# Response of the Association of German Banks to the EBA Consultation Paper on Implementation of Guidelines on Security of Internet Payments

## Details Submitter

## **Organisation**: Association of German Banks

## **Contact**: Marcus.Nasarek@bdb.de

## General comments

Since publication of the SecuRe Pay recommendations for the security of internet payments (referred to in the following as “the SecuRe Pay recommendations”) in January 2013, there have been numerous indications that supervisors in the various countries involved proceeded very differently in some cases when it came to implementing the recommendations. This was undoubtedly also due to the fact that the binding force of the recommendations was initially based merely on a self-commitment of the supervisors involved. We therefore welcome the EBA’s initiative, as it creates a uniform, binding legal basis for national supervisors.

As the requirements have basically been known since publication of the SecuRe Pay recommendations, it has been possible to launch appropriate preliminary preparations in the course of the past 22 months. Given the scale of the requirements, this period is also needed for an analysis of the impact on security management systems and planning of any measures. Proper implementation will require a similar period, and assuming that known framework conditions apply, implementation of the guidelines by financial institutions within a period of 36 months appears realistic.

As regards the cooperation between the EBA and the ECB on IT supervision, we wish to query the relevance of the Assessment Guide for the Security of Internet Payments in connection with the EBA draft guidelines.

## Consultation questions

Our comments in reply to the consultation questions and our preference are as follows:

1. The wording of PSD2 is far from having been finalised at present and security requirement aspects in particular are still being vigorously discussed. In contrast, the SecuRe Pay recommendations have been generally understood in the meantime. Particularly in view of the time available for implementation, new aspects can scarcely be adopted from the draft PSD2 at such short notice. Moreover, it is quite likely that the PSD2 requirements will change again. If so, it must be assumed that there will be a two-step approach in any case.
2. Currently, there is no sign how the suggested tightening of requirements in the PSD will look like. The current discussions in the EU Council Working Group and the Member State and European Parliament opinion-forming processes instead point to a thorough review of the draft legislation. We therefore assume that the one-step approach is rather unlikely from a procedural point of view and that the security requirements will change again. Implementation of tighter requirements by August 2015 poses unsurmountable challenges to financial institutions, especially as interpretation and planning at technical standards level has not yet taken place.

**Preference:** **We would prefer option a)**, although this option involves numerous imponderables. What is more, PSD1 does not yet feature the legal concept of “strong customer authentication”, so that the legal background to the guidelines’ central element is missing.

With the current review of PSD2 and the present guidelines in mind, it looks like implementation would be a two-step process in any case. The reasoning behind the need for implementation before publication of PSD2 is not clear, however. On top of this, the PSD2 requirements will have a huge impact on account-holding payment institutions’ security management systems. Implementation of appropriate measures may presuppose basic new developments and involve corresponding migration. It would be difficult to manage such comprehensive adjustments with the required care and security within six months.

**We therefore propose the following new option:**

1. The risks outlined can be avoided and legal certainty achieved at the same time if guidelines take effect after publication of PSD2. In view of the experience made in handling the SecuRe Pay recommendations, a timeframe of 36 months for implementation by financial institutions appears realistic.

## Comments on the guidelines

**Specific point (1):** Page 5, “Background” section

**Rationale:** While this section refers to the SecuRe Pay recommendations, it is not clear how the documents relate to one another. Will the SecuRe Pay recommendations be replaced by the EBA guidelines or do the EBA guidelines constitute the legal background to the SecuRe Pay recommendations, so that these remain in place?

**Proposal for amendment:** We suggest **explaining** in the EBA guidelines what the relationship between the EBA and SecuRe Pay Forum documents is.

**Specific point (2):** Page 7 “Comparison between the Draft EBA guidelines and the SecuRe Pay recommendations” section

**Rationale:** The “Implementation” section of the SecuRe Pay recommendations outlines a “comply or explain” approach. This approach allows the presentation of alternative measures to achieve the same security goal. It is highly relevant in practice, as financial institutions’ security management systems reflect business-specific security architectures. Solely implementing the wording of the guidelines will lead to increased redundancy or even conflicts between security measures at financial institutions. This will not only mean higher costs – a lowering of the security level cannot be ruled out either.

**Proposal for amendment:** We suggest **including** the “comply or explain” approach in the EBA guidelines.

**Specific point (4):** Page 14, “Title I – Scope and definitions” section – Definitions

**Rationale:** The concept probably meant by the term “strong transaction authorisation” is protection of the integrity of transaction data (amount and payee) and reliable verification by the account-holding financial institution. The protection mechanism is to include payer authentication data. It is in principle conceivable that this concept could be realised by using digital signatures. Experience shows that these systems pose huge challenges to the payer, payee, payment services provider and account-holding financial institution. As has been evidenced, such systems have failed to win widespread acceptance during the past two decades of their availability (in Germany, HBCI since 1995). Realising the “what you see is what you sign” concept is also a challenge. Moreover, the description of the concept in the EBA guidelines leaves open the question of what makes transaction authorisation “strong”. Should a kind of signature mechanism be meant, then basic requirements and descriptions of the technical security features of a signature procedure are missing. On top of this, it is questionable whether linking to the transaction data on the payer’s side achieves a higher level of security.

**Proposal for amendment:** We suggest **altering** the “strong transaction authorisation” concept and adding the following definition: “Protection of transaction data integrity” – The transaction data to be authorised by the payer are displayed to the payer via a secure channel. The payer is given the possibility to check and authorise the transaction data in a direct dialogue with the account-holding financial institution.

**Specific point (5):** Page 14,“Title I – Scope and definitions” section – Definition of “Credentials“

**Rationale:** Credentials are, by definition, not “physical tools”. What is meant is probably “possession” thereof. An explanation would therefore have to reflect this, i.e. personal possession of a physical element that can be assigned clearly to one person.

**Proposal for amendment:** We suggest **altering** the definition as follows: “Credentials can also mean a physical element which unambiguously belongs to only one person.”

**Specific point (6):** Page20, guideline 7.6

**Rationale:** Although, under point ii) of the “Comparison between the Draft EBA guidelines and the SecuRe Pay recommendations” section, payment schemes are not included in the guidelines, guideline 7.6 sets a requirement for payment schemes.

**Proposal for amendment:** We suggest **deleting** guideline 7.6.

**Specific point (7):** Page 28, “Annex 1: Best practice examples” section

**Rationale:** No best practice examples are necessary at legal background level. This would be a matter for supervisors at implementation level.

**Proposal for amendment:** We suggest **deleting** this section.