API STANDARD WORKING GROUP

REPORT ON THE API STANDARD IN LITHUANIA

2018

Vilnius

Abbreviations

API	Application programming interface based on *RESTful* architecture in line with the EBA-RTS requirements
AIS	Account information service
ASPSP	Account servicing payment service provider
Berlin Group	Pan-European payment solutions’ standardization initiative developing open standards
EBA	European Banking Authority
EBA-RTS	European Commission Delegated Regulation for strong customer authentication and common and secure open standards of communication
eIDAS	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market
PIS	Payment initiation service
PIIS	Confirmation on the availability of funds service
PSD2	Directive 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market
PSP	Payment service provider
PSU	Payment service user
SCA	Strong customer authentication
TPP	Credit institution, electronic money institution or payment institution providing payment initiation, account information and/or confirmation on the availability of funds services
QTSP	Qualified trust service provider according to the eIDAS Regulation

The Report was prepared by the API Standard Working Group.

Content

BACKGROUND INFORMATION

References

This section contains the list of related documents.

Number	Title	Issuer
[1]	*Berlin Group* API Specification (Version v0.99 or the final version prepared on its basis)	The Berlin Group https://www.berlin-group.org/psd2-access-to-bank-accounts
[2]	Final Report on Payment Initiation Services	ERPB http://www.ecb.europa.eu/paym/retpaym/euro/html/index.en.html
[3]	List of external codes	ISO20022.org https://www.iso20022.org/external_code_list.page
[4]	HTTP channel standard codes	RestApiTutorial.com http://www.restapitutorial.com/httpstatuscodes.html

History of revisions

Version	Revision description	Data
0.2	First draft	12/12/2017
0.3	Amendments introduced further to the oral and written comments of the Group members	12/01/2018
Final version		15/01/2018
Edited version		25/01/2018

INTRO

According to the provisions of the Second Payment Services Directive (hereinafter – PSD2) each account servicing payment service provider (hereinafter – ASPSP) – a bank, a credit union or an electronic money institution – who offers online services, should develop the open interfaces for three different intermediation services: the payment initiation service (hereinafter – PIS), the account information service (hereinafter – AIS) and the confirmation on the availability of funds service (hereinafter – PIIS). By March 2019 (as regards testing) and by September 2019 (as regards active transactions), these interfaces should be made available to other payment service providers (hereinafter – PSP). They should also meet the requirements established in the European Commission Delegated Regulation (EBA-RTS).

The EBA-RTS provides that open interfaces may be realised by the APIs or online banking based interfaces. The general opinion is that the APIs are technologically more advanced because of the possibilities of their management and integration with other products. The European and global standards are being developed for them. Therefore, it is expedient to link local standardization initiatives with the API ecosystem in particular.

The Lithuanian payment market participants seeking that APIs are secure, meet the needs of payment service users (PSUs) and contribute to market development, have set up the API Standard Working Group. Its participants were representatives of credit institutions, payment and electronic money institutions, providers of technical services and public authorities. The list of participants and the Regulations of the Working Group are provided in the annexes to this Report.

The task of the Working Group was to answer what API standard could be used in Lithuania. For this purpose the Working Group suggests using the Berlin Group API specifications [1]. When analysing the API ecosystem, the Working Group also established other relevant aspects (e.g. QTSP certificates, national registers of PSPs) the harmonised operation of which is important for the security and efficiency of payments. These areas were also incorporated in the Report.

Properly developed intermediation services are capable of competing with the ‘Bank Link’ and payment card services which are already available on the market. Also, they can be used as a basis for constructing completely new services which offer the PSUs the added value. Sustainable success of intermediation services, inter alia, will depend on the experience of payers, operational security and stability, development of API standards and economic incentives to invest in the API ecosystem. Development of other competing payment services (e.g. payment cards) will also influence the popularity of intermediation services. Despite these determinants of uncertainty, the Working Group is positive about the impact of the intermediation services on the competition and innovations.

This Report is the outcome of the Working Group’s consistent activities of nine months. The Working Group members assessed, analysed and discussed different aspects of API ecosystem and produced recommendations. The next step is the phase of individual preparation. This Report is submitted to the Bank of Lithuania, the Association of Payment and Electronic Money Institutions and the Association of Lithuanian Banks. According to the Regulations, after submission of the Report the Working Group’s activities are terminated.

SUMMARY OF RECOMMENDATIONS OF THE WORKING GROUP

Topic	Recommendations	Aimed at
The API Standard in Lithuania	• To develop the APIs according to final versions of the Berlin Group API specifications [1] for all intermediation services • Where possible, to develop the APIs as early as possible, without waiting for the latest deadlines set by the EBA-RTS	ASPSP
The API Standard in Lithuania	• To prepare and start using APIs of ASPSPs as soon as they become available, i.e. without waiting for the latest deadlines set by the EBA-RTS	TPP
Licensing and passporting for the provision of services in other Member States	• To specify clearly in the national list of PSPs the categories of PSPs providing intermediation services (a credit institution, an electronic money institution, a payment institution), the services (PIS, AIS, PIIS) provided by them, the commercial brand (if any), the passport for the provision of services in other Member States • Upon change of the information, to update immediately the data in the national list of PSPs • To provide for a possibility to export the data from the national list of PSPs in common formats	Bank of Lithuania
Issue of the eIDAS certificates	• To assess the limits of responsibilities and risks borne by QTSPs. Where appropriate, to use other additional sources of information for risk management purposes (e.g. national lists (registers) of PSPs, private directories) • Where PSPs use information caching practices, to check the TPP certificate validity at least once in 24 hours.	ASPSP
Issue of the eIDAS certificates	• To immediately notify QTSPs of the revocation (change) of the TPP license	Bank of Lithuania, TPP
Technical testing of APIs	• Where appropriate, to check via the Bank of Lithuania the information on entities that have applied for a license	ASPSP, Bank of Lithuania
Technical testing of APIs	• To follow the ERPB recommendations [2] regarding the test environment mode, operation time and availability of documentation in English	ASPSP
Technical testing of APIs	• To explain the requirements applicable when the ASPSP seeks to be exempted from the obligation to ensure the fall-back interface	Bank of Lithuania
Actual operation of APIs	• To follow the ERPB recommendations [2] regarding the particular API quality parameters (API availability (%), API response time, maximum API load, error level, level of negative authentication responses, etc.) • To use standard codes of HTTP protocol [4] and payment transaction status codes and rejected transaction reason codes according to ISO20022.org list [3] • To support the previous API version available to TPPs for six more months after release of the new main version • To arrange the account history information by sites according to the same number of transactions or to provide a link enabling to access the content of the account history information	ASPSP
Actual operation of APIs	• To use the API availability monitoring service (PING) with the established maximum 120 sec. checking frequency • To inform ASPSPs about the AIS request type (active, passive) providing the specific parameters, e.g. IP address of the PSU device, active session or key ID, or symbols 'A' / 'P'	TPP
Actual operation of APIs	• Considering actual differences applied by the banks operating in Lithuania with regard to operation status and error codes, to assess the possibilities of their convergence	Association of Lithuanian Banks
Dispute handling	• To follow the ERPB recommendations [2] regarding the resolution of disputes (the contact person, establishment of the process control elements, etc.)	ASPSP, TPP
Specifics of the transitional period	• To use the intervals of IP addresses for identification purposes, notify them to ASPSPs directly or using technical facilities the Bank of Lithuania (if any)	TPP
Specifics of the transitional period	• To avoid using pop-ups or other unpredictable dynamic elements hindering the stability of services during login sessions in which the identity of TPP was confirmed	ASPSP

