FINANSSIVALVONTA
FINANSINSPEKTIONEN
FINANCIAL SUPERVISORY AUTHORITY

PSD2-seurantaryhmä 3.5.2018

Agenda

- Kokouksen avaus
- Keskustelu paperisista tunnuslukulistoista
- RTS:n tulkintakysymyksiä
- Finanssivalvonnan saamien PSD2-tulkintakysymysten läpikäyntiä
- Muut asiat
- Seuraavat kokoukset

FINANSSIVALVONTA
FINANSINSPEKTIONEN
FINANCIAL SUPERVISORY AUTHORITY

Keskustelu paperisista tunnuslukulistoista

RTS SCA & CSC

- Komissio hyväksynyt 27.11.2017 asiakkaan vahvaa tunnistamista ja turvallista kommunikointia koskevat tekniset sääntelystandardit
  - Regulatory Technical Standards on strong customer authentication and common and secure communication
  - Voimaan 18 kk kuluttua julkaisusta virallisessa lehdessä
  - Voimaantulo 14.9.2019
- Tekniset vaatimukset asiakkaan vahvalle tunnistamiselle
- Poikkeukset asiakkaan vahvasta tunnistamisesta
- Turvallisuusvaatimukset asiakkaan henkilökohtaisten turvatunnusten suojaamiseksi
- Turvallisuusvaatimukset eri osapuolten keskinäisestä kommunikoinnista
- **Finanssivalvonta kannustaa noudattamaan standardin vaatimuksia jo ennen voimaantuloa**

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
- 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

Asiakkaan vahva tunnistaminen ja hallussapitoa koskevan elementin vaatimukset (RTS 7 art)

- Maksupalveluntarjoajien on toteutettava toimenpiteitä, joilla vähennetään sitä riskiä, että oikeudettomat tahot käyttävät ryhmään ”hallussapito” kuuluvia asiakkaan vahvan tunnistamisen tekijöitä (art 7.1)
- **Maksajan käyttäessä näitä tekijöitä niiden käyttöön sovelletaan toimenpiteitä, joiden tavoitteena on estää kyseisten tekijöiden kopioituminen** (art 7.2)
- Hallussapitoelementiksi tarkoitettu esim. älykortti, tunnistussovellus tai ns. token-laite
- Hallussapidolle asetetut vaatimukset erillisiä ja itsenäisiä suhteessa ns. two factor authentication pääsääntöön

➢ **Finanssivalvonnalla ei vielä alustavaa tulkintaa asiasta**

Pankkien ja sidosryhmien näkemyksiä

- Enemmistö pankeista ei osaa nimetä toimenpiteitä, jotka pyrkisivät estämään tunnuslukulistojen kopioitumista
  - Paperisen tunnuslukulistan voi helposti kopioida
- Muutamalla pankilla näkemyksiä, joiden perusteella tunnuslukulistojen käyttöä voisi jatkaa
- Valtaosa pankeista toivoo lisäaikaa mahdollisen muutosprosessin läpiviemiselle
- Huoli erilaisten asiakasryhmien sopeutumisesta
- Keskustelua asiasta käyty EBAn supervisory workshopissa

Fivalle esitettyjä näkemyksiä tunnuslukulistojen puolesta

- Hallussapitoa koskeva vaatimus ei ratkaiseva, koska vahva tunnistaminen tuotetaan vähintään kahdella erillisellä tekijällä
- Kokonaisuus ratkaisee, ei erilliset vaatimukset
- Sopimusehdoilla voi asettaa asiakkaalle ohjeita, joilla pyritään estämään väärinkäytöksiä
- eIDAS-sääntely mahdollistaa tunnuslukulistojen käytön
- Ei ole Suomessa esiintynyt merkittävänä riskinä väärinkäytöksille

eIDAS-sääntelyn ja PSD2-sääntelyn eroavaisuudet asiassa

- Silloin, kun verkkopankkitunnuksia käytetään muuhun sähköiseen asiointiin, sovelletaan tunnistuslakia
- Tunnistuslaki on yhdenmukaistettu eIDAS-asetuksen vaatimusten kanssa
  - Kolme varmuustasoa (matala, korotettu, korkea)
  - Korotettu: verkkopankkitunnukset ja mobiilivarmenteet
  - Korkea: Väestörekisterikeskuksen HST-kortti
- Vaatimus kopioitavuuden estämisestä koskee vain *korkean* varmuustason tunnistusmenetelmiä
  - ei koske *korotetun* varmuustason tunnistusvälineitä kuten verkkopankkitunnuksia.
- Erona on myös se, miten tunnistamisen eri elementtejä on tarkasteltava
  - eIDAS-asetus mahdollistaa vaatimusten tulkitsemisen kokonaisuutena
  - RTS edellyttää jokaisen tunnistamisen elementin tarkastelua erikseen
- Viestintävirasto ja Finanssivalvonta yhtä mieltä vaatimusten eroavaisuudesta

