FINANSSIVALVONTA
FINANSINSPEKTIONEN
FINANCIAL SUPERVISORY AUTHORITY

PSD2-seurantaryhmän kokous 27.2.2018

Agenda

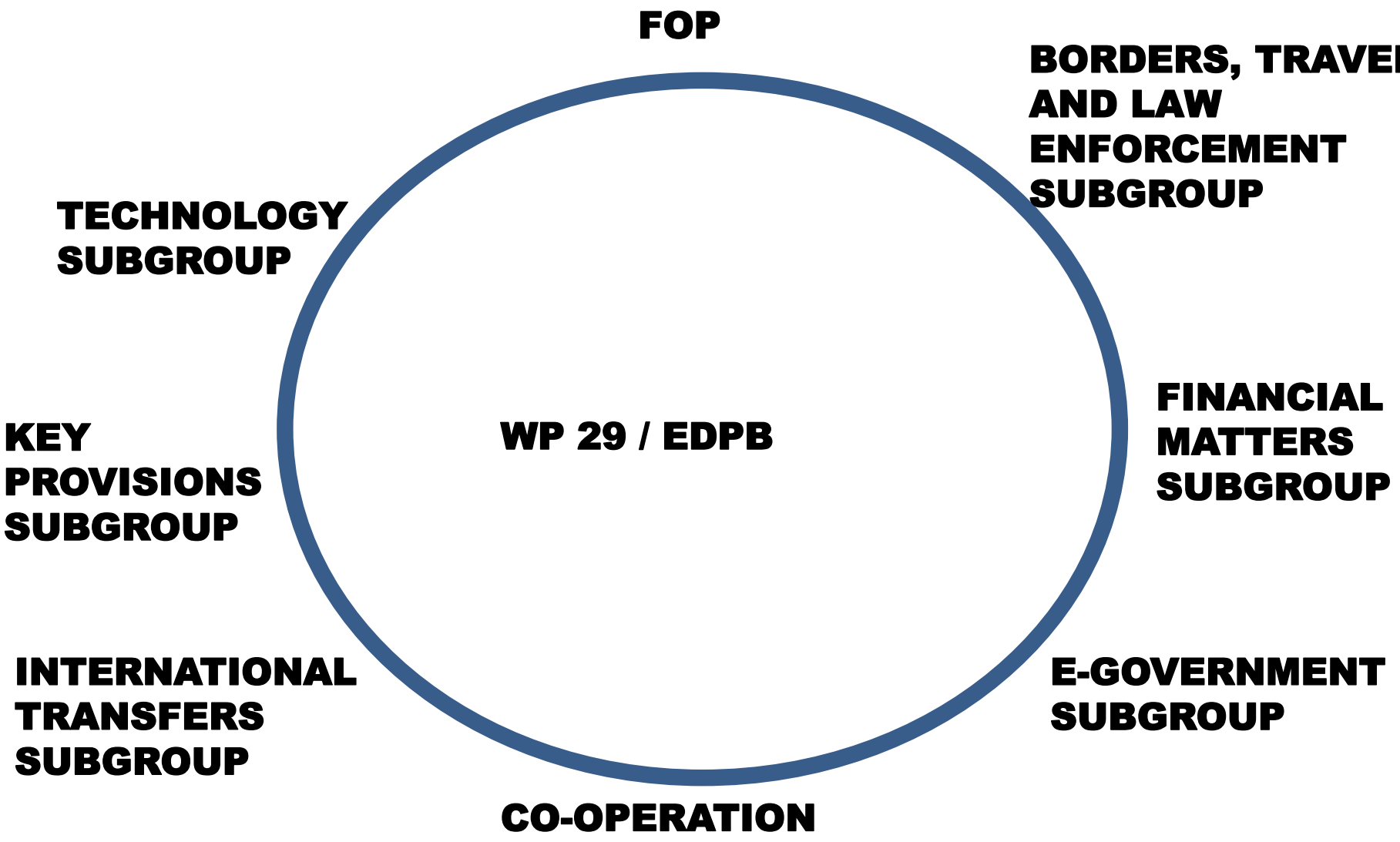
- Tietosuojavaltuutetun puheenvuoro
- Siirtymäajan tilanne
- Tunnistamiseen liittyvät kysymykset
- Maksutilin määritelmä
- Muut asiat
- Seuraavat kokoukset