1. ECOSYSTEM OF INTERMEDIATION SERVICES

The PSD2 introduces three new payment services (PIS, AIS and PIIS) based on access to data stored by ASPSPs and their payment processes. These services offer new payment account management and use possibilities the extent of which depend on technical solutions of ASPSPs (as the entity disclosing the data) and TPPs (as the entity creating the end-product).

By selecting the payment initiation service (PIS) it will be possible to initiate a payment and directly retrieve the results of its execution using only the TPP services. It will be possible to integrate this method in e-commerce, collection of payments, payment of e-invoices and other environments.

A PSU will be able to use the account information service (AIS) in order to check his/her payment account balances or retrieve the history of operations. After receipt of the user consent, the TPP will retrieve the data stored by the ASPSP and having collected and processed the information according to the conditions agreed in advance with the PSU, will communicate the results to the end-user.

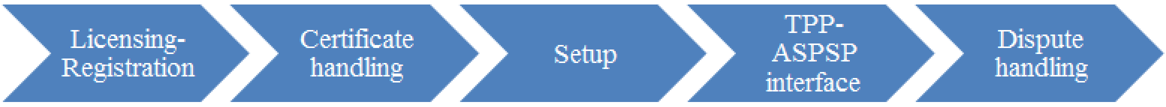
The service of confirmation on the availability of funds (PIIS) can be understood as the AIS of a narrower extent. An ASPSP, after receiving the request of the TPP regarding the availability of the particular amount of funds in a payment account, shall give the answer 'YES/NO' without indicating the actual balance of funds. PSD2 defines one of the PIIS application variants, e.g. when a payment is initiated with a payment card issued by the TPP, but funds intended for making the payment are stored with the ASPSP. Nevertheless, the PIIS is closer to the AIS, because the ASPSP has no obligation to reserve the funds or to ensure their transfer to the final payee. It is likely that the TPP will also implement other PIIS application alternatives.

To ensure smooth operation of the new payment services both good quality APIs between the ASPSP and the TPP and reliable processes in other API ecosystem-related spheres are necessary. For example, certificates issued by qualified trust service providers (QTSP) will be the main tool of identification of TPPs. Hence, activities of QTSPs will affect the overall risk map of the API ecosystem.

The ecosystem of intermediation services consists of the main five component parts (Fig. 1):

1) Licensing and passporting: all actions relating to the acquisition by the PSP of the right to provide intermediation services in the home Member State and, having informed accordingly, in other Member States;
2) Issuance of eIDAS certificates: all actions relating to the acquisition by the TPP of qualified certificates of electronic seals and/or website authentication certificates issued by QTSPs;
3) Technical testing of APIs: technical environment (e.g. ASPSP test environment) and actions allowing TPPs to ascertain the compatibility of its products with APIs developed by ASPSPs;
4) Actual operation of APIs: all actions whereby the parties implement the rights and obligations established by the PSD2, including risk management when PISs, AISs and PIISs are provided to end-users;
5) Resolution of disputes: all actions necessary for the regulation of responsibilities of ASPSPs and TPPs in the cases of disputed transactions (e.g. error transactions, cases of fraud, etc.).

Fig. 1. Main component parts of the API ecosystem



Source: Preta S.a.S.

Licensing and passporting

PSPs, except for credit institutions, acquire the right to provide PISs, AISs or PIISs when they obtain a license for such services from the supervisory authority of the home Member State. According to legal acts of the Republic of Lithuania the license of credit institutions (banks, credit unions, the Central Credit Union) automatically entitles to provide intermediation services. The entry in the national public list (register) of PSPs of the home Member State is the main proof that the PSP has the right to provide intermediation services in the home Member State and, having informed accordingly, in other Member States. Such information, including other data (e.g. the licensing date, the right to provide services in other Member States, the revocation of the license) is significant for many entities:

- the ASPSPs for assessment of the TPP transaction risks;
- the QTSP for issuance to TPPs and, where appropriate, revocation of qualified certificates of electronic seals and/or website authentication certificates;
- the PSU for distinguishing licensed TPPs from alleged TPPs participating in fraud schemes.

National lists (registers) of PSPs of Member States are accessible online, but the scope of published information, visual presentation and updating practices can differ (e.g. data export can take place through the dedicated APIs or by other means (.pdf, .cvs, .xls formats). When TPPs of different Member States apply to ASPSPs and QTSPs the latter will be exposed to the variety of national registers of PSPs, which will make automated exchanges of information with national registers difficult for the ASPSPs and QTSPs. Different traditions of the provision of information are unfavourable for PSUs as well as it may be unclear where exactly and according to what parameters the particular TPP can be found in the national registers of separate countries.

The resolution of this problem is sought by developing a new central EBA Register. As specified in the PSD2, information to the EBA Register will be supplied by national supervisory authorities according to the agreed data volume. The scope of information supplied by them and published by the EBA is established by delegated regulations of the European Commission. However, according to draft legal acts of the EBA[1] credit institutions offering TPP services will not be included in the EBA Register. That information will be available only at national level. Now it is difficult to say yet whether functional characteristics of the EBA Register (data export, level of synchronisation with national lists) will be sufficient for ensuring the needs of ASPSPs and QTSPs. Still, the EBA Register is likely to be attractive for PSUs who seek one-stop-shop access to all non-banking TPPs.

The API Standard Working Group is aware of the private initiative aimed at eliminating the weaknesses of the national and EBA registers. Preta S.a.S. (the subsidiary of EBA Clearing) is planning to act as a technical intermediary combining different national registers into a single technical environment. As noted by Preta, its directories and information services would cover not only the information relating to the TPP licence (and its termination), but also other information relevant for the API ecosystem (e.g. contact details for incident handling, API addresses). Preta is planning to offer directory services from June 2018.

