

Pankki- ja maksutilien valvontajärjestelmä
Tiedonhakujärjestelmän käyttöönoton ja ylläpidon ohje

21.10.2019

Tiedonhakujärjestelmä

Käyttöönoton ja ylläpidon ohje

Dokumentin versio 1.0

[illegible]

SISÄLLYSLUETTELO

1 Dokumentin tarkoitus	4
2 Sanasto ja lyhenteet	4
3 Tausta ja kattavuus	5
4 Tiedonhakujärjestelmän esittely	5
4.1 Tiedonhakujärjestelmän tiedot	5
4.2 Toimijat ja roolit	6
5 Prosessikuvaus	6
5.1 Liiketoimintaprosessien kulku ja roolit	7
5.2 Tullin tuki	7
5.3 Tiedon luovuttajat	8
5.4 Tiedonhakujärjestelmän kyselyrajapinta	8
5.5 Ilmoitusmenettely	8
5.6 Tiedon luovuttamisen rajapintojen testaus	8
6 Tietoturva	9
6.1 Vaatimukset varmenteille	9
6.2 Varmenteiden uusiminen ja kustannukset	9
7 Palvelutaso	10

1 Dokumentin tarkoitus

Tämä dokumentti on osa Tullin [määräystä 6/2019](#) pankki- ja maksutilien valvontajärjestelmästä. Dokumentin tarkoitus on antaa ohjeet tiedon luovuttajille tiedonhakujärjestelmän käyttöönnoton ja ylläpidon osalta. Tätä dokumenttia täydentää tiedonhakujärjestelmän kyselyrajapinnan kuvaus.

Tulli tulee julkaisemaan nämä ohjeet myös verkkosivuilla.

2 Sanasto ja lyhenteet

Termi	Selite
Pankki- ja maksutilien valvontajärjestelmä	Kansallinen pankki- ja maksutilien valvontajärjestelmä, joka koostuu Tilirekisteristä sekä tiedonhakujärjestelmästä, perustuu lakiin pankki- ja maksutilien valvontajärjestelmästä 571/2019 sekä Euroopan parlamentin ja neuvoston direktiiviin (EU) 2018/843, joka on annettu 30 päivänä toukokuuta 2018 rahoitusjärjestelmän käytön estämisestä rahanpesuun tai terrorismin rahoitukseen.
Tiedonhakujärjestelmä	Tiedonhakujärjestelmä on tiedon luovuttajan ylläpitämä sähköinen pankki- ja maksutilien tiedonhakujärjestelmä, jonka avulla tiedon luovuttaja välittää välittömästi ja salassapitosäännösten estämättä pankki- ja maksutilien valvontajärjestelmän 2 momentissa tarkoitettuja tietoja asiakkaistaan toimivaltaiselle viranomaiselle. Tulli määrää lain mukaan tiedonhakujärjestelmästä tekniset vaatimukset ja jokainen tiedon luovuttaja toteuttaa oman tiedonhakujärjestelmän, eli tiedonhakujärjestelmiä on monta.
Rekisterinpitäjä	Hajautetussa tiedonhakujärjestelmässä tiedon luovuttaja vastaa rekisterinpitäjänä tietojen saatavilla olosta ylläpitämällä tiedonhakujärjestelmää ja toimivaltainen viranomainen vastaa rekisterinpitäjänä tiedonhakujärjestelmän avulla käsittelemistään tiedoista.
Tiedon luovuttaja / Tiedonhakujärjestelmän ylläpitäjä	Tiedon luovuttajalla tarkoitetaan tahoa, jolla on lain mukaan velvollisuus ylläpitää tiedonhakujärjestelmää, jonka avulla tiedon luovuttaja välittää välittömästi ja salassapitosäännösten estämättä voimassa olevassa laissa tarkoitettuja tietoja asiakkaistaan toimivaltaiselle viranomaiselle. Tiedon luovuttajalla tarkoitetaan myös ulkomaisen maksulaitoksen, sähkörahayhteisön, luottolaitoksen ja virtuaalivaluutan tarjoajan Suomessa sijaitsevaa sivuliikettä.
Toimivaltainen viranomainen / Tiedon hyödyntäjä	Pankki- ja maksutilien valvontajärjestelmää koskevassa laissa määritelty toimivaltainen viranomainen ja asianajajayhdistys, jolla on toimivaltaan perustuva tiedonsaantioikeus käsitellä tietoja, jotka on välitetty ylläpidettyjen tiedonhakujärjestelmien avulla.
Ylläpito	Ylläpito viittaa tiedonhakujärjestelmän ylläpidon prosesseihin kuten palvelutason hallintaan, käytön tukeen, häiriöhallintaan, ongelmanselvitykseen, käyttöoikeuksien hallintaan sekä versioiden ja muutosten hallintaan. Näiden osalta vastuu on hajautettu. Tulli vastaa ainoastaan teknisistä vaatimuksista antamallaan määräyksellä.