PSD2-seurantaryhmän kokous
27.2.2018

Tietosuojavaltuutetun puheenvuoro

Reijo Aarnio
tietosuojavaltuutettu

Tietosuojavaltuutetun toimisto


FOP
BORDERS, TRAVEL AND LAW ENFORCEMENT SUBGROUP
TECHNOLOGY SUBGROUP
FINANCIAL MATTERS SUBGROUP
KEY PROVISIONS SUBGROUP
WP 29 / EDPB
INTERNATIONAL TRANSFERS SUBGROUP
E-GOVERNMENT SUBGROUP
CO-OPERATION

MIKSI WP 29:N LISTALLA?

► **havainto, että implementoitu eri tavoin MS:ssa**

MITÄ OTTAA HUOMIOON?

► **luku 4 TIETOSUOJA PSU (Payment Service User)**

► **Resital 89 refers to Directive 95/46/EU**

Maksupalveluntarjoajien suorittama maksupalvelujen tarjoaminen voi sisältää henkilötietojen käsittelyä. Tämän direktiivin mukaisessa henkilötietojen käsittelyssä olisi noudatettava Euroopan parlamentin ja neuvoston direktiiviä 95/46/EY (22) sekä direktiivin 95/46/EY ja Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 45/2001 (23) saattamiseksi osaksi kansallista lainsäädäntöä annettuja kansallisia sääntöjä. Kun henkilötietoja käsitellään tämän direktiivin soveltamiseksi, olisi erityisesti mainittava täsmällinen tarkoitus, viitattava asiaankuuluvaan oikeusperustaan ja noudatettava asiaankuuluvia direktiivissä 95/46/EY säädettyjä turvallisuusvaatimuksia, sekä kunnioitettava tarpeellisuuden, oikeasuhteisuuden, käyttötarkoituksen rajoittamisen ja tietojen säilyttämisen oikeasuhteisen enimmäisajan periaatteita. Kaikkiin tämän direktiivin puitteissa kehitettäviin ja sovellettaviin tietojenkäsittelyjärjestelmiin olisi myös sisällyttävä sisäänrakennettu tietosuoja tai oletusarvoinen tietosuoja.

EUROOPAN PARLAMENTIN JA NEUVOSTON DIREKTIIVI (EU) 2015/2366, annettu 25 päivänä marraskuuta 2015, maksupalveluista sisämarkkinoilla, direktiivien 2002/65/EY, 2009/110/EY ja 2013/36/EU ja asetuksen (EU) N:o 1093/2010 muuttamisesta sekä direktiivin 2007/64/EY kumoamisesta

94 artikla

Tietosuoja

1. Jäsenvaltioiden on sallittava, että maksujärjestelmät ja maksupalveluntarjoajat käsittelevät henkilötietoja, kun se on välttämätöntä

maksupetoksiin liittyvien rikosten torjunnan, tutkinnan ja selvittämisen turvaamiseksi. Henkilötietojen käsittelyä koskevien tietojen antamisessa yksityishenkilöille ja tällaisten henkilötietojen käsittelyssä ja muussa tätä direktiiviä sovellettaessa toteutettavassa henkilötietojen käsittelyssä on noudatettava direktiiviä 95/46/EY, direktiivin 95/46/EY saattamista osaksi kansallista lainsäädäntöä koskevia kansallisia sääntöjä ja asetusta (EY) N:o 45/2001.