The API Standard Working Group is of the opinion that notwithstanding other initiatives the aim to improve the quality of services of national lists (registers), for example, regarding practices of completeness, updating of published information and data export possibilities, remains. Good operating quality of national lists minimises the risks of API ecosystem at large (e.g. when a TPP license is terminated), irrespective of whether market participants use the lists directly or indirectly (through solutions of private companies). Accordingly, the Working Group provides recommendations (see below) to the Bank of Lithuania, as to the entity maintaining the Lithuanian list of PSPs.

Payment institutions and electronic money institutions offering intermediation services must hold professional indemnity insurance or a similar guarantee. At present, the market of insurance of this type is underdeveloped yet and insurance undertakings and their conditions are unknown. The situation, however, is expected to change and insurance services will be available to TPPs in the near future.

[1] *Drafts of the EBA:* *https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/technical-standards-on-the-eba-register-under-psd2.*

Recommendations	It is proposed that the Bank of Lithuania, as the entity maintaining the national list of PSPs: • establishes clearly in the national list of PSPs the categories of PSPs providing intermediation services (a credit institution, an electronic money institution, a payment institution), the services (PIS, AIS, PIIS) offered by them, the commercial brand (if any), the passport for the provision of services in other Member States; • upon change of information, immediately updates the data in the national list of PSPs; • offers a possibility to export the national PSP's data in common formats.

Important facts!	• Completeness, visual presentation and updating practices of information in the national registers of PSPs can differ. • The central EBA Register will exclude credit institutions operating as TPPs. • There is a possibility of short-term difference between the information of the national registers of PSPs and the central EBA Register.

Issuance of eIDAS certificates

The PSD2 establishes the obligation of the TPP for each communication session to identify itself towards the ASPSP. At the EU level, this provision will become mandatory from September 2019, but may also be applied earlier, e.g. when the ASPSP offers the API and enables their testing.

The EBA-RTS establishes that:
1) For the purpose of identification of TPPs, qualified certificates for electronic seals and/or qualified certificates for website authentication issued according to the eIDAS should be used. The certificates may be generated only by qualified trust service providers (QTSP).
2) QTSP must include the following additional data in the certificates: a) the name of the supervisory authority of the home Member State; b) the TPP registration (authorisation) number; c) the TPP function (PIS, AIS, PIIS or their combination).
It should be noted that the EBA-RTS does not establish any requirements how the ASPSP should identify itself towards the TPP, if such a need arises.

The eIDAS is a relatively new legal act and the majority of its provisions are applied only from July 2016. The qualified trust services and their providers are bound by high security requirements, and the market of such services is still developing. At present, QTSP services in the EU are offered by just a few companies, but the list of the QTSP is increasing. The eIDAS allows providing the QTSP services across the EU, accordingly, TPPs established in Lithuania will also be able to select QTSPs of another country. Nevertheless, the Working Group sees advantages in the provision of QTSP services by a company operating in Lithuania (e.g. because of the easier identification of a legal person, flexibility of response to local market needs). Notwithstanding that, the choice of the QTSP entity by TPPs will depend on the competition and the quality of services.

Although the EBA-RTS puts the equals sign between electronic seals and website authentication services, in practice, they differ in technological and legal terms. For example, only the website authentication service can ensure the confidentiality of communication and transmitted data, whereas the feature of non-repudiation of a transaction can be ensured only by the electronic seals service. Therefore, depending on technical features, a combined use of both these services might be expedient. This possibility is provided for in the Berlin Group API specification [1]. Furthermore, these services have been developed and functioned in different technological environment: website authentication services are widely used in the website and search engines, and the electronic seals service is based on the electronic signature infrastructure. These differences can affect the speed of services.

The eIDAS establishes the obligation for QTSPs, prior to the issuance of the certificate, to check the accuracy of the information included in the certificates, but does not establish the obligation to actively monitor whether the included information still corresponds to reality. Nevertheless, having received the relevant information, QTSPs must cancel the certificate within 24 hours. It is difficult to forecast whether the competitive environment will encourage QTSPs to implement the active monitoring principles. Initial QTSP service packages are likely to cover only passive monitoring of information, i.e. QTSPs will cancel (change) a certificate only after receipt of information from the certificate holder or supervisory authority of a home Member State. Therefore, it is important for ASPSPs to assess the limits of responsibilities and assumed risks of QTSPs. For example, QTSPs have the right to impose restrictions on the use of services, and when such restrictions are exceeded – not to indemnify the damage.

The entries of additional regulatory data in the eIDAS certificates will help ASPSPs to manage the counterparty risk. Nonetheless, if these entries are not coordinated at the EU level, the processing of certificates would become more difficult. Therefore, the Working Group supports the attempts of the European Telecommunications Standards Institute (ETSI) to unify at the EU level additional data entries in the certificates. According to the time limits set by the ETSI[2], the process of standardization of the PSD2 certificates should be completed by mid-2018.

[2] https://portal.etsi.org/webapp/workProgram/Report_Schedule.asp?WKI_ID=53961.

In analysing the aspect of efficiency of qualified trust services, the Working Group has assessed the possibility of caching the information of QTSP certificates. Such practice can accelerate transactions and minimise the costs of ASPSPs; however, it increases the risk that ASPSPs will grant access to the payment account to the institution which no longer has such a right. In the opinion of the API Standard Working Group, those ASPSPs who use caching in repeated transactions should verify the validity of the TPP certificates at least once in 24 hours.

Recommendations	• ASPSPs should assess the limits of responsibilities and assumed risks of QTSPs. Where appropriate, for risk management purposes ASPSPs should also use other additional sources of information (e.g. national lists (registers) of PSPs, private directories). • Those ASPSPs who apply the information caching practices should verify the validity of the certificate at least once in 24 hours. • TPPs and the Bank of Lithuania should immediately notify QTSPs of the revocation (change) of TPP license.

Important facts!	• The electronic seals and website authentication services are suitable for the TPP identification; however, they significantly differ in other aspects. Depending on circumstances, it might be expedient to use these two services in combination. • QTSPs have the right to impose restrictions on the use of services, and when such restrictions are exceeded – not to indemnify the damage. • The EBA-RTS does not establish the requirements for the identification of the ASPSP towards the TPP, if such a need arises.

Technical testing of APIs

According to the EBA-RTS, ASPSPs must provide TPPs with test environment enabling the testing of the TPP connection and the functional testing of the ASPSP's interface and provide the TPP with the testing related support. The test environment must be provided regardless of the access interface (API or online banking) planned to be developed by the ASPSP. The test environment must be provided not only to the TPP included in the national registers of PSPs, but also to those entities which have applied with a supervisory authority of a home Member State for a TPP activity license.

