LIETUVOS BANKAS
EUROSISTEMA

Feasibility study on the use of the account information service in optimising the provision of electronic money and payment institution data for supervisory services

Analysis and Research

No 1 / 2021

Series "Analysis and Research"
No 1 / 2021

ISSN 2783-5944 (ONLINE)

Feasibility study on the use of the account information service in optimising the provision of electronic money and payment institution data for supervisory services

Dovilė Meškauskė

Gedimino pr. 6, LT-01103 Vilnius, Lithuania
www.lb.lt

CONTENTS

ABBREVIATIONS AND DEFINITIONS

API	Application Programming Interface
AUTH, or authentication	procedure applied by a credit institution to verify the client's identity
Directive, or PSD2	Directive (EU) 2015/2366 of the European Parliament and of the Council
EBA	European Banking Authority
EMI	electronic money institution
FMP	financial market participant
FMSS	Bank of Lithuania Financial Market Supervision Service
client	natural or legal person
LD	Bank of Lithuania Financial Market Supervision Service Licencing Department
PI	payment institution
PSP	payment service provider
PMSD	Bank of Lithuania Financial Market Supervision Service Payments Market Supervision Division
Personalised security Credentials	data used for authentication purposes the use whereof is agreed upon by PSP and client
AMLD	Bank of Lithuania Financial Market Supervision Service Anti-Money Laundering Division
RTS	Commission Delegated Regulation (EU) 2018/389
SCA	AUTH based on two or more elements which are categorised as knowledge, possession and inherence
AIS	account information service
AISP	account information service provider

SUMMARY

The main objective of this feasibility study is to analyse an opportunity of implementing the optimisation of data management for supervisory purposes by means of the AIS service in observing the compliance of EMI and PI with the requirements for safeguarding client funds.

As part of the drawing up of the study, the existing supervisory process of safeguarding of client funds which is currently applied by FMSS PMSD was analysed, the AIS service with respect to the AIS provider was described, the survey of the credit institutions and AISPs was conducted, legal and IT feasibilities were assessed and conclusions were provided.

Having performed the feasibility study, it was established that:

1) the use of the AIS service to receive the supervisory information on client funds held by EMIs and PIs would be one of the possibilities to optimise the supervisory work of FMSS;
2) integration of AIS service could be implemented in the short and long term: (a) in the short run, AIS service would ensure the provision of balances of EMI and PI client fund accounts and it could be achieved by means of minimum time limits and financial costs; (b) in the long run, AIS service would help access all information on the account which could be consolidated, processed and applied a cross-cutting analysis to be used for the achievement of the supervisory goals. To implement one of the AIS service integrations referred to herein, the Bank of Lithuania would need to allocate additional financing sources and human resources by involving other FMSS divisions as well;
3) If the AIS service, for the purpose of receiving supervisory information, were used in such a way where the EMIs and PIs preserved the option for the Bank of Lithuania to provide relevant information through AISPs and EMIs and PIs were allowed choosing AISPs on their own, the changes in the current legal regulation would not be necessary;
4) Consolidated information received from EMIs and PIs through AISPs could be currently stored and held in the existing information acceptance systems of the Bank of Lithuania;
5) At the moment, when AIS service is used, FMSS has only limited possibilities to receive information on client funds held with EMIs and PIs on the accounts designed to safeguard client funds as the accounts of safeguarding of client funds in almost all credit institutions are not accessed via PSD2 API interfaces only because they are not classified as the payment accounts;
6) Currently, credit institutions are investing and creating premium API interfaces on the market used for the AISPs to receive relevant information for an additional fee. It is estimated that such Premium API interfaces will emerge on the market in the second half of 2021;
7) This feasibility study may be continued having updated and supplemented information and having formed a joint working group from several divisions of FMSS. For this purpose, additional actions are suggested: (a) submit a question to the EBA Q&A and request that it drafts an explanation as to whether the accounts of safeguarding of client funds should be treated as the payment accounts and be accessed via PSD2 API interfaces; (b) monitor the changes undergoing on the market; (c) develop the position of the Bank of Lithuania or interpretation for FMPs based on the response received from the EBA so that they know exactly which accounts should be accessed via PSD2 API interfaces.

This feasibility study presents the conclusions and recommendations on further actions of the Bank of Lithuania to ensure that both the Bank of Lithuania and FMPs are properly prepared for the application of the AIS service so that data needed for supervision are received, processed and analysed.

INTRODUCTION

The Bank of Lithuania FMSS, as part of its prudential supervision of EMIs and PIs and analysis of the operating practice of these institutions, observed the growing number of cases where EMIs and PIs did not comply with the requirements regarding the safeguarding of client funds set out in Article 25 of the Republic of Lithuania Law on Electronic Money and Electronic Money Institutions and Article 17 of the Republic of Lithuania Law on Payment Institutions. The Republic of Lithuania Law on Electronic Money and Electronic Money Institutions and Republic of Lithuania Law on Payment Institutions establish that EMIs and PIs must safeguard client funds by one of the following means: separate these funds from the funds of other natural or legal persons which are not electronic money holders or payment service users or insure these funds by an insurance contract, or obtain a guarantee or warrantee letter for such funds. The information presented in the annual reports of EMIs and PIs for 2019 shows that almost all EMIs and PIs which are subject to the obligation to safeguard client funds have opted for the funds separation method, therefore, FMSS focuses on the analysis of this method when carrying out the prudential supervision of EMIs and PIs.

