaan. Toisen maksupalveludirektiivin astuessa voimaan asiakas voi syöttää pankkitunnukset jo verkkokaupassa, jonka jälkeen verkkomaksupalvelun tarjoaja käynnistää maksun hänen pankkitunnuksillaan. Kuluttajan kannalta maksuprosessi yksinkertaistuu, mutta tällainen menettely aiheuttaa myös uusia tietoturvauhkia.

Tutkimustyössä tehdään kirjallisuuskatsaus verkkomaksamisen tietoliikenneturvallisuudesta ja käytetyistä salaustekniikoista sekä maksupalvelun tarjoajien toiminnasta ja sääntelystä. Lisäksi työssä esitellään Euroopan Unionin asettamia ensimmäistä ja toista maksupalveludirektiiviä sekä niiden käyttöönottoprosessia. Koska tietoturvallisuuden heikoin lenkki on useimmissa tapauksissa käyttäjä, tutkitaan myös käyttäjän manipulointia (eng. Social engineering). Osaan työn aihealueista on erittäin vähän, tai ei ole ollenkaan tieteellisiä julkaisuja. Näissä tapauksissa käytetään luotettavimpia lähteitä, kuten Euroopan Unionin virallisia julkaisuja.

Tämän työn tarkoitus on tutkia nykyisten verkkomaksupalveluiden tietoturvaa, minkä lisäksi tutkitaan toisen maksupalveludirektiivin tarjoamia vaikutuksia ja mahdollisuuksia maksupalvelun tarjoajien toimintaan. Tutkimuksessa pyritään myös tarjoamaan tietoturvallinen tapa toteuttaa maksualoitepalvelu. Tutkimuksessa tarkastellaan myös maksualoitepalvelun taloudellisia aspekteja ja verrataan sitä nykyiseen toimintamalliin.

2 Tietoliikenneturvallisuus

Tiedon turvallisuus ja salaaminen ovat nykyajan yrityksille elinehto. Kuluttajista kerätään yritysten tietokantoihin valtavia määriä enemmän ja vähemmän arkaluonteisia tietoja, eikä nykyajan trendeihin kuulu tiedon lopullinen poistaminen. Se mitä Internetiin laitetaan, pysyy siellä. Lisäksi tekniikan kehitys ja ihmisten taipumus mukavuudenhaluisuuteen on johtanut siihen, että kaiken pitäisi olla helppoa ja nopeaa, myös verkossa maksamisen ja toimimisen. Kymmenen vuotta sitten luottokortti ja sen tiedot pysyivät tallessa lompakossa, eikä niitä ollut sieltä helppo varastaa. Nyt ostosten tekeminen sekä asioiden hoitaminen ja maksaminen verkossa on arkipäiväistä ja nopeaa. Tämä tarkoittaa myös sitä, että kaikki maksamiseen ja kuluttajien tunnistamiseen tarvittava tieto liikkuu verkon yli. Identiteetti- ja korttitietovarkauksia tehtaillaankin Internetin välityksellä valtavia määriä, ja tasaisin väliajoin voi lukea isoista tietomurroista yritysten asiakastietoihin. Näistä syistä tieto- ja tietoliikenneturvallisuus ovat nousseet suureen rooliin tietotekniikan kehityksessä ja yritysten toiminnassa.

Tietoturvallisuus voidaan määritellä kymmenillä eri tavoilla. Lisäksi tietoturvallisuus voidaan jaotella useaan osa-alueeseen. Esimerkiksi Ruohonen (2002) jaottelee tietoturvan seuraaviin osa-alueisiin, joista perehdyn työssä tarkemmin vain muutamaan:

- tietoaineiston turvallisuus
- ohjelmistoturvallisuus
- tietoliikenneturvallisuus
- fyysinen turvallisuus
- laitteistoturvallisuus
- henkilöstöturvallisuus
- käyttöturvallisuus
- hallinnollinen turvallisuus

Tietoturvasta puhuttaessa tiedon ominaisuudet jaotellaan yleisesti tiedon luottamuksellisuuteen, eheyteen ja käytettävyyteen. Paavilaisen (1998) mukaan ”Tiedon käytön mahdollistaminen ja turvaaminen ovat tietoturvan tärkeimpiä vaatimuksia, minkä takia tiedon ominaisuudet on otettu tiedon turvaamisen lähtökohdiksi”. Paavilainen määrittelee kyseiset käsitteet kirjassaan seuraavasti: **Luottamuksellisuus (confidentiality):** Tiedot ovat vain niihin oikeutettujen henkilöiden ja organisaatioiden saatavilla, eikä niitä paljasteta muille. **Eheys (integrity):** Tiedot eivät muutu tai tuhoudu laitteisto-, järjestelmävian tai inhimillisen toiminnan tms. vuoksi. **Käytettävyys (availability):** Tiedot ja niiden muodostamat palvelut ovat niihin oikeutettujen henkilöiden käytettävissä tai saatavissa.

Tässä työssä tieto- ja tietoliikenneturvallisuuden tutkiminen rajattiin pääasiallisesti verkkomaksutapahtuman aikaiseen tietoliikenneturvallisuuteen. Maksuprosessin aikana järjestelmät käyttävät useita keinoja tiedon salaamiseen ja suojaamiseen, eikä normaali käyttäjä niitä monesti edes huomaa. Paytrail käyttää yhteyksien muodostamiseen salausprotokollaa, minkä lisäksi maksutiedoista lasketaan erilaisia tunnisteita maksutietojen oikeellisuuden takaamiseksi. Lisäksi rahoituslaitokset vaativat tunnistautumista korttitiedoilla, pankkitunnuksilla tai sekä että.

2.1 Sormenjälkilaskenta

Paytrailin kautta tehdyssä maksutapahtumassa tilaustiedot tarkistetaan sormenjälkilaskennalla neljässä eri välissä: Verkkokauppa - Paytrail, Paytrail - rahoituslaitos, rahoituslaitos - Paytrail, Paytrail - verkkokauppa. Tiedot tarkistetaan aina, kun niitä siirretään toimijalta toiselle. Näin voidaan varmistua siitä, ettei mahdollinen hyökkääjä ole missään välissä päässyt muuttamaan niitä.

Paytrail käyttää näihin tarkistuksiin sormenjälkilaskentaa (Eng. authcode calculation), joka perustuu MD5-laskentaan ja salaisen avaimen käyttöön. Kun maksutiedot lähetetään verkkokaupasta Paytrailin järjestelmään, niistä muodostetaan MD5-tiiviste, joka lähetetään maksutietojen mukana. Osana tiivistettä käytetään salaista avainta, jonka tietävät vain verkkokauppias ja Paytrail. Järjestelmä laskee vastaanottamistaan maksutiedoista MD5-tiivisteen, ja tarkistaa tiivisteiden yhteneväisyyden. Jos tiivisteet ovat yhtenevät, eivät maksutiedot ole muuttuneet.

2.1.1 MD5-salausalgoritmi

MD5 on niin sanottu sanomatiiviste salausalgoritmi (Eng. Message digest algorithm), jolla viestistä muodostetaan lyhyempi, lukemattomissa oleva tiiviste (fingerprint). Tarkoitus on, ettei muodostetusta tiivisteestä voida päätellä mitään alkuperäisestä viestistä. Algoritmin on kehittänyt Ron Rivest vuonna 1992 Bostonin MIT:ssä (Rivest, 2002).

Periaatteessa kaksi alkuperäistä viestiä voivat tuottaa saman MD5-tiivisteen, mutta tällaisen sattuman tuottaminen vaatisi kokoluokaltaan 2^64 kappaletta operaatiota. Todennäköisyys on häviävän pieni, ja siihen liittyvä riski erittäin vähäinen.

2.1.2 MD5-tiivisteen muodostaminen

MD5 tiiviste muodostetaan merkkijonosta viidellä askeleella. Ohjelmointikielistä löytyy yleisesti valmiit funktiot MD5:lle, mutta halutessaan algoritmin voi ohjelmoida itse. Tällöin suojaus tehdään varmasti oikein. Alla Rivestin (Rivest, 2002) ohjeet kehittämänsä algoritmin käytölle.

1. Täytebittien liittäminen
    a. Alkuperäistä viestiä jatketaan niin, että sen pituus biteissä laskettuna on 448 jakojäännös 512:sta. Viesti siis pidennetään niin, että sen pituus on 64 bittiä lyhyempi, kuin että se olisi 512 bitillä jaollinen. Tämä tehdään, vaikka alkuperäinen viesti täyttäisi pituusmääritelmän.
    b. Viestiin lisätään yksittäinen ”1” bitti, jonka jälkeen lisätään ”0” bittejä niin paljon, että em. pituusmääritelmä täyttyy.
2. Pituuden liittäminen
    a. Edellisen askelen tulokseen lisätään 64-bittinen kuvaus alkuperäisen viestin pituudesta. Jos alkuperäisen viestin pituus on isompi kuin 2^64, käytetään siitä vain 64 bittiä matalassa tavujärjestyksessä (Eng. ”Low-order 64 bits”).

Tässä vaiheessa, askeleiden 1 ja 2 jälkeen, viestin pituus on tarkalleen 512 bitin kerrannainen. Vastaavasti viestin pituus on myös 16 sanan (32-bitin kokonaisuuden) kerrannainen.

3. MD-puskurin alustaminen
    a. Sanomatiivisteen laskennassa käytetään 4-sanaista puskuria (A, B, C, D). Tässä esimerkissä jokainen on 32-bittinen rekisteri. Nämä rekisterit alustetaan heksadesimaaliluvuiksi ja järjestetään tavujärjestyksessä pienimmästä suurimpaan.
    b. word A: 01 23 45 67
       word B: 89 ab cd ef
       word C: fe dc ba 98
       word D: 76 54 32 10
4. Viestin prosessointi 16 sanan paloissa
    a. Määritellään ensin neljä lisäfunktiota, jotka jokainen ottavat syötteenä kolme 32-bittistä sanaa ja tuottavat yhden 32-bittisen sanan. Alla olevissa funktioissa on käytetty merkkiä v kuvaamaan joukko-opin yhdiste -funktiota.

b. F(X,Y,Z) = XY + not(X) Z

G(X,Y,Z) = XZ v Y not(Z)

H(X,Y,Z) = X xor Y xor Z

I(X,Y,Z) = Y xor (X v not(Z))

c. Jokaisen bitin asemassa F toimii konditionaalina: ”jos X niin Y muuten Z”. Tämä askel käyttää 64-paikkaista sinifunktiosta muodostettua taulua T[1…64]. Alla oleva kuva 1 selittää operaatiotasolla, mitä tässä askeleessa tulee tehdä.

d.

```
/* Process each 16-word block. */
For i = 0 to N/16-1 do
  /* Copy block i into X. */
  For j = 0 to 15 do
    Set X[j] to M[i*16+j].
  end /* of loop on j */

  /* Save A as AA, B as BB, C as CC, and D as DD. */
  AA = A
  BB = B

  CC = C
  DD = D

  /* Round 1. */
  /* Let [abcd k s i] denote the operation
       a = b + ((a + F(b,c,d) + X[k] + T[i]) <<< s). */
  /* Do the following 16 operations. */
  [ABCD  0  7  1]  [DABC  1 12  2]  [CDAB  2 17  3]  [BCDA  3 22  4]
  [ABCD  4  7  5]  [DABC  5 12  6]  [CDAB  6 17  7]  [BCDA  7 22  8]
  [ABCD  8  7  9]  [DABC  9 12 10]  [CDAB 10 17 11]  [BCDA 11 22 12]
  [ABCD 12  7 13]  [DABC 13 12 14]  [CDAB 14 17 15]  [BCDA 15 22 16]

  /* Round 2. */
  /* Let [abcd k s i] denote the operation
       a = b + ((a + G(b,c,d) + X[k] + T[i]) <<< s). */
  /* Do the following 16 operations. */
  [ABCD  1  5 17]  [DABC  6  9 18]  [CDAB 11 14 19]  [BCDA  0 20 20]
  [ABCD  5  5 21]  [DABC 10  9 22]  [CDAB 15 14 23]  [BCDA  4 20 24]
  [ABCD  9  5 25]  [DABC 14  9 26]  [CDAB  3 14 27]  [BCDA  8 20 28]
  [ABCD 13  5 29]  [DABC  2  9 30]  [CDAB  7 14 31]  [BCDA 12 20 32]

  /* Round 3. */
  /* Let [abcd k s t] denote the operation
       a = b + ((a + H(b,c,d) + X[k] + T[i]) <<< s). */
  /* Do the following 16 operations. */
  [ABCD  5  4 33]  [DABC  8 11 34]  [CDAB 11 16 35]  [BCDA 14 23 36]
  [ABCD  1  4 37]  [DABC  4 11 38]  [CDAB  7 16 39]  [BCDA 10 23 40]
  [ABCD 13  4 41]  [DABC  0 11 42]  [CDAB  3 16 43]  [BCDA  6 23 44]
  [ABCD  9  4 45]  [DABC 12 11 46]  [CDAB 15 16 47]  [BCDA  2 23 48]

  /* Round 4. */
  /* Let [abcd k s t] denote the operation
       a = b + ((a + I(b,c,d) + X[k] + T[i]) <<< s). */
  /* Do the following 16 operations. */
  [ABCD  0  6 49]  [DABC  7 10 50]  [CDAB 14 15 51]  [BCDA  5 21 52]
  [ABCD 12  6 53]  [DABC  3 10 54]  [CDAB 10 15 55]  [BCDA  1 21 56]
  [ABCD  8  6 57]  [DABC 15 10 58]  [CDAB  6 15 59]  [BCDA 13 21 60]
  [ABCD  4  6 61]  [DABC 11 10 62]  [CDAB  2 15 63]  [BCDA  9 21 64]

  /* Then perform the following additions. (That is increment each
     of the four registers by the value it had before this block
     was started.) */
  A = A + AA
  B = B + BB
  C = C + CC
  D = D + DD

end /* of loop on i */
```

Kuva 1: MD5-algoritmi

5. Tuloste
    a. Viestitiivisteen tuloste on A,B,C,D aloitettuna A:n matalimmasta tavusta ja loppuen D:n korkeimpaan tavuun.

2.2 Secure Socket Layer (SSL)

Secure Socket Layer (SSL) on Netscapen 1990-luvun puolivälissä kehittämä salaustekniikkaan perustuva protokolla. SSL oli ensimmäinen laatuaan ja nousikin siitä syystä nopeasti yleiseksi käytännöksi. Se estää ulkopuolista näkemästä asiakkaan ja palvelimen välisen verkkoliikenteen sisältöä, vaikka tämä pääsisikin näkemään salaamattoman verkon tietoliikennettä. (Järvinen 2002, 2006).

SSL:n tarkoitus on tiedon salaamisen ja purkamisen lisäksi toimia takeena verkkosivun aitoudesta, ja se näkyy käyttäjälle yleensä selaimen osoitepalkin vasemmassa reunassa pienenä lukon kuvana. SSL kytkeytyy päälle käyttäjän siirtyessä sitä käyttävään palveluun. SSL:n käyttöönotto edellyttää palveluntarjoajalta tarvittavien varmenteiden ja ohjelmien hankkimista. (Järvinen 2002, 2006).

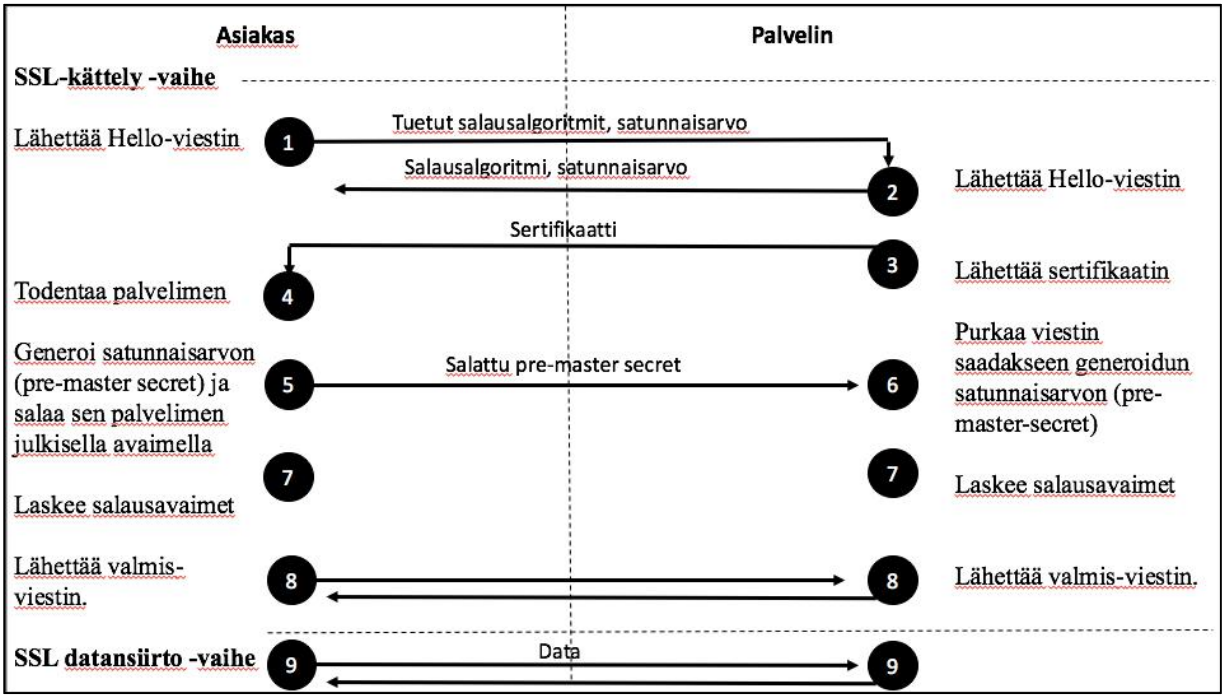
SSLv3 (SSL:n versio 3.0) on ollut laajalti käytössä vielä lähivuosiin saakka, mutta viime vuosina siitä on löydetty paljon haavoittuvuuksia. Näiden haavoittuvuuksien myötä SSL on jäänyt pois yleisestä käytöstä, ja sen on korvannut uusi salausprotokolla, joka toimii samojen periaatteiden mukaisesti. Koska SSL on ollut viimeisten kahden vuosikymmenen yleisin salausprotokolla, ja myös nykyinen käytäntö toimii samojen periaatteiden mukaisesti, käydään näitä periaatteita läpi hieman tarkemmin.

