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

German Banking Industry Committee

Answers to the

EBA Discussion Paper on future Draft Regulatory Technical Standards on strong customer authentication and secure communication under the revised Payment Services Directive (PSD2) (EBA/DP/2015/03)

8 February 2016

Introduction:

The German Banking Industry Committee (GBIC) is the joint committee operated by the central associations of the German banking industry. These associations are the Bundesverband der Deutschen Volksbanken und Raiffeisenbanken (BVR), for the cooperative banks, the Bundesverband deutscher Banken (BdB), for the private commercial banks, the Bundesverband Öffentlicher Banken Deutschlands (VÖB), for the public sector banks, the Deutscher Sparkassen- und Giroverband (DSGV), for the savings banks finance group, and the Verband deutscher Pfandbriefbanken (vdp), for the Pfandbrief banks. Collectively they represent more than 1,700 banks.

The German Banking Industry Committee welcomes the EBA Discussion Paper and the opportunity offered to provide feedback on the future draft Regulatory Technical Standards (RTS) on Strong Customer Authentication (SCA) and Secure Communication under PSD2. Please find enclosed the German Banking Industry Committee's response to the EBA discussion paper.

Summary and main concerns:

1) Concerning PSD 2 and also the EBA discussion paper, different parts of the payment chain are handled independently from each other, i.e. requirements for one part are formulated without considering the other parts of the chain. But in the interests of the security of payments, it is important to consider always the complete chain (authentication of the customer, communication with the ASPSP (directly or with the involvement of a third party), processing of a transaction by the ASPSP) in its entirety. Security requirements and standards should therefore always be defined with the complete payment chain in mind, as is already the case in the SecurePay-Recommendations and the corresponding EBA guidelines on the security of internet payments.

2) All requirements concerning strong customer authentication should apply to all service providers (TPP and ASPSP) to ensure a level playing field for all market participants.

3) Customer convenience is a major topic which has to be respected by any solutions for implementing strong customer authentication.

4) For the implementation of strong customer authentication the ASPSP has to decide based on its own risk assessment which solutions are acceptable concerning questions like the form factor of the possession element (physical or data), usage of behaviour-based characteristics as the inherence element, independence of the authentication elements, possible exemptions to the application of strong customer authentication, etc.

5) Static personalised security credentials (PSC like static passwords) or biometric data of any payment service user (PSU) should not be discriminated. The EBA should prescribe innovative solutions which do not require PSU to share their PSC with any other party.

6) Only one single/unique, non-ambiguous interface should exist to address ASPSP and for communication purposes between third parties and ASPSP. This interface should be standardised throughout Europe. It should be applied in a uniform manner to any third-party services and application scenarios. The interface definition should be defined in a transparent process carried out by the market participants involved. The standards should be usable by any participating provider free of charge and should be free of any rights of any other parties.

7) All registered and licensed third-party services should be listed in a central, uniform, European-wide register. Identification of third parties should be reliable enough to allow a liability shift to the third parties in the event of security incidents.

8) For all communication between an ASPSP and a AISP / PISP, the AISP / PISP needs to authenticate itself in a secure and reliable way. This authentication should be based on certificates containing information about the identity of the third party and information about its business role (i.e. AIS, PIS and/or PIIS provider). The certificates should be issued within a trustworthy public key infrastructure governed by a policy defined by the EBA. These certificates should only be given to registered and licensed third party providers. The certificate of a third party provider should be revoked immediately if the third party loses its registration for any reason.

Detailed answers to the questions of the EBA discussion paper:

GBIC's objective is to provide input concerning principles to be covered by the RTS that should address the challenges introduced by PSD2. The aim is to ensure a level playing field with corresponding responsibilities and liabilities for all stakeholders in the payment value chain.

4.1 Considerations prior to developing the requirements on strong customer authentication

1. With respect to Article 97(1) (c), are there any additional examples of transactions or actions implying a risk of payment fraud or other abuses that would need to be considered for the RTS? If so, please give details and explain the risks involved.

Response:

The examples referred to in item 27 iii of the discussion paper are sufficient. These examples are actions related to the activation and deactivation of payment functionalities, the amendment of trusted beneficiaries ("white lists") - or blocked beneficiaries ("black-lists"), the setting of limits or changing PSU data.

2. Which examples of possession elements do you consider as appropriate to be used in the context of strong customer authentication, must these have a physical form or can they be data? If so, can you provide details on how it can be ensured that these data can only be controlled by the PSU?

