Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e. V.
Bundesverband deutscher Banken e. V.
Bundesverband Öffentlicher Banken Deutschlands e. V.
Deutscher Sparkassen- und Giroverband e. V.
Verband deutscher Pfandbriefbanken e. V.

Die Deutsche
Kreditwirtschaft

White Paper

Requirements for a data interface for third-party services

Final Version

A. Background

Under the revised European Payment Services Directive (PSD2), so-called third-party providers ("TPPs") will be able to gain access to banking services. Article 98 of the directive states that technical authentication and communication standards should be developed for this purpose.

The German Banking Industry Committee (GBIC) is in a position to support this process as a result of the experience it has gained in the standardisation of banking interfaces. GBIC has already published various interface standards for retail and corporate banking, some of which were developed in cooperation with French banks, and which are used in France, Germany and Switzerland.

B. Procedure

GBIC proposes at least a two-stage procedure for developing a PSD2-compliant interface for TPPs. The first step should be to define a new PSP interface, which should then be discussed, agreed on and adopted by all market participants. Consultation is necessary because the interests of the various market participants are currently too diverse to be able to make any concrete proposals as things stand. For this reason, it is particularly important to ensure that the process of defining the interface is transparent to all parties involved.

Once agreement has been reached on the fundamental requirements and a basic framework, the second step should be to work out concrete technical specifications.

C. Requirements for a data interface for third-party services

GBIC sets out below what it considers to be the key requirements, broken down into the following areas:

- organisational procedures
- functional (banking) aspects
- technical processing
- authentication and authorisation

C.1 Requirements regarding organisational procedures

O1	Technical communication should take place through a single interface, which should be standardised throughout Europe and be able to deal with all third-party services and application scenarios. Banks cannot reasonably be expected to support different interfaces for different third-party services; nor can TPPs be expected to implement different bank access solutions for different member states. In addition to this uniform TPP data interface, banks must also be able to define and use their own interfaces, e.g. for proprietary services rendered to their own clients.
O2	The interface should be defined in a transparent process with the involvement of all affected market participants (TPPs, payment services providers – "PSPs"). Any proprietary specifications by third parties (such as BSI or ENI-SA) might lead to a situation where requirements have to be complied with which are not in line with market needs. GBIC believes the current New Work Item Proposal submitted by ISO/TC68/SC 2 would be suitable for this purpose.
O3	A neutral, centrally-appointed entity (e.g. ISO, CEN or ETSI) should be responsible for interface governance, i.e. for maintaining and refining the interface. Users (TPPs and banks) should be able to define new requirements for the interface using a standardised change request procedure. Such requests should then be handled in a transparent process.

O4	The interface should only be accessible to authorised entities (i.e. approved TPPs), which should have to authenticate their identity in each dialogue or service request.
O5	A formal process should be established with a neutral entity for registering and licensing third-party services. This process should be transparent for all parties involved, setting out clearly-defined criteria as to which requirements, including security requirements, need to be fulfilled for registration or licensing. All registered participating and licensed third-party services should be listed in a pan-European registration infrastructure. It would be impractical to require all European banks to access a separate register for each country. ASPSPs should also be able to take on the role of a third-party provider if necessary. Given the rules and regulations banks already applicable to banks, it may be assumed that all prerequisites are met. A certificate-based approach ("provider ID") is recommended for the technical authentication of third-party providers. The certificates should be issued by a trusted certificate infrastructure, such as one based on TSLs (Trust-service Status Lists). Payment services providers need to be able to rely on the fact that a user logging into the interface using a certificate is in fact an approved TPP pursuant to PSD2. This will involve, among other things, checking signed certificates online or with the help of blacklists and establishing a private key infrastructure based on trust centres. Authorisation to access the account will also have to be checked ex ante if necessary. It should be possible to operate trust centres without contractual arrangements in place between ASPSPs and PSPs. Policies also need to be established for the following: updates, service level (availability), relicensing, delicensing. Depending on legal requirements relating to third parties (e.g. data protection), approval processes / declarations by PSPs would need to be defined.
O6	A central list of all banks together with an address (IP address, URL) is needed so that TPPs can contact them. Alternatively, depending on the design of the interface, this information could be passed on to the TPP by the client.