Currently, the FMSS division in charge refers to the financial quarterly statements provided by EMIs and PIs and/or organises scheduled and unscheduled inspections of the documents to verify if EMIs and PIs comply with the requirements for safeguard of client funds set out in the law. During the inspections of the documents for the compliance with the requirements for safeguarding of client funds performed in 2019, the sanctions for the improper safeguarding of funds were imposed on 6 (six) EMIs and PIs, and by the end of 2020 such sanctions were imposed on 4 (four) EMIs and PIs. Practical evidence shows that EMIs and PIs generally pay their attention and start complying with the requirement laid down in the law only where the FMSS division in charge carried out the inspection and imposes a sanction for improperly held client funds and for incorrect information provided in the quarterly financial statements.

The more intense activities of EMIs and PIs enhance digital literacy of the payment market participants but they also create a favourable environment for both intentional and accidental unfair actions; therefore, to ensure that the EMI and PI supervisory process is more effective and taking account of the directions clearly defined by PSD2 and aim to focus on a payment market which operates in an electronic environment in a sustainable and fair manner, the Bank of Lithuania developed this feasibility study to enable closer monitoring and control of the compliance with the requirements for the assurance of the quality of payment services by means of digital technologies given the constantly changing economic situation, technological progress and increasing number of EMIs and PIs.

AIS service, feasibilities of its application and implementation by adapting it for the supervisory purposes were analysed when drafting the feasibility study.

1. EXISTING SUPERVISORY PROCESS FOR SAFEGUARDING CLIENT FUNDS

One of the essential prudential requirements applied to EMIs and PIs they must comply with is the adequate safeguarding of client funds. The Bank of Lithuania refers to relevant legal acts of the Republic of Lithuania and European Union in its supervision of how the EMIs and PIs comply with the requirements for safeguarding of client funds.

Pursuant to Article 10(1) of the Republic of Lithuania Law on Electronic Money and Electronic Money Institutions, EMIs have the right to issue electronic money and provide payment services. Taking account of the fact that electronic money is held in electronic media, electronic money can be held in the payment account opened by EMIs until its maturity but is can also be used to make payments. It is a slightly different case with PIs. Funds may be debited into the payment account opened by PIs to make specific payments only and they cannot stay in the PIs payment account longer than necessary for operational and technical circumstances related to the specific payment services. PIs can accept funds only with the payment order which must be executed following the terms set out in the Republic of Lithuania Law on Payments and it must take sufficient measures which ensure that the funds flowed in the payment account of the PI client from the third parties are not kept longer than necessary to make payments.

Pursuant to Article 25 of the Republic of Lithuania Law on Electronic Money and Electronic Money Institutions and Article 17 of the Republic of Lithuania Law on Payment Institutions, EMIs and PIs must hold client funds separately from the funds of other natural or legal persons which are not payment service users. If this requirement is not met, FMSS may impose the sanctions established in Article 40(1)(1) of the Republic of Lithuania Law on Electronic Money and Electronic Money Institutions and Article 34(1)(1) of the Republic of Lithuania Law on Payment Institutions. By means of these paragraphs, the legislator ensured the safeguarding of clients' interests and their funds, i. e. it entrenched the rule for immunity of client funds – such funds shall be considered the property of the clients and no execution may be levied according to arrears of the payment service provider.

As mentioned above, EMIs and PIs must safeguard client funds by separating them from the funds of other natural or legal persons which are not payment service users. One of such safeguarding means established in Article 25(1)(1) of the Republic of Lithuania Law on Electronic Money and Electronic Money Institutions and Article 17 (1)(1) of the Republic of Lithuania Law on Payment Institutions is holding client funds in different accounts in a credit institution of the Republic of Lithuania (including a branch of a foreign credit institution established in the Republic of Lithuania), a credit institution of another Member State, Bank of Lithuania or central bank of another Member State.

Currently, the FMSS PMSD of the Bank of Lithuania responsible for the supervision of the EMI and PI sector usually conducts the documentary supervision (analysis) to verify where EMIs and PIs hold the client funds and analyses the data submitted in the quarterly financial statements as well as additional information received from EMIs and PIs: account extracts, agreements, etc.

The developments in technologies and emergence of new services on the market as well as digitalisation opportunities would potentially make the use of the AIS service to receive the supervisory information on client funds held by EMIs and PIs one of the possibilities to optimise the supervisory work of FMSS. The study is therefore designed to learn if the AIS service may be applied in daily activities of FMSS and if, when it is relied on, it is possible to find out where (which credit institutions or other financial institutions) EMIs and PIs hold client funds and which amounts prior to submission of quarterly financial statements by EMIs and PIs to the Bank of Lithuania. Thus, FMSS PMSD would be able to always manage supervisory information on how EMIs and PIs comply with the requirement provided for in the law. Moreover, this would encourage EMIs and PIs to always comply with the requirement for adequate safeguarding of client funds laid down in the law.