SSL-protokollan toiminta koostuu pääosin kahdesta tasosta. Alemmalla tasolla toimii SSLRP (SSL record protocol), jota käytetään korkeampien tasojen protokollien kapselointiin. Niistä oleellisin on SSLHP (SSL handshake protocol), jonka avulla käyttäjä ja palvelin tunnistavat toisesta, neuvottelevat käytettävät salausalgoritmit ja muodostavat session aikana käytettävät salausavaimet. (Freier & Karlton, 2011). Näiden tasojen lisäksi käytössä

on protokollat hälytyksien lähettämiseen (SSL Alert Protocol) ja salausalgoritmin vaihtamiseen (SSL Cipher Spec Protocol) (Eldewahi;Sharfi;Mansor;& Mohamed, 2015).

2.2.1 SSL-kättely

Jokaisen SSL-session alussa palvelimen ja asiakkaan välillä tehdään SSL-kättely (SSL-handshake), jonka avulla palvelin voi todentaa itsensä asiakkaalle käyttäen julkisen avaimen tekniikoita. Kättelyn aikana palvelin ja asiakas lähettävät toisilleen todentamisessa käytettäviä tietoja ja luovat tarvittavat salausavaimet aloitettavalle sessiolle. Kättelyn aikana asiakkaan selain tarkistaa myös palvelimen tarjoaman varmenteen aitouden. Kun kättely on saatettu loppuun, sessio on aloitettu ja osapuolet käyttävät siinä luotuja avaimia lähetettävien tietojen salaamiseen, purkamiseen, ja tiedon oikeellisuuden varmistamiseen. (Bhiogade, 2002). Alla olevassa kuvassa 2 (Oracle, 2011) näkyvät vielä tarkemmin kättelyn aikana lähetettävät viestit ja salatun yhteyden muodostaminen.



Kuva 2: SSL-kättely

Yleisimmin SSL käyttää avainten vaihtamiseen RSA-tekniikkaa, joka on yksi julkisen avaimen salausalgoritmeistä. Julkisen avaimen tekniikat käyttävät kahta epäsymmetristä avainta. Toista tiedon salaamiseen ja toista tiedon purkamiseen. Julkista avainta voidaan jakaa vapaasti, mutta yksityisavainta ei koskaan jaeta. Julkisella avaimella salattu tieto voidaan purkaa vain yksityisellä avaimella. Vastaavasti, yksityisellä avaimella salattu tieto voidaan purkaa vain julkisella avaimella. (Bhiogade, 2002). Julkisen avaimen tekniikka esitellään tarkemmin luvussa 2.3.

2.2.2 SSL-varmenteet

SSL-sertifikaatti on sähköinen aitoustodistus, joka sisältää tietoja palvelun tarjoajasta. Varmenne osoittaa varmenteen myöntäjän tarkistaneen, että palveluntarjoaja on kyseinen palveluntarjoaja, ja että heidän palvelunsa toimii kyseisessä osoitteessa. Tämän lisäksi palveluun muodostettavan yhteyden kautta kulkeva tieto on koodattu myöntäjän salaisella avaimella. Yritykset hankkivat varmenteita niitä tarjoavilta yrityksiltä. (Järvinen, 2006, 379). SSL sertifikaatit ovat kuitenkin kenen tahansa ostettavissa, eikä sellaisen näkeminen käyttämälläsi sivustolla automaattisesti tarkoita, että kyseiseen sivustoon voisi luottaa sataprosenttisesti.

2.3 Julkisen avaimen tekniikat

Jotta voidaan tarkemmin perehtyä julkisten avainten salaustekniikoihin, tulee ensin perehtyä symmetrisen avaimen tekniikkaan. Symmetrisen avaimen tekniikka tarkoittaa viestin salaamista jollakin prosessilla siten, että se voidaan purkaa kääntämällä kyseinen prosessi ympäri. (Batten, 2013). Jos viesti esimerkiksi kirjoitetaan suomeksi ja salataan vaihtamalla jokaisen merkin paikalle sitä edustava kokonaisluku (a=1, b=2, c=3 jne.), saadaan alkuperäinen viesti vaihtamalla jokaisen kokonaisluvun kohdalle kirjain jota se edustaa. Tällaisessa tapauksessa sekä lähettäjä että vastaanottaja käyttävät viestin salaamiseen ja purkamiseen samaa prosessia, toisin sanoen salausavainta.

Viestien murtamattomuus perustuu pitkälti avainten pituuksiin. Mitä pidempi avain, sitä hankalampaa viestejä on murtaa. OWASP (Open Web Application Security Project) suosittelee tällä hetkellä käytettäväksi avaimia, joiden pituus on vähintään 2048 bittiä. Lisäksi avaimien säilytys tulee hoitaa tietoturvallisesti. (Open Web Application Security Project, 2016).

2.3.1 Diffie-Hellman avaimenvaihto

Ongelma, joka jarrutti salakirjoittamisen käyttämistä liikemaailmassa, oli salausavainten vaihtaminen. 1976 Whit Diffie ja Martin Hellman kuvasivat turvallisen menetelmän muodostaa yhteinen avain suojaamattoman yhteyden yli. Menetelmä pohjautuu eksponentteihin, ja eksponenttien ominaisuuteen kertoa niitä missä tahansa järjestyksessä saaden aina saman tuloksen. Perusidea on, että kahdella henkilöllä on molemmilla kaksi avainta: yksi viestin salaamiseen ja yksi viestin purkamiseen. Jotta avaimet olisivat käänteiset toisiinsa nähden, ne tulee sitoa toisiinsa jollain perusteellisella tavalla siten, ettei ulkopuolinen voi päätellä toista avainta toisesta. Salausavain voidaan tämän jälkeen julkaista, ja vain viestin vastaanottaja tietää oman, viestin purkamiseen käytettävän avaimen. (Batten, 2013).

Tuohon aikaan tapaa tällaisen menetelmän toteuttamiseen ei kuitenkaan ollut olemassa. Lisäksi Diffie-Hellman -tekniikka soveltuu pelkästään avainten vaihtamiseen. Ei itse viestin salaamiseen. Edelleen tarvittiin tapa lähettää tietoa salatusti salaamattoman yhteyden yli. (Batten, 2013).

2.3.2 RSA

1978 Rivest Shamir ja Adleman julkaisivat ensimmäisen menetelmän salatun tiedon lähettämiseen salaamattoman yhteyden yli. Kyseinen menetelmä tunnetaan nykyään laajalti nimellä RSA, joka tulee edellä mainittujen henkilöiden sukunimistä. Saman tyyppinen salausmenetelmä keksittiin Iso-Britannian tiedustelupalvelussa jo 1970-alussa, mutta tieto siitä pidettiin salattuna aina vuoteen 1997 saakka. RSA perustuu siihen, että suurten alkulukujen tulon jakaminen tekijöihin on hyvin vaikeaa. (Batten, 2013). RSA:han voi tutustua

tarkemmin esimerkiksi Rivestin, Shamirin ja Adlemanin paperista (Rivest;Shamir;& Adleman).

2.4 Transport Layer Security (TLS)

SSL:n vanhentuessa tilalle on tullut uusi salausprotokolla, transport layer security (TLS). Kuten edeltäjänsäkin, sen tarkoitus on tarjota tapa siirtää tietoa turvallisesti ja eheästi asiakkaan ja palvelimen välillä. Toimintaperiaatteet ovat hyvin samanlaiset kuin SSL:ssä, koska TLS on kehitetty SSLv3:n pohjalta (Dierks T. , 2008). Työn kirjoitushetkellä (7.6.2016) TLS:n uusin versio on TLS 1.2, joka on hyvin laajalti verkkosivustoilla ja verkkopalveluissa käytetty salausprotokolla.

Myös TLS koostuu pääosin kahdesta protokollasta: TLSRP (TLS Record Protocol) ja TLSHP (TLS Handshake Protocol). TLSRP tarjoaa yhteyden suojausta, jossa on kaksi perusominaisuutta: Yhteys on suojattu, ja yhteys on luotettava. Yhteys suojataan salaamalla sen yli kulkeva tieto. Yhteyden luotettavuus varmistetaan eheydentarkistus laskennoilla. Laskennoilla varmistetaan, ettei tieto ole muuttunut palvelimen ja käyttäjän välillä. Tämän lisäksi TLSRP:tä käytetään korkeampien tasojen kapselointiin, kuten SSL:ssäkin. TLS-kättelyprotokollan tarkoitus on käyttäjän ja palvelimen tunnistus, käytettävien salausalgoritmien sopiminen ja tarvittavien salausavaimien muodostaminen, aivan kuten SSL-kättelyssäkin. (Dierks T. , 2008).

2.5 SSL / TLS haavoittuvuudet

Molemmat edellä esitellyistä salausprotokollista tarjoavat tiedon eheyttä, tiedon salausta ja palvelun tunnistamista kahden keskustelevan ohjelman välillä. TLS on kehitetty täysin SSL:n pohjalta, ja ne toimivat hyvin samankaltaisilla periaatteilla. (Eldewahi;Sharfi;Mansor;& Mohamed, 2015). Näistä syistä molempien protokollien ongelmia ja parannukset käsitellään samassa luvussa. Luvussa käydään läpi oleellisimmat SSL / TLS haavoittuvuudet. Kappaleessa esitellään myös keino hyökkäyksen estää tai hankaloittaa hyökkäyksen tekemistä, jos sellaisia on löydetty. Luvussa on esitelty vain muu-

tama haavoittuvuus. Lisää haavoittuvuuksista voi lukea esim. (Eldewahi;Sharfi;Mansor;& Mohamed, 2015), (Batten, 2013), (Fedler, 2013) tai (Mayer & Schwenk, 2013).

2.5.1 SSL Stripping

SSL / TLS -kättelyn alussa palvelin ja asiakas sopivat käytettävien salausalgoritmien käytöstä (ks. kuva 1). Monet hyökkäykset pyrkivät jättämään salausprotokollan käytön kokonaan pois muokkaamalla salaamattomia protokollia, jotka pyytävät TLS:n käyttöä. Näitä protokollia luodaan erityisesti muokkaamalla verkkopalveluiden HTTP-liikennettä ja Html-sivuja. (Sheffer, 2015).

Tällaisia hyökkäyksiä kutsutaan SSLstrip-hyökkäyksiksi. Ne onnistuvat vain, jos asiakas luo yhteyden verkkopalvelimeen käyttäen HTTP-protokollaa. Yleisesti SSLstrip-hyökkäyksiä vastaan käytetään http Strict Transport Security (HSTS) -menetelmää, jonka avulla verkkosivut ilmoittavat, että niihin voi luoda yhteyden vain suojatulla yhteydellä. (Sheffer, 2015), (Hodges, 2012).

2.5.2 Browser Exploit Against SSL/TLS

Browser Exploit Against SSL/TLS (Eng. lyh. BEAST attack) hyödyntää TLS 1.0-version toteutusta, jossa salauksessa käytettävän alustusvektorin luomiseen käytettiin implisiittistä menetelmää. Sen avulla hyökkääjä voi purkaa osia salatuista paketeista ja eritoten purkaa HTTP-evästeitä, kun käytetään HTTP-protokollaa. (Sheffer, 2015). Tämä hyökkäys on estetty TLS:n versiossa 1.1 vaihtamalla implisiittinen alustusvektori eksplisiittiseksi (Dierks T. , 2006). Lisäksi BEAST-hyökkäys edellyttää, että hyökkääjä on saanut käyttäjän lataamaan koneelleen haitallista JavaScript-koodia (AlFardan & Paterson, 2013).

2.5.3 Padding Oracle On Downgraded Legacy Encryption (POODLE)

POODLE hyökkäys on SSLv3:sta löytynyt haavoittuvuus, jonka myötä SSL jäi pois käytöstä ja uudet TLS-versiot otettiin käyttöön. Kyseistä hyökkäystä voi hyödyntää myös uudempien protokollien kanssa, sillä monet SSL/TLS toteutukset sallivat TLS-yhteyden las-

kemisen SSLv3:een, jos kättely epäonnistuu. Tällaiset hyökkäykset hyödyntävät salauksessa tehtävää viestien täyttämistä, ja luovat niitä tulkitsevia oraakkeleita.

Kryptograafisia algoritmeja kutsutaan yleisesti salakirjoituksiksi. Symmetriset salakirjoitukset voidaan yleisesti luokitella kahteen ryhmään: Jono- ja lohkosalauksiin (Eng. Stream and block ciphers). Lohkosalaus ottaa salattavaa viestiä vastaan pala kerrallaan, ja käsittelee sen paloittain (block). POODLE-hyökkäykset kohdistuvat lohkosalauksiin. (Fedler, 2013).

Lohkosalauksilla on eri toimintatiloja. Yksi yleisimmistä, ja tässä kontekstissa tärkeimmistä tiloista on Cipher Block Chaining (CBC), jossa salattu pala ei riipu ainoastaan salausavaimesta, vaan myös edellisestä salatusta palasta. Koska CBC vaatii syötteen tulevan tietynkokoisina paloina, mutta salattavan viestin pituus ei välttämättä ole jaollinen näiden palojen koolla, pitää syötteeseen lisätä täytettä (padding). Täytteellä viesti kasvatetaan halutun mittaiseksi. Viestin täyttämiselle on olemassa monia eri standardeja, jotka kertovat miten täyttäminen voidaan ja tulee tehdä. (Fedler, 2013).

Monet edellisessä kappaleessa mainituista standardeista tekevät osan viestistä helposti arvattavaksi, koska täytteelle annetaan usein implisiittisiä arvoja. Yhdellä oikein arvatulla bitillä hyökkääjä voi tehdä päätelmiä viestin muista biteistä, koska CBC:ssä ne ovat riippuvaisia toisistaan. (Fedler, 2013).

2.5.4 SSLv3 Key-exchange algorithm rollback

Hyökkäys hyödyntää SSLv3:n kättely-protokollasta löydettyä suunnitteluvirhettä: Viestissä, jossa välitetään palvelimen avain, palvelin voi lähettää väliaikaista avainmateriaalia, (esim. julkisen RSA-avaimen) joka on allekirjoitettu pitkäaikaisavaimella. Ongelma on, ettei salatulle avainmateriaalle ole määritelty tyyppiä, mikä luo pohjan tyyppisekoitushyökkäkselle (Eng. Type confusion attack). SSL:n tulisi allekirjoittaa julkisten parametrien lisäksi myös niitä sisältävien viestien tulkitsemiseen tarvittava data. Tämänkaltainen hyökkäys voidaan estää tarjoamalla täsmällistä tietoa vastaanotetun viestin sisällöstä. (Wagner & Schneier, 1996).

2.6 Käyttäjän manipulointi

Vaikka käyttäjän manipulointi (Eng. Social engineering) ei suoranaisesti liity verkkomaksamisen aikaiseen tietoliikenneturvallisuuteen, johtuu valtaosa ongelma- ja virhetilanteista sekä väärinkäytöksistä *Paytrailin pääarkkitehti Karin mukaan(?)* aina jollakin tavalla käyttäjistä tai heidän tekemistään virheistä. Käyttäjän manipuloinnilla hyökkääjän tarkoitus on saada käyttäjä tarkoituksella tai vahingossa paljastamaan arkaluontoista tietoa hyökkääjälle. Verkkohuijaukset voidaan yleisesti luokitella käyttäjien manipuloinniksi.

Hyökkäykset voivat olla huijauksia tai kohdennettuja hyökkäyksiä. Kohdennetussa hyökkäyksessä kohteena on jokin tietty henkilö tai yritys. Huijauksissa haittaohjelmaa levitetään sähköpostin tai sosiaalisen median välityksellä mahdollisimman laajalti. (Patel, 2013).

2.6.1 Käyttäjän manipuloinnin vaiheet

Käyttäjän manipulointi on yleensä pitkä ja jatkuva prosessi, joka sisältää useita vaiheita. Prosessi saattaa edetä hitaasti, eikä välttämättä sisällä seuraavaksi kuvattuja vaiheita, tai etene esitetyssä järjestyksessä. Patel (2013) kuvailee vaiheita teoksessaan seuraavasti:

Tutkiminen (Eng. Research): Hyökkääjä pyrkii keräämään tietoa kohteesta. Tähän voidaan käyttää useita lähteitä ja keinoja, kuten yrityksen verkkosivut, roskakorit, julkiset dokumentit, fyysinen kanssakäyminen ja niin edelleen.

