Position Paper

BITKOM Position Paper towards the EBA consultation for the security of internet payments
13th November 2014

The German Association for Information Technology, Telecommunications and New Media (BITKOM) represents more than 2,200 companies in Germany. Its 1,400 direct members generate an annual turnover of more than 140 billion Euros and employ 700,000 people. They include more than 900 small and medium-sized enterprises, over 100 start-ups as well as nearly all global players. BITKOM represents providers of software and IT, telecommunications and Internet services, manufacturers of hardware and consumer electronics, as well as digital media and Internet economy businesses.

Federal Association
for Information Technology,
Telecommunications and
New Media

Albrechtstr. 10 A
10117 Berlin-Mitte
Germany
Tel.: +49.30.27576-0
Fax: +49.30.27576-400
bitkom@bitkom.org
www.bitkom.org

Contact
Steffen v. Blumröder
Head of
Banking & Financial Services
Tel.: +49.30.27576-126
s.vonblumroeder@bitkom.org

President
Prof. Dieter Kempf

Management
Dr. Bernhard Rohleder

BITKOM statement on the consultation for the security of internet payments

The pace of development in payments innovation has increased significantly with the development and increasing prevalence of the internet and more recently multi-functional smart phones. The evolution is still ongoing and any final scenario cannot be predicted. Regulatory neutrality must be respected as regards the various types of payment systems and methods. BITKOM therefore insists that any regulatory interference deemed necessary must not disrespect regulatory neutrality.

In order to release the economic and competitive potential the regulatory framework must accommodate this rapidly changing market, providing the right levels of security without stifling innovation. This is an evident challenge and can only inadequately be addressed by periodic regulatory reviews, such as foreseen in the recommendations.

BITKOM welcomes the opportunity to comment on the ECB recommendations for the security of internet payments and the following consultation questions of the EBA.

EBA Consultation Questions:

Do you prefer for the EBA guidelines

a) to enter into force, as consulted, on 1 August 2015 with the substance set out in this consultation paper, which means they would apply during a transitional period until stronger requirements enter into force at a later date under PSD 2 (i.e. a two-step approach); or

b) to anticipate these stronger PSD 2 requirements and include them in the final guidelines under PSD 1 that enter into force on 1 August 2015, the substance of which would then continue to apply under PSD 2 (i.e. a one-step approach).

Beyond that EBA has announced that the implementation date for the recommendations for the security of internet payments will be postponed by six month as the EBA is looking to set a date for the guidance to come into effect of 1 August 2015 instead of 1 February 2015.

The EBA has now posed a question to the market whether a one-step or a two-step approach would be preferred, because additional obligations expected to come into force with PSD 2 could be pre-empted and introduced in the Guidance, for implementation in August 2015. The current draft of PSD2, which is still in discussion between the EU institutions and the member states, extends strong authentication from that of USERS to strong authorization of TRANSACTIONS (Art 87).

1 Response to the consultation question in detail

The benefits of the ‘one step approach’ are very difficult to assess at the time of this consultation. The PSD2 is currently far from being finalized: the draft compromise text - current under discussions at the EU Council - will have to be finalized and then negotiated with the EU Parliament. It can be expected that especially Chapter 5 (Operation and security risks and authentication) of the PSD2 draft will be subjects to further aments and revised during the next few months.

BITKOM clearly prefers a two-step approach for the implementation of the Recommendation on the security of internet payments and strongly objects the idea of introducing the strong authentication rules of the draft PSD 2 already by 1 August 2015, which is probably 1,5 years earlier than the expected transformation of PSD 2 into national law of the Member states.

Furthermore, the strong authentication rules of PSD 2 are seen highly critical by market participants as an appropriate “one fits all” solution and are highly contested between EU institutions and Member States. The EBA should wait for the final results of the trialogue negotiations (depending on the date of coming into force of the PSD 2). A prior enactment of the strong authentication rules would also clearly leverage off the national implementation process of PSD 2 in the Member States.

It is therefore more appropriate to stay with a two-step approach from the perspective of democratic legitimation of the requirements and also because of a transitional period for the companies concerned to implement such requirements.

For the reasons outlined above, we would consider it to be ideal to await finalization of the PSD2 text and then review the SecuRe Pay Recommendations against these new requirements before issuing draft EBA guidelines and/or technical standards. At the very least, we recommend that the EBA Guidelines will enter into force on the 1st of August without introducing any additional authentication requirements to those already set forth by the SecurRe Pay Recommendations.

Regarding the consultation question, on the timing of entry into force of the EBA Guidelines and the PSD2 requirements, we would like to share the following observations.