Dnro
H 1741/01.02.01/2019Tiedonhakujärjestelmän käyttöönoton ja ylläpidon ohje **21.10.2019**

3 Tausta ja kattavuus

Euroopan parlamentin ja neuvoston direktiivin (EU) 2018/843 mukaan jäsenvaltioiden on perustettava keskitettyjä automatisoituja mekanismeja, jotta pankki- ja maksutilien sekä tallelokeroiden haltijat voidaan kansallisesti tunnistaa.

Pankki- ja maksutilien valvontajärjestelmän tarkoituksena on tehostaa viranomaisten tiedonsaantia digitalisoimalla pankki- ja maksutileistä saatavat tiedot sekä tehostamalla viranomaisten tiedustelujen kohdentumista. Nykyisellään tiedonsaanti on manuaalista, ja prosessit ovat kankeita, hitaita ja haastavia. Sähköisen järjestelmän kautta tiedot ovat saatavilla merkittävästi nopeammin kuin manuaalisesti. Sähköiseen tiedonvälitysjärjestelmään siirtyminen lisää yritysten ja kansalaisten tietosuojaa, kun tiedot eivät enää kulje esimerkiksi faksilla. Myös tiedon laadun osalta tavoitteena on saada parannuksia, koska manuaalisessa tiedonkeräämisessä on suurempi virheen mahdollisuus kuin automatisoidussa prosessissa, eli pankki- ja maksutilien valvontajärjestelmän kautta saatava tieto on luotettavampaa ja virheettömämpää.

Suomessa on hyväksytty kansallinen laki pankki- ja maksutilien valvontajärjestelmästä 571/2019. Laissa määritellyn mukaisesti pankki- ja maksutilien valvontajärjestelmä koostuu 1) pankki- ja maksutilirekisteristä (myöhemmin Tilirekisteri) ja 2) hajautetusta tiedonhakujärjestelmästä.

4 Tiedonhakujärjestelmän esittely

Tiedonhakujärjestelmä on tiedon luovuttajan Tullin teknisten määritysten perusteella toteuttama järjestelmä, jonka kyselyrajapinnan kautta toimivaltaiset viranomaiset voivat kysellä pankki- ja maksutilien valvontajärjestelmää koskevassa laissa määriteltyjä tietoja.

Luottolaitoksilla on tiedonhakujärjestelmän ylläpitovelvoite. Maksulaitokset, sähkörahayhteisöt ja virtuaalivaluutan tarjoajat voivat ilmoitusluonteisesti halutessaan ylläpitää tiedonhakujärjestelmää täyttääkseen tiedonantovelvoitteensa. Ilmoitus on tehtävä Tullille, jolloin näiden ilmoitusluonteisesti tiedonhakujärjestelmää yllä pitävien toimijoiden ei tarvitse toimittaa tietoja Tullin ylläpitämään Tilirekisteriin.

Tiedonhakujärjestelmässä tiedon luovuttaja vastaa rekisterinpitäjänä tietojen saatavuudesta ylläpitämällä tiedonhakujärjestelmää ja toimivaltainen viranomainen vastaa rekisterinpitäjänä tiedonhakujärjestelmän avulla käsittelemistään tiedoista. Molemmilla rekisterinpitäjillä on velvollisuus valvoa, että tietoja käsitellään lainmukaisesti. Lisäksi laissa pankki- ja maksutilien valvontajärjestelmästä on säädetty, että toimivaltaisen viranomaisen on ylläpidettävä tiedonhakujärjestelmän käytöstä lokikirjaa, jossa tulee olla laissa määritellyt vähimmäistiedot.