Koukutus (Eng. Hook): Hyökkääjä pyrkii aloittamaan keskustelun kohteen kanssa kun tutkimusvaihe on suoritettu loppuun.

Näytelmä (Eng. Play): Vaiheen tarkoitus on vahvistaa yhteyttä ja jatkaa keskustelua jotta hyökkääjä voi hyötyä haluamallaan tavalla ja hankkia haluamansa tiedot.

Poistuminen (Eng. Exit): Käyttäjän manipuloinnin viimeinen vaihe, jossa hyökkääjä poistuu tilanteesta tai lopettaa kommunikoinnin kohteen kanssa ilman, että epäilyksiä nousee.

2.6.2 Ihmis- ja laitelähtöinen käyttäjän manipulointi

Käyttäjän manipulointiin on olemassa useita eri keinoja. Patel (2013) jakaa käyttäjän manipuloinnin ihmis- ja laitelähtöiseen käyttäjän manipulointiin perustuen siihen, onko hyökkäyksen vuorovaikutuksen kohteena itse käyttäjä vai käyttäjän tietokone. Laitelähtöisessä hyökkäyksessä hyökkäykseen käytetään yleensä tietokoneohjelmaa. Käyttäjän laite voi olla myös tabletti, älypuhelin tai jokin muu älylaite. Taulukossa 1 on Patelin (2013) listaamia yleisimpiä käyttäjän manipuloinnin keinoja jaoteltuna ihmis- ja laitelähtöiseen käyttäjän manipulointiin. Osa termeistä on suomennettu vapaasti, sillä virallisia suomennoksia ei ollut saatavilla.

Ihmislähtöiset hyökkäykset	
Piggybacking (Seuraaminen)	Hyökkääjä huijaa henkilökuntaa hankkien pääsyn yrityksen rajoitettuihin tiloihin. Hyökkääjä voi esimerkiksi esittää olevansa työhaastatteluun tuleva työnhakija, jonka jälkeen hän voi yrityksen tiloissa esittää olevansa uusi työntekijä, jolla ei ole vielä henkilökorttia, mutta tarvitsee pääsyn serverihuoneeseen.
Impersonating (Imitointi)	Hyökkääjä teeskentelee olevansa yrityksen työntekijä esimerkiksi pitämällä yrityksen univormua tai pukua ja väärennettyä henkilöstökorttia.
Eavesdropping (Salakuuntelu)	Hyökkääjä salakuuntelee luottamuksellista keskustelua tai lukee luottamuksellisia viestejä. Salakuuntelua voi harrastaa esimerkiksi puhelimitse, sähköpostitse.
Reverse social engineering	Hyökkääjä esittää henkilöä, jolla on jonkinlainen auktoriteetti. Tällaisessa tilanteessa hyökkäyksen kohde kysyy tarvitsemaansa informaatiota. Tällaisia tapahtuu yleensä markkinoinnin ja teknisen tuen osa-alueilla.

Dumpster diving (Roskisdyykkaus)	Yrityksen roskista ja roskakoreista voi löytyä huonosti hävitettyä salaista materiaalia, kuten käyttäjätunnuksia, salasanoja tai tiedostonimiä.
Posing as a legitimate end user (Loppukäyttäjän teeskentely)	Tällaisessa hyökkäyksessä hyökkääjä omaksuu validin käyttäjän identiteetin ja yrittää saada informaatiota esimerkiksi soittamalla asiakaspalveluun kertoen, että on unohtanut salasanansa.
Laitelähtöiset hyökkäykset	
Pop-up windows (Ponnahdusikkunat)	Ponnahdusikkunat huijaavat käyttäjän klikkaamaan linkkiä, joka vie heidät hyökkääjän sivustolle. Sivustolla voidaan esimerkiksi pyytää henkilökohtaisia tietoja, tai pyytää käyttäjää lataaman jokin viruksen sisältämä ohjelmisto.
Insider attack (Sisäpiirin hyökkäys)	Sisäpiirin hyökkäys suoritetaan kohdeverkoston sisältä yleensä osaansa tyytymättömän työntekijän toimesta.
Phishing (Kalastelu)	Roskapostittajat lähettävät suuria määriä roskapostia esittäen niiden tulevan joltakin muulta taholta, kuten veikkausyhtiöltä ilmoittaen lottovoitosta. Viesteissä pyydetään klikkaamaan linkkiä josta pääsee antamaan henkilö- tai korttitiedot voiton maksamista varten.
The ”Nigerian 419” scam (Nigerialaiskirjeet)	Tässä huijauksessa hyökkääjä kertoo kohteelle sähköpostitse kohteen voittamasta, perimästä tai muuten saamasta suuresta rahasummasta. Hyökkääjä kuitenkin pyytää kohdetta maksamaan jonkinlaisen etumaksun tai rahansiirron, jotta rahat voidaan toimittaa kohteelle. Jos kohde maksaa ensimmäisen pyydetyn summan, pyydetään erilaisia maksuja loputtomasti lisää.
Social engineering	Tällaisissa viesteissä hyökkääjä voi esimerkiksi lähettää viestin väit-

attack through a fake SMS (Käyttäjän manipulointi huijaus tekstiviestillä)	täen sen olevan pankim tietoturvaosastolta pyytäen soittamaan tiettyyn numeroon. Jos kohde soittaa numeroon, hyökkääjä voi pyytää haluamiaan tietoja, kuten pankkitunnuksia.

Taulukko 1: Ihmis- ja laiteelähtöisiä hyökkäyksiä

Edellinen taulukko sisältää vain muutamia yleisimpiä hyökkäyksiä, ja vain mielikuvitus on rajana käyttäjälähtöisessä manipuloinnissa. Yleisiä tapoja päästä käsiksi yritysten tietoihin ovat myös esimerkiksi saastutetut muistitikut. Loistava esimerkki tällaisesta on Iranilaiseen ydinlaitokseenkin vuonna 2010 levinnyt Stuxnet-haittaohjelma, jonka epäillään saastuttaneen ydinohjelmaa hallinneet tietokoneet niihin yhdistetyn usb-muistitikun välityksellä. (Isaac;Porche;Sollinger;& McKay, 2011).

3 Maksupalvelun tarjoaja

Kun verkkokauppias haluaa vastaanottaa maksusuorituksia verkossa, tulee verkkokauppaan kehittää sitä varten asiaankuuluvat järjestelmät. Kehitystyön lisäksi verkkokauppias joutuu tekemään sopimukset verkkomaksamiseen liittyen jokaisen rahoituslaitoksen kanssa erikseen. Tällaisia rahoituslaitoksia ovat mm. pankit ja korttimaksujen prosessoijat. Maksupalvelun tarjoaja (Eng. Payment Service Provider, PSP) voi tarjota verkkokauppiaan käyttöön useita maksutapoja ja rajapinnan kautta verkkokauppaan integroitavan järjestelmän, kaikki yhdellä sopimuksella ja yhdellä teknisellä toteutuksella. Jotkut maksupalvelun tarjoajat pystyvät tarjoamaan vain yhtä maksutapaa. Maksupalvelun tarjoajia, jotka tarjoavat kauppiaan käyttöön useita maksutapoja kerralla, kutsutaan yleisesti termillä Collective Payment Service Provider (cPSP), jonka suora suomennos on kollektiivinen maksupalvelun tarjoaja. Maksuvälittäjän käyttäminen on verkkokauppiaalle todennäköisesti helpompaa ja myös taloudellisesti kannattavaa, koska se vähentää tarvittavan kehitystyön ja ylläpidon määrää verkkokaupan päässä.

3.1 Paytrail

Työn tilaajana toimii Jyväskyläläisten Lennu Keinäsen ja Niko Lehtosen vuonna 2007 perustama Paytrail Oyj. Yrityksen liikevaihto oli vuonna 2014 5,6 milj. €. Vuonna 2014 Nets osti enemmistön Paytrailistä, ja Paytrail kuuluukin nykyään Nets konserniin. Paytrailillä on tuhansia asiakkaita, ja sen voidaan sanoa olevan johtava suomalainen verkkomaksupalvelu. Työn kontaktihenkilönä toimi Paytrailin puolelta vastaava toimihenkilö (Eng. Compliance Officer) Kari Melender. (Paytrail, ei pvm), (Paytrail, 2014).

Maksupalvelun tarjoajien repertuaariin kuuluu usein paljon muutakin, kuin itse maksupalvelun tarjoaminen. Paytrail tarjoaa asiakkailleen maksupalvelun lisäksi erilliset asiakaspalvelut kuluttajille ja verkkokauppiaille itselleen. Verkkokauppiaat saavat myös käyttöönsä kauppiaspaneelin, josta voi mm. seurata oman yrityksen maksuliikennettä, tulostaa raportteja, hoitaa asiakaspalautuksia ja pelastaa maksamattomia ostoskoreja. Näiden lisäksi Paytrail tarjoaa asiakkailleen lisäarvopalveluita, kuten maksu- ja tilitystietoja tarjoavan REST-

rajapinnan ja auttavan kirjanpitoraportin. Paytrail myös tekee yhteistyötä teknisien toteuttajien ja omien asiakkaidensa kanssa tavoitteena parantaa kaikkien osapuolien liiketoimintaa ja kehittää verkkomaksamisen toimialaa.

Maksupalvelun tarjoajan ydintoiminta on kuitenkin sujuvan ja luotettavan maksupalvelun tarjoaminen. Paytrailin maksupalveluun kuuluvat kaikki suomalaiset pankit, korttimaksut ja osamaksupalvelut. Maksutapoihin kuuluu lisäksi Paytrailin kehittämä Paytrail-tili, joka on kuluttajille suunnattu nopean maksamisen mahdollistava palvelu. Paytrailin mahdollistamat maksupalvelut (ei pvm) on lueteltu alla tarkemmin.

Kotimaisten pankkien verkkomaksupainikkeet: Nordea, Osuuspankki, Danske Bank, Säästöpankki, POP Pankki, Aktia, Handelsbanken, Ålandsbanken, S-Pankki.

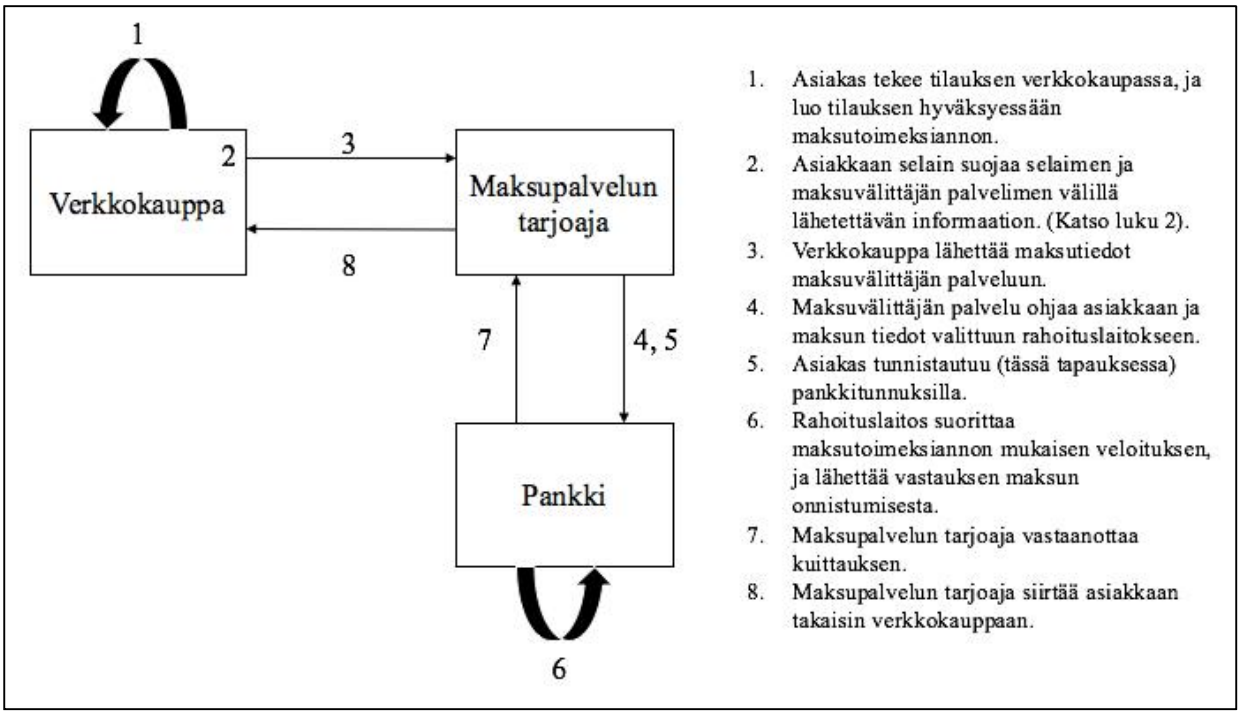
Lasku- ja osamaksupalvelut: Collector ja Jousto.

Korttimaksaminen: Visa, Visa Electron, Mastercard, American Express, Eurocard, Diners Club, JCB ja Paytrail-tili.

3.2 Maksutapahtuman vaiheet

Tutkimuksen kannalta ehdottomasti oleellisin osa on itse maksutapahtuma. Työ tarkastelee erityisesti maksutapahtuman aikaista tietoturvaa. Tässä luvussa esitelty maksutapahtuman kulku on työn kannalta siten erittäin oleellista asiaa.

Kuluttajan tilatessa tuotteita verkkokaupasta, maksuvälittäjän tehtävä on hoitaa maksutietojen turvallinen siirto kuluttajan, asiakkaan (verkkokaupan / verkkopalvelun) ja rahoituslaitoksen (pankit, korttimaksuprosessoijat) välillä. Kuvassa 2 on esitelty normaalin verkkokauppatilauksen maksutapahtuman kulku askel askeleelta (Services, ei pvm) -artikkelia mukaillen. Maksutapahtuman kulku voi vaihdella esimerkiksi maksutavasta riippuen. Alla olevat askeleet kuvaavat verkkopankkitunnuksilla suoritettavan verkkomaksun.



Kuva 3: Verkkomaksun vaiheet

3.3 Maksupalvelun tarjoajien sääntely

Kuka tahansa ei voi ryhtyä maksupalvelun tarjoajaksi. Yritys tarvitsee maksu-välittäjänä toimimiseen Suomen Finanssivalvonnan myöntämän maksulaitos-toimiluvan. Lisäksi toimintaa säädetään maksupalvelulaissa, joka ”sääntelee muun muassa palveluntarjoajan velvollisuutta antaa maksupalvelun käyttäjälle tietoja puitesopimuksesta ja toteutetuista maksutapahtumista” (Finanssivalvonta, 2014).

Finanssivalvonnan tehtäviä ovat maksulaitostoimiluvan saaneiden maksulaitosten tiedonantovelvollisuuden, maksupalvelujen toteuttamisen ja maksupalveluun liittyvien sopimuksien valvominen. Lisäksi finanssivalvonta ylläpitää Maksulaitosrekisteriä, josta löytyvät

mm. kaikki Suomalaiset maksupalvelun tarjoajat, joilla on maksulaitostoimilupa. Tällaisia yrityksiä on Suomessa tällä hetkellä noin kymmenen. (Finanssivalvonta, 2014).

Maksulaitoslaki sääntelee myös monia muita asioita maksulaitoksen johtamisesta asiakkaiden varojen säilyttämiseen (Finlex, 2010). Käytännössä maksulaitostoimilupa edellyttää sen saaneilta yrityksiltä panostuksia tietoturvaan, liittyi se sitten maksutapahtuman suojaamiseen tai asiakastietojen säilyttämiseen. Maksulaitoslain tarkoitus on turvata niin yritysten kuin kuluttajienkin oikeuksia.

3.4 Maksupalveluiden liiketoiminta

Nykymalleissa maksupalvelun tarjoajat maksavat pankeille transaktiokohtaisesti jokaisesta tehdystä verkkomaksusta. Transaktion hinta riippuu ainakin pankista, transaktioiden kokonaismäärästä ja neuvotelluista hinnoista. Yksikään maksu ei siis ole maksupalvelun tarjoajalle ilmainen, vaan siitä syntyy automaattisesti kuluja.

Kun maksupalvelun tarjoajat ottavat verkkokaupan asiakkaakseen, veloitetaan verkkokauppiaalta yleensä jonkinlainen kuukausimaksu palvelusta. Tällä kuukausimaksulla katetaan mm. maksupalvelun ylläpito ja kehitys sekä asiakaspalvelu. Lisäksi verkkokauppias maksaa tietyn provision jokaisesta verkkomaksusta, joka hänen verkkokauppansa kautta tehdään. Kun raha liikkuu Paytrailin järjestelmän kautta, vähennetään jokaisesta maksusta provisiot automaattisesti.

Esimerkki: Mikko ostaa Ville verkkokaupasta ”V” tuotteen, joka maksaa 10€ postikuluineen, ja jonka sisäänostohinta on ollut 5€. Mikko haluaa maksaa pankin ”P” pankkitunnuksillaan, ja suorittaa maksun maksupalvelun ”X” kautta. Maksupalvelu X veloittaa verkkokauppiaalta transaktiosta 0,50€. Pankki P veloittaa maksupalvelulta X samasta transaktiosta 0,25€.