According to the EBA-RTS, test environment of the ASPSP currently operating on the market must be made available to the TPP by March 2019, at the latest. This target date is concurrent to other obligation of the ASPSP, i.e. to enable the TPP to get familiarised with the technical documentation of the access interface. Nevertheless, it is important in this context to consider the time when certificates issued by QTSPs under the eIDAS will appear and become available in the market. When the ASPSP changes the technical specification of its access interface, the specification should be made available to TPPs and institutions that have applied for their license not less than three months before the new interfaces are activated.

Recommendations of the ERPB [2] supplementary to the EBA-RTS requirements establish that:
1) the test environment should support full end-to-end testing;
2) access to test environment and quality of service during business hours should be ensured;
3) technical documentation shall at least be available in English.
The API Standard Working Group agrees with the ERPB and suggests the ASPSPs to follow them.

There are several ways for the ASPSPs to retrieve information about the entities that have applied for a license: 1) obtain the confirmation directly from the entity; 2) obtain the confirmation from the supervisory authority of the entity's home Member State, including the cases when the entity has its head office in another Member State; 3) obtain the confirmation from the Bank of Lithuania, including the cases when the entity has its head office in another Member State. The Working Group suggests the ASPSPs to apply the latter alternative and, where appropriate, to verify the information on the applicant through the Bank of Lithuania.

The EBA-RTS establishes that ASPSPs who choose to implement the API will have to ensure fall-back interfaces based on the online banking infrastructure. However, those ASPSPs, who will ensure quality APIs will be relieved from the obligation to have a fall-back interface. The process of determining quality APIs consists of several phases, of which the first phase is based on the ASPSP test environment and active actions of TPPs. In this case, TPPs would verify not only the compatibility of their products with interfaces of ASPSPs, but also the quality of the ASPSPs' APIs, which, as established by the EBA-RTS, must be satisfactory. It is expected, that the Bank of Lithuania, after consulting the EBA, will provide a more detailed explanation of this process.

Recommendations	• ASPSPs should follow recommendations of the ERPB regarding the test environment mode, operating hours and documentation in English. • Where appropriate, ASPSPs should check through the Bank of Lithuania the information on the entities that have applied for a license. • The Bank of Lithuania should explain the requirements applicable in those cases when the ASPSP seeks exemption from the obligation to ensure a fall-back interface.

Important facts!	• The test environment should be provided regardless of the interface type (API or online banking). • The test environment should be provided to licensed TPPs and entities that have applied for a license.

Actual operation of APIs

After a TPP obtains the required license and the QTSP certificate and the technical compatibility with the ASPSP's interfaces is successfully verified in test environments, the ASPSPs and the TPPs are ready for the phase of live transactions. The EBA-RTS sets the latest possible beginning of this phase – September 2019. Still, on the initiative of the ASPSP and the TPP, the stage of live transactions can also begin earlier, on condition that preparatory phases (APIs, TPP license, QTSP certificates, testing) are completed successfully.

September 2019 is also a deadline of other aspects relevant for the API ecosystem. From September 2019 'screen scraping' practices will no longer be possible. All TPPs will have to identify themselves towards ASPSPs and use the dedicated access interfaces of ASPSPs.

In addition, in the cases specified in the PSD2, from September 2019, PSPs will have to use the strong client authentication (SCA). In accordance with national legal acts, the SCA can also be mandatory for online transactions until September 2019. For example, this obligation for PSPs operating in Lithuania arises from Resolution No 03-172 of the Board of the Bank of Lithuania of 30 September 2014 on the approval of minimum security requirements applicable to online payments (as amended). From September 2019, the EBA-RTS, as a legal act of direct application, will supersede the national SCA requirement leading to the harmonisation of the application of SCA across the EU.

The actual operation of APIs to a great extent depends on the possibilities of API specifications, API quality metrics and harmonised operation of other parts of the API ecosystem. Lithuanian banks are planning to apply the Berlin Group API specifications in respect of all three intermediation services. For more information about the Berlin Group API specifications please refer to the section 'API standard in Lithuania'.

The EBA-RTS establishes high requirements for the quality of APIs. The API availability and quality parameters will have to be at least as stringent as those set for online banking interfaces. An interruption of even a few minutes in the operation of API would give rise to the obligation of the ASPSP to activate a fall-back access interface based on the online banking solutions. The ASPSPs who seek avoiding investments in a fall-back interface will have to fulfil even higher API quality requirements (e.g. immediately respond to any API related problems).

The ERPB [2] has set the specific API quality parameters: API availability (%), API response time, maximum API load, error rate, authentication failures, etc. The API Standard Working Group recommends the ASPSPs operating in Lithuania to apply these parameters. It is further recommended that TPPs use the API availability monitoring service – PING – with the established verification frequency of maximum 120 seconds.

Other processes described in this section will also be partially used in the actual provision of intermediation services (Table 1). A TPP, acting on the basis of a PSU's consent for a payment transaction, will submit a request to an ASPSP who according to the QTSP certificate data will authenticate the TPP and determine other parameters relevant for risk management (e.g. a supervisory authority of a home Member State). In order to additionally verify whether a particular TPP still holds the license for intermediation services or is licensed to provide intermediation services in a non-home Member State, the ASPSP can consult national registers of PSPs or private directory service providers. Further communication between the ASPSP and the TPP takes place according to the API specification functionality based on the 'request and answer' principle. When the time comes to authorise the payment transaction, the ASPSP allows the TPP to use the authentication procedure established by the ASPSP. Where necessary, the SCA is applied. After the transaction, the TPP notifies its results to the PSU. If the PSU denies having authorised the transaction, the process of resolution of disputed situations, which defines the responsibilities of the parties and, where appropriate, the sharing of inflicted damage, is initiated. The provision of intermediation services can also require other interfaces (e.g. with electronic authentication providers when the ASPSP relies on electronic authentication tools of third parties, or with merchants when the TPP offering the PIS integrates its solutions with the merchant's website), which, however, are excluded from the object of investigation of this Working Group.

Table 1. Main interfaces used in the provision of intermediation services

Interface	Brief description
TPP – supervisory authority of a home Member State	An applicant TPP applies with a supervisory authority of a home Member State for obtaining a license to provide intermediation services in a home Member State and, as appropriate, in other Member States. After issuance of the license, the TPP is included in the national registers of PSPs, the central register of the EBA and private directories.
TPP – QTSP	A TPP applies to a QTSP for the qualified electronic seals and/or website authentication certificate necessary for the identification.
QTSP – supervisory authority of a home Member State	Prior to issuing the certificate, the QTSP verifies the information provided by the TPP against the information available in the national registers of PSPs.
PSU–ASPSP	A PSU has a valid service agreement with an ASPSP for a payment account accessed online and disposes personalised security features agreed with the ASPSP.
PSU–TPP	A PSU agrees to use the services of a TPP concluding for that purpose a single payment or a framework agreement with the TPP.
TPP–ASPSP	Communication between a TPP and an ASPSP on test environment, as well as on live environment and disputes handling.
ASPSP–QTSP	An ASPSP verifies the validity of the certificate issued by the QTSP to the TPP each time or at the selected periodicity.
ASPSP – supervisory authority of a home Member State	As appropriate, the ASPSP verifies the validity of the TPP license in the national registers of PSPs or private directories.