Tulli antaa tiedonhakujärjestelmästä määräyksen ja tukea määräyksen tulkintaan liittyen, mutta Tulli ei vastaa eikä valvo tiedonhakujärjestelmän toteutusta.

4.1 Tiedonhakujärjestelmän tiedot

Tiedonhakujärjestelmän avulla välitetyt tiedot toimivaltaiselle viranomaiselle on määritelty laissa pankki- ja maksutilien valvontajärjestelmästä. Tietojen ajallinen ulottuvuus johdetaan rahanpesun ja terrorismin rahoittamisen estämistä koskevan lain 3 luvun 3 §:stä, jossa on täsmällisesti ja tarkkarajaisesti säädetty asiakkaan tuntemistiedot ja niiden säilyttämisestä. Lisäksi viidennen rahanpesudirektiivin 40 artiklan 1 kohdan b) alakohdan mukaan asiakkaan tuntemistietojen säilyttämisaikaa sovelletaan myös tietoihin, jotka ovat saatavilla 32 a artiklassa tarkoitettujen keskitettyjen mekanismien kautta.

4.1.1 Vastuu tietojen oikeellisuudesta

Rekisterinpitäjällä on suoraan EU tietosuoja-asetuksesta johdettu osoitusvelvollisuus, että henkilötiedot ovat täsmällisiä ja tarvittaessa päivitettyjä; rekisterinpitäjän on toteutettava kaikki mahdolliset kohtuulliset toimenpiteet sen varmistamiseksi, että käsittelyn tarkoituksiin nähden epätarkat ja virheelliset henkilötiedot poistetaan tai oikaistaan viipymättä ("täsmällisyys"); Rekisterinpitäjällä on myös ilmoitusvelvollisuus. Rekisterinpitäjän on ilmoitettava henkilötietojen oikaisusta, poistosta tai käsittelyn rajoituksista jokaiselle vastaanottajalle, jolle henkilötietoja on luovutettu. Pankki- ja maksutilien valvontajärjestelmää koskevan lain mukaan rekisteröidyllä ei ole kuitenkaan oikeutta saada tietää keille viranomaisille tietoja on ehditty luovuttaa. Lisäksi tästä syystä rekisteröidyn oikeuksien turvaamiseksi tulee toimivaltaiselle viranomaiselle myös välittää tieto, mikäli rekisteröity on kiistänyt tietojensa paikkansapitävyyden. Toimivaltaisella viranomaisella on kuitenkin oikeus käyttää henkilötietoja aikana, joka kuuluu tiedon luovuttajan selvittäessä tietojen oikeellisuutta.

4.2 Toimijat ja roolit

Tässä luvussa on esitetty pankki- ja maksutilien valvontajärjestelmän rajapintojen toimijat ja roolit.

Taulukko 1. Pankki- ja maksutilien valvontajärjestelmän rajapintojen toimijat ja roolit

