German Banking Industry Committee

Die Deutsche Kreditwirtschaft

Response

to the EBA Consultation Paper on the draft Regulatory Technical Standards specifying the requirements on strong customer authentication and common and secure communication under PSD2 (EBA-CP-2016-11)

Register of Interest Representatives
Identification number in the register: 52646912360-95

Contact:
Bettina Schönfeld, Christoph Schmidt, Wulf Hartmann

Telephone: +49 30 1663 2316/2327/3140
Email: bettina.schoenfeld@bdb.de, christoph.schmidt@bdb.de, wulf.hartmann@bdb.de

Berlin, 12 October 2016

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 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 approximately 1,700 banks.

Coordinator:
Association of German Banks
Burgstraße 28 | 10178 Berlin | Germany
Telephone: +49 30 1663-0
Telefax: +49 30 1663-1399
www.die-deutsche-kreditwirtschaft.de

Summary

The German Banking Industry Committee (GBIC) welcomes the EBA consultation 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 GBIC's response to the EBA consultation paper.

Main concerns:

1) As soon as an ASPSP offers a dedicated communication interface in accordance with Article 19 to third-party PSPs, third-party PSPs should be obliged to use this interface. Bypassing this communication interface for their access to the payment accounts should no longer be feasible. For example, using screen scrapping or other existing online banking interfaces to access payment accounts, as TPPs do today, should not be compliant with PSD2 as soon as a communication interface in accordance with Article 19 is supported by the ASPSP.

2) From our point of view, it is highly important that implementation of the exemptions is optional for an ASPSP and that an ASPSP cannot be forced by other parties to process transactions without strong customer authentication. The reason for this is that the ASPSP is always liable in case of fraud. Another reason might be the request by the PSU to apply strong customer authentication for any access to its payment account without any exemptions.

3) GBIC does not agree with the content of paragraph 29 of the *Rationale* section, i.e. the exclusion of behavioural data as an inherence element of strong customer authentication. No element of strong customer authentication should be excluded a priori by the RTS as long as no relevant studies exist indicating problems with the security of that element.

4) The maximum amount of €10 stated in Article 8 (2) (d) (i) for electronic remote payment transactions without strong customer authentication have a negative impact on existing user-friendly payment products making use of the current ceiling of €30 under the so-called SecuRe Pay recommendations. Furthermore, this exemption will become useless, since less than 5% of transactions are for less than €10. Like in the SecuRe Pay recommendations and PSD1, the maximum amount should be set at (at least) €30. Above this amount, the limits should be determined by the ASPSP based on its own risk management in line with Article 95 of PSD2. The limits can be adjusted by individual agreements with the PSU taking into account the individual readiness to assume risks of the PSU.GBIC strongly supports the specification of a parameter dealing with transaction-risk analysis for the exemptions, as it allows ASPSPs to shift liability to the merchant if the risk is too high.

5) We agree with the requirement to use certificates issued by a qualified trust service provider under an eIDAS policy for mutual identification of PSPs.

However, website certificates (as stipulated in section 8 of the eIDAS Regulation 910/2014) are not the right tool for this identification. Website certificates are used to identify a website on a server and are not usually used to identify the requester side (i.e. the PSP sending a request to the ASPSP). For this reason, electronic seals issued by a qualified trust service provider should be used instead of website certificates.

6) The term "trusted execution environment" should not be used, since this term is already defined by the Global Platform initiative. Using this term as defined by Global Platform would lead to a very strong requirement that cannot be implemented with mobile devices that are currently available, or will be available within the foreseeable future, in the marketplace. Instead, a term like "segregated execution environment" should be used which could be interpreted by using known security mechanisms such as sandboxing, analysis of software to detect possible manipulations, device identity solutions and jail- break detection.

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.

Requirements of the strong customer authentication

Q1: Do you agree with the EBA's reasoning on the requirements of the strong customer authentication, and the resultant provisions proposed in Chapter 1 of the draft RTS?