Source: API Standard Working Group.

When open access interfaces are realised through APIs, the EBA-RTS prohibits the ASPSP from requesting that the PSU is redirected to the ASPSP's website for authentication of the PSU. This means that the TPP is responsible for the adaptation to the requirements of the ASPSP as regards the authentication of the PSU and the visual authentication in the TPP's environment as well as for the related security procedures. When tools (e.g. code generators) issued by the ASPSP are used, PSUs will be able to enter personalised security features directly in the TPP environment. In the case of use of electronic authentication tools issued by third parties, TPPs will not take part in the transmission of personalised security features to the ASPSPs. Still, the EBA-RTS does not prohibit the ASPSPs from offering an access interface which would redirect the PSU to the ASPSP's website for the authentication of the PSU, if the TPP so requests. This might be attractive for those TPPs who aim at mitigating the risks they face in the process of authentication of PSUs.

The trust of PSUs in the intermediation services is one of the key factors in the development of these services. The greatest risk of losing the trust of the PSUs arises in transitional period during which the TPPs potentially will be able to access a greater PSU data array than required for the provision of intermediation services. The PSD2 prohibits the TPPs from requesting and storing excessive data of PSUs. Nevertheless, even single cases of wrong processing of the PSU data are likely to damage the reputation of services. For more information on the specifics and risks of the transitional period please refer to section 'Specifics of transitional period'.

Attractiveness of the API ecosystem will also depend on the ability of the TPP to integrate intermediation services with e-commerce, collection of payments, payment of e-invoices or other environments relevant for the end-users. It is likely that some TPPs will develop the model of single transactions applicable in the cases of e-commerce into the model of regular transactions (e.g. e-wallet). In that case, the TPP's e-wallet solution can become one of the main channels for initiating regular payment transactions of PSUs.

Uniform use of the transactions status and error codes on the market would facilitate the provision of intermediation services. The API Standard Working Group recommends the ASPSPs to use:
1) the standard codes of the HTTP protocol [4];
2) the external codes of the of payment transactions according to ISO20022.org list [3];
3) the external status reason codes of rejected transactions according to ISO20022.org list [3].

Additional codes, i.e. intermediate status codes of payment transactions and internal error codes of the ASPSPs activities currently are not standardized and can respectively differ in each ASPSP. The values of these codes will be explained in the API technical documentation of ASPSPs. The API Standard Working Group recommends that the Association of Lithuanian Banks, taking account of actual differences in transaction status and error codes between banks operating in Lithuania, assesses the possibilities of their convergence.

The API Standard Working Group further recommends that:
1) the ASPSPs support the previous version of the API accessible to the TPP for six more months after release of the new main version;
2) the ASPSP providing the account history information to the TPP offering the AIS divides the sites according to the same number of transactions (e.g. 3 000 entries) (the information on the total number of sites should be specified in the response message) or provide a link enabling to access the content of the account history information;
3) a TPP, when submitting the AIS requests, informs an ASPSP on the request type: active (on the basis of active request of a PSU) or passive (without active involvement of a PSU according to requirements of the EBA-RTS). In that case, the TPP should provide the specific metrics, e.g. IP address of the PSU’s device, ID of the active session or key or the symbols ‘A’/‘P’, respectively meaning active or passive requests.

Recommendations	An ASPSP should: • follow recommendations of the ERPB regarding the specific quality metrics of the API (API availability (%), API response time, maximum API load, error level, level of negative authentication responses, etc.); • use standard codes of HTTP protocol [4] and status codes of payment transactions and status reason codes of rejected transactions according to ISO20022.org list [3]; • support the previous API interface version available to TPP for six more months after release of the new base version; • arrange the account history information by sites according to the same number of transactions or to provide a link enabling to access the content of the account history information. A TPP should: • use the API availability monitoring service (PING) with the established checking frequency of maximum 120 seconds; • inform an ASPSP about AIS request type: active or passive, by providing the specific parameters, e.g. IP address of a PSU device, ID of active session or key, or symbols ‘A’ / ‘P’.

Important facts!	• On the initiative of ASPSPs and TPPs, actual use of API can also start before September 2019, provided that the TPP obtains a license and QTSP certificate and tests of the API’s compatibility with products of the TPP are successful.

Resolution of disputes

For the purpose of management of incidents (errors, fraud, disputes, etc.) which occur from time to time in the sphere of payment services a separate process is required. It is often contemplated in agreements of the parties. However, the feature of the API ecosystem, i.e. that ASPSPs and TPPs can operate without concluding a mutual agreement and even from different jurisdictions stimulates the need to look for alternative solutions.

Theoretically, resolution of disputes can be standardised and automated at least to a certain extent. However, there are no such initiatives at the international level. Moreover, the volume of disputes currently is unclear, which makes the adoption of the process automation investment decisions more difficult.

The PSD2 establishes the general principles and responsibilities regarding the settlement of disputes between the ASPSP and the TPP. It is expected that in most cases these principles will be sufficient for the parties to settle incidents peacefully. Still, it cannot be ruled out that due to the lack of the concrete process recognised by all parties certain disputes can be unreasonably delayed and finalised only after the court’s decision.

The ways of smoother handing of disputes are being sought. To that end, the ERPB [2] has formulated the minimum requirements:
1) each party (an ASPSP, a TPP) should designate a contact person capable of communicating both in the national and English languages, and provide the contact details on their website, technical documentation of the API or directories;
2) each party should provide for additional elements facilitating the management of problem situations. The list of such elements is published in Annex 8 to the Report of the ERPB [2];
3) the parties should ensure the resolution of disputes at least through the manual communication;
4) disputes should be handled bilaterally and if the parties cannot reach an agreement, mediation could be considered before going to court.
The Working Group agrees to the proposals of the ERPB and recommends each party to follow them.

Recommendations	• ASPSPs and TPPs should adhere to the recommendations of the ERPB [2] regarding the handling of disputes (a contact person, establishment of the process management elements, etc.).

Important facts!	• The possibility of ASPSPs and TPPs to operate without a mutual agreement and from different jurisdictions stimulates the need to look for alternative solutions of problem situations. The preconditions for peaceful resolution of disputes are the proper preparation and cooperation of the parties.