V hyötyy myyntitapahtumasta 4,50€ (10€-5€-0,50€),

X hyötyy maksutapahtumasta 0,25€ (0,50€-0,25€) ja

P hyötyy maksutapahtumasta 0,50€.

Yhden transaktion kannattavuuden voidaan siten laskea olevan maksupalvelulle 50% (0,50/0,25). Esimerkissä käytetyt luvut ovat vain viitteellisiä, eivätkä pohjaudu minkään maksupalvelun nykyisiin kuluihin. Toimintamallit saattavat toki vaihdella maksupalvelukohtaisesti, eivätkä jotkut palvelut esimerkiksi tarjoa asiakaspalvelua verkkokaupan asiakkaille. Palveluita karsimalla voidaan päästä eroon esimerkiksi kiinteästä kuukausimaksusta.

4 Maksupalveludirektiivit

Maksupalveludirektiivit ovat Euroopan komission tekemiä lakiehdotelmia, jotka sääntelevät EU:n alueella toimivien maksupalvelun tarjoajien toimintaa. Niillä luodaan yhteinen laillinen pohja toimialan yrityksille, ja suojellaan kuluttajien yksityisyyttä & varoja. Ensimmäinen maksupalveludirektiivi otettiin käyttöön vuonna 2009. Toinen maksupalveludirektiivi on annettu vuoden 2015 lopussa, ja otetaan EU-maiden lainsäädäntöön vuoden 2017 lopussa. Tässä luvussa esitellään molemmat maksupalveludirektiivit ja niiden käyttöönottoprosessi yleisellä tasolla.

4.1 EU-direktiivin käyttöönottoprosessi

Euroopan unionin (EU) direktiivi on yksi oikeudellinen väline, jolla EU:n politiikat voidaan panna täytäntöön. Direktiivi on EU:n toimielinten käytössä olevan joustava väline, jota käytetään pääasiassa maidenvälisten lakien yhdenmukaistamiseen. Direktiivit ovat lainsäädäntöohjeita, jotka edellyttävät EU-mailta tiettyjä tuloksia. Direktiivit antavat jäsenvaltioiden lainsäädäntöelimille vapauden päättää keinot, joilla tulokset saavutetaan. (Euroopan Unioni, 2015).

EU:n päätöksenteossa käytetään yleisimmin ns. tavallista lainsäätämisjärjestystä. Sen mukaisesti Euroopan parlamentti hyväksyy EU:n säädökset yhdessä Euroopan neuvoston kanssa. Euroopan parlamentti koostuu suorissa vaaleissa valituista jäsenistä, kun taas neuvoston muodostavat kaikkien jäsenmaiden hallitusten edustajat. Lakiehdotusten muodostamisesta ja täytäntöönpanosta huolehtii Euroopan komissio, joka sisältää yhden EU-komissaarin jokaisesta jäsenmaasta. (Euroopan unioni, 2010).

Kun säädös on hyväksytty, se saatetaan jäsenmaiden viranomaisten tietoon. Jos säädös edellyttää kansallista täytäntöönpanoa, säädöksessä ilmoitetaan myös määräaika sen täytäntöönpanolle. Annetussa määräajassa maan on ryhdyttävä muuttamaan lakejaan ja määräyksiään niin, että ne saavuttavat säädöksessä asetetut tavoitteet. Määräaika voi vaihdella, ja olla hyvinkin pitkä. Esimerkiksi ensimmäinen maksupalveludirektiivi annettiin

13.11.2007, mutta se oli saatettava voimaan vasta 1.11.2009. (Kemppinen, 2002), (Euroopan komissio, ei pvm).

Jos määräaikaa rikotaan, voi Euroopan komissio nostaa kanteen kyseistä maata vastaan EU:n tuomioistuimessa. Täytäntöönpanon laiminlyöminen voi tällaisessa tapauksessa johtaa sakkoihin. Suomen osalta säädösten edellyttämien yhteisölakien täytäntöönpano on yleisesti ottaen sujunut hyvin. (Euroopan Unioni, 2015), (Kemppinen, 2002).

4.2 Ensimmäinen maksupalveludirektiivi (PSD)

Direktiivit ovat erittäin laajoja ja pitävät sisällään jopa satoja erillisiä kohtia, joita niiden avulla säädellään. Tässä työssä maksupalveludirektiiveistä käsitellään vain tutkimuksen kannalta oleellisia osia.

Ensimmäinen Euroopan Unionin (EU) laajuinen maksupalveludirektiivi on tullut voimaan 1.11.2009. Sillä luotiin laillinen perusta EU:n laajuisille sähköisen maksamisen yhtenäismarkkinoille, ja muodostettiin kattava joukko sääntöjä kaikille EU:n sisällä toimiville maksupalvelun tarjoajille. Samalla direktiivi tarjoaa vaaditun laillisen alustan koko SEPA-alueelle. (Euroopan komissio, 2016).

Kuluttajan kannalta tarkoitus oli tehdä kansainvälisistä verkkomaksuista yhtä helppoja, tehokkaita ja turvallisia kuin kotimaan rajojen sisällä tehdyistä verkkomaksuista. Lisäksi direktiivin tarkoitus oli tehostaa kilpailua avaamalla markkinoita uusille tulokkaille edistäen tehokkuutta ja kustannusten pienentämistä. (Euroopan komissio, 2016).

Kuluttajille suunnatussa artikkelissa Euroopan Komissio (Euroopan komissio, ei pvm) kertoo tarkemmin direktiivin kuluttajille tuomista hyödyistä. Maksupalvelun tarjoajan tulee ennen maksamista esittää yksityiskohtaiset tiedot itsestään, mahdollisista käyttörajoista, käsittelyajasta, veloitettavista kuluista ja palautusoikeuksista. Maksutapahtuman jälkeen kuluttajalle tulee esittää suoritetun maksun määrä, päivä ja mahdolliset muut veloitettavat kulut, jotta kuluttaja voi tarkastaa tiedot. Näin asiakas saa selkeämmän kuvan maksutapahtuman kokonaiskuluista ja veloituksista. Direktiivi myös nopeutti verkkomaksamista mää-

räten maksupalvelun tarjoajat käsittelemään maksutoimeksiannot viimeistään seuraavan päivän päättyessä 1.1.2012 alkaen. Kun kilpailu direktiivin myötä avautuu, tarjoaa se kuluttajalle myös laajemman skaalan maksutapoja. (Euroopan komissio, ei pvm).

4.3 Toinen maksupalveludirektiivi (PSD2)

Euroopan komissio päätti tarkastaa maksupalveludirektiivin vuonna 2013, jotta sitä voitaisiin modernisoida, ja laajentaa sen vaikutusvaltaa useampiin rahoituslaitoksiin. Tähän asti alalla on ollut toimijoita joita ensimmäinen maksupalveludirektiivi ei ole koskenut. Tällaiset maksupalvelun tarjoajat tuovat alalle lisää innovatiivisuutta, kilpailua, halvempia transaktioita ja vaihtoehtoja verkkomaksuille. Direktiivin tarkastamisella halutaan tuoda myös tällaiset toimijat direktiivin piiriin. Direktiivin koskiessa kaikkia toimijoita se luo tasapuolisemmat lähtökohdat kilpailulle ja helpottaa uusien toimijoiden astumista alalle. Aiemmin tietynlaiset palvelut ovat olleet vain suurien yritysten tarjottavissa, mutta toisen maksupalveludirektiivin myötä myös pienemmät toimijat voivat alkaa tarjota samankaltaisia palveluita. (European Commission, 2015), (Apigee, 2016).

Yksi, ehkä uuden maksupalveludirektiivin oleellisin muutos, on sen sisältämä ”Access to Accounts” -sääntö (PSD2 XS2A). Sen myötä pankit joutuvat tarjoamaan kolmansille osapuolille turvallisen pääsyn asiakkaiden tileihin ja tilitietoihin ohjelmointirajapintojen kautta, jos tilinhaltija näin päättää. Tällaisen muutoksen myötä kolmannet osapuolet voivat käyttää tarjoamissaan palveluissa tietoja, jotka tähän asti ovat olleen vain pankkien saatavilla. (European Commission, 2015), (Apigee, 2016).

4.3.1 Payment Initiation Service Providers

PSD2 ottaa huomioon myös uudenlaiset ”Payment Initiation Service Providers” (PISP) -maksupalvelun tarjoajat, jotka vapaasti suomennettuna ovat maksualoitepalvelun tarjoajia. Tällaiset palvelut eivät ole kuuluneet maksupalveludirektiivin piiriin, eivätkä niitä siten ole välttämättä valvottu toimivaltaisen viranomaisen toimesta. Tämä nostaa joukon lainopillisia ongelmia mm. Kuluttajansuojaan, tietoturvallisuuteen, kilpailuun ja tiedon suojaami-

seen liittyen. (Council of the European Union, 2015). PISP-toiminta on aspekti, joka PSD2:ssa on työn tilaajan Paytrailin kannalta hyvin oleellinen.

Tällaiset palvelut luovat yhteyden suoraan verkkokaupan ja asiakkaan verkkopankin välille, jotta verkkomaksu voidaan suorittaa normaalina tilisiirtona. Tällainen palvelu ei missään kohtaa ei missään ota vastaan asiakkaan varoja. Maksu suoritetaan suoraan asiakkaan tililtä kauppiaan tilille. (Council of the European Union, 2015). Käytännössä asiakas syöttää verkkopankkitunnukset verkkokaupassa, minkä jälkeen maksualoitepalvelun tarjoajan järjestelmä kirjautuu asiakkaan verkkokauppaan asiakkaan verkkopankkitunnuksilla, ja suorittaa maksun hänen puolestaan.

Maksualoitepalvelu perustuu joko suoraan tai epäsuoraan pääsyyn asiakkaan tilille. Tilipalvelua tarjoavien rahoituslaitosten (Eng. Account Servicing Payment Service Provider), eli Suomessa pankkien, tulisi tarjota suora pääsy asiakkaan tilille maksualoitepalvelua varten. Maksualoitepalvelu antaa maksunsaajalle varmistuksen maksun onnistuneesta suorituksesta heti, ja antaa kauppiaalle mahdollisuuden vapauttaa tuote tai palvelu ilman viivettä. Lisäksi se tarjoaa verkkomaksamiselle edullisen ratkaisun niin asiakkaan kuin kauppiaan näkökulmasta.

4.3.2 PSD2-vaatimukset

PSD2:ssa määritellään toimijoille yhteisten pelisääntöjen lisäksi myös teknisten toteutusten standardit (Eng. Regulatory Technical Standards, RTS). Tällaisten ehtojen tarkoitus on vahvistaa yritysten ja kuluttajien tietoturvaa ja tietosuojaa. Teknisten vaatimusten määrittelyt ovat työn kirjoitusvaiheessa vasta luonnosvaiheessa, joten ne joudutaan tilanteen vuoksi käsittelemään keskeneräisinä. Takaraja lopullisen standardin toimittamiselle on tammikuussa 2017**.** Euroopan pankkiviranomainen (Eng Euro Banking Authority, EBA) on tehnyt standardista ensimmäisen luonnoksen ja julkaissut sen korjauspyynnöistä keskusteluasiakirjan. (Council of the European Union, 2015). Näiden korjausehdotusten pohjalta EBA korjaa standardia, ja pyytää Melenderin arvion mukaan vielä korjausehdotuksia päivitettyyn versioon ennen lopullisen standardin julkaisemista. Luvussa käsitellään vain toimeksiantajan ja tutkimuksen kannalta oleellisia osia standardista.

Maksupalvelun tarjoajat ovat vastuussa turvallisuustoimenpiteistä, joiden tulee olla suhteessa tietoturvariskeihin. Kaikki sähköiset maksupalvelut tulee toteuttaa turvallisesti, käyttäen tekniikoita jotka takaavat luotettavan käyttäjän tunnistamisen ja vähentävät riskien toteutumista mahdollisimman tehokkaasti. Pankkien tulee tarjota PISP-toimijoille mahdollisuus luottaa pankkien tarjoamiin tunnistuspalveluihin maksualoitteiden tekemisiksi. (Council of the European Union, 2015)**.**

Tässä luvussa käsitellyt vaatimukset on referoitu EU-neuvoston (2015) PSD2 ehdotuksesta.

Artikla 38: Jäsenmaiden tulee mukaan varmistaa, että maksupalvelun tarjoajat tarjoavat tai mahdollistavat seuraavat tiedot ja ehdot maksupalvelun käyttäjälle:

a) Tietojen erittely tai uniikki tunniste joka maksupalvelun käyttäjän tulee antaa, ennen kuin maksumääräys voidaan asianmukaisesti aloittaa tai suorittaa.
b) Maksun suorittamisen enimmäisaikamäärä tulee esittää käyttäjälle.
c) Kaikki käyttäjän kulut maksupalvelusta kyseiseen maksuun liittyen, ja tarvittaessa erittely näiden maksujen määristä.

Artiklat 39-42: Lisäksi jäsenmaiden tulee varmistaa, että maksualoitepalvelun tarjoajien tulee ennen maksun aloittamista tarjota tai mahdollistaa maksajalle maksualoitepalvelun tarjoajan nimi, pääkonttorin maantieteellinen osoite, muut yhteystiedot ja toimivaltainen viranomainen. Siinä tapauksessa, että maksupalvelun toimii yrityksen sivukonttorissa, tulee tarjota kyseisen sivukonttorin osoite.

Maksualoitepalvelun tarjoajan tulee välittömästi maksun käynnistämisen jälkeen tarjota tai mahdollistaa käyttäjälle ja tarvittaessa maksunsaajalle seuraavat tiedot:

a) Vahvistus maksumääräyksen onnistuneesta käynnistämisestä.
b) Viite, jolla maksaja ja maksunsaaja voivat tunnistaa maksutapahtuman, maksunsaaja voi tunnistaa maksajan ja tarvittaessa muut maksun yhteydessä siirretyt tiedot.
c) Maksutapahtuman rahallinen kokonaismäärä.

Lisäksi kun maksumääräys suoritetaan maksualoitepalvelun tarjoajan kautta, tulee palvelun tarjoajan mahdollistaa maksajalle ja tilipalvelun tarjoajalle maksun viite.

Samat tiedot tulee tarjota käyttäjälle myös maksumääräyksen vastaanottamisen ja maksun suorittamisen jälkeen.

Artikla 58: Maksualoitepalvelun tarjoajan tulee varmistaa, että maksajalla on oikeus käyttää maksualoitepalvelua. Lisäksi maksualoitepalvelun tarjoajalla on seuraavat velvoitteet:

a) Olla missään vaiheessa pidättämättä asiakkaan varoja maksualoitepalvelun tarjoamiseen liittyen.
b) varmistaa, etteivät palvelun käyttäjän henkilökohtaiset käyttäjätiedot joudu kolmannen osapuolen käsiin (pois lukien käyttäjä ja käyttäjätunnukset toimittanut osapuoli), ja että ne siirretään turvallisten ja tehokkaiden kanavien läpi.
c) varmistaa, ettei mitään maksupalvelun käyttäjästä palvelun aikana saatuja tietoja tarjota muille kuin maksun vastaanottajalle ja vain käyttäjän nimenomaisella suostumuksella.
d) itsensä todentaminen tilin omistajan tilipalvelun tarjoajalle jokaisen maksun yhteydessä ja kommunikoinnin hoitaminen tietoturvallisesti tilipalvelun tarjoajan, maksajan ja maksunsaajan välillä.
e) olla tallentamatta arkaluonteisia maksutietoja maksupalvelun käyttäjästä.
f) olla pyytämättä muita tietoja, kuin mitä palvelun tarjoamista varten tarvitaan.
g) olla käyttämättä, tallentamatta tai tarkastelematta mitään dataa minkään muun kuin maksupalvelun tarjoamisen takia, ja ainoastaan käyttäjän nimenomaisella suostumuksella.
h) olla muuttamatta summaa, vastaanottajaa tai muita maksun ominaisuuksia.

Maksualoitepalvelun tarjoamista ei saa myöskään tehdä riippuvaiseksi tilipalvelun ja maksualoitepalvelun tarjoajan välisen sopimuksen olemassaolosta.

5 Ohjelmointirajapinnat

Ohjelmointirajapinnat (Eng. Application Programming Interface, API) ovat suurella todennäköisyydellä tapa, jolla pankit tulevat suurella todennäköisyydellä tarjoamaan PSD2:n vaatimat tiedot kolmansille osapuolille. API:t ovat sovellusten välisiä rajapintoja, jotka mahdollistavat ylemmän tason toimintojen tarjoamisen. Ne mahdollistavat sovellusten välisen kommunikoinnin, jossa yksi sovellus kutsuu toisen sovelluksen toimintoja. (EBA Working Group, 2016)**.**

Kaikki ohjelmointirajapinnat ovat rajapintoja, mutta kaikki rajapinnat eivät ole ohjelmointirajapintoja. API:t perustuvat ajattelutapaan, jonka mukaan rajapintojen tulisi olla skaalautuvia, uudelleenkäytettäviä ja turvallisia tarjoten kehittäjille helppokäyttöisyyttä itsepalvelun avulla. Teknisestä näkökulmasta katsottuna API:t ovat standardisoituja vaatimusjoukkoja siitä, miten sovellusten tulisi keskustella keskenään. (EBA Working Group, 2016)**.** Standardeja tarjoavat useat eri tahot ja yhteisöt, mutta yleisesti standardit sisältävät EBA:n (2016) mukaan seuraavat osa-alueet:

1. **Datansiirto:** Tapa jolla dataa siirretään turvallisesti. Käytännössä kaikki API:t käyttävät HTTP/HTTPS protokollaa kuljetuskerroksena (Eng. Transport Layer) koska se on yksinkertainen ja laajalti yhteensopiva.
2. **Tiedonvaihto:** Vaihdetun tiedon muoto. Yleisimmät muodot ovat XML ja JSON.
3. **Tiedon saatavuus:** Käytön hallintaa. Kenellä on pääsy tietoihin ja ja miten pääsy saavutetaan. Tähän on olemassa useita standardeja, joista yleisimmät ovat SAML ja OAuth 2.0.
4. **API malli:** Tap, jolla API:t suunnitellaan. Yleisimmät tekniikat ovat REST (REpresentational State Transfer) ja SOAP (Simply Object Access Protocol). REST esitellään tarkemmin luvussa 5.2.

