Quali-Sign Ltd

www.quali-sign.com

Comments submitted on 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

Michael Adams

28th August 2016

Question 1: 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?

Yes.

Question 2: 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 initiating the payment, as foreseen in Article 2.2 of the draft RTS.

Yes I agree.

With respect to the 'dynamic linking' procedure, where data is being re-keyed (for example, into a chip and pin card reader), it is sensible for the input data to be kept to a minimum (one time password + amount + payee). However, where data is not being re-keyed (e.g. when cryptographic signatures are used), I assume that it is acceptable for the authentication code to be generated from the whole ISO20022 payment message, not just a subset of the data.

I strongly agree with the concept of segregation. I recommend that Article 2.2b is clarified as follows "The channel, device or mobile application through which the information linking the transaction to a specific amount and a specific payee is displayed and the authentication code is generated shall be independent or segregated from the channel, device or mobile application used for initiating the electronic payment transaction."

Segregation should be deemed to have been achieved in the case where a payment instruction is transmitted to the bank and then subsequently authorised by a personal user, via a separate device or channel, before being released for processing. The device used to initiate the payment must have no ability to fraudulently manipulate the payment.

I believe it is appropriate to allow a PSU to initiate a low value payment (e.g. < Eur50) from their mobile device without segregation. This could take place either at point of sale or remotely and would allow a consumer to pay a bill via scanning a QR Code. In this situation, strong customer authentication would be mandatory. What I am suggesting is a relaxation of only the segregation rules for low value payments.

Question 3: 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?

I am not aware of other threats.

I support the notion that the PSP is ultimately responsible for auditing the quality of the strong customer authentication procedure. To achieve this, in the case where the PSP does not supply the authentication device itself, I believe it is reasonable for the PSP to mandate the use of a Qualified Signature Creation Device (QSCD) in the generation of the authentication code. According to the eIDAS regulation, it is the combination of the hardware & operating system that is certified as a QSCD, not the mobile banking (smartphone / tablet) apps themselves. However, I am concerned that a lack of availability of certified QSCD mobile devices would be a significant impediment to the establishment of innovative solutions.

Question 4: Do you agree with the EBA's reasoning on the exemptions from the application of Article 97 on strong customer authentication and on security measures, and the resultant provisions proposed in Chapter 2 of the draft RTS?

Yes.

In the case a particular payment falls within the exemption criteria and strong customer authentication is not performed, which party is liable in the event of financial loss? If it is the PSU, they should be given the option to waive the exemptions and demand that strong customer authentication is always mandatory.

Question 5: Do you have any concern with the list of exemptions contained in Chapter 2 of the draft RTS for the scenario that PSPs are prevented from implementing SCA on transactions that meet the criteria for exemption?

No, I do not have any concerns with the list of exemptions.

With respect to whether these exemptions should be mandatory on the PSP, in principle I am happy that these exemptions are not mandatory. However I have the following concern:-

Consider the case of a third party provider, who is looking to supply their customers with an innovative mobile banking app. They wish to provide a convenient user experience, without compromising on security. They are willing to implement strong customer authentication for all payments, creating the authentication codes via electronic signatures with cryptographic keys maintained within the trusted hardware / software zone of the mobile device.

If a PSP is able to mandate the use of a strong customer authentication hardware device (e.g. smartcard), supplied only by themselves, this would prevent the TPP from delivering a convenient user experience compared to the PSP's own mobile banking app, which does not require the use of a smartcard. In this case the TPP is disadvantaged and there is not a level playing field.

The TPP would not mind if:-

- The PSP mandates strong customer authentication for all payments.
- The PSP provided an API infrastructure that mandates the use of cryptographic keys only.

However the TPP would mind if the PSP mandated a specific hardware device to store the cryptographic keys (e.g. smartcard or the trusted hardware / software zone of a mobile device). The TPP must have the choice.

Question 6: 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?

I do agree with the EBIA's reasoning, however I believe that it is worth clarifying the following:-

Where a PSU uses cryptographic keys to represent the 'possession' element of strong customer authentication and corresponding certificates are issued to support these keys, in my view, these certificates must be issued to the PSU by a Certificate Authority (or Qualified Trust Service Provider). Furthermore, the PSU must be able to request that these certificates be suspended or revoked by the CA/provider and have the confidence that this would be enough to block access to their account by the PISP and AISP.

I also believe it is worth differentiating between the 'strong customer authentication' credentials used with payment initiation compared to account information requests. For payment initiation, the PSU must always be involved. However for account information requests, the PSU need not be directly involved.

Using EBICS as an example, a PSU is issued with three certificates, separate from any certificate used to establish an HTTPS connection. These are:-

1) An identification and authentication certificate. This is used with every communication to the server, including payment initiation and account information requests.
2) An encryption certificate. This is used to decrypt data (e.g. account information or payment status reports) that is downloaded from the server.
3) A bank-technical signature certificate. This is used to digitally sign data that is transmitted to the bank.

The 'identification and authentication' and the 'encryption' certificates do not convey personal authorisation. They equate to an eIDAS website certificate as opposed to an eIDAS certificate for electronic signatures. These certificates can be operated by an AISP service, for example, without the PSU's direct involvement (i.e. their physical action to unlock the corresponding private key). In the case of a mobile phone app, a background schedule could be configured by the user for the app to automatically connect to the PIS/AIS to check on the availability of new reports to download or new payments that require authorisation. The user would be required to authenticate in order to activate the background service. They could then receive a notification, rather than having to manually launch the app and check themselves.

The 'bank-technical signature key', when issued to a personal authorisation user, would correspond with an eIDAS certificate for electronic signatures. This certificate (and corresponding private key) is under the sole control of the PSU. Strong customer authentication for payment initiation cannot be performed without direct involvement of the PSU (i.e. only they can unlock the private key, with knowledge or inheritance, for example).

Question 7: 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?

Yes, I am very supportive of this approach.

Question 8: 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?

I am very supportive of the use of ISO 20022. I suggest that in order to support interoperability further, where the Common Global Implementation (CGI) initiative has endorsed a specific version of an ISO 20022 format, only this version should be utilised.

Question 9: With regards 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 ?

With regards to the identification of PISP's and AISP's, where the PISP or AISP is centrally hosting its service, I agree with the approach that the PISP or AISP must identify themselves via the use of an eIDAS website certificate issued by a qualified trust services provider (QTSP).

However where the PISP / AISP provides their customers with software (such as a mobile app) that communicates directly with the PIS/AIS, rather indirectly via a PISP/AISP hosted service, there should be alternative means to identify the provider of the software. This is on the assumption that a dedicated eIDAS website certificate would need to be procured for each installation of the software, i.e. for each mobile device.

Article 13b references "Mechanisms ensuring that the authentication software delivered to the payment services user via the internet has been digitally signed by the payment services provider;"

Perhaps this should be expanded to clarify that any software delivered to the PSU via the internet by either the PSP or PISP or AISP, must be digitally signed by the provider, using an eIDAS web site certificate, issued by a QTSP. The corresponding signature proof must be made available to the PSP/ASP, whenever a connection is established. This could then be used to identify the PISP/AISP.

Question 10: 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 rationale for such frequency.

In the case where the AISP is performing data analytics, I believe a limit of two requests per day is sufficient.

However, in the case of payment approvals, where the PSU is being asked to approve payments that have already been transmitted to the PIS (in support of segregation requirements), it would be very beneficial to the PSU for the PISP to notify them that a payment order is awaiting their approval. In this case, two requests per day would be very restrictive.