.

2. SPECIFICS OF TRANSITIONAL PERIOD

The application of majority of provisions of the PSD2 in Member States should begin from 13 January 2018. However, there are several reasons for which (all or part of) provisions of the PSD2 in Member States will be applied later:
1) some Member States (e.g. Belgium, Sweden, Netherlands, Lithuania) are late with transpositions of provisions of the PSD2 to national law;
2) the European Commission and the EBA are late with the approval of certain technical standards and guidelines;
3) the PSD2 has set the transitional period until the application of the EBA-RTS which is 18 months after the date of entry into force;
4) the PSD2 has provided for a possibility for PIS and AIS providers that have provided such services before 12 January 2016 to continue to perform the same activities in their territories during the transitional period.

The first two reasons are likely to cease to exist during the first half of 2018. This will not have a material impact on the API ecosystem, because final results in other spheres, e.g. as regards the standardization of QTSP certificates, are also expected only somewhere in the middle of 2018. Due to delay in technical standards and guidelines, the EBA recommends to follow final drafts of documents published on the website of the EBA[3].

Supervisory authorities of the majority Member States envisage encouraging PIS and AIS providers that have provided such services before 12 January 2016 to apply for a TPP's license. PSPs operating in Lithuania that hold (unrestricted activity) licenses of a payment institution or of an electronic money institution and that have provided PIS or AIS services before entry into force of legal acts implementing the PSD2 benefit from a special (accelerated) licensing procedure. Those PSP after submission of an application for changing the license and the required documents will have their license changed within 20 working days; however, the Bank of Lithuania will seek that such entities can provide the aforementioned services continuously.

Hence, one of the essential circumstances of transitional period most probably is the deferral of application of the EBA-RTS provisions until September 2019. By then, a TPP will be able to provide intermediation services by using 'screen scraping' and without using access interfaces of ASPSPs. Nevertheless, some Member States are considering a possibility to introduce the obligation on TPPs to identify themselves also during transitional period and will encourage TPPs to start using interfaces of ASPSPs as soon as they become available.

The draft Law of the Republic of Lithuania on Payments also establishes the obligation for a TPP for each communication session to identify itself towards the ASPSP. The API Standard Working Group has analysed different possible TPP identification alternatives and recommends:
1) confirming identity of a TPP according to intervals of IP addresses to be notified by the TPP to an ASPSP directly or through technical facilities of the Bank of Lithuania (if applicable);
2) during login sessions in which a TPP has identified itself, an ASPSP should avoid using pop-ups or other unpredictable dynamic elements hindering the stability of services.

The API Standard Working Group notes that 'Bank Link' services characterised by technical stability and security remain a good alternative of 'screen scraping' during transactional period. Those services could be used further until access interfaces functioning according to the EBA-RTS are available on the market. However, 'Bank Link' services would be unsuitable for those who are planning to offer AIS services.

The entry into force of legal acts transposing provisions of the PSD2 will lead to a change in one of the principal provisions of security observed by PSUs since the very outset of online banking. Disclosing one-time online banking login passwords to TPPs will become a normal practice for PSUs. Until present, PSUs have been continuously encouraged to avoid doing that. Accordingly, the need appears to explain

[3] The following legal acts may be relevant for the API ecosystem: 1) EBA guidelines on major incident reporting; 2) EBA guidelines on security measures for operational and security risks; 3) European Commission delegated regulations on EBA Register.

these changes to PSUs and help PSUs in distinguishing licensed TPPs from alleged TPPs participating in fraud schemes.

Recommendations	• For confirming its identity, a TPP should use intervals of IP which will be notified by the TPP to an ASPSP directly or through technical facilities of the Bank of Lithuania (if applicable). • During login sessions in which a TPP has identified itself, an ASPSP should avoid using pop-ups or other unpredictable dynamic elements hindering the stability of services.

Important facts!	• The main circumstance of transitional period – deferred application of the EBA-RTS provisions until September 2019. • There is a need to properly explain to PSUs how to distinguish between licensed TPPs from alleged ones.

3. API STANDARD IN LITHUANIA

According to provisions of the PSD2, each ASPSP – a bank, a credit union or an electronic money institution – who offers online services should develop access interfaces for each intermediation service (PIS, AIS, PIIS). If each ASPSP develops APIs according to its unique specifications, only in Lithuania there would be over 30 different APIs for each service and in the European Union this figure would exceed 4 000. In such circumstances, the possibilities of TPPs to develop intermediation services would become difficult even at the national level. Due to that, communities of payment service providers in Lithuania and other countries seek to use the standard API specifications.

In its activities, the API Standard Working Group devoted the greatest attention to the Berlin Group API standardization initiative [1]. The Berlin Group was one of the first to clearly announce about its plans to standardize the API specifications according to the PSD2 requirements, and its representatives became actively engaged in the activities of the ERPB. The Nordic – Baltic banks, including parent undertakings of the banks operating in Lithuania also participated in the activities of the Berlin Group. The API Standard Working Group has access to draft versions of specifications of Berlin Group and is thus able to follow the progress of this initiative.

The Berlin Group is a pan-European payment solutions standardization initiative developing open standards since 2004. The main features of its activities: 1) the Berlin Group does not implement itself its developed standards; 2) its standards are open and free at present. The draft API specifications were developed with the involvement of banks, but the public consultation was open to all market players. In 2018, the Berlin Group is planning to publish the information about further development of API specifications. The Berlin Group is also working on its position whether ASPSPs will have to certify their APIs in order to confirm their compliance with the standard specifications.

In addition to the Berlin Group, there are four more API standardization initiatives known at present: ‘Open Banking UK’ of the United Kingdom, ‘STET PSD2 API’ of France, and Polish and Slovak initiatives. Detailed comparison of all API standardization initiatives is provided in Annex No 3 to the ERPB Report [2]. The annex shows that all initiatives are essentially based on the same technological solutions (e.g. REST, TLS, JSON). Nevertheless, now it’s not easy to identify differences in their functionality, because the majority of the initiatives are being improved to ensure their compliance with the EBA-RTS requirements.

When preparing this Report, the Berlin Group’s API specifications were not finally approved yet, although the public consultation regarding draft documents has already taken place. In the opinion of the API Standard Working, the drafted documents are of good quality and the information is provided in sufficient detail. The API Standard Working Group has no reason to question the Berlin Group’s competence and abilities to finalise the documents being drafted.

The Berlin Group’s API specification documents submitted for public consultation show that some services provided using APIs will be mandatory for ASPSPs and some of them – optional (see Table 2). A decision on their implementation will rest upon ASPSPs.