5.1 Rajapintojen avoimuus

Ohjelmointirajapinnat tarjoavat tietoturvaa sekä kustannustehokasta pääsyä dataan ja/tai toiminnallisuuksiin. Riippuen siitä, voidaanko rajapintaan päästä käsiksi organisaation ulkopuolelta, määritellään se joko yksityiseksi tai avoimeksi rajapinnaksi. Avoin rajapinta tarkoittaa, että rajapintaan on pääsy myös organisaation ulkopuolelta. (EBA Working Group, 2016). Rajapintoja voidaan luokitella myös tarkemmin. EBA (2016) kuvailee niitä seuraavasti:

Yksityinen API: Yksityiset API:t ovat suljettua ja siten tahojen saatavilla yksinomaan API:n tarjoajan harkinnan alaisesti.

Kumppani API: Tällaiset API:t ovat avoimia kahdenvälisten sopimusten alaisille kumppaneille. Myös kumppani API:t ovat tahojen saatavilla yksinomaan API:n tarjoajan harkinnan alaisesti. Esimerkki tällaisesta kahdenvälisestä sopimuksesta tiettyihin tietoihin liittyen on pankin ja toiminnanohjausjärjestelmän tarjoajan välinen API.

Jäsen API: Tällainen API on avoin kaikille muodollisille jäsenille, jotka kuuluvat yhteisöön, jolla on hyvin määritellyt jäsenyyssäännöt. Tulevaisuudessa myös PSD2:n valtuutetut maksualoitepalvelut kuuluvat tähän kategoriaan, koska vain valtuutetut tai rekisteröidyt kolmannet osapuolet (Eng Third Party Providers, TPP) voivat saada pääsyn.

Tuttava API: Tällainen API on kaikkien saatavilla, ja se vaatii käyttäjää suostumaan ennalta määritettyjen ehtojen noudattamiseen.

Julkinen API: Myös julkinen API on kaikkien saatavilla, ja kuka tahansa voi käyttää sellaista. Julkiset rajapinnat vaativat yleensä jonkinlaisen rekisteröinnin kautta. Rekisteröinnin tarkoitus on käyttäjän tunnistaminen ja todentaminen.

5.2 REST-rajapinta

Kuten luvussa 5 mainittiin, REST-arkkitehtuuri on hyvin yleinen tapa toteuttaa rajapintoja. Fielding (2000) esitteli REST-arkkitehtuurin väitöskirjassaan tapana, jolla modernin Internetin tulisi toimia. REST on monista muista arkkitehtuureista johdettu hybridi-arkkitehtuuri.

5.2.1 REST-arkkitehtuurin rajoitukset

Fielding (2000) määrittelee REST-arkkitehtuurin joukkona rajoituksia seuraavasti:

REST-kuvauksen aloituspiste on Nollatyyli (Eng. Null Style). Suunnittelija aloittaa suunnittelun puhtaalta pöydältä rakentaen arkkitehtuuria tutuista komponenteista, kunnes arkkitehtuuri vastaa suunniteltavan järjestelmän tarpeita.

1) Ensimmäinen rajoite on asiakas-palvelin (Eng. Client-Server) arkkitehtuurista lainattu vastuiden erottelu (Eng. Separation of concerns). Erottelemalla käyttöliittymän vastuut tietovaraston vastuista käyttöliittymän siirrettävyys alustojen välillä paranee. Lisäksi skaalautuvuus paranee palvelimen komponentteja yksinkertaistamalla.
2) Seuraava rajoitus on otettu asiakas-tilaton palvelin (Eng. Client-Stateless-Server) arkkitehtuurista, ja se koskee asiakkaan ja palvelimen vuorovaikutusta: Kommunikoinnin luonteen tulee olla tilatonta (Eng. Stateless) siten, että jokainen pyyntö asiakkaalta palvelimelle sisältää pyynnön ymmärtämiseen vaaditut tiedot, eikä mitään palvelimelle tallennettua tietoa tarvitse käyttää. Session tila on siten täysin ylläpidetty asiakkaan puolella. Rajoitus parantaa näkyvyyttä, luotettavuutta ja skaalautuvuutta. Näkyvyys paranee, koska valvontajärjestelmän ei tarvitse yksittäistä pyyntöä pidemmälle. Luotettavuus paranee, sillä osittaisista virhetilanteista palautuminen helpottuu. Skaalautuvuus paranee, koska kun palvelinkomponenttien ei tarvitse ylläpitää tilaa, ne voivat nopeasti vapauttaa resursseja.
3) Verkon tehokkuuden parantamiseksi lisätään välimuistin rajoitukset asiakas-välimuisti-tilaton palvelin arkkitehtuurista. Välimuisti rajoitukset edellyttävät, että

palvelinpyynnön vastauksen tietojen tulee olla implisiittisesti tai eksplisiittisesti luokiteltu niin, että se voidaan tai ei voida tallentaa välimuistiin. Jos vastaus voidaan tallentaa välimuistiin, asiakkaan välimuistille annetaan oikeus käyttää vastauksen dataa myöhemmin uudelleen ja vastaavin tuloksin. Välimuistia käyttämällä jotkut pyynnöt osa vuorovaikutuksista voidaan kokonaan tai osittain jättää pois, parantaen mm. tehokkuutta ja skaalautuvuutta.

4) Keskeinen ominaisuus, joka erottaa REST-arkkitehtuurin muista, on sen painotus yhtenäiselle rajapinnalle komponenttien välillä. Käyttämällä komponentti rajapinnassa ohjelmistokehityksen yleisyys-periaatetta järjestelmän kokonaisarkkitehtuuri yksinkertaistuu ja vuorovaikutusten näkyvyys paranee. Toteutukset erotetaan niiden tarjoamista palveluista, mikä edistää niiden itsenäistä kehittymistä. Miinuksena mainittakoon, että yhtenäinen rajapinta heikentää tehokkuutta, sillä informaation siirtäminen hoidetaan standardisoidusti, eikä sovelluksen tarpeita vastaavalla tavalla. REST on suunniteltu suurirakeisen hypermedian siirtämiseen Internetin yleistapauksen optimoimiseksi.
5) Jotta käyttäytymistä voitaisiin edelleen parantaa Internetin asteella, lisätään monikerroksisen järjestelmän rajoitukset. Monikerroksisuus mahdollistaa arkkitehtuurin rakentumisen hierarkisista kerroksista rajoittamalla komponenttien toimintaa siten, että yksikään komponentti ei näe välittömästi seuraavaan kerrosta pidemmälle. Näin asetetaan raja kokonaisarkkitehtuurin kompleksisuudelle ja edistetään alustan itsenäisyyttä.
6) Viimeiseksi lisätään rajoitus ladattavan koodin (Eng. Code-on-demand) – arkkitehtuurista. REST mahdollistaa asiakastoimintojen laajentamisen sallimalla koodin lataamisen ja suorittamisen sovelmien (Eng. Applet) ja skriptien muodossa. Ominaisuuksien lataaminen käyttöönoton jälkeen parantaa järjestelmän laajennettavuutta. Se kuitenkin vähentää näkyvyyttä, ja onkin sen vuoksi REST-arkkitehtuurin ainoa valinnainen rajoite.

5.2.2 Paytrailin REST-rajapinta

Paytrail tarjoaa asiakkailleen REST-rajapinnan maksujen luomiseen palvelinten välisellä pyynnöllä. Maksu luodaan yksinkertaisella HTTP POST -pyynnöllä, joka lähettää maksutiedot joko XML tai JSON -viestinä. Pyyntö palauttaa muiden tietojen ohella maksulinkin, johon asiakas voidaan suoraan ohjata maksun suorittamista varten, tai joka voidaan lähettää esimerkiksi asiakkaan sähköpostiin. Integroimalla REST-rajapinnan suoraan verkkokauppa-alustan taustajärjestelmään verkkokauppias voi esimerkiksi luoda hylätyistä ostoskoreista maksulinkkejä. Alla on esimerkki kevyessä versiossa lähetettävästä XML-viestistä ja palautettavasta maksulinkistä.

REST-pyynnön XML-viesti

```
<?xmlversion="1.0"encoding="UTF-8"?>
<payment>
    <orderNumber>12345678</orderNumber>
    <currency>EUR</currency>
    <locale>fi_FI</locale>
    <urlSet>
        <suc-
        cess>https://www.esimerkkikauppa.fi/sv/success</succe
        ss>
        <fail-
        ure>https://www.esimerkkikauppa.fi/sv/failure</failur
        e>
        <pending></pending>
        <notifica-
        tion>https://www.esimerkkikauppa.fi/sv/notify</notifi
        cation>
    </urlSet>
    <price>99.00</price>
</payment>
```

REST-pyynnön XML-vastaus

```
<?xmlversion="1.0"encoding="UTF-8"?>
<payment>
    <orderNumber>12345678</orderNumber>
    <token>[SECRETTOKENSTRINGGENERATEDBYAPI]</token>
    <url>https://payment.paytrail.com/payment/load/token/[SEC
    RETTOKENSTRINGGENERATEDBYAPI]</url>
</payment>
```

6 Maksualoitepalvelu Paytrailin näkökulmasta

Paytrailin kannalta oleellisin osa uudesta maksupalveludirektiivistä on maksualoitepalveluiden siirtyminen direktiivin alaisuuteen. Maksualoitepalveluiden tarjoajat tulevat olemaan Paytrailin suoria kilpailijoita, minkä lisäksi maksualoitteiden tarjoaminen on bisnesmallina vakavasti otettava mahdollisuus. Se tarjoaa mahdollisuuksia mm. uudenlaisten palveluiden ja halvempien transaktioiden tarjoamiseen verkkokauppiaille kuin kuluttajillekin.

Tässä luvussa käydään läpi maksualoitepalvelun tarjoamista Paytrailin näkökulmasta. Lisäksi tarkastellaan tällaisen palvelun riskejä, teknistä toteutusta sekä hyötyjä ja haittoja. Luvussa otetaan myös kantaa toteutukseen sekä tietoturvallisuuden että käytettävyyden kannalta. Koska PSD2 on vielä määrittelyvaiheessa, eikä lopullisia teknisiä vaatimuksia tai transaktiohintoja ole vielä saatavissa, joudutaan joitain aspekteja käsittelemään yleisten mielipiteiden ja olettamuksien pohjalta.

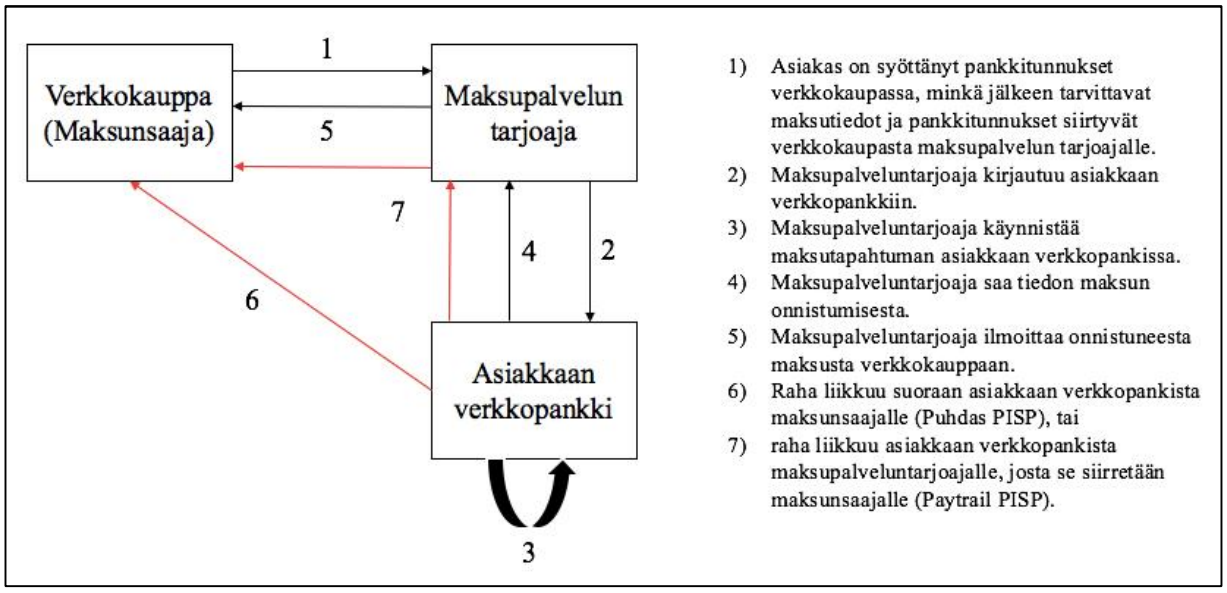
6.1 Toimintamallit

Melenderin kanssa käymieni keskustelujen pohjalta tulimme siihen tulokseen, että Paytrail voisi harjoittaa PISP-toimintaa kahdella selkeästi toisistaan erilaisella tavalla. Näistä molemmissa omat hyödyt ja haitat. Ensimmäisenä esiteltävä vaihtoehto on puhdas PISP-malli, jossa otetaan vastaan asiakkaan pankkitunnukset, ja niiden avulla käynnistetään maksu suoraan asiakkaan verkkopankista. Tässä mallissa maksu suoritetaan suoraan maksunsaajalle, eli raha liikkuu asiakkaan verkkopankista suoraan maksunsaajalle. Paytrail toimii vain ja ainoastaan maksun käynnistäjänä, eivätkä rahat missään vaiheessa käy Paytrailin järjestelmässä. Tällainen toimintamalli on PISP-toimijan ”normaali” toimintamalli, ja tulee oman arvioni mukaan olemaan lähivuosina hyvin suosittu, ainakin uusien toimijoiden keskuudessa.

Toinen esiteltävä malli, kutsuttakoon sitä vaikka termillä Paytrail-PISP, on hieman normaalista PISP-mallista poikkeava. Myös tässä mallissa otetaan vastaan asiakkaan pankki-

tunnukset, ja siirrytään asiakkaan verkkopankkiin käynnistämään maksu. Maksu suoritettaisiin tässä mallissa ensin Paytrailin tilille, jonka jälkeen se siirrettäisiin vasta kauppiaan tilille. Raha siis kulkisi Paytrailin tilin kautta, ei suoraan maksunsaajalle. Menettely vastaa toiminnaltaan hieman enemmän nykyistä toimintamallia.

Toimintamallit eroavat toisistaan vain rahan liikkumisen osalta. Käyttäjän kannalta molemmat voidaan toteuttaa toimimaan samalla tavalla. Molemmat edellä kuvatuista malleista on esitelty visuaalisesti kuvassa 3. Tiedon liikkumista on esitetty mustin viivoin ja rahan liikkumista punaisin viivoin.



Kuva 4: Maksualoitepalvelun toimintamallit

6.2 Maksualoitepalvelun toteuttaminen

Molempien luvussa 6.1 kuvattujen toimintamallien tekninen toteutus on tietoturvan kannalta hyvin samankaltainen. Rahan siirtäminen Paytrailin järjestelmän kautta ei juuri vaikuta palvelun toteuttamiseen tai sen tietoturvaan. Maksualoitepalvelun toteuttaminen käsitellään siksi yhdessä osassa.

Tietoturvallisen sovelluksen kehittäminen on valtava työ, eikä tutkimuksessa voida ottaa kantaa tällaisen palvelun toteuttamiseen alusta loppuun. Lisäksi käytettävien tekniikoiden suositukset muuttuvat vuosien saatossa. Näistä syistä työssä käsitellään ainoastaan maksutapahtuman aikaista tietoturvaa ja tapoja sen toteuttamiseen yleisellä tasolla. Esimerkiksi käytettäviin salausmenetelmiin tai palvelinpuolen turvallisuusratkaisuihin oteta kantaa.

Maksualoitepalvelun toteuttamisessa tietoturva tulee ottaa erittäin tarkasti huomioon. Jos maksupalvelun tietoturvassa on puutteita, hyökkääjän käsiin voi joutua arkaluonteisia tietoja verkkokauppojen asiakkaista, kuten henkilötietoja, henkilötunnuksia, korttitietoja tai pankkitunnuksia. Hyökkääjä saattaa myös pystyä aiheuttamaan vähemmän vakavaa haittaa luomalla esimerkiksi ylimääräisiä maksuja tai kaatamalla asiakkaan yhteyden. Lisäksi hyökkääjien olisi pitänyt pankkitunnuksia urkkiakseen murtautua pankkien järjestelmiin, jotka on erittäin tietoturvallisesti toteutettu. PSD2:n ja maksualoitepalvelun myötä saattaa riittää, jos hyökkääjä löytää haavoittuvuuden kolmannen osapuolen, tai jopa verkkokaupan järjestelmästä.