2. DESCRIPTION OF AIS PROCESS WITH RESPECT TO AIS PROVIDER

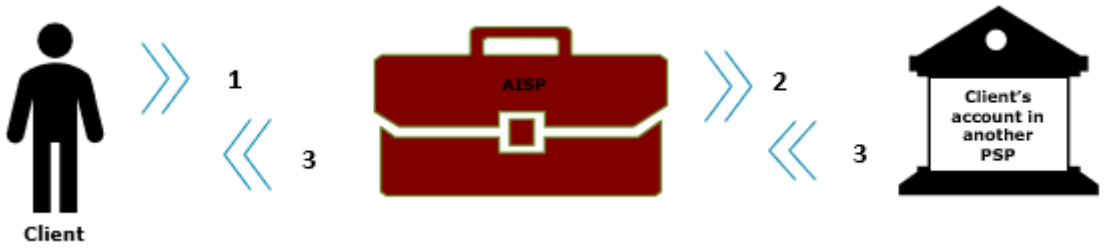
2.1. AIS SERVICE PROCESS

According to the provisions of the Directive which entered into force on 13 January 2018, all financial institutions offering a solution of a dedicated API shall be available to PSPs as of 14 September 2019 already, and here the AISPs, in the context of the Directive, emerge to exploit the potential of the open banking API integration in one of the payment services, such as the provision of the AIS service.

The Directive defines the AIS service as an online service to provide consolidated information on one or more payment accounts held by the payment service user with either another PSP or with more than one PSPs, whereas AISP is a payment service provider providing the AIS service.

The AIS service is a data service only. In their systems, AISPs accumulate the collected client's account information in different credit institutions and submit it in a user-friendly form by enabling the client to track the balance in one place, see the history of expenses and information on performed transactions. It is worth mentioning that a classic description of the AIS service provided in the Directive slightly differs in comparison with the models of the provision of the AIS service existent on the market and in light of trends in the market. The AIS service can be provided on the market to assess creditworthiness, for example, where a client can fail to see consolidated information as it is immediately provided to a third party; therefore, it may be stated that this standard (classic) AIS service described in the Directive is rarely observed on the market. However, although the market has various modifications of the AIS service, it is important to note that the AIS service may be provided only upon the client's consent which is equivalent to an agreement; thus, no other additional agreements are directly concluded with the client in case the AIS service is provided. The AIS service is provided through the account servicing PSP, where the AISP connects to the client's payment account and downloads relevant data. This information may be received only with the client's consent for the provision of such data. Nevertheless, the main source is the data, and the data create the channel 'Accounts – AISP – Recipient' (see Chart 1).

Chart 1. AIS service



The client requests (1) the AISP to collect specific information from his payment accounts in another PSP; the client also authorises the AISP to connect to the payment accounts that he specified through the API interface (2). The AISP collects information and submits it to the client in a user-friendly form (3). The received account information is encrypted and used to provide a one-off AIS service during one session.

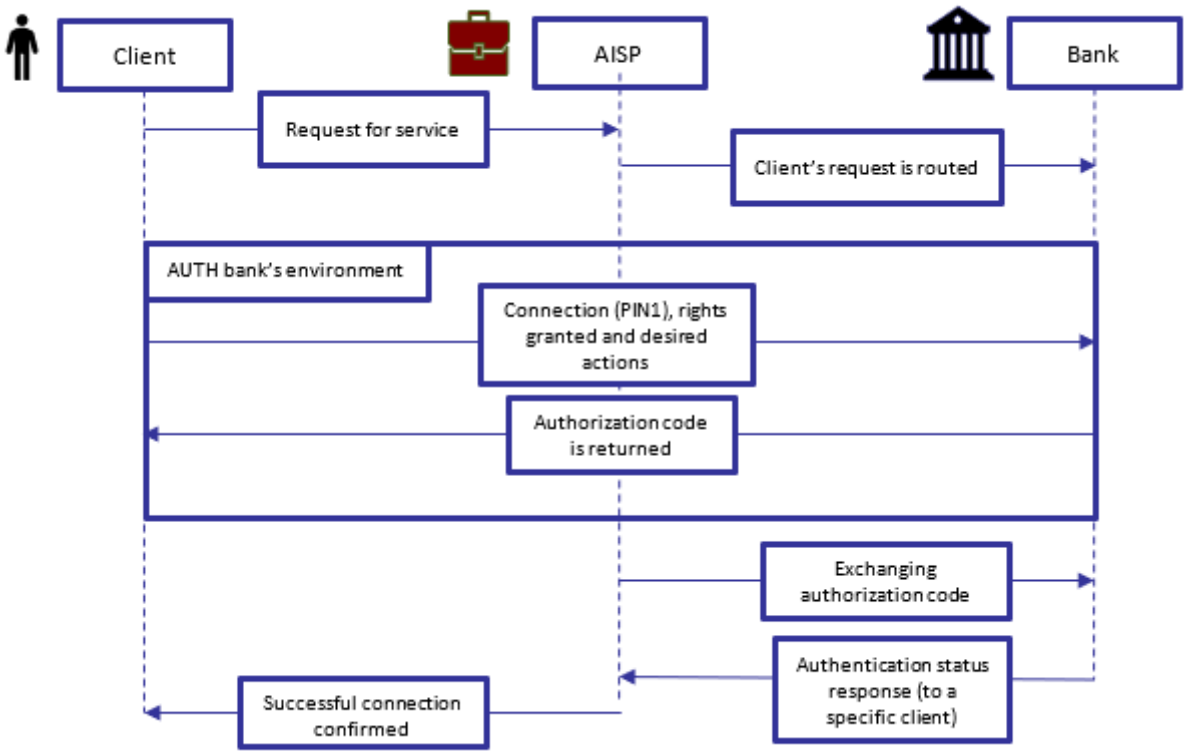
Stages of the provision of the AIS service:

1) the client wishing to access the AISP website must connect (or be routed) through the account servicing PSP which will provide the account information to the AISP in the future, through the AISP partner or connect directly through the AISP website;
2) the client agrees with the terms and conditions for the provision of services by the AISP and gives a consent that this acceptance is necessary;

3) the client is usually not requested to create a personal account but there are cases where that personal account is necessary and the client creates such an account;
4) the client specifies which information may be accessed by the AISP (time limit, scope and level of detail);
5) AISPs access the client's account information through the interface of account servicing PSPs based on requirements set out in Commission Delegated Regulation 2018/389 with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication;
6) the client is authenticated though personalised security credentials provided to the client by the account servicing PSP;
7) AISPs submit an inquiry to account servicing PSPs based on the information defined by the client and download that information;
8) AISPs summarise and process information collected by account servicing PSPs (e.g. name and surname, payment account number, balances of account and list of payment orders) so that this information could be easily and comprehensively provided or made available to the client (e.g. information is provided on a dedicated website and/or in a mobile application by forwarding data by email, or it is formatted to be downloaded in a separate file. The data may be provided in a *csv* file by sending it to the client's email during the AIS process;
9) at the client's request, consolidated information may be provided by AISPs to the AISP partner through which the client connected to the AISP (this functionality is not required but it is used in some versions of the provision of the AIS service. It depends on the models of the AISP operation);
10) where access and submission of information expires or desired information is received, AISPs no longer have access to the payment account or another source; also, they generally do not store that information unless the client decides otherwise (it must be noted that the Republic of Lithuania Law on Payments entitles the AISPs to store client's data for 3 (three) years).

The entire process described above is generally based on the microservice infrastructure, i. e. it is divided into small independent logical increments (see Chart 2) and lasts for several dozens of seconds. Each logical increment plays its role and is responsible for an individual part of overall functionality. All services provided mutually communicate through HTTPS protocols and have a secure communication. Each service has its own database and login data. The system identifies the customer by means of a validation function. Authorisation and authentication of third parties take place through API of the credit institutions based on the standards of the Directive, and OAUTH2 used means that it is only the client who may establish the rights and actions to be taken with a specific payment account in a credit institution. Based on the requirements of Commission Delegated Regulation 2018/389, the client must update the given consent every 90 days. By updating the consent, the client may opt for granting the same rights or he may change them and specify the rights other than the ones specified before. AISPs send the request to the credit institution and the credit institution sends the reply. Clients are provided with several options of self-identification and authorisation of enquiries: they can use *SmartID*, *MobileID* or other qualified identification methods compliant with the requirements. Each action related to the payment account must be confirmed by the client.

Chart 2. Stages of the provision of AIS service



When undergoing the stages of the provision of the AIS service, AISPs shall ensure the following:

1) the service is provided only with an explicit consent of the client;
2) the client's personalised security credentials, except for the client and issuer of personalised security credentials, are accessed by other parties and AISPs transfer such credentials through secure channels;
3) during each login session, the client identifies himself and securely connects to the account servicing PSP, as provided for in Article 98(1)(d) of the Directive (identification, authentication, notification, and information);
4) access is granted only to payment accounts indicated by the client and to related information on payment transactions;
5) sensitive information related to the client's payment accounts is not published;
6) data which are not related to the client's payment account are not used and/or stored.

Some models of AISP operation have the feature where the AIS service provided by AISPs may be integrated in a mobile application and/or website of the AISP partner which may operate both in Lithuania and in other EU and EEA Member States. In that case, to protect the interests of the AIS service clients, the clients registered with the AISP partner's system must be informed that the AIS service provided by AISPs is used in this system.

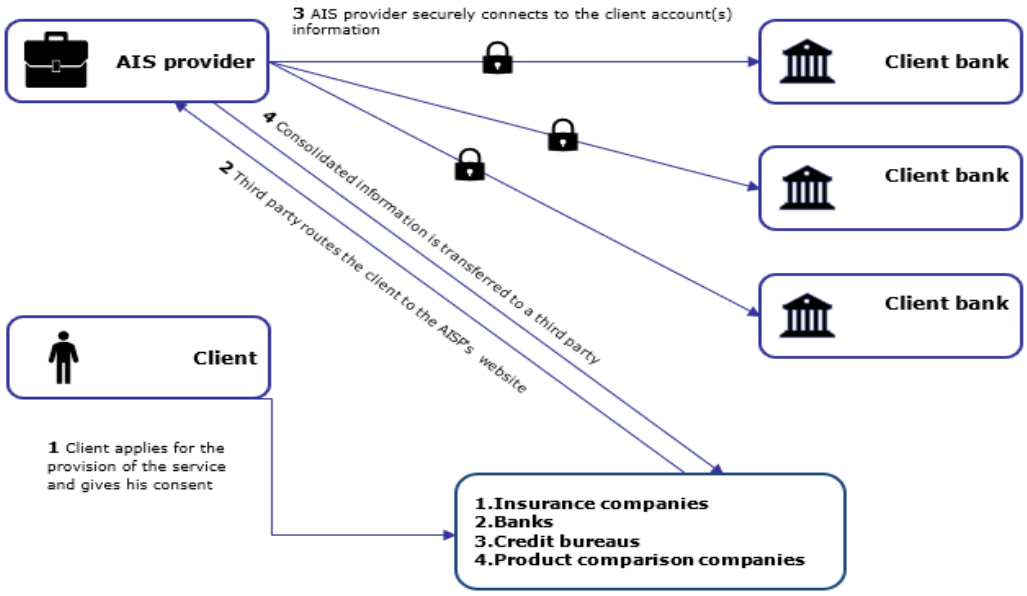
AISP partners are usually the credit institutions of various countries or companies providing other services (e. g. insurance, credit, etc.) which have the functionality of the AIS service provided by AISPs integrated in their mobile applications and/or website. AISP partners are usually unable to access the clients' financial information or see it but that information may be provided to the AISP partner with an individual consent of the client. AISPs are obliged to ensure the receipt of all necessary consents from the clients based on the requirements of legal acts prior to transferring client's data to the third parties wishing to receive information