Finanssivalvonnalle toimitettavia lisänäkemyksiä

- Aikatauluun liittyviä näkemyksiä mahdollisen muutosprosessin läpiviemiselle
- Minkälaisia vaihtoehtoja tai suunnitelmia on erilaisille asiakasryhmille
  - Yhdenvertaisuus ja syrjimättömyys peruspankkipalveluiden tarjoamisessa
- Onko saatavilla sisäistä tilastotietoa väärinkäytöstapausten liittymisestä verkkopankkitunnuksiin ja tunnuslukulistojen kopioimiseen?

FINANSSIVALVONTA
FINANSINSPEKTIONEN
FINANCIAL SUPERVISORY AUTHORITY

RTS SCA & CSC liittyviä tulkintakysymyksiä

Mitä maksutilitietoja AISP tai PISP on oikeutettu saamaan?

- Uusi rajapinta ja pääsy asiakkaan nimeämiin *maksutilitietoihin* on luotava vastaavanlaajuiseksi, joka asiakkaalla itsellään verkkopankissa tai mobiilipankissa on
  - Pankin toteutettava pääsy asiakkaalle tarjotun laajemman asiointikanavan mukaisesti
  - Verkkopankki vs. mobiilipankki
- Henkilöllisyyteen liittyvät nimi, syntymäaika, osoite yms. tiedot eivät kuulu PSD2 sääntelyn piiriin
  - Pankilla ei velvollisuutta tarjota pääsyä näihin tietoihin
- PISP:lle tarjottava välittömästi kyllä/ei -tieto varojen riittävyydestä
  - PISP:lle ei tarjota tilin saldotietoa
- PIS ja AIS erillisiä palveluita, vaikka samalla palveluntarjoajalla olisi lupa tarjota molempia palveluita
  - PIS palvelussa ei voi hyödyntää AIS palvelun avulla saatavaa dataa

Asiakkaan vahva tunnistaminen ja maksutilitietoja koskeva poikkeus (RTS 10 art)

- Vahvaa tunnistamista ei vaadita, kun asiakkaan pääsy rajoittuu seuraaviin tietoihin:
  - Tilin saldotieto
  - Maksutapahtumat, jotka on toteutettu edeltävien 90 päivän aikana yhden tai useamman nimetyn maksutilin välityksellä
- Vahva tunnistaminen vaaditaan kuitenkin aina:
  - Kun asiakas kirjautuu tietoihin ensimmäisen kerran verkossa
  - On kulunut yli 90 päivää siitä, kun asiakas edellisen kerran katsoi maksutapahtumatietoja verkossa ja asiakkaan vahvaa tunnistamista sovellettiin
- 90 päivän laskuri ei ole riippuvainen kanavasta, mitä asiakas käyttää
  - Ei erillisiä kanavakohtaisia 90 päivän laskureita
  - Asiakkaan kirjautumiset sekä verkkopankkiin että mobiilipankkiin kuuluvat samaan 90 päivän laskentaan
  - Avoinna kysymys kuuluvatko AISP kirjautumiset samaan 90 päivän laskentaan vai eri laskentaan?

Redirection-malli

- Rajapinnan toteutus ns. redirection mallilla
- Yleisesti pankkien käytössä oleva malli
- Redirection-mallin ei itsessään voida katsoa olevan RTS 32 artiklassa tarkoitettu este
  - Voidaan käyttää rajapintaratkaisussa
  - Ratkaisevaa, miten redirection on toteutettu
  - Mallia ei saa rakentaa asiakkaalle hankalaksi
- Pankilla ei velvollisuutta ylläpitää useampaa rajapintamallia
  - Kannustetaan kuitenkin vaihtoehtoisen menetelmän ylläpitämiseen ottaen huomioon erilaiset kanavat ja käyttötavat

Asiakkaan vahva tunnistaminen ja yritysmaksupoikkeukset (RTS 17 art)