Response:

Examples of possession elements are already sufficiently described in the EBA guidelines on the security of internet payments under the definition of strong customer authentication (EBA/GL/2014/12, Title I – Scope and Definitions, item 12).

Basically, the possession element is supposed to have physical form. However, the ASPSP may decide based on its own risk assessment to accept data as a possession element.

Examples of a possession element being data are (a) software tokens, which are physically secured or (b) data securely combined with a physical element. In contrast, data stored in "hardened applications" are considered as examples of a physical form. Hardening means that the application includes security mechanisms against malware attacks. Hardening ensures that these data can only be controlled by the PSU.

For any regulation on the usability of possession elements it has to be taken into account that strong competitive constraints exist within the financial sector. For this reason, it is important to establish a level playing field in Europe for all ASPSP and other participating parties. In addition, any regulation of this topic must not prohibit usable and convenient customer products.

3. Do you consider that in the context of "inherence" elements, behaviour-based characteristics are appropriate to be used in the context of strong customer authentication? If so, can you specify under which conditions?

Response:

Regarding this topic the term "behaviour-based characteristics" is understood to mean biometric characteristics of the PSU. Behaviour-based characteristics are not understood to be the transaction flow behaviour of the PSU.

Behaviour-based characteristics are regarded as an appropriate "inherence" element if the method provides an appropriate security level.

GBIC suggests that ASPSPs should decide based on their own risk assessment whether to accept behaviour-based characteristics as a factor of strong customer authentication.

4. Which challenges do you identify for fulfilling the objectives of strong customer authentication with respect to the independence of the authentication elements used (e.g. for mobile devices)?

Response:

As already cited in point 18 of the rationales of the EBA DP, customer convenience is a major topic which has to be respected by any solutions given to customers. For example, customers expect to be able to order and to pay with the same device.

Independence of the authentication elements need NOT necessarily be achieved by physically separated devices. Logical channel separation may also be used to achieve the independence of the authentication elements. For mobile devices this can be achieved, for example, if the entry of the password and the generation of the transaction code are done by different apps which both exist on the same mobile device.

The ASPSP has to decide based on its own risk assessment which solutions are accepted to assure the independence of the authentication elements.

5. Which challenges do you identify for fulfilling the objectives of strong customer authentication with respect to dynamic linking?

Response:

The following aspects concerning dynamic linking should be taken into account:

(a) Dynamic linking has to provide confirmation of the intention of the PSU to perform exactly the given transaction.

(b) The process of dynamic linking must be comprehensible and reliable for the PSU so that the PSU is able to identify/confirm the transaction data linked to the dynamic code.

(c) The dynamic linking solution must not restrict the convenience of the PSU.

(d) It is expected that all requirements concerning the strong customer authentication of the PSU must apply to all service providers to ensure a level playing field for all market participants.

6. In your view, which solutions for mobile devices fulfil both the objective of independence and dynamic linking already today?

Response:

As already stated in question 4 solutions based on a logical separation of the password entry and the generation of the transaction code by different apps on the same mobile device already fulfil both the objective of independence and dynamic linking.

Solutions based on a special device like a dynamic transaction code (TAN, Transaction Authentication Number) generator implemented as a separated device with a second element already fulfil both the objective of independence and dynamic linking.

4.2 The exemptions to the application of strong customer authentication

7. Do you consider the clarifications suggested regarding the potential exemptions to strong customer authentication, to be useful?

Response:

The suggested clarification regarding the potential exemptions to strong customer authentication is useful. But it should not be taken as an exhaustive list.

Note on 42. B.: The establishment or amendment of an element of a white list requires strong customer authentication.

For the applicability of 42. D.: the detailed criteria should be defined by the ASPSP based on its own risk assessment.

8. Are there any other factors the EBA should consider when deciding on the exemptions applicable to the forthcoming regulatory technical standards?

Response:

Read-only access to account information could be offered by the ASPSP without strong customer authentication based on the risk assessment of the ASPSP and agreement between ASPSP and PSU.

9. Are there any other criteria or circumstances which the EBA should consider with respect to transaction risks analysis as a complement or alternative to the criteria identified in paragraph 45?

Response:

The precise criteria to be considered by an ASPSP for the evaluation of the risk of transactions have to be decided by the ASPSP based on its own risk assessment.

The RTS should only – if at all – include examples of such criteria, but not a comprehensive list. Future innovations based on new criteria not known today must be possible.

4.3 The protection of the payment service users' personalised security credentials

10. Do you consider the clarification suggested regarding the protection of users personalised security credentials to be useful?

