EUROPEAN FINANCIAL CONGRESS

Instytut Badań
nad Gospodarką Rynkową
Do Studzienki Str. 63
80-227 Gdańsk, Poland

tel. +48 58 524 49 01
fax. +48 58 524 49 09

efc@ibngr.pl
www.efcongress.com

Position of the European Financial Congress[1] in relation to the European Banking Authority's consultation document on RTS specifying the requirements on strong customer authentication and common and secure communication under PSD2[2]

Methodology for preparing the answers

The answers were prepared in four stages:

Stage 1

A group of experts including more than 60 specialists were invited to participate in the survey. They received selected extracts of the consultation document as well as the consultation questions in Polish. The experts were guaranteed anonymity.

Stage 2

The European Financial Congress received 23 opinions from key financial market institutions in Poland and from individual experts. All the responses were collected, anonymised and presented to the experts who took part in the consultations. The experts were asked to mark in the other consultation participants' opinions the passages that should be included in the final position as well as the passages they did not agree with. Experts could also adjust their positions under the influence of arguments presented by other experts that they had not known previously.

Responses were obtained from:

- banks,
- FinTechs, IT firms, e-commerce firms and financial infrastructure companies,
- insurance companies and investment funds,
- regulatory bodies,
- consulting firms and law firms,
- the academia.

Stage 3

A seminar on PSD2 was held by the EFC for experts invited to participate in the survey.

Stage 4

On the basis of the responses received, the survey project coordinators from the European Financial Congress prepared the final version of the European Financial Congress's answers.

---

[1] European Financial Congress (EFC – www.efcongress.com). The purpose of the regular debates held within the EFC is to ensure the financial security of the European Union and Poland. The organizer of the EFC is the Gdańsk Institute for Market Economics - the first independent think tank in Central and Eastern Europe, founded in 1989 by a group of economists associated with the democratic opposition and the "Solidarity" movement

[2] www.eba.europa.eu/documents/10180/1548183/Consultation+Paper+on+draft+RTS+on+SCA+and+CSC+%28EBA-CP-2016-11%29.pdf

Answers of the European Financial Congress to the consultation questions

Q1
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?

In general, we agree with the arguments of EBA concerning the need to introduce Strong Customer Authentication (SCA) and the proposals regarding the verification procedure and requirements. The present-day customer authentication process used by ASPSPs in Poland in the context of payment transactions is highly advanced and makes use of a number of solutions (e.g. the authorisation code is sent in the form of an SMS code, which the customer enters online to confirm the transaction; another solution is the BLIK system, Polish standard for electronic payments and cash withdrawals from ATMs based on a mobile application – the customer uses a six-digit code displayed in his/her application and enters it as part of the payment process on the website, following which he/she confirms the amount and the payee in his/her mobile phone). Given the variety of solutions, we suggest that the requirements should not be made too specific and that we rely on current risk assessment methods used by ASPSPs. In this context, we concur with EBA, which suggests flexibility for PSPs to adapt their own technical solutions, while complying with specific security requirements, including dynamic linking of the code to the amount and payee (draft RTS, p. 11, paragraphs 24-25).

However, the following suggestions should be taken into account:

1. In Article 7 the auditing entities should be limited to "external independent and certified auditors". It would also seem reasonable to adopt specific time limits for performing such an audit.

2. Clarify the measures to limit the risks of multi-purpose devices being stolen or intercepted – according to some experts, such measures should be at least itemised.

3. Add requirements for logical device authentication – some experts believe that, in addition to a requirement on device information, Article 1(3)(e) should also specify a requirement concerning its logical authentication. This means assigning a trusted device to the customer, as is currently the case with banking applications.

4. Clarify the rules on the generation of authorisation codes – the system should ensure that the authorisation process is secure by preventing retrieval (generation) of a valid authorisation code based on the knowledge of a large number of previously used authorisation codes. Currently, Article 1(2)(b) refers exclusively to a security measure ensuring that it is not possible to generate a valid authorisation code based on the knowledge of a single, previously used authorisation code.

5. Specify how valid authorisation codes should be stored – the system should define the method for storing (processing) valid authorisation codes, as it is defined for confidential data in the Payment Card Industry Data Security Standards (PCI DSS).