Maksutapahtuman aikainen tietoturva tuleekin toteuttaa useassa kerroksessa: Osapuolien tunnistaminen, salatun yhteyden muodostaminen, tiedon salaaminen yhteyden sisällä ja salatun tiedon oikeellisuuden varmistaminen ovat näistä tärkeimpiä. Lisäksi palveluntarjoajan tulee ottaa huomioon myös fyysinen tietoturva ja henkilöstön aiheuttamat riskit.

6.2.1 Osapuolien tunnistaminen

Maksutapahtuman aikana maksupalvelu ottaa yhteyttä verkkopankkiin, ja käynnistää maksun asiakkaan puolesta. Pankin tulee jokaisen maksun yhteydessä tunnistaa maksualoitepalvelun tarjoaja, joka yrittää ottaa heidän järjestelmäänsä yhteyttä. Ensisijainen tunnistaminen voidaan tehdä esimerkiksi IP-osoitteen ja TLS-sertifikaatin perusteella. Maksupalvelu ilmoittaa käyttämänsä palvelinten IP-osoitteet pankille, joka tunnistaa näistä IP-osoitteista tulevat yhteydenotot kyseiseksi maksupalveluksi. Sertifikaatteja tarkastamalla yhteydenoton voidaan tunnistaa tulevan taholta, joka on saanut sertifikaatin luotettavalta myöntäjältä.

Huono puoli IP-osoitteiden käyttämisessä tunnistamistarkoituksessa on niiden vaihtuvuus. IP-osoitteet voivat muuttua esimerkiksi päivitysten tai ongelmatilanteiden johdosta. Jos uusia IP-osoitteita ei ole etukäteen otettu huomioon, ei palvelu enää toimi, koska pankin järjestelmä katsoo yhteydenoton tulevan epäluotettavasta IP-osoitteesta. Tosin varapalvelintenkin osoitteet voi ennestään tiedottaa tarvittaville tahoille. IP-osoitteen tarkistaminen on tietoturvan kuitenkin kannalta melko turvallinen menetelmä.

6.2.2 Salatun yhteyden muodostaminen

Kun salattu yhteys muodostetaan, tulee ottaa huomioon mm. luvussa 2.5 esitellyt haavoittuvuudet. Salausprotokollien haavoittuvuudet kohdistuvat yleensä vanhoihin versioihin. Kun jostakin tekniikasta havaitaan haavoittuvuus, se korjataan, ja julkaistaan uusi, tietoturvallisempi versio. Kuten luvussa 2.2.1 esitellyssä SSL-kättelyssä, myös TLS-kättelyssä päätetään käytettävät salausalgoritmit ja käytettävän salausprotokollan versio. Suurin osa salausprotokollien haavoittuvuuksista voidaan välttää sallimalla salatulle yhteydelle vain uusimpien versioiden ja vahvojen salausalgoritmien käyttö.

SSL-versioiden 1, 2 ja 3 käyttö tulisi estää, ja vain versiot TLS 1.0, 1.1 ja 1.2. tulisi sallia. Lisäksi käytettävien salausavainten tulee olla vähintään 2048 bitin mittaisia, ja salausalgoritmeista tulisi sallia vain ajankohtaisten suositusten mukaiset menetelmät. Lisäksi kaikki sivut tulee tarjoilla HTTPS-yhteyden yli. Jo pelkän CSS-sivun tarjoilu HTTP-yhteyden luo

mahdollisuuden Man In The Middle (MItM, Mies välissä) –hyökkäyksille. Mitään sisältöä ei tule tarjoilla sivulle suojaamattoman yhteyden yli. (Open Web Application Security Project, 2016).

6.2.3 Maksutietojen oikeellisuuden varmistaminen

Luvussa 4.3.2 on kuvattu tietoja, joita maksualoitepalvelun tarjoajan tulee tarjota asiakkaalle, pankille ja maksunsaajalle jokaiseen maksutapahtumaan liittyen. Kun maksutietoja siirrellään asiakkaan, maksupalvelun tarjoajan, pankin ja maksunsaajan välillä, tulee varmistaa, etteivät tiedot ole muuttuneet missään välissä. Vaikka maksutiedot kulkevatkin hieman eri tavalla kuin aiemmin, on näiden tietojen oikeellisuuden varmistaminen erittäin tärkeää. Tietojen muuttuminen maksun aikana voi viitata meneillään olevaan hyökkäykseen.

Tietojen oikeellisuus voidaan varmistaa tiivistealgoritmilla. Maksutiedot voidaan lähettää esimerkiksi HTML Form -muodossa. Yhdessä kentässä lähetetään maksutiedoista laskettu tiiviste. Maksutietojen lisäksi tiivisteen laskemiseen käytetään salaista tunnistetta, joka on ainoastaan tarvittavien maksussa mukana olevien osapuolien tiedossa. Maksun eri osapuolien tulee laskea maksutiedoista sama tiiviste. Näiden tiivisteiden yhteneväisyys voidaan tarkistaa. Jos tiivisteet ovat samat, voidaan maksutietojen olettaa tulevan oikealta taholta ja pysyneen muuttumattomina. Jos tiivisteet eroavat toisistaan, maksu keskeytetään.

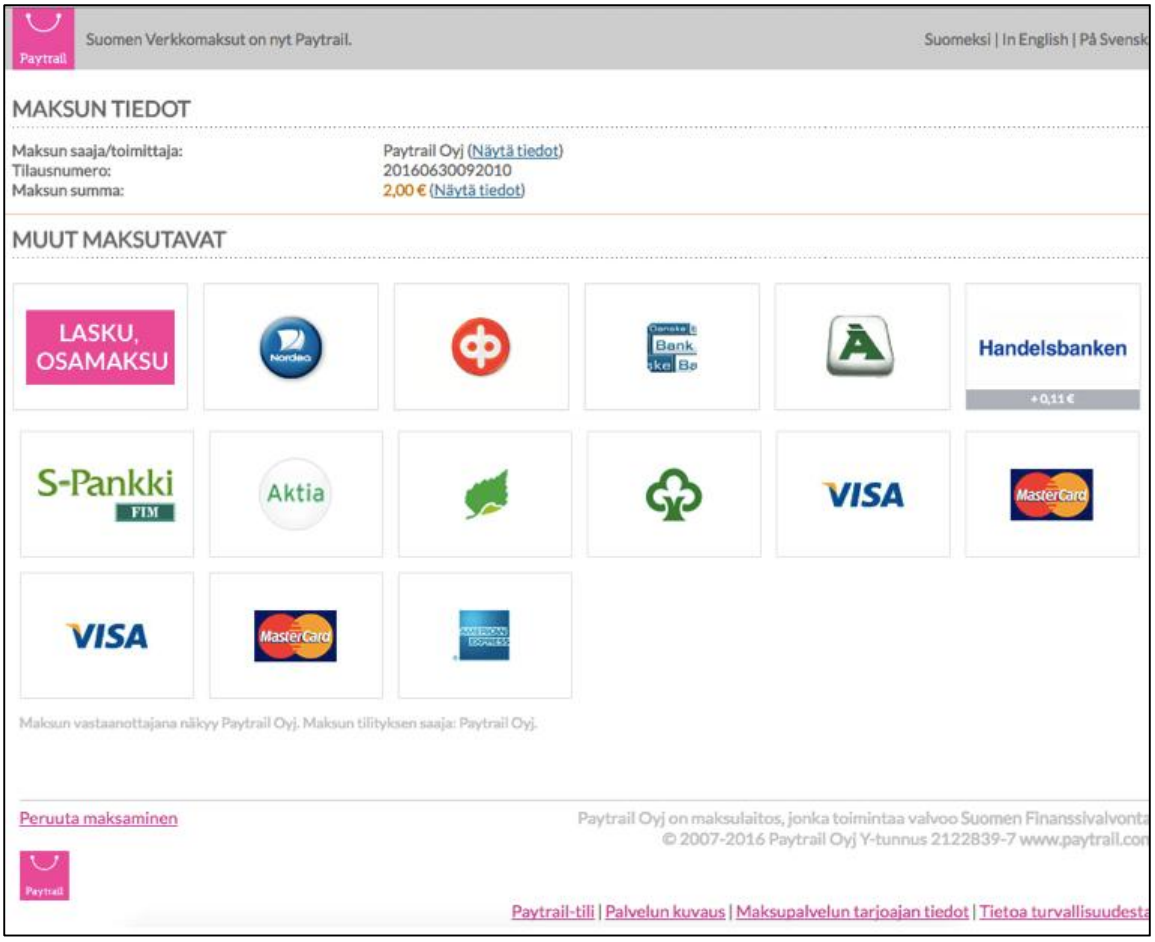
National Institute of Standards and Technology (NIST) on määritellyt tämänhetkiset, turvalliseksi katsotut tiivistealgoritmit vuoden 2015 elokuussa. Kyseiset standardit koostuvat SHA-2 joukon tiivistealgoritmeista. Nämä algoritmit on toistaiseksi katsottu tietoturvallisiksi, eikä niistä ole vielä löydetty nykyteknologioilla hyödynnettäviä tunnettuja haavoittuvuuksia. NIST:n järjestämä 5 vuotta kestänyt kilpailu uuden SHA-3 algoritmin löytämiseksi päättyi vuonna 2012, ja lienee vain ajan kysymys, kunnes SHA-3 joukko määritellään ja otetaan laajempaan käyttöön. (Dunn, 2012), (National Institute of Standards and Technology, 2015).

6.3 Maksualoitepalvelun käyttöliittymä

Kuten kaikki muutkin verkkopalvelut, tulisi maksualoitepalvelu tehdä mahdollisimman helppokäyttöisesti ja selkeästi. Lisäksi toteutuksen tulee herättää käyttäjässä luottamusta ja olla tietoturvallinen. Tässä luvussa otetaan kantaa palvelun toteutukseen toiminnallisten ja ulkoasullisten seikkojen osalta.

Maksualoitepalvelun voi toteuttaa periaatteessa kahdella eri tavalla: Joko ohjaamalla asiakkaan verkkokaupasta Paytrailin järjestelmän maksusivulle, tai toteuttamalla maksusivun verkkokauppaan. Paytrailin nykyisessä maksupalvelussa kauppias voi käyttää näistä molempia. Maksusivulla asiakas näkee maksun tiedot ja pääsee valitsemaan sopivan maksutavan. Nykyisessä toteutuksessa asiakas siirretään kirjautumaan valitsemaansa verkkopankkiin maksutavan valinnan jälkeen.

Maksualoitepalvelu lyhentää ja selkeyttää maksuprosessia huomattavasti, sillä asiakasta ei enää tarvitse ohjata maksusivulta omaan verkkopankkiinsa. Jos maksusivu on lisäksi toteutettu verkkokaupan puolelle, asiakas pysyy koko maksuprosessin ajan verkkokaupan maksusivulla. Nykyinen järjestelmien välillä siirtely voitaisiin siinä tapauksessa unohtaa. Tällöin verkkomaksaminen selkeytyy prosessina huomattavasti parantaen käytettävyyttä ja maksujen onnistumisprosenttia. Paytrailin nykyinen maksusivu on esitelty kuvassa 4.



Kuva 4: Paytrailin maksusivu

6.3.1 Maksusivun toteuttaminen verkkokauppaan

Kun maksusivu tuodaan verkkokauppaan, maksuprosessi lyhenee ja selkeytyy. Yksi välivaihe, kolmannen osapuolen maksusivu, putoaa pois. Mitä enemmän asiakasta siirrellään palvelusta toiseen, sitä todennäköisemmin hän kokee prosessin sekavaksi ja/tai menettää luottamuksensa palveluun. Lisäksi teknisten ongelmien mahdollisuus kasvaa, kun maksuprosessissa on tiedon liikuttelua asiakkaan toiminnoista riippuen monen eri järjestelmän välillä. Todennäköisyys maksun epäonnistumiseen kasvaa. Lisäksi, kun maksusivu toteutetaan verkkokaupan puolelle, saa verkkokauppias itse määritellä ulkoasun. Näiden seikkojen pohjalta maksusivun toteuttaminen verkkokaupan puolelle olisi suositeltava vaihtoehto.

Maksupainikkeet voidaan asetella verkkokauppaan esimerkiksi kuvan 4 tyylisesti. Jokaisella pankilla on oma kuvake, josta painamalla asiakas viestii haluavansa maksaa kyseisen pankin tililtä. Kun asiakas painaa, verkkokauppa pyytää asiakasta syöttämään sopivat pankkitunnukset. Tarvittaessa pyydetään vielä avainlukua sisäänkirjautumista ja maksun vahvistamista varten. Lopuksi verkkokauppa vahvistaa maksun onnistuneen.

Maksusivun toteuttaminen verkkokaupan puolelle aiheuttaa kuitenkin tietoturvariskejä. Luvussa 6.4.2 kuvataan tarkemmin tällaisen menettelyn aiheuttama MItM-hyökkäyksen riski. Jos maksusivu toteutetaan verkkokaupan puolelle, tulisi koko sivusto tarjota käyttäjälle suojatun yhteyden yli.

6.3.2 Erillisen maksusivun toteuttaminen

Jos maksualoitepalvelu toteutetaan kuten kuvassa 4, eli Paytrailin järjestelmän sisäisellä maksusivulla, voitaisiin nykyisen maksusivun pohjaa käyttää hyödyksi. Sen ulkoasu on käyttäjille tuttu, eikä suuria muutoksia pankkipainikkeisiin tarvitsisi suuria. Ainoa ero olisi, että kuten verkkokauppaan toteutetussa maksusivussa, myös tässä vaihtoehdossa asiakkaan pankkitunnukset otetaan vastaan maksusivulla, eikä häntä ohjata valitsemaansa verkkopankkiin.

Tällaisen palvelun tietoturva voidaan toteuttaa aukottomammin, sillä asiakkaan tulisi ensin siirtyä Paytrailin palveluun. Vaikka maksusivulle ei nykyisessä maksupalvelussa syötetä pankkitunnuksia tai korttitietoja, on se kuitenkin suojatun yhteyden takana. Suojatulle sivustolle siirtymisen jälkeen MItM-hyökkääjä ei enää näe verkkoliikenteen sisältöä, eikä käyttäjän huijaaminen onnistu ilman salauksen purkamista.

6.4 Maksualoitepalvelun riskit

PISP-toiminnassa maksupalvelun tarjoaja verkkokaupassa tilauksen tehnyt kuluttaja syöttää pankkitunnukset tilauksen maksamista varten jo esimerkiksi verkkokaupan maksusivulla. Tämä osa maksusivusta lähettää ne salatun yhteyden yli maksupalvelun tarjoajalle, joka kirjautuu niillä asiakkaan verkkopankkiin, ja käynnistää maksun sieltä käsin. Maksun

käynnistäminen tehdään koneellisesti, eikä kukaan luonnollinen henkilö pääse asiakkaiden pankkitunnuksiin käsiksi.

Nykyiseen toimintamalliin verrattuna toiminta muuttuu pääasiassa siltä osin, että maksupalvelu vastaa pankkitunnusten turvallisesta siirtämisestä verkkopankkiin ja asiakkaan verkkopankkiin kirjautumisesta. Nykyisissä järjestelmissä asiakas siirretään valitsemaansa verkkopankkiin antamaan verkkopankkitunnukset. Tällainen menettely kuulostaa aluksi hyvin pelottavalta, koska kuluttajat antavat pankkitunnuksen kolmansien osapuolien käyttöön. Pankkitunnukset kuitenkin salataan kaiken aikaa, eikä esimerkiksi kolmansien osapuolien työntekijöiden tule päästä niitä näkemään. Lisäksi esimerkiksi DIBS harjoittaa tällaista maksupalvelua jo nykyisellään myös Suomessa, eikä mikään laki kiellä sitä. PSD2:n myötä tällaiset toimijat saadaan direktiivin alaisuuteen sekä tarkempaan valvontaan ja säätelyyn.

PSD2 vaikuttaa verkkomaksamisen tietoturvaan myös epäsuorasti. Erilaisten huijaussivustojen on helpompi toimia, kun pankkitunnuksia otetaan asiakkaalta vastaan jo verkkokaupan puolella. Tässä luvussa esitellään maksualoitepalvelun tuomia riskejä, niiden vakavuutta ja tapoja ehkäistä kyseisiä riskejä.

6.4.1 Huijaussivustot

Kokenutkaan käyttäjä ei välttämättä tunnista aitoa ja luotettavaa verkkosivustoa huijaussivustosta. Aiemmin asiakas on ohjattu pankin verkkopalveluun suorittamaan maksu itse. Kun pankkitunnuksia aletaan PISP-toiminnan kasvun myötä lisääntyvissä määrin ottamaan asiakkailta vastaan jo verkkokaupan puolella, on hyökkääjän mahdollista luoda huijaussivusto esimerkiksi jostakin tunnetusta verkkokaupasta. Jos asiakas syöttää pankkitunnukset huijaussivustolle, saa hyökkääjä asiakkaan pankkitunnukset tietoonsa, ja voi esimerkiksi tehdä tilisiirron omalle tililleen.