2. Maksupalveluntarjoajat voivat vain maksupalvelunkäyttäjän nimenomaisella hyväksynnällä saada, käsitellä ja säilyttää sellaisia henkilötietoja, jotka ovat tarpeen niiden maksupalvelujen tarjoamiseksi.

”explicit consent”

TIETOTURVASTA

EBA → kehittää ja tarkastelee ”regulatory technical standards” (RTS)

Esim. ”strong authentication” (SCA)

Res 94 → art. 97

(94): Tunnistamista ja yhteydenpitoa koskevia teknisiä sääntelystandardeja laatiessaan pankkiviranomaisen olisi järjestelmällisesti arvioitava yksityisyysnäkökohta ja otettava se huomioon määrittääkseen kuhunkin saatavilla olevaan tekniseen vaihtoehtoon liittyvät riskit sekä korjaavat toimenpiteet, jotka voitaisiin toteuttaa tietosuojaan kohdistuvien uhkien minimoimiseksi.

97 artikla
Tunnistaminen

1. Jäsenvaltioiden on varmistettava, että maksupalveluntarjoaja soveltaa asiakkaan vahvaa tunnistamista, jos

a) maksaja käyttää maksutiliään verkon kautta;
b) maksaja käynnistää sähköisen maksutapahtuman
c) maksaja toteuttaa etäkanavan kautta minkä tahansa toimen, joka voi johtaa maksupetokseen tai muunlaisen väärinkäytöksen riskiin.

2. Jäsenvaltioiden on 1 kohdan b alakohdassa tarkoitettujen sähköisten maksutapahtumien käynnistämisen osalta varmistettava, että maksupalveluntarjoajat soveltavat sähköisten etämaksutapahtumien osalta asiakkaan vahvaa tunnistamista, johon sisältyy tekijöitä, joilla maksutapahtuma kytketään dynaamisesti määriteltyyn määrään ja tiettyyn maksunsaajaan.

97 artikla
Tunnistaminen

3. Jäsenvaltioiden on 1 kohdan osalta varmistettava, että maksupalveluntarjoajat ovat ottaneet käyttöön riittäviä turvatoimenpiteitä suojatakseen maksupalvelunkäyttäjien henkilökohtaisten turvatunnuksien luottamuksellisuuden ja eheyden.

4. Edellä olevaa 2 ja 3 kohtaa sovelletaan myös silloin, kun maksutapahtumat käynnistetään maksutoimeksiantopalvelun tarjoajan välityksellä.
Edellä olevia 1 ja 3 kohtaa sovelletaan myös silloin, kun tietoja pyydetään tilitietopalvelun tarjoajan välityksellä.

5. Jäsenvaltioiden on varmistettava, että tiliä ylläpitävä maksupalveluntarjoaja antaa maksutoimeksiantopalvelun tarjoajan ja tilitietopalvelun tarjoajan käyttää sellaisia tunnistamismenettelyjä, jotka tiliä ylläpitävä maksupalveluntarjoaja tarjoaa maksupalvelunkäyttäjälle 1 ja 3 kohdan ja, jos maksutoimeksiantopalvelun tarjoaja osallistuu maksutapahtumaan, 1, 2 ja 3 kohdan mukaisesti.

HAVAITTUJA EROJA IMPLEMENTOINNISSA ERI JÄSENMAISSA

1. Art 94 (1) ja (2)

2. (explicit) consent – käsite

vrt. GDPR

KUKA VALVOO 4. LUKUA

- DPA
- FIVA
- YHDESSÄ

Jos tämä olisi epäselvä, seuraisi;

- **OSS ylikansallisissa caseissa?**
- **harmonisointi vaarantuu**

- **HUOM! WP29 EI OLE KUULTU RTS:STÄ ENNEN KUIN KOMISSIO SEN JULISTI SITOVAKSI**

→ MANDAATTI FMS:lle

WP 29 6.-7.2.2018

(FMS)
Financial Matters Subgroup 17.1.2018

- **arvioi onko PSD2 GDPR:n mukainen;**

  1) suostumus (94.2 art.)
  2) Ovatko RTS SCA:sta ok
  3) Miten rekisteröidyn informointi on hoidettu suhteessa GDPR:ään
  4) ”Screenscraping” siirtymäaikana