- Yritysten maksuprosesseissa, jotka välitetään muulla tavoin kuin RTS:n mukaisella rajapinnalla, voidaan hyödyntää poikkeusta asiakkaan vahvasta tunnistamisesta
  - Mikäli valvova viranomainen on vakuuttunut, että kyseiset maksuprosessit tarjoavat vähintään saman turvallisuustason kuin PSD2:ssa edellytetään
  - Mikäli kyseiset prosessit eivät ole kuluttajien käytettävissä
- EBAn workshop: jatkotyö poikkeusten yhdenmukaisuuden varmistamiseksi
  - poikkeusten kohdistaminen ja kriteerit
  - väärinkäytöstilastot
- Alustava toimintamalli: Finanssivalvonnalle kuvaus palvelusta (ml. turvallisuus- ja tunnistamisratkaisut) ja riskiarvio
  - Fiva arvioi tapauskohtaisesti tarvitaanko esim. tapaamista tai lisäselvityksiä

EBAn jatkotyö – RTS SCA & CSC

- Valvova viranomainen voi myöntää tilinpitäjäpankille poikkeuksen velvollisuudesta ylläpitää dedikoidun rajapinnan varajärjestelmää (ns. fall back-poikkeus, RTS 33 art.)
  - Prosessiin kuuluu EBAn konsultointi
- Fall back-poikkeuksen kriteereistä sekä valvovan viranomaisen ja EBAn välisestä tietojenvaihdosta valmisteilla ohjeistusta (EBA Guidelines)
  - Julkiselle konsultaatiolle mahdollisesti jo kesäkuussa?
- RTS SCA & CSC liittyvistä tulkintakysymyksistä valmisteilla EBA Opinion
  - Mahdollisesti jo kesäkuussa?
  - Opinion ei kuitenkaan kata yritysmaksupoikkeuksia
- Fraud-Guidelinen lopullinen versio julkaistaneen kesäkuussa

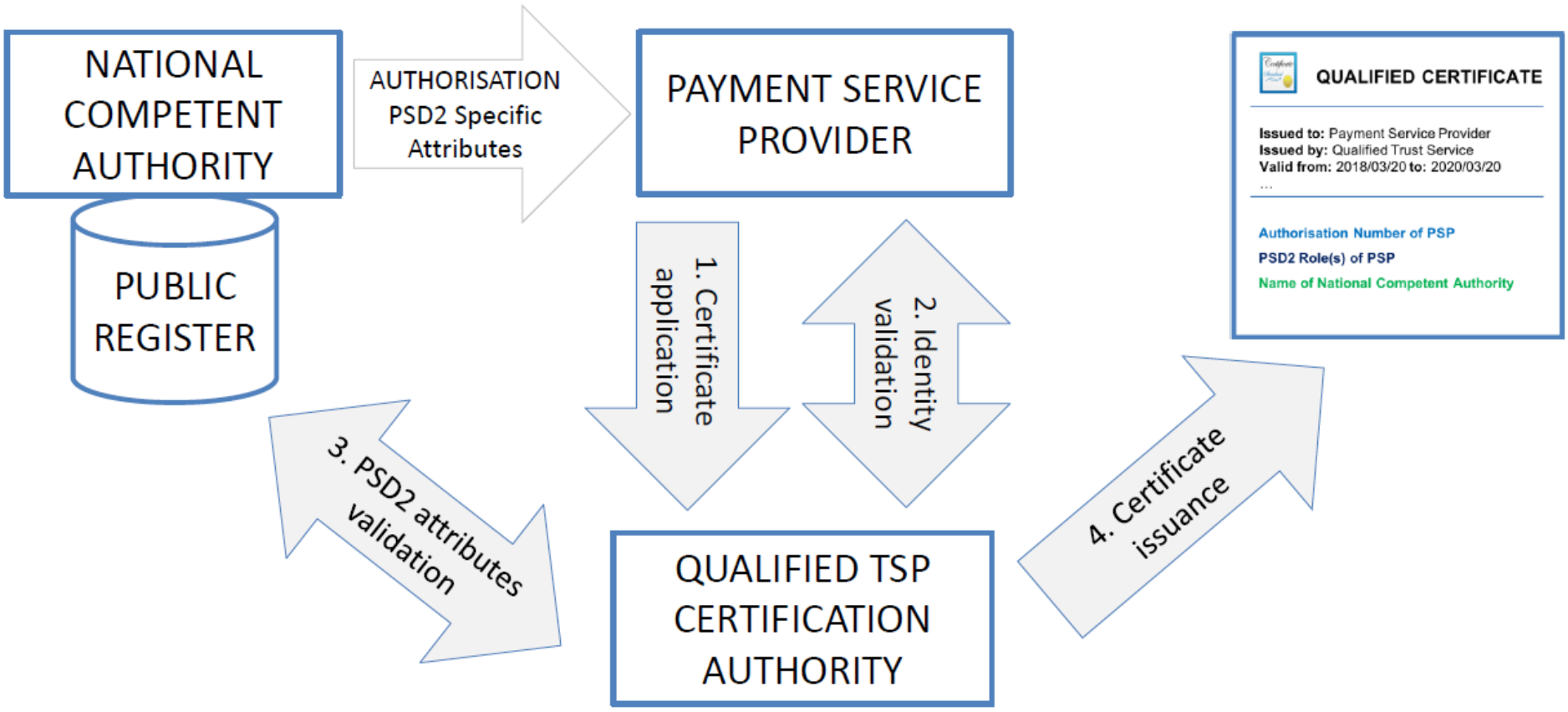
Varmenteet palveluntarjoajan tunnistautumiseen