Huijaussivustoilta suojautuminen teknisestä näkökulmasta on miltei mahdotonta, ja niiden tunnistaminen onkin pitkälti käyttäjän vastuulla. Käyttäjän tulisikin aina varmistua sivuston aitoudesta ennen pankkitunnuksien antamista. Huijaussivuston voi tunnistaa ainakin

muutoksista verkkopalvelun osoitteessa. Jos oikea verkkokauppa toimii osoitteessa www.villenverkkokauppa.com, voi hyökkääjä varata huijaussivustolle esimerkiksi osoitteen www.vvillenverkkokauppa.com. Ero on pieni, mutta oleellinen.

Lisäksi käyttäjä voi tarkistaa verkkosivuston sertifikaatin. Verkkokaupan sivuilla sertifikaatissa tulisi näkyä verkkokaupan tietoja. Jos tiedot vaikuttavat epäilyttäviltä, tai yhteys ei ole salattu, voi tilauksen keskeyttäminen olla viisasta.

6.4.2 Mies välissä -hyökkäys

MItM-hyökkäykset saattavat yleistyä, jos pankkitunnuksia aletaan ottaa vastaan jo verkkokauppojen ostoskoreissa. Jos koko sivusto, eli verkkokauppa tai verkkopalvelu, ei ole suojatun yhteyden takana, voidaan MItM-hyökkäyksellä estää käyttäjän pääsy sivuston suojattuihin osiin. Lisäksi se tarjoaa erilaisia mahdollisuuksia huijata käyttäjää esimerkiksi kirjoittamaan pankkitunnukset suojaamattomalle sivulle, jolloin hyökkääjä saa ne tietoonsa. Periaatteessa maksusivun toteuttaminen verkkokaupan puolelle edellyttäisi verkkopalvelun kaikkien sivujen asettamista suojatun yhteyden taakse.

Suojatun yhteyden käyttäminen on nykyään hyvin yleistä, ja suuri osa verkkopalveluista tarjoillaan suojattujen yhteyksien yli. Varmasti löytyy kuitenkin verkkopalveluita, jotka käyttävät vanhentuneita salausprotokollia tai toimivat suojaamattomien yhteyksien yli. Maksupalvelun integroiminen suoraan tällaiseen verkkokauppaan tarjoaisi hyökkääjälle paljon mahdollisuuksia.

6.5 Maksualoitepalvelun taloudelliset aspektit

PSD2 tulee vaikuttamaan myös taloudellisesta näkökulmasta katsottuna. Sen myötä pankkien tulee tarjota rajapinnat kolmansien osapuolien palveluita varten, mikä helpottaa kolmansien osapuolien toimimista verkkomaksamisen alalla. Pankkien vastuulle jää kuitenkin raskaan pankki-infrastruktuurin ylläpitäminen, rajapintojen kehittäminen ja ylläpitäminen,

joten on vielä epäselvää, kuinka pankit kattavat kulujaan esimerkiksi näiden rajapintojen osalta. Varmastikaan ei voi olla niin, että pankit pakotetaan kehittämään ja ylläpitämään palveluita, mutta eivät saa niistä rahallista hyötyä. Kolmannet osapuolet eivät siis luultavasti saa rajapintoja käyttöönsä täysin ilmaiseksi.

Maksualoitepalvelu on mahdollisuus kannattavampaan liiketoimintaan, ja tuo mukanaan monia rahanarvoisia hyötyjä. Tässä luvussa käsitellään luvussa 6.1 esiteltyjen mallien keskeisiä taloudellisia hyötyjä ja haittoja.

6.5.1 Transaktiohintojen laskeminen

Molemmat luvussa 6.1 esitellyistä malleista tulevat mahdollistamaan nykyistä edullisemmat transaktiohinnat, mikä on hyvin olennaista, kun puhutaan maksupalvelun tarjoajan liiketoiminnasta. Suurilla transaktiomäärillä vain muutamien senttien erot saattavat merkitä suuria muutoksia liiketoiminnan kannattavuudessa. Puhtaan PISP-toiminnan kulut olisivat kuitenkin pienemmät, sillä transaktioita tulee yhtä verkkomaksua kohden vain yksi. Jos raha kierrätetään maksupalvelun tarjoajan kautta, tulee transaktioita kaksi, ja siten kulut ovat suuremmat.

Luvun 3.3 esimerkissä verkkokaupan kulut pankkitransaktiosta olivat 0,50€ ja maksupalvelun kulut samaisesta transaktiosta 0,25€. Kun pankit pakotetaan avaamaan rajapinnat PISP-toiminnalle, tulevat transaktiohinnat tippumaan. Pankkien pitää kuitenkin voida jotenkin hyötyä ylläpitämästään infrastruktuurista, jolla mahdollistetaan mm. Kyseiset rajapinnat. Tämän takia transaktioista ei todennäköisesti tule täysin maksuttomia.

Demonstraation vuoksi voidaan arvioida edellä mainitun esimerkin pankkitransaktion hinnan putoavan siten, että se tulevaisuudessa maksaa palveluntarjoajalle 0,15€. Oletetaan, että palveluntarjoaja perii siitä verkkokauppiaalta edelleen 0,50€. Tämän myötä yhden transaktion kannattavuus olisi nyt 70% (0,35/0,5), kun se aiemmin oli 50%. Maksupalvelu voisi helposti siis laskea myös verkkokauppojen transaktiohintoja. Tulevista transaktiohinnoista voidaan kuitenkin esittää tässä vaiheessa vain arvailuja.

6.5.2 Ostetun palvelun välitön vapauttaminen

Nykyisessä toteutuksessa asiakas palautetaan maksutapahtuman pankin palvelusta takaisin verkkokaupan ilmoittamaan onnistuneen maksun osoitteeseen. Kun asiakas saapuu kyseiselle sivulle, voi verkkokauppa olettaa maksumääräyksen suorittamisen onnistuneen. Tämä menetelmä todistaa pankin vain ohjanneen asiakkaan ilmoitettuun onnistuneen maksun osoitteeseen, eikä se varmuudella osoita, että varat olisi siirretty.

Kun maksupalvelu pääsee itse käynnistämään maksun asiakkaan verkkopankista, voidaan maksun onnistumiseen luottaa paljon paremmin. Tällöin myös maksunsaaja, eli verkkokauppa voi luottaa siihen, että kun maksupalvelun tarjoaja ilmoittaa maksun onnistumisesta, on raha myös siirtynyt. Kun maksun käynnistymisen onnistuminen voidaan luotettavasti todeta heti maksutapahtuman jälkeen, voidaan myös ostettu palvelu vapauttaa heti maksun jälkeen. Tämä tarkoittaisi mm. Pienempiä viiveitä verkkokauppojen tilausten käsittelyssä.

6.5.3 Tilitysviiveiden lyheneminen

Tällä hetkellä yksi maksupalveluiden epäkohdista ovat tilitysviiveet. Kun maksutapahtuma on tehty, voi kulua vielä useita vuorokausia, kunnes varat ovat siirtyneet maksunsaajan tilille. Tämä on varsinkin pienille verkkokaupoille hyvin ongelmallista, sillä maksujen viipyminen voi aiheuttaa esimerkiksi ongelmia varastojen täydentämisessä. Viiveet johtuvat pankkimaksujen tapauksessa pankkien nykyisestä tavasta ajaa maksutapahtumat tietyin väliajoin, ei reaaliajassa.

Jos maksualoitepalvelu toteutetaan puhtaasti PISP-mallisesti, eivät varat koskaan siirtyisi maksupalvelun tarjoajan järjestelmään, vaan ne siirrettäisiin suoraan maksunsaajalle. Tällöin rahan liikkumisesta poistuisi kokonaan se aika, minkä raha viettää maksupalvelun tarjoajan tilillä, sekä matkalla sieltä maksunsaajalle. Toisaalta reaaliaikaiset maksujärjestelmät ovat yleistymässä, minkä myötä tilitysviiveet tulevat joka tapauksessa minimoitumaan muutaman vuoden kuluessa. Tämä tulee pienentämään pankkimaksujen tilitysviiveitä huomattavasti, ja helpottamaan verkkokauppojen toimintaa.

6.5.4 Markkina-aseman vakaus

Paytrail on johtava suomalainen maksupalveluiden tarjoaja. PSD2 tarjoaa helpomman pääsyn ja uudenlaisia mahdollisuuksia heidän suorille ja epäsuorille kilpailijoilleen sekä helpomman toimialalle pääsyn uusille toimijoille. Konservatiivisesti ajateltuna uusi direktiivi on Paytrailin markkina-aseman kannalta huolestuttavaa, sillä ilman muutoksia on mahdollista, että maksupalvelu jää uusien, innovatiivisempien ja halvempien maksupalveluiden jalkoihin.

Maksupalveluita tarjoavat tahot tulevat Suomessa mitä luultavimmin toimimaan maksulaitostoimiluvan alaisesti, mikä vähentää alalle pyrkivien yritysten määrää. Maksulaitostoimiluvan hankkiminen vaatii yritykseltä mm. vakavaraisuutta ja vahvoja panostuksia tietoturvaan, joten mikä tahansa aloitteleva yritys ei sellaista voi saada. Lisäksi Paytrail on Suomessa jo melko tunnettu brändi, johon konservatiiviset Suomalaiset kuluttajat ovat viime vuosina alkaneet luottaa hieman paremmin. Uuden toimialalle tulevan start-up yrityksen voi olla hankalaa saada tarvittavaa luottamusta, jotta kuluttajat uskoisivat pankkitunnuksia heidän haltuunsa. Toisaalta kuluttajan luottamukseen voidaan vaikuttaa esimerkiksi kolmannen osapuolen vähäisellä näkyvyydellä.

PSD2 tulee lisäämään kilpailua alalla, ja vanhojen toimijoiden tulee joko muuttaa toimintaansa, tarjota uudenlaisia palveluita tai perustella nykyisten palveluiden paremmuus sekä kuluttajille että verkkokauppiaille. Jättämällä PSD2 huomioimatta niillä on varteenotettava mahdollisuus menettää markkinaosuuksia uusille toimijoille.

6.5.5 Transaktiokulujen laskuttaminen

Verkkokauppiaat maksavat jokaisesta verkkomaksusta transaktiokuluja (katso luku 3.3). Kun maksupalvelun tarjoaja toteuttaa asiakkaan antaman maksumääräyksen, siitä yleensä laskutetaan transaktiokulut suoraan. Tämä on helppo ja sujuva tapa sekä verkkokauppiaalle että maksupalvelun tarjoajalle. Jotkut yritykset haluavat, että transaktiokulut laskutetaan jälkeenpäin isommissa erissä, esimerkiksi kuukausittain. Tämä voi esimerkiksi helpottaa verkkokauppiaan yrityksen sisäistä kirjanpitoa.

Puhtaassa PISP-mallissa transaktiokulujen laskuttaminen transaktion ohessa ei olisi mahdollista, sillä varat siirtyvät suoraan asiakkaalta maksunsaajalle. Tällöin transaktiokulut jouduttaisiin laskuttamaan aina erikseen, mikä on epäkannattavaa sekä taloudellisesti että käytännön kannalta. Varsinkin pienille verkkokaupoille kuukausittaiset laskutuskulut voivat olla huomattava meno.

Paytrail PISP-mallissa transaktiokulujen laskuttaminen onnistuisi transaktion aikana, sillä varat siirretään Paytrailin järjestelmän kautta. Paytrail PISP-mallissa transaktiokulut voidaan laskuttaa myös jälkikäteen, mikäli verkkokauppias niin haluaa. Tämä aspekti voidaan siten lukea puhtaan PISP-mallin haitaksi, ja Paytrail PISP-mallin hyödyksi.

6.5.6 Lisäarvopalveluiden tuottaminen

Paytrailin nykyinen maksupalvelu mahdollistaa mm. auttavan kirjanpitoraportin tarjoamisen heidän asiakkailleen. Kirjanpitoraportin data saadaan Paytrailin järjestelmän kautta kulkevista maksuista. Maksualoitepalvelun myötä maksujen mukana saattaa kulkea vähemmän dataa, eikä esimerkiksi kirjanpitoraporttiin saada välttämättä kaikki samoja tietoja, kuin nykyisessä toteutuksessa. Maksualoitepalveluun siirtyminen voi siis heikentää mahdollisuuksia nykyisten lisäarvopalveluiden tarjoamiseen. Tämä jää kuitenkin nähtäväksi, kunnes määritellään mitä tietoja maksujen yhteydessä siirretään. Lisäksi PSD2 mahdollistaa uudenlaisten lisäarvopalveluiden tarjoamisen.

7 Pohdinta

Tässä työssä tutkittiin toista verkkomaksamisen tietoturvaa, toista maksupalveludirektiiviä ja sen vaikutuksia verkkomaksamisen tietoturvaan. Tietoturvan ohella tutkittiin myös muita vaikutuksia ja mahdollisuuksia, joita PSD2 tuo mukanaan verkkomaksamisen ja pankkitoiminnan alalle. Tutkimus on erittäin ajankohtainen, sillä direktiivi on annettu, mutta sen lopullinen muoto Suomen lainsäädännössä ei vielä ole tiedossa. Pankit ja maksupalveluiden tarjoajat odottavat tietoja mm. teknisistä vaatimuksista jotta osaavat tehdä tarvittavat muutokset ja päivitykset järjestelmiinsä. Tutkimuksen alkuvaiheessa tietoja PSD2:sta löytyi vain hyvin vähän, mutta tutkimuksen aikana tietoa alkoi löytyä yhä enemmän ja enemmän. Kiinnostus aihetta kohtaan kasvaa jatkuvasti. Lisäksi Melenderin mukaan PSD2:ta käsiteltiin EBAday 2016 –tapahtumassa erittäin laajasti, mikä kertoo sen merkittävyydestä. Tutkimuksen aikainen ajankohta kuitenkin myös rajoitti tutkimusta hieman, sillä esimerkiksi lopullisia teknisiä vaatimuksia ei oltu vielä julkistettu. En usko tämän kuitenkaan juuri vaikuttaneen tutkimuksen tuloksiin.

Tutkimus käsittelee PSD2:n ja PISP-toiminnan tietoturvariskejä ja tarjoaa keinot näiden riskien käsittelyyn. Tutkimuksessa käsitellään myös tietoturvallinen tapa toteuttaa maksualoitepalvelu ja otetaan kantaa myös tällaisen palvelun käyttöliittymän toteuttamiseen. Asetettu tutkimusongelma käsiteltiin siis suunnitelman mukaisesti. Tutkimus on myös erittäin hyvin yleistettävissä. Se on katsaus uuteen ja laajaan aiheeseen, joka koskettaa tuhansia pankkeja ja muita toimijoita Euroopan talousalueella. Tutkimuksen tuloksia voidaan hyödyntää PSD2:n osalta koko Euroopan alueella toiseen maksupalveludirektiiviin tutustumisessa ja esimerkiksi maksualoitepalvelun kehitystyön suunnittelussa.

Verkkomaksamisen ala on suomessa nuori, ja se elää jatkuvassa muutoksessa. Pankkipalvelut sen sijaan ovat kehittyneet verrattain hyvin hitaasti. Toinen maksupalveludirektiivi tulee muuttamaan verkkomaksamista ja vähittäispankkitoimintaa ennen näkemättömällä tavalla, kun pankkien toimintaan kohdistetaan pakotteita. Avattavat rajapinnat mahdollistavat uudenlaisten verkkomaksu- pankkipalveluiden tarjoamisen, ja PSD2:n myötä Eurooppa ottaa ison askeleen kohti avointa pankkitoimintaa.

PSD2 vaatii eniten työtä nimenomaan pankeilta, sillä niiden tehtäväksi jää kehittää ja ylläpitää kyseisiä rajapintoja. Jos pankit aikailevat rajapintojen kehityksessä, ne saattavat jäädä kehityksessä jälkeen ja alkaa menettää asiakkaitaan. Pankkien tulisi varautua uuteen aikakauteen panostamalla rajapintojen kehitykseen jo ennen kuin PSD2 astuu voimaan, ja pyrkimällä aikaiseen yhteistyöhön kolmansien osapuolien kanssa houkutellakseen uusia toimijoita käyttämään juuri heidän rajapintojaan. Näin pankit voivat kääntää PSD2:n edukseen, kun sen yleisesti katsotaan olevan huono asia niiden kannalta. Rajapintoja voi kehittää askelittain, esimerkiksi ensiksi tarjoten kolmansille osapuolille mahdollisuuden PISP-toimintaan, ja myöhemmin laajentaen tarjontaa tili- ja transaktiotietoihin. Niillä pankeilla, jotka avaavat rajapinnat ensimmäisinä, on kilpailuetu muihin pankkeihin nähden.

Kolmannet osapuolet pääsevät hyödyntämään näitä rajapintoja ja visioimaan uudenlaisia palveluita, joita ennen tavoittamattomissa olevat tiedot mahdollistavat. Pankkien toiminta on pysynyt viimeiset vuosikymmenet melko koskemattomana, ja ne ovat saaneet itse sanella pankkipalvelujen kehittämisestä. Pankkien kehitystä on yritetty vauhdittaa mm. ensimmäisellä maksupalveludirektiivillä ja vapauttamalla julkishallinnon rekistereissä olevia kansalaistietoja (Omadata), mutta toiminta ei ole muuttunut innovatiivisempaan suuntaan. PSD2:n myötä pankkipalveluiden kehitysvastuu siirretään pankeilta kolmansille osapuolille. Pankeilla on yhtäläiset mahdollisuudet hyödyntää PSD2:ta joko käyttämällä muiden pankkien rajapintojen yli tarjoamia tietoja tai kaupallistamalla omat rajapintansa. On mielenkiintoista nähdä, mitä kaikkia palveluita vähittäispankkitoiminnan alueella tarjotaan muutaman vuoden kuluessa.