WP 29 6.-7.2.2018

HUOM! FMS: EP ja Neuvosto
voivat vastustaa RTS:ää TUNNISTUKSESSA (SCA)

HUOM! FMS:lla ”some concerns”

Screenscrapingistä → tiedossa ei ole,
onko nämä EP:n ja NEUVOSTON tiedossa

FMS sai jatkomandaatin

KIITOS KUUNTELUSTA

Lisätietoja: www.tietosuoja.fi

Reijo Aarnio
tietosuojavaltuutettu

Siirtymäajan tilanne

- Finanssivalvonnan kannanotto siirtymäajan tilanteesta 10.1.2018
- Asiakasrajapinnan hyödyntäminen screen scraping menetelmällä mahdollista mikäli
  - Palveluntarjoajan tunnistautuminen pankille pystytään toteuttamaan riittävän luotettavasti ja turvallisesti ja
  - Pääsy asiakkaan tietoihin pystytään rajaamaan vain asiakkaan nimeämiin maksutilitietoihin
- Finanssivalvonnan kirje pankeille 21.2.2018
  - Yhteistyövelvoite voimassa, pankit eivät saa estää luvan saaneita palveluntarjoajia tarjoamasta uusia maksupalveluja
  - Lista kysymyksiä, joiden pohjalta Finanssivalvonta arvioi, miten pankit mahdollistavat asiakkaiden oikeuden käyttää uusia maksupalveluja siirtymäaikana
  - Uusien rajapintojen valmistumistilanne ja tehostettu seuranta

Tunnistamiseen liittyvät kysymykset

Asiakkaan vahva tunnistaminen

- Sähköisessä tunnistamisessa käytettävä menettelyä, joka perustuu vähintään kahteen kolmesta toisistaan riippumattomasta vaihtoehdosta
  - Jokin, mitä vain maksupalvelun käyttäjä **tietää** (salasana, pin-koodi)
  - Jokin, mitä vain maksupalvelun käyttäjällä on **hallussaan** (sirukortti, matkapuhelin, tunnistussovellus)
  - Maksupalvelun käyttäjän yksilöivä **ominaisuus** (sormenjälki, kasvojen muoto, silmän iiris)

Asiakkaan vahvan tunnistamisen käyttö

- Palveluntarjoajan on käytettävä vahvaa tunnistamista, jos maksaja
  - käyttää maksutiliään tietoverkon välityksellä
  - käynnistää sähköisen maksutapahtuman
  - toteuttaa etäkanavan kautta toimen, johon voi liittyä väärinkäytöksen riski
- Poikkeukset säädetään komission asetuksella
  - Tekniset sääntelystandardit asiakkaan vahvasta tunnistamisesta ja osapuolten turvallisesta kommunikoinnista
- RTS:n velvoite ja poikkeukset voimaan syksyllä 2019?
- Vastuunjako, jos asiakasta ei ole todennettu vahvasti (voimaan 13.1.2018)
  - Asiakas ei vastaa väärinkäytöstä
  - Tilinpitäjäpankilla ensisijainen vastuu asiakkaalle, mutta takautumisoikeus kolmannelta palveluntarjoajalta