Table 2. The Berlin Group’s API Specification services the implementation of which will be decided by ASPSPs

API aspect	Brief description
List of accessible accounts	An AIS service variation which allows TPPs determining the list of accessible accounts without direct participation of PSUs.
Session support	Session mode allows TPPs changing intermediation roles during one logical transaction. For example, before providing the PIS the TPPs acting as AIS can retrieve from ASPSPs the list of accessible payment accounts and allow PSUs to choose the account from which to initiate the payment. The session mode inter alia allows using SCA only once where this is compatible with provisions of the EBA-RTS.
TPP identification at the application layer	The Berlin Group’s API specification establishes mandatory TPP identification at the transport layer. TPP identification at application layer is optional.

Methods ensuring SCA	The Berlin Group's API specification is neutral as regards PSU authentication methods selected by ASPSPs. Moreover, it allows realising three different SCA modes: 1) when personalised security credentials are embedded by PSUs in the controlled environment of TPPs; 2) when personalised security credentials decoupled by PSUs in the controlled environment of the electronic identification provider; 3) when personalised security credentials are redirected by PSUs in the controlled environment of ASPSPs. The EBA-RTS establishes that ASPSPs may not require TPPs to use the latter method, but they can offer it in addition to other methods.
OAuth2 protocol	This protocol may be used for developing a PSU's consent in AIS service.
Message syntax (JSON, XML)	Messages of intermediation services may be defined using JSON or XML syntax. JSON will probably be more popular in the case of intermediation services provided to natural persons, and XML – to legal persons.

Source: The Berlin Group's API specification.

Intermediation services under the Berlin Group's API specification are realised by means of these processes:
1) PIS of one (separate) payment;
2) generating the AIS consent;
3) retrieval of the list of accessible accounts;
4) retrieval of given account balances;
5) retrieval of given account transaction history;
6) PIIS.
ASPSP must ensure not all these processes – giving the AIS consent and of the list of accessible accounts are services optional for ASPSPs.

The API Standard Working Group conducted the survey of banks – members of the group regarding the use of the Berlin Group API specification in Lithuania. The results have shown that banks operating in Lithuania are planning to use the Berlin Group API specification for all intermediation services (PIS, AIS, PIIS). Still, the majority of banks don't yet know what optional features of the Berlin Group API specification they will implement and have not set the particular start dates for API operation. Three banks have notified of their plans to use the OAuth2 protocol.

The API Standard Working Group recommends all ASPSPs operating in Lithuania to develop APIs according to the final versions of the Berlin Group API specifications for all intermediation services. Currently, the Working Group sees no need to establish that optional features of the Berlin Group API specification are mandatory. Market participants have not expressed the need for the development at the national level the extended services compatible with the Berlin Group API specifications either.

The ASPSPs that select not to follow any of the API standardization initiatives should responsibly assess the possible consequences. For example, if such ASPSP seeks exemption from maintaining a fall-back access interface, the difficulties can arise in finding the sufficient number of TPPs who would test dedicated APIs of ASPSPs. Furthermore, unique APIs can completely discourage TPPs from using the interfaces of ASPSPs. Less accessible ASPSPs, respectively, can disappoint their clients, in particular those for whom intermediation services will be attractive.

Recommendations	The ASPSP should: • develop APIs according to the final versions of the Berlin Group API specifications for all intermediation services; • taking account of the possibilities, develop APIs as early as possible, without waiting for the latest deadlines set in the EBA-RTS. The TPP should prepare and start using the APIs of ASPSPs as soon as they become accessible, i.e. without waiting for the latest deadlines set in the EBA-RTS.

4. FURTHER DEVELOPMENT OF THE API ECOSYSTEM

The API Standard Working Group has identified several areas which are likely to affect the future development of the API ecosystem:
1) amendments to the EBA-RTS;
2) establishment of the criteria applied by supervisory authorities for the quality APIs exempting ASPSPs from the obligation to have a fall-back interface;
3) extension of functionality of the Berlin Group API specifications;
4) introduction of instant payments;
5) development of authentication procedures.

The European Commission established a mandatory review of the EBA-RTS. By March 2021, the EBA will have to revise the provisions of the EBA-RTS enabling the home competent authority to exempt ASPSPs from the obligation to set up a fall-back access interface. Where necessary, the EBA will have to propose new wordings of requirements which are likely to be focused on further incentives for ASPSPs to develop quality APIs.

The present version of the EBA-RTS allows the home competent authority, after consulting the EBA, to exempt ASPSPs from the obligation to set up a fall-back access interface. The criteria for assessing the quality APIs are unknown at present. The European Commission is planning to set up a forum of market experts, which will help supervisory authorities to apply the uniform API quality criteria. Probably, in addition to the quality API parameters the requirements encouraging ASPSPs to develop their APIs according to the European API standardization initiatives will also be included.

The Berlin Group is planning to continue developing the functionality of API Specifications. This may be done by extending the possibilities of core or extended services. The latter may be developed within a smaller group of ASPSPs (e.g. at country level). It is likely that those changes will facilitate the use of the Berlin Group API Specifications in the provision of these services: 1) initiation of bulk payments; 2) initiation of deferred date payments; 3) initiation of standing orders, etc.

In November 2017, SEPA instant credit transfers were launched in EU. It is expected that in 2–3 years the majority of the EU banks will be ready for instant payments. Three largest banks of Lithuania (Luminor Bank, SEB bankas and Swedbank) signed with the Bank of Lithuania the Memorandum on the implementation of the instant payments service. By this Memorandum, the banks committed to ensure, no later than by autumn of 2019, a possibility for their clients both to receive and to make instant payments.

A possibility to initiate instant payments through TPPs will address the so-called problem of the merchant’s guarantee. It is important for a merchant to know whether goods or services selected at the time of purchase are already paid up, because this allows managing business risks before goods are dispatched or services are provided. The API Standard Working Group has identified that at present merchants receive from banks the final confirmation of the executed payment through ‘Bank Link’ services in different time, i.e. the bank’s response can vary from several seconds to several minutes. This issue is addressed by merchants differently. Some merchants wait for a final answer from the bank delaying their business processes, while others take on the risk of possibly revoked payment or even purchase the guarantee from third parties. This problem will cease to exist once instant payments are introduced, because the response about the (un)successful payment will be received in a few seconds.

Initially, the API ecosystem relies on already developed means of authentication of PSUs. Currently, such means are usually directly or indirectly managed by ASPSPs, while TPPs can hardly influence the process of authentication. This is effective in the case of single transactions. Nevertheless, as the relationship between PSUs and TPPs becomes continuous, the authentication of PSUs can lose its effectiveness, for example, if the process is duplicated in the environments of ASPSPs and TPPs. In addition, due to means of authentication of PSUs managed by ASPSPs, at present TPPs have no real possibilities to help ASPSPs realise the SCA exemptions. The API Standard Working Group has identified and discussed in detail this issue, but has failed to arrive at its quick solution. To a certain extent the resolution of this issue could be facilitated by new authentication procedures providing for the formal role and responsibilities for all parties to a transaction: ASPSPs, TPPs and PSUs.