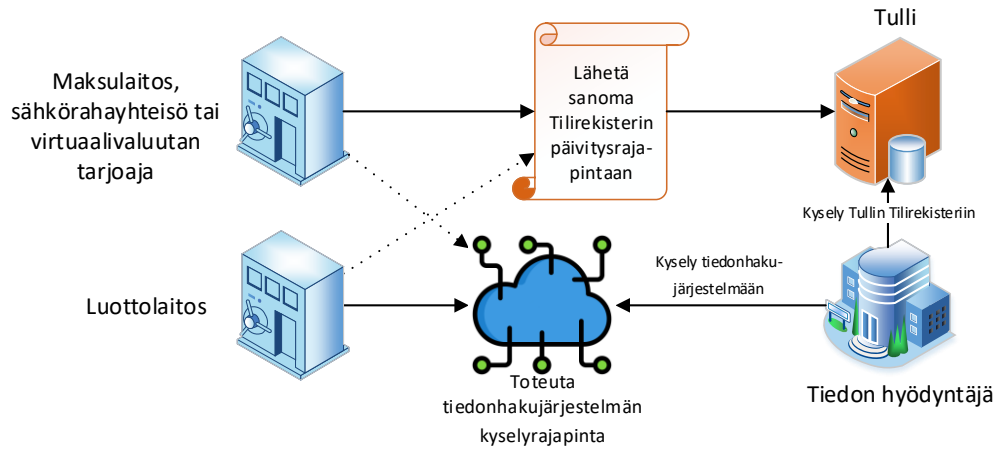
Toimijat	Tiedonhaku- järjestelmän rajapinnan toteuttajat	Tiedonhaku- järjestelmän kyselyrajapinnan hyödyntäjät
Tiedon hyödyntäjä		X
Luottolaitos	A	
Maksulaitos	B	
Sähkörahayhteisö	B	
Virtuaalivaluutan tarjoaja	B	

- X) aina
A) lähtökohtaisesti
B) ilmoituksella

Tiedon hyödyntäjät ovat tiedonhakujärjestelmän kyselyrajapinnan käyttäjiä, joita ovat toimivaltaiset viranomaiset ja asianajajayhdistys. Luottolaitokset ovat lähtökohtaisesti tiedonhakujärjestelmän rajapinnan toteuttajia, mutta luottolaitos voi liittyä Finanssivalvonnan poikkeusluvalla Tilirekisterin tietojen toimittajaksi. Maksulaitokset, sähkörahayhteisöt ja virtuaalivaluutan tarjoajat ovat lähtökohtaisesti Tilirekisterin tietojen toimittajia, mutta voivat ilmoituksella toteuttaa tiedonhakujärjestelmän rajapinnan.

5 Prosessikuvaus

Kuvassa 1 on esitetty käyttötapauskaavio pankki- ja maksutilien valvontajärjestelmän keskeisimmistä liiketoimintaprosesseista.



Kuva 1: Käyttötapauskaavio.

5.1 Liiketoimintaprosessien kulku ja roolit

Tiedonhakujärjestelmän liiketoimintaprosessin tiedon hyödyntäjän ensimmäinen tehtävä on rajapintojen käyttöoikeuden hakeminen rajapinnan toteuttavalta luottolaitokselta tai muulta tiedon luovuttajalta. Käyttöoikeuden hakemisen tarve rooleittain nähdään taulukosta 2.

Tiedon hyödyntäjän on haettava rajapintojen käyttöoikeutta jokaiselta tiedonhakujärjestelmän toteuttajalta erikseen.

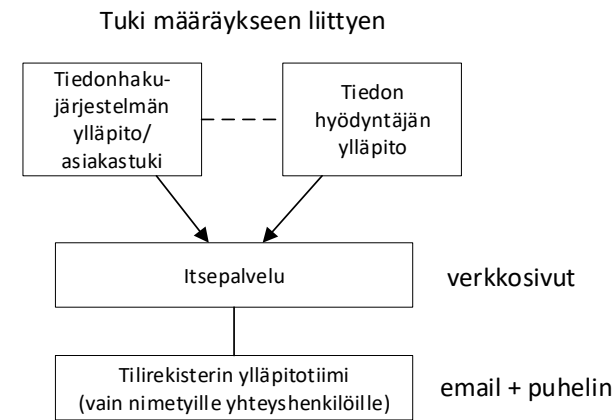
Taulukossa 2 on listattu Tiedonhakujärjestelmän liiketoimintaprosessien prosessiaskleet yleisellä tasolla ja niihin liittyvät roolit.