through the AIS service. It is important to note that this service is provided only to the registered clients under the AIS agreement concluded with the client. The client needs to accept the terms and conditions for the provision of the AIS service provided by AISPs to see information on his financial situation in the AISP partner's mobile application and/or on the website. The consent field must additionally contain information on the service provider as well. The client may link his account with the payment accounts by giving his consent to connect to his account servicing PSP where he has the payment account. On the basis of said consent, AISPs now connect to the client's payment account in the name of the AISP.

The AIS service enables the client to see various content in a mobile application and/or on the website and it generally looks like this: (i) payment history analysis is shown (categorization by income and expenses), for example, expenses by types: leisure, utility services, food, etc.; (ii) functionality of recognition of fixed costs is installed (client's fixed costs under the client's payment history); (iii) balance of account is shown (mapping of the client's account balance history based on accounts in all credit institutions); (iv) free space is calculation – information on the amount still to be spent by the client. It is calculated by evaluating the client's projected costs.

As the AIS service is becoming increasingly popular, both newly established and already operating EMIs and PIs offer diverse versions of this service (see Chart 3).

Chart 3. Versions of the use of AIS service



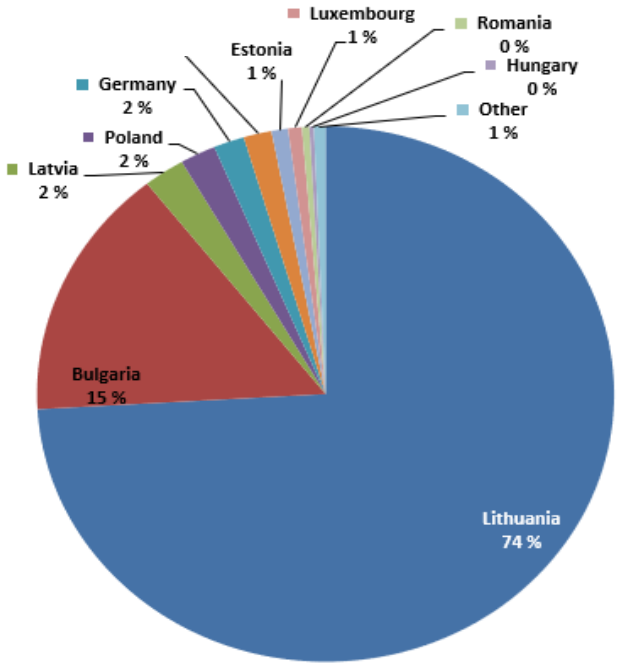
2.2. COMPARISON OF AIS SERVICE FUNCTIONALITY WITH THE THEORETICAL AIS SERVICE PROCESS

The statements provided by EMIs and PIs to the Bank of Lithuania (*data of Q2 of 2020*) showed that EMIs and PIs hold most of client funds with the credit institutions in Lithuania[1], Bulgaria, Latvia, Germany and Poland (see Chart 4); it was therefore of high importance to clarify whether the accounts for holding EMIs and PIs' client funds were accessible via PSD2 API when using the AIS service and thus make sure if the theoretical

[1] According to the data provided by EMIs and PIs, most accounts for holding client funds in Lithuania were opened with the Bank of Lithuania (around 40%).

process of AIS service described in Chapter 2.1 would work in practice as well by relying on the AIS service process analysed in the feasibility study. For this purpose, six banks and two credit unions operating in Lithuania were surveyed.

Chart 4. Amount of client funds held by EMIs and PIs in credit institutions by countries, data of Q2 of 2020



The credit institutions were asked if the information of such accounts, which are also called safeguarding accounts, (outstanding funds, extract of the account, transactions made, etc.) was accessible via PSD2 API interfaces. As many as six respondent credit institutions out of eight specified that those accounts and information contained therein were not accessible via PSD2 API interfaces and mentioned the main reason for that – such accounts are not classified as payment accounts in credit institutions. There were only two credit institutions which mentioned that such accounts held in them could be accessible via PSD2 API interface. It must be noted that the credit institutions establish the classification of accounts by themselves.

Since EMIs and PIs hold client funds not only in the accounts in the credit institutions operating in Lithuania, but also in the credit institutions operating in other European countries, the decision was made to select three AISPs and survey them with regard to the opportunity to access such accounts. Three AISPs were selected for the survey by selecting them with a view to geography of the provision of the AIS service and number of API integrations with the credit institutions.

It must be noted that AISPs were surveyed individually and the surveys were conducted by phone or by means of *Microsoft Teams* application. As the survey was conducted orally and all three respondents provided almost identical answers (it was only the name of the countries that differed), the summarised answers of AISPs are provided below without distinguishing the name of a specific AISP and by presenting the information as a joint answer of all AISPs.

