European Banking Authority (EBA)

(webform)

12. oktober 2016
Vår ref 16-1084

Public Hearing on draft RTS on strong customer authentication

Finans Norge har i samarbeid med Bits AS utarbeidet svar til det europeiske banktilsynets (EBA) forslag til regulatoriske tekniske standarder om krav til sterk kundeautentisering og felles sikkerhetskrav i henhold til det reviderte betalingsdirektivet.

Forslaget fra EBA finnes her på deres hjemmesider.
Finans Norges svar er meldt tilbake til EBA den 12. oktober 2016 på fastsatt svarskjema (web).
Spørsmålene og svarende *vedlegges* nedenfor.

Eventuelle spørsmål kan rettes til Rune Hagen i Bits AS
e-post: rune.hagen@bits.no
Mobil: 958 16 258

FINANS NORGE

Jan Digranes
direktør

Gunnar Harstad
spesialrådgiver

European Banking Authority (EBA) - Consultation Paper on the draft Regulatory Technical Standards specifying the requirements on strong customer authentication and common and secure communication under PSD2 – response from Finance Norway.

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?

Comments from Finance Norway
Finance Norway acknowledges the main aspects of EBA's reasoning. In general, we support a risk-based approach where relevant. Before giving more detailed comments to the content of the CP, Finance Norway finds it appropriate to make a concrete proposal regarding eID schemes and the reasoning behind the proposal.
eID schemes Finance Norway suggests to add a new article 7 in Chapter 1 of the RTS: *In case of use of an eID scheme falling under Regulation 910/2014 and compliant with articles 1 – 6 the eID scheme may require that the customers' PSC shall be entered directly into an interface approved by the eID scheme.* **Rationale** In Norway 83 percent of the population aged over 15 years possess eIDs/e-signatures. The eID schemes play a fundamental role for the digitization of the Norwegian society. The eID schemes allow customers to access a whole array of services offered by both public entities (e.g. national registers and tax authorities) and private entities which include secure electronic authentication and secure electronic signing. The same eIDs are by far the most commonly used method for authentication and e-signing in online banking. Therefore, the content of the RTS is not only important for PISPs, AISPs and ASPSPs but is also fundamental for maintaining the general public's trust in existing eID schemes. If this trust is broken the consequence will not only be that further digitization of the Norwegian society will be brought to a halt, but it will be a setback for the digitization already achieved. Unregulated payment initiation and account information activities in the Norwegian market have based their services on "sharing of the customers' PSC". These PSCs are, as mentioned, linked to the use of general purpose eIDs. A business model allowing customers to enter their PSC into software/hardware operated by a PISP/AISP and then in turn for the PISP/AISP to pass on these PSC into the secure environment offered by the eID scheme is clearly in infringement with the basic principle of customers' "sole control" of activation for electronic signature creation and/or eID. "Sole control" is laid down as a principle in EU-legislation on eID and e-signatures. The business model with "sharing of credentials" also seriously weakens the eID schemes' ability to carry out important fraud detection measures similar to those listed in article 1.3 (e) in the draft RTS. We would like to emphasize that the whole purpose of eID schemes is to offer private and public entities trust in the authentication procedures of the eID scheme (rely on the authentication procedures). Within the financial sector and especially for new third party players like PISP and AISP the existence of open eID solutions in the Norwegian market give these enterprises access to use well established eID schemes most suitable for the services they will offer. We believe that innovation, increased