Response:

GBIC welcomes most of EBA's reasoning on the requirements of the strong customer authentication. However, GBIC has some concerns about some details and limitations. GBIC suggests that the following points be taken into consideration for finalisation of the RTS.

In accordance with recital 95 of PSD2, it should be clarified that telephone banking and paper based-initiation of payment transactions are out of scope of these RTS.

It should be clarified that card-based payment transactions initiated by the PSU holding an account with an ASPSP in the EEA at a terminal situated in a country outside of PSD2 regulation are out of scope of these RTS.

GBIC does not agree with the content of paragraph 29 of the *Rationale* section, i.e. the exclusion of behavioural data as an inherence element of strong customer authentication. No element of strong customer authentication should be excluded a priori by the RTS as long as no respective studies are available indicating problems with the security of that element. The RTS should be as flexible as possible at this point in order to allow future innovation of secure and user-friendly solutions for the strong customer authentication, as is also stated in paragraph 28 of the *Rationale* section.

GBIC understands electronic remote payment transactions according to Article 97 (2) of PSD2 to be internet payments. Payments initiated at ATMs, self-service banking terminals or point-of-sale terminals are not electronic remote payment transactions, so that strong customer authentication can be performed without dynamic linking. These payments are carried out in a closed and specially secured network, i.e. even not in the "open internet". The terminals (ATMs, self-service banking terminals or point-of-sale terminals) to be used by the PSU for initiating these payments are part of this closed security infrastructure.

Article 1 (3) (e) should be limited to mechanisms that prevent, detect or block authentication fraud. In order not to prevent future innovations, GBIC proposes the following modification to the article:

"*…prevent, detect and block, to the extent possible, transactions based on compromised PSCs or authentication codes. These mechanisms ~~shall~~ may take into account, but not be limited to: i ……. and ii*."

As regards Article 1 (3) (e), the term "*final execution*" of the transaction should be used instead of "*final authorisation*", because this would be closer to the wording of PSD2.

As regards Article 2 (1), it cannot be assured by the ASPSP that the payer is made aware at all times of the amount and of the payee during the authentication procedure. Instead, the authenticity of the displayed amount and of the payee can be ensured only at the time the PSU confirms the amount and the payee. Hence (a) and (b) should be formulated as follows:

(a) *The payer is made aware ~~at all times~~ of the amount of the transaction and of the payee at the time the payer confirms the transaction.*
(b) *The authentication code … by the payer when ~~initiating~~ confirming the transaction*.

We strongly support the clarification in Article 2 (4) concerning the dynamic linking of a batch of electronic remote payment transactions to several payees.

Article 6 (1) defines the requirements related to the independence of the elements in a strict and very theoretical way. The definition should be formulated as follows: "*PSPs shall ensure independence of the elements used for the strong authentication procedures in terms of the technology used, algorithms and parameters, in order to prevent the breach of one element possibly compromising the reliability of other elements, unless a significant effort is being made by the attacker*." Otherwise a PIN and a smart card could not be used as elements of strong customer authentication, since these elements are not independent if the PIN is verified by the smart card.

The term "*trusted execution environment*" should not be used, since this term is already defined by the Global Platform initiative. Using this term as defined by Global Platform would lead to a very strong requirement that cannot be implemented with mobile devices that are currently available, or will be available within the foreseeable future, in the marketplace. Instead, a term like "*segregated execution environment*" should be used which could be interpreted by using known security mechanisms such as sandboxing, analysis of software to detect possible manipulations, device identity solutions and jailbreak detection.

Q2: In particular, in relation to the "dynamic linking" procedure, do you agree with the EBA's reasoning that the requirements should remain neutral as to when the "dynamic linking" should take place, under the conditions that the channel, mobile application, or device where the information about the amount and the payee of the transaction is displayed is independent or segregated from the channel, mobile application or device used for the initiating the payment, as foreseen in Article 2.2 of the draft RTS?