6. Point to the need to use Public Key Infrastructure with a Certificate Authority – applying the "HTTP over TSL" (HTTPS) information exchange standard requires using the trusted environment of a PKI. In particular, the use of self-signed certificates with no involvement of a trusted website (Certificate Authority) is unacceptable. If the document refers to the HTTPS protocol, it should also refer to the need to use PKI.

In addition, according to some experts the following should be considered:

i. The need to take into account, to a larger extent, user and customer experience requirements (UX, CX) – this applies for example to the provision in Article 2(2)(b), which requires that a separate communication channel, application, and device be used for confirming transaction details. Introducing this requirement would affect the quality of the services provided by mobile payment applications. When making mobile payments, users of payment services use a single device and application to initiate, verify and authorise a transaction.

Therefore some experts suggest that RTS should provide for exemptions from the channel segregation principle based on the technology and risk management policy applied by the PSP. They also point that the rules on SCA for one-click payments and repeated (automatic) transactions should not be so restrictive.
However, where malware is installed on the device, if the channels are not separated, this may pose a security risk for the user and their funds.

ii. The possibility to rely on risk assessment and agreed principles on "liability shift" between ASPSPs and PSPs – according to one of the experts the so-called "liability shift" rule protects users from losses. This kind of liability shift is used in card schemes and both merchants and payers benefit from this setup. Merchants could offer better user experience and convenience, such as one-click payments. All this is possible now because acquirers/PSPs can perform risk based approach which very often gives similar level of security as SCA. EBA should consider whether it is possible to base the approach much more on risk and practical aspects instead of fixed rules - it should be possible not to apply SCA when the rules of "liability shift" are agreed by ASPSPs and PSPs, as is the case with card schemes (where card organizations are responsible for setting the rules of the scheme) or bilateral agreements between payment instrument issuers and acquirers.

Q2

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.

The document should better clarify the notion of the segregation of the channel, mobile application or device through which information linking the transaction to a specific amount and a specific payee is displayed from the channel, mobile application or device used for initiating the payment transaction. To this end, the provisions specifying the requirements in this respect should be made more specific. As it seems, segregating the channel where information about the amount and payee is displayed from the channel where the payment was initiated is possible within a single physical device.

This can be done, for example, by using different sessions for initiating payments transactions and sending the authorisation code or by using 2 SSL channels. In such a case, the proposed solutions would not affect the functioning of mobile applications compared to what is observed on the Polish market today.

If such a definition is not adopted, experts warn that the quality of services provided via mobile applications used for making electronic payment transactions may worsen. In practice, when making mobile payments, users of payment services use the same device and application to initiate, verify, and authorise the transaction. Bearing this in mind, consideration should be given to providing in RTS for exemptions from the channel segregation principle based on the technology and risk management policy applied by the service provider.

In addition, we think that the rules on dynamic linking should be based to a greater extent on risk assessment by ASPSPs. This follows from the fact that the Standard provides that when a fraud is caused by inadequate securities on the part of an ASPSP and causes losses to the customer, the financial liability rests with the ASPSP. Thus, with sufficiently high minimum requirements in place, the decision on the restrictiveness of the security measures to be used could be left to the ASPSP.

Q3

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?

Most experts point that the definitions in Articles 3-5 are very broad and their scope already covers a sufficient set of potential risks. In our opinion, the draft RTS addresses a sufficient list of issues related to the protection of authentication elements, and we believe that the list should not be made more specific. RTS should rather provide examples of definition components since the level and rate of crime development in this area is very high, and at the current stage, all likely scenarios cannot be adequately addressed by laws.

The examples of risks and methods for mitigating them include:

1. Requirements arising under card regulations (Payment Card Industry Data Security Standard):
a. Authentication system building and management
b. Security measures for storing confidential data required for the authentication system operation
c. Detecting and removing authentication system errors
d. Building and management of the authentication system access rights control system
2. Certificate management rules – issuing / receiving certificates; method for data exchange between entities.
3. Behavioral and "smart" risk assessment systems based on non-standard and unauthorised user actions. Some entities request that when such behaviours are detected (even if AIS/PIS certification is in place), the relevant ASPSP should be allowed to deny access or service.