O7	As part of the registration process (see O5), TPPs will receive a unique provider ID that proves their status as a PSD2-compliant provider and which they can use to authenticate themselves vis-à-vis European PSPs. It will be up to the PSP to check as part of its own risk management processes that the certificate is valid and has not been revoked.
O8	From a structural perspective, the interface should consist of separate layers which are independent of one another both functionally and in terms of the role model. For example, the model to be used might look like this: 1. A transport layer defines technical processing and hence fundamental communication (establishing a connection, service request/response, error logging, security procedures, etc.). 2. A security layer contains the procedures used for authentication, authorisation, and confidentiality. This layer also includes management functions for authentication instruments used by clients in direct communication between client and bank, and which are therefore outside the scope of the new interface. 3. An application layer is used to transport functional data for the bank. The purpose of this is to prevent any changes in bank data (or definitions of new banking transactions) from impacting the other layers. 4. A presentation layer is maintained by the TPP, i.e. it would define the manner in which data are displayed on the client's device.
O9	It should be possible to limit the functionality available through the interface to the legal minimum. For instance, the exception mentioned in recital 51a – the application of less strict security requirements for low-risk payments (such as POS-based micro-payments) – should not be defined as a general rule. At present, this is an individual decision taken by each bank on the basis of corresponding risk parameters. At the same time, the interface should be structured in a way that facilitates functional extensions by each bank: this would enable the interface to accommodate any future additions to the PSD. The interface's technical architecture must not impede functionality, nor require substantial investment should new functions be added.
O10	Account information service: based on their risk management assessment and a contractual agreement with the client, banks may offer read-only access to accounts without strong authentication.

O11	Payment coverage enquiry service/payment instrument issuers (third-party card issuers): to what extent should account holders be informed about enquiries? Account holders will be informed only about the time of the enquiry, the amount the enquiry concerned, the ASPSP's reply and the identity of the PIISP. The exact nature of replies to PIIs needs to be clarified. The provision of information about the existence of the client and the account should be avoided.
O12	Uniqueness of the interface Interface specifications should be sufficiently strict to prevent any ambiguity or individual interpretation. Likewise, technical parameters and protocols should be sufficiently unique to allow TPPs to establish a connection to a PSP and to use permitted services simply on the basis of its provider ID and the relevant address (e.g. an URL).
O13	Version handling The interface should be designed in a manner that allows for version handling at a protocol level: this means that communications using different versions should be supported on the basis of clearly-defined version information within the protocol. Moreover, version-neutral access should be provided (e.g. by way of a special XML namespace), allowing access to all standardised and approved protocol versions. This will ensure error-free communication between any TPP and any bank.

C.2 Functional requirements for banks

F1	Existing standards (ISO 20022, SEPA pain, camt) should be used for transmitting functional banking data. Where necessary, specific data allocation guidelines will need to be developed to ensure that third-party services only receive the data they require.
F2	The interface should include an authorisation procedure to control the types of transaction permitted for use by a third-party service. For instance, it needs to be ensured that payment initiation services cannot retrieve any information about account movements.
F3	There should be only one or several pre-defined data exchange formats for each service area: for example, a payment initiation service should only be allocated pre-defined payment formats, while only data exchange formats for account information should be linked with an account information

	service.
F4	The interface protocol should provide options for the transmission of functional banking information (IBAN, BIC) outside standardised formats in order, for example, to obtain routing information without having to read the entire banking format.
F5	The interface should permit PSPs to communicate the type and scope of the services available to third-party services, as well as the parameters of the respective service, to the third-party service – e.g. when establishing the dialogue. This would enable the third-party service to consider such information for communication purposes[1].
F6	Account-servicing banks should be permitted to set up general blacklists for clients who do not wish to communicate via TPPs.