Annex 1

API STANDARD WORKING GROUP MEMBERS

UAB Argentum Mobile

UAB Banking Cluster LT

UAB Baltic Amber Solutions

Danske Bank A/S Lithuanian Branch

UAB Elektroninių mokėjimų agentūra

UAB Etronika

Ministry of Finance of the Republic of Lithuania

UAB Forbis

Lithuanian Central Credit Union

Bank of Lithuania

Association of Lithuanian Banks

Association ‘Lithuanian Credit’

AB Lietuvos paštas

Luminor Bank AB

UAB Medicinos bankas

Association of Payment and Electronic Money Institutions

Mokėjimo terminalų sistemos, UAB

UAB Neo Finance

UAB OPAY solutions

Paysera LT, UAB

AB SEB bankas

Swedbank, AB

AB Šiaulių bankas

UAB WoraPay

Annex 2

REGULATIONS OF THE API STANDARD WORKING GROUP

CHAPTER I
GENERAL PROVISIONS

1. These Regulations define the functions, composition and work procedure of the API Standard Working Group (hereinafter – the Working Group).

2. The Working Group has been formed taking account of the aim expressed by the payment market participants to work out the agreed position on the application programming interface (hereinafter – the API) standard in Lithuania.

3. According to provisions of the Payment Services Directive (EU) 2015/2366 each online account servicing payment service provider must ensure at least one secure API interface. By formulating the agreed position on the API standard in Lithuania the Working Group will contribute to the development of the payment market and to increasing the attractiveness of payment accounts available in Lithuania.

CHAPTER II
FUNCTIONS

4. By 31 October 2017, the Working Group shall prepare a Report on the API Standard in Lithuania (hereinafter – the Report) and submit it to the Bank of Lithuania, the Association of Payment and Electronic Money Institutions and the Association of Lithuanian Banks.

5. In preparing the Report the Working Group shall:

5.1. follow the API technical requirements established by the European Commission;

5.2. take account of the recommendations of the Euro Retail Payments Board (ERPB) for the API;

5.3. consider the API needs of the account servicing payment service providers, payment initiation service providers and account information service providers;

5.4. assess, as far as possible, the needs of the payment initiation service users and account information service users;

5.5. assess the API standardization initiatives being implemented in the European Union (e.g. CAPS, the Berlin Group, etc.) and their compliance with the needs of providers and users of payment services;

5.6. where appropriate, consult IT, personal data protection experts, public sector institutions, enterprises and organisations representing enterprises and consumers.

6. Due to objective reasons, the Chair of the Working Group has the right to extend the Report preparation deadline, but for not more than two months. After submission of the Report activities of the Working Group shall be terminated.

7. The Working Group shall not prepare the intellectual content protected by copyrights. The entity delegating its member shall concurrently confirm that the contribution of its member to the activities of the Working Group is not and will not be protected by copyrights.

CHAPTER III
COMPOSITION OF THE WORKING GROUP

8. The Working Group shall consist of the Chair and members of the Working Group.

9. The members may be representatives delegated by:

9.1. payment service providers that provide payment services in Lithuania;

9.2. organisations representing payment service providers;

9.3. the Ministry of Finance of the Republic of Lithuania;

9.4. the Bank of Lithuania;

9.5. enterprises developing and/or providing IT solutions to payment service providers in Lithuania.

10. Maximum number of members – 25.

11. Institutions referred to in paragraph 9 of these Regulations that delegate their member shall notify the Bank of Lithuania by e-mail: PSD2@lb.lt. The Bank of Lithuania shall approve the member

delectated by the institution, provided that the total number of the Working Group members does not exceed the number specified in paragraph 10 of these Regulations. The institution shall be considered to be participating in the activities of the Working Group only when the institution receives a positive approval from the Bank of Lithuania by e-mail.

12. The institution shall have the right to change the Working Group member delegated by it, by notifying the Bank of Lithuania by e-mail: PSD2@lb.lt. The institution's member shall be considered to be changed only when the institution receives a positive approval from the Bank of Lithuania by e-mail.

13. The Chair of the Working Group shall have the right to cancel the membership of a member who misses three Group's meetings in a row. The Bank of Lithuania shall notify the relevant institution of the cancellation by e-mail.

14. Other interested parties may also participate in the activities of the Working Group as observers. For that purpose they have to approach the Bank of Lithuania by e-mail: PSD2@lb.lt. A decision on the observer's participation in the activities of the Working Group shall be made by the Chair of the Working Group taking account of validity of the participation interest of the interested party and practical organisation of activities of the Working Group (e.g. number of seats in the conference room). The decision of the Chair of the Working Group to allow or refuse the interested party's participation as observer may be changed by the Working Group members by voting at the meeting. Only having received a positive approval of the Chair of the Working Group by e-mail, the interested party shall be considered to be participating as observer in the activities of the Working Group.

15. The Chair of the Working Group shall be the member of the Working Group delegated by the Bank of Lithuania.

CHAPTER IV
PROCEDURE OF WORK

16. The work of the Working Group shall be arranged by the Chair of the Working Group.

17. The form of work – a meeting, which can also take place by electronic means, i.e. issues may be deliberated and voting can take place by e-mail or teleconferencing.

18. The time and draft agenda of the meeting shall be approved by the Chair of the Working Group. Members of the Working Group shall be notified of the meeting and draft agenda no later than five working days before the meeting date. Material to be discusses at the meeting shall be submitted to the Working Group members no later than two working days prior to the day of the meeting. Meetings shall take place in the premises of the Bank of Lithuania.

19. Each member of the Working Group, having agreed with the Chair of the Working Group on the issue of practical arrangements of the Working Group's activities, can invite to the meeting up to two persons from the institution represented by him.

20. A meeting shall be valid if attended by more than a half of the Working Group members, including the Chair of the Working Group.

21. Decisions of the Working Group during meetings shall be passed by a 2/3 majority vote of the Working Group members attending the meeting. The minority opinion shall be objectively reflected in the minutes and report of the meeting.

22. During the meeting, taking account the observations and proposals received from the Working Group members, the agenda of the meeting and the minutes of the previous meeting shall be approved.

23. The Working Group shall publish the agendas, minutes and report of the meetings on the internet website of the Bank of Lithuania.

24. In the event of uncertainty regarding any aspect of activities of the Working Group which is not contemplated in these Regulations a decision on further actions shall be taken by the member of the Board of the Bank of Lithuania who is in charge of the retail payments area.