Poikkeukset asiakkaan vahvaan tunnistamiseen

- Maksutilin tiedot
  - Saldo ja tilitapahtumat 3 kuukaudelta
  - Tunnistautuminen 90 päivän välein
  - Aina ensimmäisellä kerralla
- Lähimaksaminen
  - Maksut alle 50 euroa
  - Kumulatiivinen 150 euroa tai korkeintaan viisi maksua peräkkäin
- Liikenne- ja parkkimaksuautomaatit
- Tunnetut maksunsaajat ja toistuvat maksutapahtumat
- Maksut omien tilien välillä
- Pienmaksut verkossa
  - Maksut alle 30 euroa
  - Kumulatiivinen 100 euroa tai korkeintaan viisi maksua peräkkäin
- Maksutapahtumien riskiarvio
  - Korkeintaan 500 euroa
  - Väärinkäytösten prosenttirajat

Vertailu: RTS vs. eIDAS-vaatimukset

- Verkkopankkitunnukset ovat Suomessa myös vahva sähköinen tunnistusväline, jota koskee oma erillinen lainsäädäntö
  - Tunnistuslaki
  - eIDAS-asetus
  - Viestintäviraston määräykset ja ohjeet
- RTS- ja eIDAS-vaatimusten eroja käyty läpi Viestintäviraston kanssa
  - Pääosin vaatimukset yhteneviä
  - Molemmissa tunnistautumisen perustuttava kahteen kolmesta tekijästä: tieto, hallussapito, ominaisuus
- Tunnistetut eroavaisuudet:
  - Tunnistuslain mukaisissa ratkaisuissa ennalta määrätyt auditointivaatimukset
  - RTS on tiukempi paperisten tunnuslukulistojen suhteen (7 artikla)
  - RTS sisältää vaatimuksia dynaamiseen linkitykseen (5 artikla)

Tulkintakysymys paperisista tunnuslukulistoista

Article 7 Requirements of the elements categorised as possession

1. Payment service providers shall adopt measures to mitigate the risk that the elements of strong customer authentication categorised as possession are used by unauthorised parties.

2. The use by the payer of those elements shall be subject to measures designed to prevent replication of the elements.

- Löytyykö argumentteja sille, miten paperiset tunnuslukulistat läpäisisivät kohdan 2 vaatimukset
- Finanssivalvonta valmistelee asiasta virallisen linjauksen ottaen huomioon yhdenvertaisuuskysymykset
- Näkemyksiä voi esittää sähköpostitse 16.3.2018 asti (psd2(at)finanssivalvonta.fi)

Varmenteet palveluntarjoajan tunnistautumiseen

- Kolmannen palveluntarjoajan on pystyttävä tunnistautumaan tilinpitäjäpankille
- Komission tekninen sääntelystandardi edellyttää seuraavia tunnistautumismenetelmiä:
  - Sähköisen leiman hyväksytty varmenne (eIDAS-asetus 3 art 30-kohta)
  - Verkkosivustojen todentamisen hyväksytty varmenne (eIDAS-asetus 3 art 39-kohta)
- Hyväksytyt varmennetuotteet merkitään luotetulle listalle
  - Mahdollista käyttää missä tahansa jäsenvaltiossa hyväksyttyä tuotetta
- Varmenteesta käytävä ilmi:
  - Palveluntarjoajan tyyppi: tilinpitäjäpankki, maksutoimeksiantopalvelu, tilitietopalvelu, korttipohjaisen maksuvälineen liikkeeseenlaskija
  - Viranomainen, jolta palveluntarjoaja on saanut toimiluvan

ETSI määrittelee varmenteen tarkemmat toteutukset

- ETSI kehittää parhaillaan määrityksiä varmenneratkaisulle, joka täyttäisi sekä eIDAS-asetuksen että PSD2:n vaatimukset

- Standardiluonnos ETSI TS 419 495 on parhaillaan lausunnoilla
  - *PSD2 Qualified Certificates as specified by ETSI in TS 119 495*

- Tulossa kaikille avoin info- ja keskustelutilaisuus ETSIssä 20.3.2018

EBAn jatkotyö

- EBAssa käynnistynyt jatkotyö vahvan tunnistamisen ja turvallisen kommunikoinnin RTS:n tiimoilta, mm:
  - Kriteerit ns. yritysmaksupoikkeusten ja fall-back järjestelmän ylläpitoa koskevien poikkeusten käsittelyyn ja muihin RTS:n asioihin, joissa edellytetään joko kansallisen valvojan tai EBAn tulkintaa
  - Fivan osallistuu tähän työhön