C.3 Requirements for technical processing

T1	The interface should be based on commonly-used internet standards (such as XML, XML Schema, XML Signature, Web Services, JSON or REST-API).
T2	The interface should support service-oriented as well as dialogue-oriented modes of operation: • In a service-oriented mode (such as payment initiation services), a service request may be submitted within a request/response cycle. Service-oriented mode requires the prior exchange of technical and functional requirements, since it is impossible to exchange such information during the process. • In dialogue-oriented mode, specific parameters may be negotiated for this dialogue as part of an initialisation process. These parameters will then apply to a service request submitted during the dialogue. Account information services are an example of dialogue-oriented services.
T3	Dialogue-oriented mode should support the exchange of interface properties via parameters. This will allow the provision of different services to TPPs depending on their respective provider ID.

[1] For instance, a PSP should be able to inform an account information service in advance of how many previous days' account movement information is available.

T4	The interface's operational security needs to be ensured: this means that TPPs need to be able to clearly recognise, based on protocol behaviour, whether or not a service request has been executed. Moreover, in the event of a rejection, functional information should be provided as to how the error can be remedied. In particular, it should be evident whether or not a rejected service request may be resubmitted without change.
T5	Resubmission checks Where a service request is resubmitted again, this should be recognisable at the protocol level in order to prevent multiple executions.
T6	Fragmentation Responses to service requests such as account information services may be several megabytes in size. It therefore needs to be possible at protocol level to transmit response messages in defined parts.
T7	Error handling The interface protocol should handle errors transparently. Unique types of error (or error classes) should be defined, allowing third parties to trigger automatic error-handling routines without having to analyse error response texts. Error classes such as "information", "warning" or "error" should facilitate initial analyses by third parties.
T8	The technical connection of TPPs for communication purposes will be via internet protocols.

C.4 Security requirements (authentication and authorisation)

S1	The security and/or authentication method should be transparent for the interface: the interface format specification should not oblige interface users to employ a specific type of authentication. The purpose of this requirement is to ensure that the interface is as independent as possible of the authentication procedures used by different banks. Authentication data will be evaluated in upstream or downstream systems, thus allowing the use of the same interface regardless of the diverse authentication procedures used by various PSPs. It needs to be ensured that TPPs do not obtain any information regarding

	users' identification data for their bank. Such data needs to be passed through without the TPP being able to view and/or store it.
S2	Misuse of a PSU's static personalised access data (PSCs such as static passwords) or biometric data should be rendered impossible. The EBA should prescribe innovative solutions which do not require clients to disclose their PSCs to third parties.
S3	Given that primary liability lies with ASPSPs, PSPs should only be permitted to use ASPSPs' own authentication procedures. The use of a PSP's existing authentication procedures should only be allowed if these procedures are already available at the ASPSP. Exception: if a bank decides to discontinue offering a certain procedure in online banking because, for instance, it no longer fulfils security requirements, this may lead to a transitional phase during which the authentication procedures in online banking and for the PSD2 interface are not the same.
S4	The interface protocol should be able to support both single-step and two-step request/response procedures. For example, a single-step procedure would be conceivable for an account information service that submits a specific request (including provider authentication), receiving the requested data in response. An example of a two-step procedure is a payment initiation service with a given minimum risk class, where a confirmation of the data contained in the payment order submitted is required (a "challenge") and may lead to a context-sensitive one-time password.
S5	Security procedures need to be described in a sufficiently abstract and encapsulated manner to allow a description through unique identifiers (or profiles, where applicable). Such identifiers would be used to clearly identify a security procedure (and the associated processes) for both partners using the interface. For example, profile names such as "SEC1", "SEC2", etc. might be used to summarise different signature, padding, or hash procedures. The TPP and the bank would then negotiate a suitable procedure on the basis of profile names only, which would help reduce the complexity of the interface.
S6	To ensure data confidentiality, a standard encryption method (such as TLS) using up-to-date encryption mechanisms should be used for data encryption between the TPP and a PSP.