Response:

Yes, GBIC agrees with the EBA's reasoning on this question. The requirements as to when the "dynamic linking" should take place should be neutral.

Q3: In particular, in relation to the protection of authentication elements, are you aware of other threats than the ones identified in articles 3, 4 and 5 of the draft RTS against which authentication elements should be resistant?

Response:

No, in relation to the protection of the authentication elements, GBIC is not aware of any other threats.

Exemptions from application of strong customer authentication

Q4: Do you agree with the EBA's reasoning on the exemptions from the application on Article 97 on strong customer authentication and on security measures, and the resultant provisions proposed in chapter 2 of the draft RTS?

Response:

GBIC agrees with most of EBA's reasoning on the exemptions from the application of the strong customer authentication. However, we have some concerns about some details and limitations. GBIC suggests that the following points be taken into consideration for finalisation of the RTS.

For the scope of Article 8 (1) (a), the term "*sensitive payment data*" is essential. We assume (in accordance with the EBA Guidelines on the security of internet payments) that only data that could be misused for electronic remote payment transactions, e.g. phishing according to recital 96 of PSD2, is considered to be sensitive data.

The strong customer authentication of the PSU that is required according to Article 8 (1) (a) for initial access to the PSU's payment account online and after 30 calendar days has to be obtained for such access for each AISP separately.

The ASPSP and PSU may agree on a shorter timeframe than 30 calendar days where SCA should not be exempted for access by the PSU to information of its payment account online.

For technical reasons, the term "*30 calendar days*" should be used instead of "*one month*".

The exemption defined in Article 8 (2) should be an exemption in accordance with Article 97(1) of PSD2 (i.e. exemption from the need to apply strong customer authentication) and not, as stated, an exemption in accordance with Article 97 (2) of PSD2 (i.e. exemption from dynamic linking). Otherwise this exemption would be useless.

The maximum amount of €10 stated in Article 8 (2) (d) (i) for electronic remote payment transactions without strong customer authentication have a negative impact on existing user-friendly payment products making use of the current ceiling of €30 under the so-called SecuRe Pay recommendations. Furthermore, this exemption will become useless, since less than 5% of transactions are for less than €10. Like in the SecuRe Pay recommendations and PSD1, the maximum amount should be set at (at least) €30. Above this amount, the limits should be determined by the ASPSP based on its own risk management in line with Article 95 of PSD2. The limits can be adjusted by individual agreements with the PSU taking into account the individual readiness to assume risks of the PSU.

The exemptions under Article 8 (1) (b) should apply to both contactless and contact payments at a point of sale.

GBIC strongly supports the specification of an exemption dealing with transaction-risk analysis for the exemptions as proposed in Article 98 (3) (a) of PSD2. The exemption should be based on the level of risk involved.

At a broad level, the following criteria could be considered:

- Consumer device level (device type, OS/browser, malware (not) present, rooted/jailbroken, device identification, etc.).
- Connection level (direct/indirect, IP address, IP geolocation, ISP, etc.).
- Application level (language of the application, etc.).
- Payer level (profiling, user interaction profiling, click-path profiling, etc.).
- Transactional level (history, beneficiary account, amount, country, urgent/non-urgent payment, etc.).
- Payee or beneficiary level (profiling).
- Big data (data related to fraud/threat environment, customer claims).

In addition, the criteria for this transaction risk-analysis should be principles-based. It is up to the PSP to decide on the exact fraud detection capabilities based on its own risk analysis and appetite.

These exemptions based on transaction-risk analysis naturally have to be applied regardless of whether the transaction is initiated by the PSU directly or whether it is initiated by a PISP.

In addition to white lists (list of trusted beneficiaries) managed by the PSU, white lists managed by ASPSPs should also be possible. Example: white list containing all acceptors having a contract (or authorisation or license) with a given payment scheme.