Taulukko 2. Liiketoimintaprosessin askeleet ja roolit

Prosessiaskel	Roolit
Rajapintojen käyttöoikeuden hakeminen	Tiedon hyödyntäjä
Tiedonhakujärjestelmän kyselyrajapinnan käyttöoikeuden myöntäminen	Tiedonhakujärjestelmän ylläpitäjä/tiedon luovuttaja
Tietojen kysely tiedonhakujärjestelmän kyselyrajapinnasta	Tiedon hyödyntäjä

5.2 Tullin tuki

Tulli tarjoaa tukea tiedonhakujärjestelmien ohjeisiin ja niiden toteuttamiseen, toimintamalleihin ja sisältöön liittyen. Ensimmäinen tukimuoto on Tullin julkaisemat verkkosivut, joissa on julkaistu ohjeita. Tämän lisäksi voidaan ylläpitoon ottaa yhteyttä puhelimen ja sähköpostin avulla arkisin kello 6:30-18:00



Kuva 2. Tullin tuki toimintamalleihin ja sisältöön liittyen

5.3 Tiedon luovuttajat

Tiedonhakujärjestelmässä pankki- ja valvontajärjestelmää koskevassa laissa määritellyt tiedot toimitetaan välittömästi ja salassapitosäännösten estämättä toimivaltaisille viranomaisille ja salassapitosäännösten estämättä tiedonhakujärjestelmän avulla.

5.4 Tiedonhakujärjestelmän kyselyrajapinta

Mikäli tiedon luovuttaja toteuttaa tiedonhakujärjestelmän, tiedon hyödyntäjät voivat tehdä kyselyitä sen avulla. Tiedon luovuttajan on todennettava toimivaltaiset viranomaiset varmenteella jokaisen tietopyynnön yhteydessä (katso luku 6.1).

Tiedonhakujärjestelmän kyselyrajapinnan yleiskuvaus löytyy [rajapintakuvauksesta, luku 4.](#)

5.5 Ilmoitusmenettely

Tulli antaa määräyksen ja ohjeistuksen tiedonhakujärjestelmän kyselyrajapinnan toteuttamisesta. Luottolaitosten tulee ilmoittaa tiedonhakujärjestelmän toteuttamisesta Tullille. Sama käytäntö koskee maksulaitoksia, sähkörahayhteisöjä tai virtuaalivaluutan tarjoajia, jotka ilmoittavat Tullille tekevänsä tiedonhakujärjestelmän. Tulli informoi toimivaltaisille viranomaisille eli tiedon hyödyntäjille tiedonhakujärjestelmän toteuttamisesta.

Jos luottolaitos on Finanssivalvonnan poikkeusluvalla liittynyt Tilirekisteriin, voi se myöhemmin toteuttaa tiedonhakujärjestelmän ja siirtyä käyttämään sitä. Kun luottolaitos ilmoittaa päätöksestä Tulliin, Tulli lähettää tiedonhakujärjestelmän kyselyrajapintaa koskevan määräyksen ja ohjeistuksen, jonka avulla luottolaitos voi toteuttaa tiedonhakujärjestelmän. Kun luottolaitos ilmoittaa tiedonhakujärjestelmän kyselyrajapinnan olevan valmis ja testattu, Tulli sulkee luottolaitoksen päivitysrajapinnan Tilirekisteriin. Sama menettely koskee maksulaitoksia, sähkörahayhteisöjä ja virtuaalivaluutan tarjoajia, jotka ovat jo ottaneet Tilirekisterin käyttöön ja ilmoittavat myöhemmin toteuttavansa tiedonhakujärjestelmän.

5.6 Tiedon luovuttamisen rajapintojen testaus

Integraatio jokaiseen tiedon luovuttajaan testataan erikseen.

Tulli toteuttaa API-kyselyn, jolla tietoja voidaan kysellä tiedon luovuttajilta. Testauksessa on tarkoitus varmistaa ainakin kaikkien niiden tietotyyppien toimivuus, joita kyseinen tiedon luovuttaja tulee tuotannossa lähettämään tiedonhakupöytäkirjaan. Tiedonhakupöytäkirjan rajapinnan toiminta testataan lähettämällä Tullin asiakasympäristössä API-kyselyitä tiedon luovuttajien järjestelmiin ja verifioidulla saadut vastaukset.

6 Tietoturva

Tiedonhakupöytäkirjan tietoturva perustuu tiedonsiirtoyhteyksien suojaamiseen TLS-salauksella. Järjestelmän tiedon luovuttajat ja tiedon hyödyntäjät tunnistavat toisensa palvelinvarmenteiden avulla. Lisäksi määrämuotoinen sanomaliikenne on allekirjoitettu digitaalisesti.