Response:

The clarifications are useful but by no means exhaustive. There are technical solutions (e.g. OAuth[1], SAML[2], 3DSecure) to ensure that customers need not share the PSC with AIS/PIS providers.

Regarding 51. B.: It should be possible for the PSU to store its PSC within a mobile device which does not necessarily contain a secure element.

Regarding 51. E.: The habit of sharing PSCs increases the risk that a PSU may give its PSC to non-registered third parties or fraudsters.

11. What other risks with regard to the protection of users' personalised security credentials do you identify?

Response:

The access and usage of the PSC by PIS and AIS providers must be clarified with regard to PSD II article 66 and 67. It must be ensured that the PSC is only accessible by the PSU and the issuer. For example, it should be clarified that PIS and AIS providers should not have more information about the PSC than the issuer itself (i.e. keys, passwords should not be visible to PIS or AIS since these are also not known by the issuer).

The introduction of third parties into the payment chain increases the risk situation for the affected banks and for the financial sector in general. Compromise of third-party systems and processes, fraudulent third-party provider and insider attacks at third parties are possible. By attacking a single PIS or AIS provider, the probability of attacks on accounts of many different ASPSP will increase substantially (risk of concentration).

Furthermore it has to be taken into account that if AIS and PIS providers do not respect the requirement that the PSC are only accessible to the issuer and the

[1] The OAuth 2.0 Authorization Framework, Internet Engineering Task Force (IETF), Request for Comments 6749, Oct 2012

[2] Security Assertion Markup Language

user, there is a potential risk that the PSC may be reused for other purposes not explicitly allowed in PSD II and requested by the PSU.

12. Have you identified innovative solutions for the enrolment process that the EBA should consider which guarantee the confidentiality, integrity and secure transmission (e.g. physical or electronic delivery) of the users' personalised security credentials?

Response:

For the full life cycle of the PSC all processes should be performed by the ASPSP using secure processes.

13. Can you identify alternatives to certification or evaluation by third parties of technical components or devices hosting payment solutions, to ensure that communication channels and technical components hosting, providing access to or transmitting the personalised security credential are sufficiently resistant to tampering and unauthorized access?

Response:

There are no available alternatives for AIS/PIS providers. Any AIS/PIS solution should be certified and evaluated by third parties along the lines of existing GBIC and EMVCo approval processes. ASPSPs are already regulated and therefore alternatives to evaluation and certification like internal assessments exist.

14. Can you indicate the segment of the payment chain in which risks to the confidentiality, integrity of users' personalised security credentials are most likely to occur at present and in the foreseeable future?

Response:

If PSC are given to third parties (PIS-, AIS-providers), the transmission to the third party and the storage/usage by the third party will increase the risk to the confidentiality and integrity of the PSC.

If in future a PSU is allowed to enter its PSC on internet pages not belonging to the ASPSP, the risk will increase substantially that a PSU may also enter its PSC on fraudulent pages of a fraudulent provider. All efforts of the ASPSP to sensitize its customer to the need for secure handling of its PSC would be foiled.

4.4 Considerations prior to developing the requirements on common and secure open standards of communication

15. For each of the topics identified under paragraph 63 above (a to f), do you consider the clarifications provided to be comprehensive and suitable? If not, why not?

Response:

The topics identified under paragraph 63 are suitable but not comprehensive.

(a) In addition to AIS and PIS providers, also a PIIS provider (payment instrument issuer provider) has to be considered.

(b) It is not sufficient to define minimum requirements. A precisely defined communication protocol needs to be standardized. Ideally, interoperability of interacting market participants is achieved through standardisation. Open standards are standards that can be developed jointly by all interested market participants. As there is no international account interface standard at present and EBA will merely define generic requirements, uniform EU-wide implementation cannot be ensured. Implementation of the technical requirements will ultimately be left to the market. As a result, there is a danger that both banks and third-party service providers will have to support several different standards, which immediately raises the question of interoperability. In a worst-case scenario, there could, however, be a large number of different interfaces if banks and third-party service providers offer proprietary solutions that meet EBA's generic requirements. This would not be in the interests of either banks or third-party service providers.

(c) Access may be restricted or blocked by the ASPSP in the event of any abnormal access by frequency or volume (e.g. denial of service attacks).

(d) In case of a renewed request of an AIS the ASPSP should be able to limit the account information to the latest data which are not already delivered to the AIS.

(e) After the ASPSP has delivered the answer to a single request the ASPSP should be entitled to terminate the current access to the account.

16. For each agreed clarification suggested above on which you agree, what should they contain in your view in order to achieve an appropriate balance between harmonization, innovation while preventing too divergent practical implementations by ASPSPs of the future requirements?