The 'strong transaction authentication' (as introduced by the latest PSD2 compromise draft texts) is quite restrictive and its implementation requires further assessment by the PSPs: as it was not mandatory under the SecuRe Pay Recommendations on Internet Security, it needs to be more carefully analyzed and assessed by the market. Any authentication linked to a transaction has an impact on the checkout processes, which is non-trivial for payment provides and users. Moreover, the rationale for introducing this new authentication step – which was not included in the PSD2 Commission proposal or the EU Parliament Report on the PSD2 - has hardly been explained. We would recommend the EU regulators to explain the aim of the 'strong transaction authentication', e.g. what is the fraud mechanism that it intends to counter, whether the exemptions to strong customer authentication – as per the SecuRe Pay Recommendations - apply also to 'strong transaction authentication', etc.

Finally, implementation of this additional authentication requirement by payment providers will require additional technical work and product change planning, which entails additional investment of time and money vis-à-vis what already foreseen by the payment stakeholders for the entry into force of the SecuRe Pay Recommendations.

2 Strong transaction authentication: (Best practice 7.3)

BP 7.3 of the SecuRe Pay Recommendations refers to strong customer authentication potentially including "elements linking the authentication to a specific amount and payee". As mentioned above, the current draft of the Italian Presidency compromise text on the PSD2 is mandating this approach in Article 87(1a) by requiring PSPs to "*apply strong customer authentication that shall include elements dynamically linking the transaction to a specific amount and a specific payee*". While this requirement can be acceptable as a best practice – as it is in the current draft EBA guidelines – as it allows PSPs to assess how, when and in what circumstances to apply such a authentication, mandating it as a 'one size fits all' approach through the PSD2 – or in anticipation of PSD2 via the so called

one-step approach by the EBA guidelines – would be too restrictive, entailing the risk of stifling innovation.

3 General remarks on the payment security approach (Ref: Rationale/ strong customer authentication definition)

3.1 Need of a broader definition of strong authentication

We would further propose that the definition of "strong authentication" should be phrased broader than the current concept of the SecuRe Pay Recommendations and the PSD2 of a two-factor authentication. Strong customer authentication should be any authentication method allowing secure identification of the legitimate user of a specific payment instrument.

The current definition of strong customer authentication – provided by the ECB Recommendations – by equating "strong" with "two-factor" authentication, fails to include additional factors like multi-factor authentication methods which use elements such as geo-localization/real-time information/customer behavioral pattern/biometric identification technologies, etc.

As these factors are becoming increasingly relevant – especially thanks to modern technologies – ***it is advisable for security rules to allow for a broader interpretation of what is regarded being 'strong authentication'***. Current practice of risk-based anti-fraud measures should be given proper attention by policy makers. (as an example: currently available technologies allow payment service providers and merchants to closely map customers' behavior: for known users and recurring transactions – when falling within a pattern of 'normal' behavior – it should be allowed a smoother transaction experience than deployment of the two-factor authentication).

The current definition of strong customer authentication, referencing to two-factor authentication as the only authentication methods for retail payments incurs the risk to hinder innovation and technological advancement in the EU. The PSD as well as the 2nd EMD have both been designed on the basis of technical neutrality and as being open for technological improvements (see in particular considerations 7 and 8 of the 2nd EMD); the EBA guidelines should uphold these principles. **We recommend the EBA Guidelines to open the strong authentication definition for the ongoing development authentication technologies and to ensure that innovation is adequately catered for.**

3.2 Technology neutrality should underpin future-proof security policies

Technology development – especially in the digital area – happens much faster than any policy drafting or review. To prevent quick obsolesce security policies should not limit innovation: this can be achieved by catering for new security technologies. As the area of authentication has already benefited considerably from new technologies, EU policies should adequately encourage adoption of innovative developments to prevent widening the gap between EU and the most

advanced technological countries. **To adequately embrace innovation, future proof regulations should have an outcomes based approach**: i.e. quantify the security objectives whilst providing payment service providers with the flexibility on how to achieve them. Unfortunately the SecuRe Pay Recommendations fail to do so, but we would welcome adoption of the outcome based approach by the EBA Guidelines.