- 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
- Palveluntarjoaja hankkii varmenteen itse varmenteiden myöntäjältä
  - Revokointia voi hakea palveluntarjoaja tai Finanssivalvonta

ETSIn työ on loppumetreillä

- ETSI kehittänyt määritykset varmenneratkaisulle, joka täyttää sekä eIDAS-asetuksen että PSD2:n vaatimukset
- ETSI final draft julkaistu 18.4.2018
- Varmenteesta käytävä ilmi:
  - Yksilöivä tunniste (authorisation number)
  - Palveluntarjoajan rooli: tilinpitäjäpankki, maksutoimeksiantopalvelu, tilitietopalvelu, korttipohjaisen maksuvälineen liikkeeseenlaskija
  - Viranomainen, jolta palveluntarjoaja on saanut toimiluvan (home NCA)
- Alustava näkemys: erilliset varmenteet eri palvelutyypeille

Varmenteen hakuprosessi



Lähde: ETSI

FINANSSIVALVONTA
FINANSINSPEKTIONEN
FINANCIAL SUPERVISORY AUTHORITY

Finanssivalvonnalle esitettyjä tulkintakysymyksiä ja muut asiat

Luottolaitoksen velvollisuus tarjota maksutilipalveluita maksulaitoksille (MLL 41 d §)

- MLL:n uusi säännös velvoittaa luottolaitoksen tarjoamaan luvan saaneelle maksupalveluntarjoajalle (maksulaitoksille ja MLL 7 ja 7 b §:ssä tarkoitetuille toimijoille) maksutilipalveluita syrjimättömin ja oikeasuhtaisin perustein
- Säännöksen tarkoituksena on turvata maksulaitoksille mahdollisuus tarjota maksupalveluita ja edistää kilpailua
- Säännös jättää pankille harkintavaltaa tilanteisiin, jolloin asiakkuudesta voi kieltäytyä
- Säännös koskee myös maksutilipalvelujen perusteetonta rajoittamista
  - Esteetön ja tehokas maksupalveluiden tarjonta tulee mahdollistaa
  - Pankin asettamat ehdot maksupalvelujen tarjonnalle tulee olla objektiivisia, syrjimättömiä ja oikeasuhtaisia riskeihin nähden

Palvelun epäämisestä on ilmoitettava Finanssivalvonnalle (MLL 41 d §)

- Jos luottolaitos epää tilipalvelujen tarjonnan, on sen ilmoitettava Finanssivalvonnalle epäämisestä ja sen perusteista
- Ilmoituksen toimitus ja sisältö:
  - Ilmoitus tulee toimittaa Finanssivalvonnan kirjaamoon (kirjaamo(at)finanssivalvonta.fi)
  - Jokainen kieltäytyminen tulee ilmoittaa omana ilmoituksenaan
  - Ilmoituksen sisällöstä tulee käydä ilmi syy kieltäytymiselle riittävästi perusteltuna
  - Ilmoitus tulee tehdä mahdollisimman pian kieltäytymispäätöksen jälkeen
  - Ilmoitus tulee otsikoida selkeästi: esim. ”Ilmoitus maksutilipalvelusta kieltäytymisestä”
- Finanssivalvonnalle tehtävällä ilmoituksella merkitystä luottolaitoksen menettelyn asianmukaisuuden yleisen valvonnan näkökulmasta

Muita asioita

- Pohjoismainen valvojakokous fintech- ja PSD2-asioissa 28-29.5.2018 Helsingissä, agendalla mm.
  - Rajatun verkon poikkeus
  - Asiakasvarojen hallussapito
  - Valvojien innovaatiokeskukset
  - ICO (Initial Coin Offering)
- Siirtymäajan tilanne
  - Finanssivalvonnalle esitelty siirtymäajan ratkaisuja

Seuraavat kokoukset

- Ma 11.6. klo 9.30-11.30
- Syksyn ensimmäinen kokous arviolta syyskuussa

Kiitos!