Response:

The clarifications and requirements of the RTS must incorporate at least the following points:

(a) Relating to "Open and common Standard": Only a single, non-ambiguous interface should exist for technical addressing of banks and communication purposes; this interface must be standardized throughout Europe, and must be applied in a uniform manner to any third-party services and application scenarios. The interface definition must take place in a transparent process carried out by the market participants involved. The standards must be usable by any participating provider free of charge and must be free of any rights of any other parties. It needs to be clarified that besides those standards other standards in the customer-to-business relationship may coexist as long as they fulfill the requirements of secure communication. The overall governance should be addressed in the forthcoming RTS. At a minimum, a body should be assigned the task of developing and maintaining the standards, and defining and monitoring the rights and responsibilities of all stakeholders. This independent body should be made up of multi-stakeholders, and be open and transparent.

(b) Relating to "PSP Identification": A formal process must be established, by a neutral entity, for registering and licensing third-party services. This process must be transparent for all parties involved, setting out clearly-defined criteria as to which requirements must be fulfilled for registration or licensing. All registered and licensed third-party services must be listed in a central, uniform, European-wide register. Identification of third parties must be reliable enough to allow a liability shift to the third parties in the event of security incidents.

(c) Relating to "Secure communication": The authentication of the AISP/PSPP has to be secure, i. e. using certificates which have to contain the roles of the PSPs. The communication interface between PIS/AIS-provider and ASPSP must be usable regardless of which mechanisms have been used for the authentication of the PSU.

(d) Relating to "minimal functional requirements": Using parametrization should make the interface flexible and open for new scenarios. The interface must be designed in a manner that allows for version handling at a protocol level: this means that communications using different versions must be supported on the basis of clearly-defined version information within the protocol.

(e) Relating to "Security controls": The authentication of the PSU by AIS/PIS providers should be based on the authentication provided by the ASPSP using PSC issued by the ASPSP.

(f) Relating to "technical requirements": The interface should be based on commonly-used internet standards (such as XML, XML Schema, XML Signature, Web Services, TLS, JSON or REST-API). The interface protocol must provide for transparent error handling and flow control for large-sized messages. Data formats should be based on existing ISO messages (pain, pacs, camt).

(g) The authentication of AIS/PIS/PIIS providers and ASPSP could be based on qualified electronic seals as defined by eIDAS. See also 4.5. This is of course only valid for the communication between AIS/PIS providers and ASPSP. The communication with the PSU is not in the scope of this requirement.

(h) The authentication of a PSU by AIS/PIS providers should rely on the authentication of the PSU by the ASPSP without the necessity to store or access PSC of the PSU by the AIS/PIS provider. Solutions based on open and common standards already exist.

17. In your opinion, is there any standards (existing or in development) outlining aspects that could be common and open, which would be especially suitable for the purpose of ensuring secure communications as well as for the appropriate identification of PSPs taking into consideration the privacy dimension?

Response:

No, standards that comprehensively fulfil the above mentioned requirements in our view do not exist today. If the development of a new common and open standard is intended, the interface should be based on commonly used internet standards (such as XML, XML Schema, XML Signature, Web Services, TLS, JSON or REST-API).

Electronic seals in accordance with eIDAS could be used for the identification and authentication of AIS/PIS/PIIS providers and ASPSP (Clarification: Electronic seals in accordance with eIDAS cannot be used for authorization).

For the authentication of the PSU, a protocol in accordance with an open and common international industry standard such as OAuth, SAML or 3D-Secure could be used.

18. How would these requirement for common and open standards need to be designed and maintained to ensure that these are able to securely integrate other innovative business models than the one explicitly mentioned under article 66 and 67 (e.g. issuing of own credentials by the AIS/PIS)?

The following aspects concerning designing and maintaining the common and open standard should be taken into account:

(a) The specific security and/or strong customer authentication must be transparent for the interface, i.e. the interface format specification should not force the interface user to apply certain types of authentication.

(b) Security procedures must be described in a sufficiently abstract and encapsulated manner. The procedures must be referenced through unique identifiers (or profiles). The communication partners (AISP/PISP/ASPSP) have to use these identifiers to uniquely identify the security procedures (padding, hash procedure, type of signature) and processes for both partners.

(c) Interface specification must be sufficiently strict to prevent ambiguity or individual interpretation. Technical parameters and protocols must be sufficiently unique to allow a third party provider (AIS/PIS/PIIS provider) to establish a connection to an ASPSP.