competition and access for new third party players will thrive in environments where eID schemes are commonly used. Against this background, Finance Norway strongly emphasizes that the RTS in a clear and unambiguous manner excludes the possibility of "sharing of the PSC" for eIDs/e-signatures compliant with EU-legislation.
Rationale 19: PSD2 Art 97.5 says that PISP has the right to rely on the authentication procedures provided by ASPSP. Rationale 19 continues along this to say that the authentication procedure is "in the sphere of the competence of the ASPSP", unless the PISP issues its own credentials. Finance Norway agrees that the SCA shall occur fully in the sphere of competence of the ASPSP. Finance Norway are also in favour of stating this explicitly in chapter 1 of the RTS.
Rationale 19.b): We believe that there is a need for clarification on how Article 74.(2) of the PSD2 shall be interpreted after the transitional period, and in particular how this article shall be applied supported by when transactions are performed according to the exemptions from SCA given in chapter 2 of the RTS. It is not the understanding of Finance Norway that Art.74.(2) can be made redundant by EBA excluding any risk elements from the draft RTS.
Art 1.: The term "authentication code" does not seem to be properly defined. The definition should make sure that the difference between "authentication code" and "personalised security credentials" are commonly understood.
Art.1.2.: The security features of the authentication code should be explained in a technology neutral way.
Art.1.2.(b): We find the phrase "generated for the same payer" unnecessary.
Art1.3.(b) – We find this statement about "excluding which authentication element" that failed, too categorical. Many PSPs experience a demand for having user-friendly and informative web functions. There are situations where a feedback to the payer about what went wrong during authentication may prove helpful. We understand that Art1.3.(b) also is intended to be applicable for card payments. It seems to be good and common practice to inform the user whether the card or the PIN (or fingerprint) verification failed.
Art.1.3.(d): We agree that HTTP over TLS is good practice and a reasonable minimal requirement for the time being. However, good practice and adequate requirements will change over time. Further, names of individual specifications or products should not be a part of the RTS. We would prefer to finalise Art.1.3.(d) with "by relying where on standardised state-of-the-art secure communication protocols, ~~including but ….. HTTP over TLS~~."
Art 1.3.(e) The point items i. – v. seem to be valid for internet-based payments. We find that some clarification might be needed for card based payments at terminals. In particular, we raise the question whether offline card payments are still supported, e.g. as a fall back? It should be clarified in i) which PSP is assumed to have access to a blacklist in a fall back situation. A generalisation of this question is if Art.1.3.(e) is applicable to other parties than the ASPSPs, e.g. an acquiring PSP?
Art. 3.1 and 3.2 : These paragraphs should not allow for ambiguity by referring to non-defined "unauthorised parties". This wording should be replaced by "**to any party other than the payer**".
Art.6.2.: Consumer multi-purpose devices cannot be totally within the sphere of control of the PSP. They must be considered largely outside the scope of control of a bank. Therefore, the basis for risk mitigation should be the possible **consequences** of the multi-purpose device being compromised."
Art.6.3.(a): "Trusted Execution Environment" is the name of a Global Platform standard, which cannot be assumed to be present in all relevant multi-purpose devices. It

should be replaced by “a segregated secure environment.”

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.

Comments from Finance Norway
Generally: We support the idea of “time neutrality”, i.e. that several possible choices exist when the dynamic linking take place. The term “payee” is not clear. Payments are often not sent directly to the intended payee, but to and trough an account held by an identity not known to neither the payer nor the intended payee. The dynamic linking should include the intended payee, ref the definition of payee in PSD2 (article 4 (9)).
Rationale 23 and 24: A digital signature generated over transaction data by an authenticated payment user must be fully acceptable. This is indicated by paragraph 24, but should preferably also be visible in the RTS-text itself.
Rationale 26: In general, we support technology neutrality. Channel separation is only one of several techniques to mitigate the risks related to user authentication. There are a number of techniques that may be combined to reduce and mitigate risks. Rationale 26 should be written to consistently and clearly state that independence or segregation is one example to mitigate risk – as is done in the last sentence.
Art 2.2.(b): A requirement for separation (channel, application or device), if read literally, will create serious problems for relevant and user friendly mobile payments. We believe that this has not been EBAs intention. E.g. device separation is a more drastic requirement than requiring application separation within one device. This should be clarified in the final draft RTS. Alternatively, the second sentence of Art.2.2.(b) is removed.

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?

Comments from Finance Norway
Articles 3, 4 and 5 should not go into details and specific rules about authentication elements. The most important issue here, which should be reflected by the RTS, is that PSPs providing authentication elements must have a security policy which is based upon an understanding of the risks associated with the authentication procedure. A PSP must be able to explain and defend its security policy (including a password policy) to an auditor. New threats appear quickly, as also countermeasures do. We would hence warn against being very specific, and a list that seems complete today might be obsolete next month.
Art 5 : If the list of security features is kept, then «protection against presentation attacks » should be added.

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?

Comments from Finance Norway
Finance Norway is in favor of a risk based approach and find support for this in PSD2 Art. 98.3(a): stating exemptions based on "the level of risk involved in the service provided". It is our perception that the text in Rationale 54 and chapter 2 of the RTS does not substantiate this.
Rationale 53 The exemptions criteria should not be an exhaustive detailed list, but leave it to the PSP to apply exemptions based on its own risk analysis. A regulatory detailed list will be outdated as new techniques become available, be they to prevent fraud or to commit fraud.
Rationale 54: We believe that risk consideration should be an integral part of the RTS, and, in particular, any exemptions, or situations where SCA is not to be considered mandatory, must incorporate elements of risk based analysis. A PSP may have access to a large set of data that influence the perception of risk associated with an authentication and a payment transaction. The PSP should be held responsible for determining whether a particular payment situation may be exempted from general requirements to SCA.
Art.8: Recurring card-based payments should be addressed in this article.
Art.8: It is stated clearly in Rationale 41 that exemptions to strong authentication should be applied by the ASPSP only. We suggest that is added to the Art 8 text.
Art.8.1.(b): We are in principle in favour of a risk based approach leading to conclude when exemptions from SCA can be applied. We would also point out that when the RTS give rules for exemptions for contactless transactions, such rules are not found for traditional card payments. We suggest that similar exemption rules are given for contactless and for "contact" payments at point of sale.
Art.8.1.(b): We propose that: "…transaction at a point of sale" is changed to "….transaction at point of sale". (This to avoid the misinterpretation that the limits are related to use of contactless payments only in one single point of sale)
Art.8.1.(b) and Art.8.2.(d): If it is the intention that the logic in Art 8.1.(b) and Art.8.2.(d) (respectively "limits of both the following conditions" and ("all the following conditions are met") is the same, this should be expressed with the same words. As long as there are only two main conditions, we think that a logic using "both" would be most suitable.