Tiedonhakupöytäkirjan yhteydet tulee olla suojattu TLS-salauksella käyttäen TLS-protokollan versiota 1.2 tai korkeampaa. Yhteyden molemmat päät tunnistetaan palvelinvarmenteilla käyttäen kaksisuuntaista kättelyä (mutual TLS authentication). Palvelinvarmenteiden vaatimukset on kuvattu luvussa 6.1.

Sanomien sisältö tulee olla allekirjoitettu SOAP XML -tietueina allekirjoitusvarmenteiden avulla. Allekirjoitusvarmenteet on kuvattu tarkemmin luvussa 6.1.

6.1 Vaatimukset varmenteille

Tiedonhakupöytäkirjan ulkoiset yhteydet suojataan varmenteilla. Tiedonhakupöytäkirjan tiedon luovuttajan ja tiedon hyödyntäjän tulee hankkia varmennevaatimukset täyttävä palvelin- ja järjestelmäallekirjoitusvarmenteet ja asentaa ne järjestelmään. Sanomien allekirjoitukseen tarvitaan lisäksi allekirjoitusvarmenne. Teknisesti sama varmenne voi toimia sekä palvelin- että allekirjoitusvarmenteena tai varmenteet voivat olla erillisiä. Tyypillisesti palvelinvarmenne asennetaan tietoliikennesyhteyskäyttöön edustapalvelimeen ja allekirjoitusvarmenne vastaukset muodostavaan taustapalvelimeen.

Varmenteet hakee se taho, joka muodostaa ja välittää vastaukset tiedon hyödyntäjien kyselyihin. Jos tiedon luovuttaja itse tekee nämä vaiheet, varmenne haetaan tiedon luovuttajalle. Jos käytetään palveluntarjoajaa, joka muodostaa ja välittää sanomat ilmoitusvelvollisen puolesta, palvelinvarmennetta hakee palveluntarjoaja. Tällöin ilmoitusvelvollisen tulee valtuuttaa palveluntarjoaja allekirjoittamaan lähetettävät sanomat.

6.2 Varmenteiden uusiminen ja kustannukset

Varmenne tulee uusida hyvissä ajoin ennen sen vanhenemista. Vanhentunutta varmennetta ei voi käyttää. Ellei osapuolten välillä ole toisin sovittu, tietojen luovuttajan tulee ilmoittaa toimivaltaiselle viranomaiselle varmenteensa uusimisesta vähintään kuukautta ennen sen käyttöönottoa ja toimittaa kopio varmenteesta.

Myös toimivaltaisten viranomaisten eli tiedon hyödyntäjien on uusittava omat varmenteensa varmennetoimittajan kanssa säännöllisin välein. Siitä ei erikseen ilmoiteta ilmoitusvelvollisille tiedon luovuttajille, koska oletetaan, että tiedon luovuttaja tarkistaa toimivaltaisen viranomaisen varmenteiden hyväksytyjen varmentajien listaa vasten. Toimivaltaisten viranomaisten varmenteiden voimassaolon voi tarkistaa VRK:n varmennehakemistosta.

Pankki- ja maksutilien valvontajärjestelmistä annetun lain 4 § 3 momentin sekä 8 §:n mukaan toimivaltaisella viranomaisella on oikeus saada tiedot maksuttomasti, ja näin ollen tiedon luovuttaja vastaa käyttämänsä varmenteen kustannuksista.

Dnro
H 1741/01.02.01/2019Tiedonhakupöytäkirjan käyttöönoton ja ylläpidon ohje **21.10.2019****7 Palvelutaso**

Toimivaltaisten viranomaisten kyselyvastaus on oltava noudettavissa "välittömästi" ja "suodattamatta".

Tiedonhakupöytäkirjan kyselyrajapinta tulisi olla saatavilla 24/7, mutta saatavuusvaatimus on 99,5 % ajasta kello 07:00-22:00. Saatavuusvaatimuksen toteutuminen lasketaan keskiarvona kalenterikuukausittain.