(d) The interface must be designed in a manner that allows the handling of different versions. Communication using different versions of the interface must be supported on the basis of clearly defined version information within the protocol. Access to all standardized and approved versions must be supported.

(e) Only PSC issued by an ASPSP and authentication procedures of the ASPSP should be used for strong customer authentication. The ASPSP liability for unauthorized payment transactions (article 73) means the ASPSP must be responsible for the PSC and authentication procedures to be used for strong customer authentication.

4.5 Possible synergies with the regulation on electronic identification and trust services for electronic transactions in the internal market (e-IDAS)

19. Do you agree that the e-IDAS regulation could be considered as a possible solution for facilitating the strong customer authentication, protecting the confidentiality and the integrity of the payment service users' personalized security credentials as well as for common and secure open standards of communication for the purpose of identification, authentication, notification, and information? If yes, please explain how. If no, please explain why.

Response:

No, e-IDAS cannot be considered as a possible solution for facilitating the strong customer authentication. A clear distinction has to be made between the different topics "strong customer authentication", "protection of the confidentiality and integrity of the PSC" and "secure communication between participating service provider (AISP/PISP/ASPSP)".

Strong customer authentication: The electronic identification mechanisms/schemes regulated by e-IDAS are not useful for achieving strong customer authentication within payment services or account information services. As proven by some analysis in Germany, the effort and investment required for the integration in banking services is very high without any commensurate benefit. From the point of view of the PSU, the usage is not very convenient. These identification mechanisms/schemes are not open. In general it is not possible, for example, to enhance this authentication by elements which are dynamically linked to transaction data. Strong customer authentication based on "qualified trust services" like electronic signatures is possible. The decision to support/accept electronic signatures should be made only by the ASPSP based on its risk management and its business requirements. Therefore the usage of electronic signatures for strong customer authentication should not be regulated by the RTS to be prepared by EBA.

Protection of the confidentiality and integrity of the PSC: The e-IDAS regulation does not (to the best of our knowledge) contain any solution for the protection of the confidentiality of the personalised security credentials of a PSU. Only high-level requirements exist, but these do not give more details than the corresponding requirements of the PSD II.

20. Do you think in particular that the use of "qualified trust services" under e-IDAS regulation could address the risks related to the confidentiality, integrity and availability of PSCs between AIS, PIS providers and ASPSPs? If yes, please identify which services and explain how. If no, please explain why.

Response:

A clear distinction has to be made between the different topics "protection of the confidentiality and integrity of the PSC" and "secure communication between participating service provider (AISP/PISP/ASPSP)".

Protection of the confidentiality and integrity of the PSC: The e-IDAS regulation does not (to the best of our knowledge) contain any solution for the protection of the confidentiality of the personalised security credentials of a PSU. Only high-level requirements exist, but these do not give more details than the corresponding requirements of the PSD II. Therefore the usage of qualified trust services under e-IDAS regulation cannot be used to address the risks related to the confidentiality and integrity of PSCs.

Secure communication between participating service provider (AIS/PIS/ASPSP): In order to establish secure communication between an AIS/PIS provider and an ASPSP, the communication partners have to be authenticated securely by each other. As part of this authentication it has to be proven that the AIS/PIS provider has been registered/approved by EBA and that this registration/approval is still valid. In addition, the status of the provider has to be proven, i.e. whether it is an AIS provider or a PIS provider (since the services an ASPSP has to provide to a provider depend on its status). The authentication of PIS/AIS providers and ASPSP could be based on electronic seals based on qualified certificates issued by qualified trust service providers under e-IDAS regulation. For this EBA should define a policy to be implemented by the qualified trust service provider. Compliance with this policy should assure at least that (1) only PIS/AIS providers registered/approved by EBA will get a corresponding certificate, (2) a parameter contained within the certificate states the role of the certificate owner (i.e. AIS provider or PIS provider or ASPSP), (3) if the registration/approval of a PIS/AIS provider is withdrawn by EBA (or a national supervisory authority) the certificate is cancelled by EBA (or a national supervisory authority) immediately (i.e. in addition to the certificate owner also EBA (or a national supervisory authority) has got the right to cancel a certificate).

For all other services the use of qualified trust services under the e-IDAS regulation should be optional and therefore not regulated by the RTS to be prepared by EBA.

References:

The answers are based on the following documents:

- EBA Discussion Paper on future Draft Regulatory Technical Standards on strong customer authentication and secure communication under revised Payment Service Directive (PSD II), EBA/DP/2015/03, 8.12.2015

- PSD II – Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC

- White Paper „Requirements for a data interface for third-party services", German Banking Industry Committee, July 2015