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?

Comment from Finance Norway
We repeat that there should be a possibility for an ASPSP to apply a risk based approach to decide which transactions that should be exempted from SCA. A number of more detailed comments are found in the reply to the previous question.

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?

Comments from Finance Norway
Finance Norway supports the general ideas. PSC must be protected and only be known to the payment service user and by the verification system at the ASPSP. Especially this is fundamental for eID schemes. Please refer to our suggestion under question 1. We understand that such protection is actually the content of the wording "prevent their disclosure to unauthorised parties" in article 3. However, we have some more detailed comments.
Art 9.1.(a): "*Data on* personalised security credentials" should be defined, or a more precise term should be used. We are in favour of a risk-based approach here as well. It does not always seem necessary to mask a one-time password.
Art 9.1.(c): We believe that the concept of being "tamper resistant" should be clarified. Storing of keys etc. in tamper resistant devices at central sites seem reasonable, but e.g. is it a realistic requirement to say that all distributed usage of cryptographic material must take place in tamper resistant environments?
Art 9.2: We certainly agree that procedures for management of cryptographic equipment etc. shall be documented. But, there should be no requirement to make this publicly available. PSPs must however be prepared to give this documentation to certified auditors and competent authorities.
Art 10: As a main rule, we mean that PSC shall not be handled by payees. If there are situations where there are strong arguments for a payee to store and handle PSC, this must be explained and justified. We are afraid that Art10 can be seen as being in conflict with Rationale 19.a which is about authentication within the ASPSP's sphere of competence. We would find it most useful if the ideas of Rationale 19.a is included in the RTS text itself.
Art 13.(b): "Digitally signed" is use of one specific technology for software distribution to ensure origin and integrity. We suggest to reword this to say that «origin and integrity are ensured ».
Art.14.: We favour a more risk-based approach here. Renewal of a non-compromised element is not necessarily a high-risk activity. It seems too rigorous to require exactly the same procedures for renewal and re-activation of credentials in a trusted setting.

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?

Comments from Finance Norway
We have a number of comments regarding the interface between PSPs. These are found under individual points, for this question and question 8. The Articles of Chapter 4 should state clearly which parts of the chapter is relevant for remote electronic payments, and for card payments, i.e. for Art 17.
Art.17.1: The term "secure bilateral identification" should be defined. It should also be described between what types of communicating entities this must take place.
Art 19.4: A detailed interface description might contain information that can be seen as business sensitive for the ASPSP, or even might be misused for attacking the ASPSP. The specification of the interface should hence not be made publicly available, but the ASPSP should be obliged to make the interface description available to PISPs and AISPs that are registered as authorised third party providers.
Art 21.5 (and to some extent 19.2) might be read as if the AISP and PISP can handle the payment service user's credentials. We understand that there is an established principle that handing over of credentials shall not occur. This should made be clear in Art 21.5. Furthermore, we would appreciate if Art 21.5 either distinguished between credentials and authentication codes, or that there was a visible explanation for how these two have the same rules.
Art 22.4 In order for the ASPSP to perform fraud prevention according to art 1.3.(e) it is necessary that the payment initiation provider to transmit to the ASPSP all information related to the payment. We therefore propose the following wording: "Payment initiation service providers shall provide account servicing payment service providers with all payment information, included information collected from the payment service user, when initiating the payment transaction."

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?

Comments from Finance Norway
The RTS should remain agnostic vis-à-vis any particular standard to ensure that the RTS remain future proof.

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?

Comments from Finance Norway
Finance Norway believes that use of qualified web site certificates is a correct way to go for authentication between PSPs. However, being the holder of a qualified web site certificate, does not say anything about the operation and security of the PSP. PSPs must be expected to protect their private keys according to common standards for server-to-server communication. **Rationale 34** only refers to public e-identity schemes. Also private entities will provide services under the e-IDAS regulation. In the RTS there should not be any distinction between a public e-identity scheme and a private e-identity scheme. ***Art 20.1 and 20.3:*** There is also a certain risk that qualified web site certificates provided by listed Qualified Trust Service Providers, are widely enough deployed by the time the RTS is applicable.

Question 10:
Finance Norway replies “NA”.