3.3 Consumer convenience should not be neglected

The main challenge with digital payment security is to find the right balance between a great user experience and security. In a rapidly changing payment environment this is especially tricky. However, **customer convenience is an essential element in the authentication process and merits careful consideration**. A cumbersome process is likely to lead to customer friction, which leads to avoidance strategies that frustrate the security objectives. Experience shows that customer usability is equally important in maintaining overall security, as it is in encouraging a safe use of the product and prevents abandonment of transaction or avoidance strategies. When security is successfully combined with convenience, an effective security outcome is achieved. When the two depart, product use may suffer or security may be compromised. **We recommend the EBA guidelines to acknowledge the need to reconcile convenience and security.**

3.4 Global payment security practices are not contemplated

E-commerce is a global business, so any rule that is enforced upon the industry should ideally have a global perspective. For a global business such as digital payments, fragmentation of the applicable rules undermines its full potential and reduces business opportunities. **EU policy makers should ensure security measures enforced within the EU are in line with global security practice**. This is to ensure the competitiveness of the EU digital market on the global market. **We urge the EBA guidelines to ensure consistence with global security practices to avoid creation of a "European fortress"**.

3.5 Commercial concerns with regards to strong transaction authentication

It is proven that even a soft, static password based 3D-Secure authentication leads to significant drop-off by consumers during the payment transaction. Merchants claim significant drops in payment completion conversion by –10% up to –30% in case customers have to use a static 3D-Secure password. Therefore there is a major concern that a strong customer authentication will significantly harm business even more while overall economical relevant fraud loss (not only card not present fraud) in Europe is just 3.8bps (according ECB statistics).

Strong customer authentication influences flows of instant payment methods while deferred payment methods like payment upon open invoice, payment by credit/installments are not hit during the checkout. There is a concern that merchants will push those payment methods that split merchant checkout from payment and/or SecuRe Pay will significantly unfairly disrupt the payment market dynamics in favor of a few providers/payment methods. Those deferred payment methods (e.g. Payments upon open invoice, payment by installments, payments upon delivery) also come with a credit scoring of customer or significant new consumer fraud risks like payment for a parcel without knowing exactly what is in the parcel. Credit based payment also leads to the fact that poorer customer segments will face more complex payment flows while more wealthy buyers will face less complex flows.

In case there is no risk/liability for the consumer within a payment transaction (e.g. payment provider assumes risk of fraud, insurance covering fraud or merchant fully accepts liability of risk of fraud) there should be an exception/option that no strong authentication is necessary if buyer is protected anyhow.

Furthermore, the alternative authentication measure proposed in guideline 7.1 first bullet point should be amended. As of now the concept of “white lists” inadequately favors larger and established e-commerce merchants; customers will tend to include them in the white list. Smaller merchants and new market entrants should be able to prove their trustworthiness by a certificate similar to the currently (for other purposes) used “Trusted Shop” certificate and should upon obtaining such certificate automatically be included in a general “white list”.

4 Scope of the Guidelines

There are many differences between direct debits and other payments e.g. credit transfers, e-money Transfer, etc. A credit transfer or an e-money transfer is final after issuing and execution. In the case of direct debits a mandate and not the payment itself is issued from the internet environment. If the payment is issued and executed in a second step, it is not final. After debiting the account the debtor has the right to refund the amount within a period of eight weeks.
The working group on the Pan-European use of electronic mandates for SEPA Direct Debit of the ERPB, shared by the ECB, requires proper debtor authentication, e.g. using means of strong customer authentication defined in the proposal of the EU Commission for the review of the PSD2. It is a decision of the creditor to use a proper debtor authentication. If he uses other methods, then the creditor should accept the risk of an after eight-week refund claim.

5 General remarks on the Guidelines as such

5.1 Comply or Explain and Justify

Notwithstanding our concerns with respect to higher ranking European law, the guidelines do not clearly express whether and in how far they will be binding for financial institutions. The ECB SecuRe Pay Recommendations foresee the

principle of “Comply” or “Explain and Justify”. The wording of the proposed EBA guidelines, in particular the auxiliary verb “should” which appears in most guidelines, suggests that this principle will be upheld also in the EBA guidelines.

The text of the guidelines should be amended in this respect or should at least suggest such understanding to the competent authorities addressed in the guidelines.

5.2 ECB recommendations vs. EBA guidelines

While ECB and EBA published press releases on their cooperation with respect to security of payments and the guidelines state that the “entry of force date of the guidelines will be the 1 August 2015, which constitutes an extension of six months compared to the implementation date that had been set for the SecuRe pay recommendations”, it is still unclear whether payment services providers will have to comply with the ECB recommendations as of 1 February 2015 or not. The ECB and / or the competent authorities should provide a clear statement on this.

5.3 Definitions

The terms “authentication” and “authorisation” should be given the same meaning as in the PSD (definitions and Article 54, respectively) or in PSD2 (definitions and Article 57 draft PSD2, respectively), when enacted. This would avoid confusion among market participants.