Q5: Do you have any concern with the list of exemptions contained in chapter 2 of the draft RTS for the scenario that PSP's are prevented from implementing SCA on transactions that meet the criteria for the exemptions?

Response:

From our point of view, it is highly important that implementation of the exemptions is optional for an ASPSP and that an ASPSP cannot be forced by other parties to process transactions without strong customer authentication. The reason for this is that the ASPSP is always liable in case of fraud and should be free to apply any appropriate risk mitigation measures. Another reason might be the request by the PSU to apply strong customer authentication for any access to its payment account without any exemptions.

Protection of the confidentiality and the integrity of the payment service users' personalised security credentials (PSCs)

Q6: Do you agree with the EBA's reasoning on the protection of the confidentiality and the integrity of the payment service users' personalised security credentials, and the resultant provisions proposed in Chapter 3 of the draft RTS?

Response:

GBIC agrees with most of EBA's reasoning on the protection of the payment service users' personalised security credentials. However, we have some concerns about some details and limitations. GBIC suggests that the following points be taken into consideration for finalisation of the RTS.

Article 9 (1)(b) should be formulated as follows:

"*Personalised security credentials ~~data~~ as well as cryptographic material ~~related to the encryption of the personalised security credentials~~ are not stored in plain text unless they are stored either in a tamper-resistant device or in a device which is under the control of the payment service user if this device is tamper-evident*."

Article 9 (1) (c) should be formulated as follows:

"*Secret cryptographic material ~~related to the encryption of the credentials~~ is stored in ~~secure and~~ a tamper-evident ~~resistant~~ device which is under the control of the payment service user ~~and environments~~*."

Article 14 should make clear that the process for the renewal of personalised security credentials may be simplified if the existing personalised security credentials can be used to secure this process for renewing the credentials.

Common and secure open standards of communication for the purpose of identification, authentication, notification, and information

Q7: Do you agree with the EBA's reasoning on the requirements for common and secure open standards of communication for the purpose of identification, authentication, notification, and information, and the resultant provisions proposed in Chapter 4 of the draft RTS?

Response:

GBIC agrees with most of EBA's reasoning on the requirements for common and secure open standards. However, we have some concerns about some details and limitations. GBIC suggests that the following points be taken into consideration for finalisation of the RTS.

Article 19 (7) requires an ASPSP to make available a testing facility, including support, for connection and functional testing by providers. This general requirement needs to be further specified and limited in order to avoid unacceptable and unlimited burdens and costs for ASPSPs. Article 19 (7) should therefore include the following points:

- Only providers registered by national authorities are allowed to use the testing facilities and the support. For other providers, an ASPSP may deny any support.
- To use the testing facilities, a provider has to use test certificates in accordance with Article 20.
- If a group of ASPSPs supports the same communication interface, it is sufficient if this group of ASPSPs makes available only a single testing facility and centralised support.
- Any support is always provided using the language of the country of the ASPSP.
- Testing facilities and support are only available during usual working days and usual working hours determined by the ASPSP.
- Testing facilities are limited to a syntactical check of the request and the delivery of a syntactically correct answer.
- Functional testing support does not include the management of special test accounts, the delivery of test personalised security credentials and the execution of test payment transactions.

As regards Article 20, we refer to our reply to question Q9.

As regards the registration of TPPs, we assume that an ASPSP already registered by the local authority does not need any further registration if this ASPSP wants to offer services as an AISP and/or PISP. Trust service providers issuing certificates in accordance with Article 20 should issue corresponding certificates to ASPSPs without any need for further registration.

GBIC is strongly in favour of provision of a directory service containing all registered PSPs. This can be either a centralised directory service operated by a European organisation or distributed directory services operated on behalf of the national authorities. The content of the directory service should be accessible in an electronic

and automated manner through standardised request messages with standardised responses.

It must be ensured that a PSP certificate in accordance with Article 20 is revoked as soon as the PSP's registration is withdrawn for any reason by the national authority.