Firstly, AISPs mentioned that current accessibility of the accounts other than payment accounts via PSD2 API interfaces was very limited and only some credit institutions established in Germany, Nordic countries and Poland were granting access to trust accounts or safeguarding accounts via PSD2 API, but they are scarce. It would seem that the purpose of the accounts is 'verbal' only and that the main difference between them is

how they are called but AISPs confirmed that the accounts do differ with respect to technology where it comes to the very structure of the account, therefore, an individual integration process would be necessary to distinguish and map them via API interface.

AISPs mentioned that their clients, to order AIS services from them, were more frequently requesting both information from the payment accounts and information from pension funds, loans or savings accounts, but it was not so easy to receive such data from the credit institutions. The reason for this is very simple – according to the Directive, the credit institutions are obliged to provide AISPs with information on the client's payment accounts only free of charge, therefore, should AISPs wish to receive information from other accounts of the client as well, given the client's consent, that service could be provided only for a fee. Both credit institutions and AISPs, during the survey, claimed that the demand for such services was observed on the market, therefore the credit institutions were currently making additional investments and creating Premium API interfaces for the AISPs to receive relevant information for an additional fee. None of the respondent AISPs has come across the paid version of API interface yet, therefore, there were no broader discussions on this topic; it was only mentioned that such Premium API interfaces should emerge on the market at the end of 2021. All AISPs mentioned that they would not have technological difficulties in terms of integration of Premium API interface and this would take 1 to 5 days depending on the technical specification, country and other aspects. AISPs indicated that to access client fund safeguarding accounts via Premium API by means of the AIS service this discussion should be elaborated one or two years later, but they assured that the provision of this service would be really feasible in the future; they, however, were unable to specify the price of the service or its availability, or prospects offered.

The summary of the replies of AISPs and credit institutions leads to the conclusion that the main reason for accessibility of accounts via PSD2 API interfaces is a different treatment of the definition of the account which has the attributes (functionality) of the payment account.

Both the Directive and Republic of Lithuania Law on Payments present a clear definition of the payment account. Payment account shall mean an account opened in the name of one or several payment service users, used to execute payment transactions but the Directive does not cover, in essence, the opening of the payment account and its functionality. The position of the Supervision Service of the Bank of Lithuania with respect to funds held in payment accounts of 29 February 2016[2] notes that the definition of the payment account is particularly wide to cover any payment accounts from and to which payment transactions can be executed. Although account opened for payment service users of different PSPs are generally defined as payment account and payment transactions executed from payment accounts are applied the provisions of the Republic of Lithuania Law on Payments, the functionality of payment accounts opened by different PSPs is not uniform as it is established in legal acts governing the activities of those entities. The position of the Bank of Lithuania on the right of electronic money institutions and payment institutions to access bank accounts opened with credit institutions of 25 May 2020[3] (hereinafter – the Position) notes that the Directive establishes the supervisory requirements for the separation and holding of funds of clients of EMIs and PIs. These requirements have been transposed into Article 17 of the Republic of Lithuania Law on Payment Institutions and Article 25 of the Republic of Lithuania Law on Electronic Money and Electronic Money Institutions accordingly, therefore, EMIs and PIs, alongside other natural and legal persons, are entitled to hold bank accounts for other purposes which are not related to the provision of financial services to the clients of EMIs and PIs, and use other services related to the bank account. The position distinguishes three types of bank accounts based on the purpose of the bank accounts, nature and other characteristics: settlement account of EMIs and PIs, account for safeguarding EMIs and PIs' client funds and bank account to make payments of the clients of EMIs and PIs. The bank account designed to safeguard EMIs and PIs' client funds

[2] https://www.lb.lt/uploads/documents/docs/550_d022323c305ae8e090e763fa8d814094.pdf.

[3] https://www.lb.lt/uploads/documents/docs/25732_b7ae2d861350055f0d4250654f8c0a87.docx.

relevant for the purpose of this feasibility study is defined as a bank account (including the account opened under the deposit agreement, except for fixed-term irrevocable deposits) used exceptionally for safeguarding of EMIs and PIs' client funds only, if EMIs and PIs, having received client funds, still have such funds at the end of the working day. EMIs and PIs holding those accounts should at least be ensured a possibility of returning client funds (or part thereof) to the same payment account held by EMIs and PIs designed to make clients' payments that the funds were transferred from, or to another account opened in the name of EMIs and PIs and agreed upon with the credit institution. The agreement concluded with the credit institution may provide that this bank account cannot be used to make payments on behalf and/or for the benefit of the clients of EMIs and PIs, including payments to and/or from third parties (except for cases, where the account for safeguarding of EMI and PI client funds is also a bank account designed to make payments of EMI and PI clients).

To sum up the positions of the Bank of Lithuania mentioned above, it is to be concluded that the accounts for safeguarding EMI and PI client funds would not be considered as the payment accounts only where the agreements concluded with the credit institutions do not establish that such bank accounts may not be used to make payments on behalf of and/or for the benefit of EMI and PI clients, including payments to and/or from third parties. If the agreement established that the accounts for safeguarding of EMI and PI client funds were also the payment accounts to make payments of EMI and PI clients, they would be treated as the payment accounts and should be accessed via PSD2 API interfaces.