Ennen kuin tekniset vaatimukset ja uusien rajapintojen taloudelliset aspektit selviävät, voidaan vain arvailla esimerkiksi maksualoitepalvelun kannattavuutta Paytrailin näkökulmasta. Sillä aikaa voidaan kuitenkin visioida, millaisia palveluita PSD2 mahdollistaa, kun se astuu voimaan. Oman arvioni mukaan suurin osa seuraavista palveluista on kaikkien saatavilla muutaman vuoden kuluessa.

7.1 Keskitetty verkkopankki

Kun kolmannet osapuolet pääsevät hakemaan tilitietoja ja käynnistämään maksuja kuluttajien puolesta, voidaan tarjota keskitettyjä verkkopankkipalveluita. Tällaiseen palveluun henkilö voisi lisätä tilejä kaikista suomalaisista pankeista ja hoitaa kaikkien pankkien asioita samasta verkkopankista. Asiakas saisi itse lisätä palveluun haluamansa tilit eikä niitä voisi lisätä palveluun ilman asiakkaan erillistä, nimenomaista suostumusta.

Tällainen palvelu helpottaisi kuluttajien arkea ja pankkipalveluiden kilpailuttamista. Halpa asuntolaina voidaan ottaa pankista A, juoksevia tuloja ja menoja voidaan hoitaa pankin B tililtä ja korkeakorkoinen säästötili saadaan pankista C. Kaikkien pankkien tilit ja toiminnot voitaisiin kuitenkin keskittää yhteen ja samaan palveluun. Asiakas saisi keskitetyt palvelut parhaaksi katsomiltaan pankkipalveluiden tarjoajalta.

Keskitetyn verkkopankin ei tarvitsisi myöskään koostua vain yhden henkilön tileistä tai olla yhden henkilön hallittavissa. Tällaisella palvelulla voitaisiin tarjota pankkipalveluita koko perheelle, ryhmälle tai vaikkapa yrityksille. Yksityishenkilöt voisivat tunnistautua verkkopankkitunnuksilla, jonka jälkeen heillä olisi pääsy ryhmän tilitietoihin. Ryhmään kuuluvat jäsenet voisivat tehdä heidän käyttöoikeuksilleen mahdollistettuja toimintoja ja lisätä omia tilejään ryhmän tarkasteltavaksi. Pienen yrityksen tilien tai perheen talouden hallinta voisi tällaisen palvelun myötä helpottua huomattavasti ilman, että kaikkia palveluita pitäisi ottaa samasta pankista.

Keskitettyihin pankkipalveluihin voisi myös lisätä analysointityökaluja ja henkilökohtaisen talouden hallinnan työkaluja. Tällä hetkellä Osuuspankin Pivolompakko tarjoaa henkilökohtaisen talouden analysointia kuluttajan tuloihin ja menoihin perustuen. Pivolompakko tukee toistaiseksi kuitenkin vain Osuuspankin asiakkaita. Tällaiset työkalut voisivat tarjota esimerkiksi ennusteita varallisuuden kehittymisestä, erittelyä kulujen muodostumisesta sekä säästö- ja sijoitusvinkkejä.

7.2 Reaaliaikaiset lainat

Kun kolmannet osapuolet pääsevät käsiksi kuluttajien tilitietoihin, voidaan verkkomaksua suorittavan asiakkaan tilin saldo tarkastaa asiakkaan suostumuksella maksamisen yhteydessä. Jos maksun aikana käy ilmi, ettei asiakkaalla ole tarpeeksi saldoa maksun suorittamiseen, voidaan hänelle tarjota reaaliaikaista lainaa toiselta yksityishenkilöltä. Ennen kuin reaaliaikaiset maksut toimivat kaikkien pankkien välillä, ainakin samasta pankista annettu laina olisi lainanottajan käytössä välittömästi, ja verkkomaksu voidaan suorittaa loppuun.

Lainapalvelu voisi toimia yksityishenkilöiden välillä maksualoitepalvelun periaatteella. Kun sopiva lainanantaja ja –ottaja löytyvät, voidaan lainanantajalle ilmoittaa siitä reaaliajassa, ja suorittaa maksu lainanantajan tililtä lainanottajalle. Tämän jälkeen verkkomaksu voidaan suorittaa loppuun. Maksun jälkeen lainanantaja saa korkoa lainasta, ja lainanottaja on saanut reaaliajassa tarvitsemansa lainan.

Yksityishenkilöt voisivat ilmoittautua lainapalveluun lainanantajiksi, ja ilmoittaa rajaehdot lainan antamiselle. Lainanottajien luotettavuutta voitaisiin arvioida esimerkiksi luottotietojen ja mahdollisten aiempien otettujen lainojen ja niiden takaisinmaksun perusteella. Yksityishenkilöiden välille voitaisiin automaattisesti tehdä sitova lainasopimus, jolloin lainan maksamatta jättämiselle on normaalit lainmukaiset seuraamukset.

7.3 Virtuaalilompakko-palvelun laajentamismahdollisuudet

Tässä luvussa käsitellään Paytrail-tilin laajentamismahdollisuuksia. Paytrail tili on virtuaalilompakko, ja laajentamismahdollisuudet ovat yleistettävissä mihin tahansa virtuaalilompakko-palveluun.

Paytrail on kehittänyt kuluttajille suunnatun Paytrail-tilin, joka mahdollistaa nopean verkossa maksamisen pelkällä sähköpostisoitteella ja salasanalla. Normaalissa korttimaksussa, jossa käytetään vahvaa tunnistautumista, tulee maksajan ensin syöttää korttitietoja sen jälkeen vielä vahvistaa verkkomaksu pankkitunnuksilla. Tämän lisäksi kuluttajan tulee vielä syöttää osoitetiedot. Paytrail-tiliä luodessaan kuluttaja antaa haluamansa maksukortin tie-

dot ja tunnistautuu verkkopankkitunnuksilla. Tämän jälkeen maksaminen onnistuu helposti vain sähköpostitunnuksella ja salasanalla. Lisäksi Paytrail-tili mahdollistaa omien toimitusosoitteiden tallentamisen sekä verkkokauppatilausten tarkastelun ja palautusten hoitamisen. Paytrail-tili voidaan periaatteessa ottaa käyttöön missä tahansa verkkokaupassa, ja se on tällä hetkellä käytössä tuhansissa suomalaisissa verkkokaupoissa.

Vähittäistavarakaupassa maksaminen on siirtynyt lähimaksuun ja NFC-teknologiaan, mutta tuntuva osa verkko-ostoksista tehdään edelleen kannettavilla tietokoneilla. Myös Paytrail-tilin maksutapojen päivittäminen olisi kuitenkin paikallaan. Jotta Paytrail-tili voisi vielä jatkossa kilpailla vakavasti otettavana maksutapana, tulisi sen mahdollistaa lähimaksaminen NFC-teknologian avulla. Tässä luvussa ei kuitenkaan oteta sen tarkemmin kantaa Paytrail-tilin maksutapoihin, vaan ominaisuuksiin ja palveluihin joita sen kautta voisi PSD2:n myötä tarjota.

Paytrail-tiliä voitaisiin laajentaa esimerkiksi joillakin luvuissa 7.1 ja 7.2 kuvatuista toiminnoista. PSD2:n myötä Paytrail-tiliin voitaisiin mahdollistaa pankkitilien lisääminen, joilta maksaminen onnistuisi jatkossa pelkällä sähköpostiosoitteella ja vaihtuvalla tunnusluvulla. Lisäksi Paytrail-tiliin voitaisiin hakea pankkitilien saldot, joten asiakas näkisi helposti miltä tililtä hän voi ja mistä hänen ehkä kannattaa verkkomaksu suorittaa. Paytrail-tiliin voitaisiin myös yhdistää reaaliaikainen lainapalvelu, jolloin lainan siirtäminen lainanottajalle ja lainojen takaisinmaksut voitaisiin hoitaa Paytrail-tilin teknisen alustan kautta.

Jo käytössä olevan tuotteen yhdistäminen verkkopankkien tarjoamiin rajapintoihin olisi huomattavasti pienempi työ, kuin kokonaan uuden palvelun kehittäminen. Lisäksi Paytrail on valmiin asiakaskunnan omaava tunnettu toimija verkkomaksamisessa, joten kuluttajat saattaisivat ottaa tuotteen hyvin vastaan.

PSD2:n myötä markkinoilla tullaan näkemään pankkitoimintoja tarjoavia maksu- ja tilitietopalveluiden tarjoajia. Paytrail on suomalaisten kuluttajien keskuudessa tunnettu ja luotettava verkkomaksupalveluiden tarjoaja, jonka olisi helppo osittain liukua ns. hybridipankkitoimintaan. Paytrail-tilin kehittäminen keskitetyksi verkkopankiksi, joka mahdollistaa normaalien verkkopankkitoimintojen lisäksi helpon verkkomaksamisen, henkilökohtaisen

taloudenhallinnan ja reaaliaikaiset yksityishenkilöiden väliset lainat, voisi tuoda Paytrailille paljon uusia kuluttaja-asiakkaita ja täysin uudenlaista näkyvyyttä.

8 Lähdeluettelo

AlFardan, N.;& Paterson, K. (2013). *www.ieee-security.org.* Haettu 3. 3 2016 osoitteesta Lucky Thirteen: Breaking the TLS and DTLS Record Protocols: http://www.ieee-security.org/TC/SP2013/papers/4977a526.pdf

Apigee. (26. 1 2016). Financial Services Series: Getting Ready for PSD2, Open Banking & Beyond. Noudettu osoitteesta https://www.youtube.com/watch?v=7VtUheDbyUM

Batten, L. M. (2013). *Public Key Cryptography : Applications and Attacks (1).* Wiley: IEEE Press.

Bhiogade, M. (2002). *Where parallels intersect*. Haettu 22. 1 2016 osoitteesta http://www.proceedings.informingscience.org/IS2002Proceedings/papers/Bhiog058Secur.pdf

Council of the European Union. (2. 6 2015). *Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on payment services in the internal market and amending Directives 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC.* Haettu 15. 6 2016 osoitteesta European Council: http://data.consilium.europa.eu/doc/document/ST-9336-2015-INIT/en/pdf

Dierks, T. (4 2006). *The Transport Layer Security (TLS) Protocol - Version 1.1*. Haettu 3. 3 2016 osoitteesta The Transport Layer Security (TLS) Protocol - Version 1.1: https://www.ietf.org/rfc/rfc4346.txt

Dierks, T. (8 2008). *The Transport Layer Security (TLS) Protocol Version 1.2*. Haettu 18. 2 2016 osoitteesta https://www.ietf.org/rfc/rfc5246.txt

Dunn, J. (4. 10 2012). *NIST declares 'Keccak' SHA-3 winner after five-year competition*. Haettu 5. 7 2016 osoitteesta http://www.techworld.com/news/security/nist-declares-keccak-sha-3-winner-after-five-year-competition-3402110/

EBA Working Group. (5 2016). Understanding the business relevance of open APIs and Open Banking for banks. Euro Banking Association.

Eldewahi, A. E.;Sharfi, T. M.;Mansor, A. A.;& Mohamed, N. A. (2015). *SSL/TLS Attacks: Analysis and Evaluation*. Haettu 18. 8 2016 osoitteesta http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7381362&tag=1

Euroopan komissio. (11. 2 2016). *Directive on Payment Services (PSD)*. Haettu 25. 2 2016 osoitteesta http://ec.europa.eu/finance/payments/framework/index_en.htm

Euroopan komissio. (ei pvm). *Maksupalveludirektiivi - Mitä etua kuluttajalle?* Haettu 25. 2 2016 osoitteesta http://ec.europa.eu/internal_market/payments/docs/framework/psd_consumers/psd_fi.pdf

Euroopan unioni. (19. 4 2010). *EU:n oikeus*. Haettu 25. 2 2016 osoitteesta http://europa.eu/eu-law/index_fi.htm

Euroopan Unioni. (30. 8 2015). *Euroopan unionin direktiivit*. Haettu 25. 2 2016 osoitteesta http://eur-lex.europa.eu/legal-content/FI/TXT/?uri=URISERV%3Al14527

European Commission. (8. 10 2015). *Payment Services Directive: frequently asked questions*. Haettu 14. 6 2016 osoitteesta http://europa.eu/rapid/press-release_MEMO-15-5793_en.htm?locale=en

Fedler, R. (2013). Padding Oracle Attacks. 7. München. Haettu 14. 6 2016 osoitteesta Padding Oracle Attacks: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.637.1398&rep=rep1&type=pdf

Fielding, R. T. (2000). *Architectural Styles and the Design of Network-based Software Architectures.* Irvine: University of California. Haettu 5. 7 2016 osoitteesta https://www.ics.uci.edu/~fielding/pubs/dissertation/fielding_dissertation.pdf

Finanssivalvonta. (2014). *Maksupalvelun tarjoajat*. Haettu 26. 1 2016 osoitteesta http://www.finanssivalvonta.fi/fi/Finanssiasiakas/Palveluntarjoajat/Maksupalvelu/Pages/Default.aspx

Finlex. (2010). *Maksulaitoslaki*. Haettu 26. 1 2016 osoitteesta http://www.finlex.fi/fi/laki/ajantasa/2010/20100297

Freier, A.;& Karlton, P. (8 2011). *The Secure Sockets Layer (SSL) Protocol Version 3.0*. Haettu 18. 2 2016 osoitteesta https://tools.ietf.org/html/rfc6101

Hodges, J. J. (11 2012). *Internet Engineering Task Force.* Haettu 3. 3 2016 osoitteesta HTTP Strict Transport Security (HSTS): https://tools.ietf.org/html/rfc6797

Host Merchant Services. (ei pvm). *How do payment gateways work?* Haettu 27. 1 2016 osoitteesta http://www.finlex.fi/fi/laki/ajantasa/2010/20100297

Isaac, R.;Porche, I.;Sollinger, J.;& McKay, S. (2011). *A Cyberwork that Knows no Boundaries*. Haettu 5. 7 2016 osoitteesta http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-042.pdf

Järvinen, P. (2002). *Tietoturva & yksityisyys.* Porvoo: WS Bookwell.

Järvinen, P. (2006). *Paranna tietoturvaasi.* Porvoo: WS Bookwell.

Kemppinen, R. (2002). *Suomi Euroopan unionissa.* Helsinki: Eurooppatiedotus.

Man Young, R. (2013). *Wireless Mobile Internet Security (2nd Edition).* John Wiley & Sons.

Mayer, C.;& Schwenk, J. (2013). *Lessons Learned From Previous SSL/TLS Attacks - A Brief Cronology Of Attacks And Weaknesses.* IACR Cryptology ePrint Archive.

National Institute of Standards and Technology. (8 2015). *Secure Hash Standard (SHS)*. Haettu 6. 7 2016 osoitteesta http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf

Open Web Application Security Project. (19. 6 2016). *Transport Layer Protection Cheat Sheet*. Haettu 5. 7 2016 osoitteesta https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet

Paavilainen, J. (1998). *Tietoturva*. Jyväskylä: Suomen Atk-kustannus Oy.

Patel, R. (2013). *Kali Linux Social Engineering.* Packt Publishing.

Paytrail. (3. 12 2014). *Nets on ostanut enemmistöosuuden suomalaisesta Paytrail Oyj:stä*. Haettu 5. 7 2016 osoitteesta http://www.paytrail.com/blog/nets-on-ostanut-enemmisto-osuuden-suomalaisesta-paytrail-oyjsta

Paytrail. (3. 5 2016). *Paytrail - Integration guide*. Haettu 6. 7 2016 osoitteesta http://docs.paytrail.com/en/index-all.html#payment-api.rest

Paytrail. (ei pvm). *Paytrail maksutavat*. Haettu 5. 7 2016 osoitteesta http://www.paytrail.com/maksutavat

Paytrail. (ei pvm). *Paytrail tekee verkossa ostamisesta ja myymisestä mukavaa*. Haettu 5. 7 2016 osoitteesta http://www.paytrail.com/tarinamme

Rivest, R. (4 1992). *The MD5 Message-Digest Algorithm*. Haettu 2. 2 2016 osoitteesta http://tools.ietf.org/html/rfc1321?ref=driverlayer.com

Rivest, R.;Shamir, A.;& Adleman, L. (ei pvm). *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems.* Haettu 8. 6 2016 osoitteesta MIT computer science and artificial intelligence laboratory: https://people.csail.mit.edu/rivest/Rsapaper.pdf

Ruohonen, M. (2002). *Tietoturva.* Porvoo: WS Bookwell.

Services, H. M. (ei pvm). *How do payment gateways work?* Haettu 27. 1 2016 osoitteesta http://www.finlex.fi/fi/laki/ajantasa/2010/20100297

Sheffer, Y. H.-A. (2 2015). *Internet Engineering Task Force (IETF).* Haettu 3. 3 2016 osoitteesta Summarizing Known Attacks on Transport Layer Security (TLS) and Datagram TLS (DTLS): https://tools.ietf.org/html/rfc7457

Wagner, D.;& Schneier, D. (1996). *Analysis of the SSL 3.0 Protocol.* Haettu 18. 2 2016 osoitteesta Schneier on security: https://www.schneier.com/cryptography/paperfiles/paper-ssl-revised.pdf