GBIC strongly endorses paragraph 69 a) of the *Rationale* section in the RTS. In order to clarify it, Article 19 should be enhanced by the following: As soon as an ASPSP offers a dedicated communication interface in accordance with Article 19 to third-party PSPs, third-party PSPs should be obliged to use this interface. Bypassing this communication interface for their access to the payment accounts should no longer be feasible. For example, using screen scrapping or other existing online banking interfaces to access payment accounts, as TPPs do today, should not be compliant with PSD2 as soon as a communication interface in accordance with Article 19 is supported by the ASPSP. The ASPSP will ensure that the availability of its dedicated communication interface to third-party PSPs is the same as for the already existing productive systems.

Q8: In particular, do you agree that the use of ISO 20022 elements, components or approved message definitions, if available, should be required to ensure the interoperability of different technological communication solutions implemented between PSPs for the provision of AIS, PIS or for the confirmation on the availability of funds? Do you see any particular technical constraint that would prevent the use of such industry standards?

Response:

Yes, ISO 20022 elements, components and message definitions should be used to ensure interoperability.

Q9: With regard to identification between PSPs, do you agree that website certificates issued by a qualified trust service provider under an e-IDAS policy would be suitable and allow for the use of all common types of devices (such as computers, tablets and mobile phones) for carrying out different payment services?

Response:

We agree with the requirement to use certificates that are issued by a qualified trust service provider under an eIDAS policy for mutual identification of PSPs. However, website certificates (as stipulated in section 8 of the eIDAS Regulation 910/2014) are not the right tool for this identification. Website certificates are used to identify a website on a server and are not usually used to identify the requester side (i.e. the PSP sending a request to the ASPSP). For this reason, electronic seals issued by a qualified trust service provider should be used instead of website certificates.

Electronic seals are specified and regulated in section 5 of the eIDAS Regulation 910/2014.

The specific attributes of the certificates required under Article 20 (3) are highly important. However, these attributes and the handling of these attributes are neither specified nor regulated by the eIDAS Regulation. To reach a minimum level of interoperability and a minimum level of security, requirements concerning the handling of these specific attributes need to be defined by a common policy that has to be implemented by each trust service provider issuing certificates in accordance with Article 20. Among other things, this common policy must contain rules on the revocation of PSP certificates if this PSP's registration is withdrawn by the national authority. A common policy for the handling of the specific attributes is especially important since these certificates can be used cross-border within all countries covered by PSD2.

Trust service providers issuing certificates in accordance with Article 20 should support the distribution of certificate revocation lists (CRLs) and online certificate status protocols (OCSPs) in a reliable and efficient manner. An ASPSP should be able to check on the status of a certificate in real time whenever it needs to.

These certificates are used for mutual identification of PSPs. The devices used by the PSU are of no concern regarding such mutual identification of PSPs.

Q10: With regards to the frequency with which AIS providers can request information from designated payment accounts when the payment service user is not actively requesting such information, do you agree that the proposed limit of no more than two times a day achieve an appropriate balance between allowing AISP to provide updated information to their users while not negatively impacting the availability of the ASPSP's communication interface? If not, please indicate what would be in your view the appropriate frequency and rational for such frequency?

Response:

The proposed limit of no more than two times a day for requests by an AISP where the PSU is not actively requesting such information is an appropriate balance.

Access in accordance with Article 22 (5) (b) should only be allowed if the PSU has given its explicit consent to the ASPSP that the AISP can request information online. This includes the definition of the parameters' duration (at most 30 calendar days) and frequency (at most twice a day) for such access without the active involvement of the PSU. The ASPSP has to be informed about these parameters by the AISP as part of the initial request. SCA has to be applied to the transaction defining these parameters. This allows the PSU to gain transparency and to limit access to its account (consumer protection). In addition, the PSU should have the possibility to withdraw or limit the options in Article 22 (5) (b).