An individual position or interpretation of the Bank of Lithuania should be drafted for the credit institutions to know exactly which accounts must be accessed via PSD2 API interfaces. This position or interpretation, however, would only affect the credit institutions operating in Lithuania, whereas it would make no impact on credit institutions operating in other Member States; therefore, this question should be addressed to EBA Q&A at first.

2.2.1. LEGAL AND IT EVALUATION

Article 42(4)(2) of the Republic of Lithuania Law on the Bank of Lithuania establishes the right of the Bank of Lithuania to receive the documents, copies thereof, other data and information from public institutions and registers, supervised financial market participants, other natural and legal persons for the supervisory purposes free of charge. According to Article 42(5) of the Republic of Lithuania Law on the Bank of Lithuania, the Bank of Lithuania may receive said information and data directly, in cooperation with other institutions, with the assistance of other persons and with the assistance of law enforcement bodies.

Based on said provisions of the Republic of Lithuania Law on the Bank of Lithuania, it must be concluded that there are no obstacles in receiving supervisory information through AISPs as the technical solutions are not defined in the law. It must be noted that in the case at issue it would be EMIs and PIs, where the information of accounts opened in the name whereof is collected and serviced during the provision of AIS, that would be the AIS service users instead of the Bank of Lithuania itself. The Bank of Lithuania, in this case, would be a third party which would be provided with the relevant information through AISP by EMIs and PIs under an individual consent. The Bank of Lithuania would not take part in the relationships between EMIs and PIs – it would only serve as a recipient of information. The Bank of Lithuania, having received consolidated information from EMIs and PIs through AISPs, could store and hold it in the existing information acceptance systems of the Bank of Lithuania. Sensitive information stored in the system would be protected based on the security requirements of the Bank of Lithuania. It would also enable other FMSS divisions concerned to access that information within their competence and/or use information received in the EMI and PI risk management model.

If the AIS service, for the purpose of receiving supervisory information, were used in such a way where the EMIs and PIs preserved the option for the Bank of Lithuania to provide relevant information through AISPs

and EMIs and PIs were allowed choosing AISPs on their own, the changes in the current legal regulation would not be necessary due to that method of submission of information. EMIs and PIs could give their consent or authorise AISPs to transfer information to the Bank of Lithuania on behalf of EMIs and PIs. In this case, the responsibility for the correctness of information transferred to the Bank of Lithuania would further remain with EMIs and PIs themselves (they would need to ensure that AISP transfers information to the Bank of Lithuania following the terms and conditions laid down in legal acts). The Bank of Lithuania would not take part in the relationships between EMIs and PIs – it would only serve as a recipient of information, therefore, it would not assume additional liability with respect to EMIs and PIs, accordingly.

Other financial risks could be related to personal data protection and information protection risk, since if the Bank of Lithuania managed more information, it should apply higher standards and more secure measures for its protection and this would give rise to higher costs of the service acquisition.

As mentioned above, the AIS service market is not currently extensively developed; it is therefore difficult to forecast the level and depth and, most importantly, timing of such services which could be offered by AISPs to the customers. The rapid development of the open banking market, however, gives a great significance to the AIS service potential in this context. Based on the information collected in this feasibility study, it may be concluded that the use of AIS service would create additional alternatives in the activities of FMSS as well, i. e. receipt of supervisory information would be facilitated, and optimisation and digitalisation of FMSS's actions and processes would be boosted. If the AIS service were launched at the initial stage of the FMSS activities, it would be possible to receive balances of accounts and other account information from all supervised FMPs, thus this would open an opportunity to optimise the scope of work of several FMSS divisions, for example, the AIS service would facilitate the verification of payment transactions for the AMLD, establishment of the origin of funds held with FMPs for the LD, whereas the PMSD could track the balances of client fund accounts. Subsequently, broader access to the data of the accounts would enable monitoring the dynamics of executed payments.

The feasibility study revealed that AIS service integration, however, may be divided into two categories: the AIS service integration project which could be implemented in the short run, and the project which could be implemented in the long run. In the short run, the AIS service would ensure the provision of balances of EMI and PI client fund accounts and it could be achieved by means of minimum time limits and financial costs. This would also facilitate daily activities of FMSS employees and would make the work more efficient. This use of the AIS service would apply in the transitional period, i. e. until more innovative solutions are developed. In the long run, AIS service would help access all information on the account which could be consolidated, processed and applied a cross-cutting analysis to be used for the achievement of the supervisory goals; thus, it would be contributed to the implementation of one or several long-term strategic goals of the Bank of Lithuania for 2021-2025: development of a joint and effective data management set-up, advance, centralised and efficient collection of statements (and) data as well as development of an advance analytical platform for data integration and storage.

It must be noted that the projects of development of said alternatives are not attributed to the priority ones. The short-run and long-run categories are provided taking account of the fact that the Bank of Lithuania should allocate additional human resources by involving several FMSS divisions and financing sources to implement one of the above projects of AIS service integration. A more comprehensive cost analysis of the AIS service integration projects has not been conducted.

To sum up, it may be concluded that FMSS, to currently use the AIS service, would only have limited opportunities to receive information on client funds held in EMIs and PIs' accounts for safeguarding client funds, as the Directive has only recently been applied in the market; moreover, most credit institutions do not treat such accounts as payment accounts, therefore, as mentioned afore, this would require an individual position or interpretation of the Bank of Lithuania which would be based on the Q&A reply submitted by EBA.