Maksutilin määritelmä

Maksutilin määritelmä (kertaus)

- Maksutili on tili, jota voidaan käyttää maksutapahtumien toteuttamiseen (MPL 8 § 5 k)
- Maksutapahtuma on toimenpide, jolla varoja siirretään, nostetaan tai asetetaan käytettäväksi (MPL 8 § 3 k)
- Olennaista voidaanko maksutiliä käyttää tietoverkon välityksellä:
  - Jos maksutiliä voidaan käyttää tietoverkon välityksellä, maksutiliä pitävän palveluntarjoajan on sallittava maksajan käynnistää maksutapahtuma maksutoimeksiantopalvelun tarjoajan välityksellä (MPL 38 a § 1 mom)
  - Jos maksutiliä voidaan käyttää tietoverkon välityksellä, maksutiliä pitävän palveluntarjoajan on sallittava maksupalvelun käyttäjän käyttää tilitietopalveluja (MPL 82 a § 1 mom)
- Tiliä koskevien sopimusehtojen perusteella määräytyy, voidaanko tiliä käyttää maksutapahtumien toteuttamiseen
- Fivan vanha tulkinta: maksutili on tili, jolta tilinomistaja voi vapaasti tallettaa ja vapaasti nostaa varoja
- Maksutilejä ovat esim.: käyttötili, säästötili, luottokorttitili
- Maksutilejä eivät ole esim.: määräaikaistalletustili, arvo-osuuksien hoitotili

Maksutilin määritelmän piiriin kuuluvat tilit

- Finanssivalvonta ei käy yksitellen läpi maksutiliä ylläpitävien palveluntarjoajien tilejä ja listaa, mitkä niistä kuuluvat maksutilin käsitteen piiriin
  - Yritysten compliance-toimintojen tehtävä
  - Edellyttää tarkastelua tili kerrallaan
  - Finanssivalvonnasta voi kysyä tulkinta-apua
- **Pääsääntö**: Kolmas palveluntarjoaja ei voi saada tiliin laajempia käyttöoikeuksia kuin asiakkaalla itsellään on, esim.:
  - Jos asiakas ei voi suorittaa tililtä maksuja, niin tällöin tiliä ei voida myöskään käyttää maksutoimeksiantojen käynnistämiseen
  - Jos asiakas ei voi käyttää tiliä tietoverkon välityksellä, myöskään kolmannella palveluntarjoajalla ei ole tätä oikeutta

Säästötilit

- Jos tili on sellainen, että tilisiirrot ovat mahdollisia ainoastaan kyseisen tilin ja toisen samassa pankissa olevan saman asiakkaan tilin välillä, onko kyse maksupalvelulain määritelmän mukaisesta maksutilistä?
- HE 169/2009: ”*Maksutilinä pidetään myös esimerkiksi sellaista säästötiliä, jolle tilinomistaja voi tallettaa varoja tai jolta tilinomistaja voi nostaa varoja ilman että siitä tulee erikseen sopia palveluntarjoajan kanssa. Maksutilinä ei sitä vastoin pidetä esimerkiksi määräaikaistalletustiliä*”
- Tällaista tiliä ei voida käyttää maksutoimeksiannon käynnistämiseen, koska tilisiirto mahdollinen vain samassa pankissa olevalle saman asiakkaan tilille.
- Säästötili kuitenkin kuuluu maksutilin käsitteen piiriin
  - Voiko tiliä käyttää tietoverkon välityksellä?
  - **Tilitietopalvelujen käyttäminen sallittava, mikäli säästötilin käyttäminen tietoverkon välityksellä on mahdollista**

