SWIFT Response to the European Banking Authority discussion paper on future RTS on strong customer and secure communication under PSD2

08 February 2016

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?

SWIFT believes that possession elements can indeed be in data form. In the event that they are in data form we would, however, recommend that other means of authentication are used in combination with them and that mitigating controls are established to avoid dependence on any single form of authentication. Examples of such controls include: the restriction of data that can be used at the payment service user's (PSU) premises; the stringent control of access to the data; a requirement for a second person to approve a transaction; and limiting transactions to a maximum value based on risk.

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?

Yes, we agree that behaviour-based characteristics are appropriate and can complement inherence, knowledge, and possession elements. Anomalies in normal patterns of behaviour during the customer authentication process can be particularly helpful in identifying fraudulent activity.

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)?

The practicality or convenience of some authentication methods can lead to over-dependence on them. An example includes the use of SMS for verification by the same mobile phone that was used to make the payment. This type of over-dependency can be difficult to avoid but it should be managed as far as possible. An ideal customer authentication process would include several independent methods of authentication, used in combination with each other.

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

It is impractical to require a PSU to confirm the amount and payee for each transaction when making bulk payments. In this situation, dynamic linking should be applied to the aggregated amount, rather than to each payment amount individually.

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

Yes, the clarifications suggested are useful.

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

Yes, the clarification suggested is useful. We suggest that a common baseline of personalised security credentials should be defined and protected, but how they should be protected should be left to the discretion of the Payment Service Provider.

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

Obsolete personalised security credentials should be safely destroyed so that they cannot be reactivated and re-used.

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?

No, we cannot suggest an alternative to a third-party review that would provide the same level of assurance.

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?

We believe that the clarifications outlined in paragraph 63 are comprehensive and suitable. We would also recommend that a minimum baseline set of requirements is specified, although how they should be met should not be specified.

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 harmonisation, innovation while preventing too divergent practical implementations by ASPSPs of the future requirements?

The clarifications suggested should not be too restrictive, particularly as regards the underlying technology. This will keep costs down where systems already meet the minimum set of requirements. Specifying standards is helpful, as long as the standards are common and open, and thus do not hinder innovation.

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' personalised 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.

We agree that that e-IDAS regulation could be considered as one of the solutions for facilitating strong customer authentication, however it should not be the only solution as there may be other ways to achieve strong customer authentication.

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.

Strong Customer Authentication based on the use of (personal) credentials is key, and is well addressed by e-IDAs. Indeed, under the e-IDAS regulation, the use of electronic seals partially addresses risks related to confidentiality and the integrity of personalised security credentials, whilst the electronic signature seal creation device gives some degree of assurance on the confidentiality and accountability electronic signatures. The protection of personal credentials to ensure their validity over time is, however, equally important to consider – and is an element that is not covered the e-IDAS regulation. This element should be further addressed.

On the other hand, the e-IDAS regulation is quite specific on how technical solutions should be implemented. Our recommendation is that any further guidelines on how strong customer authentication should be achieved should be sufficiently flexible to allow the industry to develop innovative and varied solutions.

---------- END ----------