CONCLUSIONS

The following main conclusions were drawn having analysed the currently applied supervisory process for safeguarding of client funds, provided the description of the AIS service process with respect to AISPs, and performed legal and IT evaluation in this feasibility study:

1) the data contained in annual statements for 2019 provided by EMIs and PIs show that almost all EMIs and PIs subject to the obligation to protect client funds have opted for the fund separation method, therefore, FMSS, while carrying out the prudential supervision of EMIs and PIs, will further focus on the analysis of this method by organising scheduled and unscheduled inspections of documents and will encourage EMIs and PIs to always comply with the requirement set out in the law with regard to adequate protection of client funds, thus, the process of collecting information necessary for document inspections will need to be inevitably optimised;
2) The rapidly intensifying activities of EMIs and PIs in Lithuania inspires the Bank of Lithuania to develop IT technological progress so that the EMI and PI supervision process is more speedily and closely monitored and controlled by means of digital technologies. The use of the AIS service to receive the supervisory information on client funds held by EMIs and PIs would be one of the possibilities to optimise the supervisory work of FMSS. Thus, FMSS would be able to always manage supervisory information on how EMIs and PIs comply with the requirement provided for in the law;
3) having summarised the results of the survey of credit institutions operating in Lithuania, it came to light that the accounts for safeguarding of client funds in almost all credit institutions were not accessed via PSD2 API interfaces because they were not classified as the payment accounts. Therefore, for the credit institutions to know exactly which accounts must be accessed via PSD2 API interfaces, an individual position or interpretation of the Bank of Lithuania should be drafted covering this issue on the basis of the Q&A reply submitted by EBA;
4) having summarised the data of the survey of selected AISPs, it came to light that current accessibility of the accounts other than payment accounts via PSD2 API interfaces was very limited and only some credit institutions established in Germany, Nordic countries and Poland were granting access to trust accounts or safeguarding accounts via PSD2 API. It also became apparent that accessibility or feasibility of this service is still not refined in the market but, as the survey has shown, the demand for accessibility to such accounts is increasingly growing, therefore, the credit institutions are currently making additional investments and creating Premium API interfaces for the AISPs to receive relevant information for an additional fee. It is intended to have such Premium API interfaces on the market at the end of 2021, therefore, it is recommended to return to this feasibility analysis one or two years later and continue the feasibility study analysis having updated the information;
5) having assessed legal information, it was established that if the AIS service, for the purpose of receiving supervisory information, were used in such a way where the EMIs and PIs preserved the option for the Bank of Lithuania to provide relevant information through AISPs and EMIs and PIs were allowed choosing AISPs on their own, the changes in the current legal regulation would not be necessary. EMIs and PIs could issue their consents or authorise AISPs to transfer information to the Bank of Lithuania on behalf of EMIs and PIs. In this case, the responsibility for the correctness of information transferred to the Bank of Lithuania would further remain with EMIs and PIs themselves. If the Bank of Lithuania, however, intended to oblige EMIs and PIs to use the services of a specific AISP which would be selected by the Bank of Lithuania itself, such actions would require the changes in legal acts and a more comprehensive legal analysis for lawfulness and reasonableness of those actions;
6) having analysed technical IT capacity of the Bank of Lithuania, it was established that consolidated information received from EMIs and PIs through AISPs could be currently stored and held in the existing information acceptance systems of the Bank of Lithuania;

7) based on the information collected in this feasibility study, it may be concluded that the use of AIS service would create additional alternatives in the activities of FMSS, i. e. receipt of supervisory information would be facilitated, and optimisation and digitalisation of FMSS's actions and processes would be boosted. At first, the AIS service used would enable receiving balances of accounts and other account information from all supervised FMPs, thus this would open an opportunity to optimise the scope of work of several FMSS divisions, for example, the AIS service would facilitate the verification of payment transactions for the AMLD, establishment of the origin of funds held with FMPs for the LD, whereas the PMSD could track the balances of client fund accounts; Broader access to the data of the accounts would enable monitoring the dynamics of executed payments;
8) the feasibility study revealed that AIS service integration may be divided into two categories: the AIS service integration project which could be implemented in the short run, and the project which could be implemented in the long run: (a) in the short run, AIS service would ensure the provision of balances of EMI and PI client fund accounts and it could be achieved by means of minimum time limits and financial costs; (b) in the long run, AIS service would help access all information on the account which could be consolidated, processed and applied a cross-cutting analysis to be used for the achievement of the supervisory goals; thus, it would be contributed to the implementation of one or several long-term strategic goals of the Bank of Lithuania for 2021-2025: development of a joint and effective data management set-up, advance, centralised and efficient collection of statements (and) data as well as development of an advance analytical platform for data integration and storage. To implement one of the projects of AIS service integration mentioned above, the Bank of Lithuania would need to allocate additional human resources by involving several divisions of FMSS and financing sources;
9) it is recommended to return to this feasibility study a year or two later and implement further actions during this period instead: (a) submit a question to the EBA Q&A and request that it drafts an explanation as to whether the accounts of safeguarding of client funds should be treated as the payment accounts and be accessed via PSD2 API interfaces; (b) monitor the changes undergoing on the market; (c) develop the position of the Bank of Lithuania or interpretation for FMPs based on the response received from the EBA so that they know exactly which accounts should be accessed via PSD2 API interfaces; (d) having updated and supplemented information, continue the feasibility study by forming a joint working group from several divisions of FMSS.