Luottokorttitilit

- HE 169/2009: ” *Maksutilin määritelmän piiriin kuuluvat myös luottokorttitilit ja muut niitä vastaavat maksutapahtumien toteuttamiseen käytettävät tilit. Maksutili voi siis olla myös tili, jolle maksupalvelun käyttäjä ei pane varoja.*”
- Edellyttää luottokorttitilin sopimusehtojen tarkastelua:
  - Voiko asiakas maksaa tililtä esim. laskuja tai tehdä tilisiirtoja vai onko maksutapahtumat rajoitettu vain kortin kautta tehtäviin tapahtumiin
  - Kolmas palveluntarjoaja ei voi saada laajempia oikeuksia kuin asiakkaalla
- Luottokorttitilejä voidaan tyypillisesti käyttää tietoverkon välityksellä
  - Tällöin tilitietopalvelujen käyttäminen sallittava

Muut asiat

Maksutoimeksiantopalvelu ja asiakasvarojen hallussapidon kielto

- Maksutoimeksiantopalvelun tarjoaja ei saa pitää hallussaan maksajan varoja maksutoimeksiantopalvelun tarjoamisen yhteydessä (MPL 38 a 3 mom 1 k)
- Jos maksutoimeksiantopalvelun tarjoaja tarjoaa sellaista *muuta maksupalvelua*, johon liittyy asiakkaan varojen hallussapitoa, tulevat kyseistä muuta maksupalvelua koskevat säännökset sovellettaviksi
  - Muuhun maksupalveluun tarvitaan sitä koskeva toimilupa
- Maksulaitos, jolla oikeus tarjota sekä PSD1:een perustuvia maksupalveluita että PSD2:een perustuvia maksutoimeksiantopalveluita:
  - Ei voi yhdistää näitä maksupalveluita: **valittava jompikumpi toteutustapa tapahtumaketjulle**
  - Maksu tulee käynnistää suoraan asiakkaan tililtä maksunsaajan tilille
  - Ei voi ohjata maksutoimeksiantopalvelun käynnistämisen yhteydessä asiakkaan varoja oman asiakasvaratilin kautta maksunsaajalle
  - Maksunsaaja ei voi valtuuttaa maksutoimeksiantopalvelun tarjoajaa ottamaan vastaan asiakasvaroja maksusaajan puolesta

Muut asiat

- Määräysten ja ohjeiden päivitysversiot julkaistu (8/2014 ja 8/2016)
  - EBAn formaatin mukainen häiriöilmoituslomake ja uudistettu Fivan häiriöilmoituslomake pyritään julkaisemaan tällä viikolla
  - Fivan häiriöilmoituslomakkeelle tehty rakenteellisia muutoksia ja lomake muutettu Excel-muotoon
- Tulossa: valvottavatiedote siitä, mitä vanhoilta toimijoilta vaaditaan luvan voimassapitämiseksi
  - Maksulaitokset ja rekisteröidyt maksupalveluntarjoajat -> MLL 19 a ja 19 b §:ien mukaisia tietoja.
- Finanssivalvonnan Innovaatio-HelpDeskiin on tullut paljon kysymyksiä mm. AIS/PIS-palvelujen aloittamisesta – konkretisoitunevat hakemuksiksi vähitellen.
- PII-vastuuvakuutus (AIS ja PIS toimintaan). Fiva ei ainakaan lähiaikoina tule antamaan omaa ohjeistusta. EBAsta ehkä tulkintoja asiaan.

Seuraavat kokoukset

- Neljäs kokous: 23.3. klo 9-11
- Viides kokous: To 3.5. klo 13.30-15.30
- Kuudes kokous: Ma 11.6. klo 9.30-11.30

- Kesäloman jälkeen ensimmäinen kokous elokuun lopulla

FINANSSIVALVONTA
FINANSINSPEKTIONEN
FINANCIAL SUPERVISORY AUTHORITY

Kiitos!