Q4

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?

In the draft RTS, EBA has in fact toughened its position on allowable exemptions from strong customer authentication compared to its Guidelines on the security of internet payments issued in August 2015. In our opinion, specifying uniform and rigid exemptions from the strong authentication procedure required from banks is not a good solution. Crime and techniques used by criminals in this area have been developing very fast, as a consequence of which adopting a rigid approach to exemptions will, on the one hand, provide inadequate security against future crime scenarios for banks, and on the other, will not allow advanced risk management techniques to be used in this area. Meanwhile, customer experience would be seriously affected. We believe that the balance applied in Poland between strong authentication of sensitive operations and payment transactions and simple passive online access to customer's account without additional authentication is a better solution.

Two important comments about the proposals presented in Chapter 2 of RTS emerge from the feedback we have received. The first one concerns the limits laid down in Article 8 (EUR 50 and 150 for contactless payment electronic transactions and EUR 10 and 100 EUR for remote electronic payment transactions). A vast majority of the experts believe that the maximum transaction amounts not requiring strong authentication should be defined at national level based on local modalities (e.g. card transaction limits, real purchase power of money, etc.), among other factors.

The other frequent comment expressed by most representatives of the financial community in Poland concerns the postulate to adopt a more restrictive list of exemptions from SCA based on results of risk analyses conducted by ASPSPs, or to treat the presented list of exemptions as a maximum one. In such a situation, ASPSPs could put in place additional SCA requirements, e.g. based on their own risk assessment algorithms.

Such additional risk assessment mechanisms (or additional SCA exemptions) for individual transactions could take into account other risk factors not governed by regulations today, such as:

1. velocity values connected with the transaction,
2. geographical location based on IP geolocation, mobile location, merchant location
3. habits connected with type of merchandise – jewelry , toys, food
4. habits connected with type of delivery – electronic (virtual) vs standard shipment
5. device used:

a. PC – using cookie files and device fingerprinting or if applicable any personal certificates
b. Mobile devices (phone, tablet, smartwatch), unique mobile application ID, device ID
c. Internet of goods (TV, refrigerator) – unique device ID

The above factors should be used for monitoring transactions and user behaviour to detect any unusual patterns where strong authentication may be activated.

We also believe that when using multiple factors connected with the customer profile and behavior, it could be considered as a standalone inherence element. Unlike some other

indicators of strength (e.g. time limited SMS code, which could be compromised by losing the mobile device) behaviour patterns cannot be changed easily and fast.

In addition to the above, experts postulate specific exceptions to be taken into account in the proposed exemptions or restrictions to them:

1. Regarding Article 8(1)(a) – the time limit after which the User must use strong authentication again should depend on the types of data available after the authentication, which would be strictly defined.

2. Regarding Article 8(1)(b) – clarifying the method for calculating the cumulative limit of EUR 150, e.g. by specifying the applicable time limit

3. Regarding Article 8(2)(a) – the list of trusted beneficiaries should be protected against unauthorised change. Any changes in the list of trusted beneficiaries should be audited (who, when, how has changed the list). It should be stressed once against that this exemption, in particular, should be subject to additional risk assessment by the ASPSP because cases of fraud using this mechanism are known on the Polish market.

4. Regarding Article 8(2)(d) – clarifying the method for calculating the cumulative limit of EUR 100, e.g. by specifying the applicable time limit

Q5

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?

In general, again most experts opt for the solution whereby ASPSPs perform an individual risk assessment for each transaction and based on this take the final decision whether or not strong authentication is required.

We assume that banks will be allowed to apply the exemptions defined by the draft RTS on an optional basis. In other words, if a bank obtains information that its customer's account may be targeted by a criminal attack, it will nevertheless be allowed to apply a strong authentication procedure (even for very low value transactions). The bank will always have the final decision in this respect.

Such an approach is based on the rule that the responsibility lies with the payment service providers engaged in the transaction. Payment service providers should be free to take additional authentication measures based on their own policies and safety procedures. Once non-standard behaviours occur, in particular the risk to provide extensions should remain with the service provider.

Furthermore, it seems that the limits for the different types of transactions should be defined at national level based on local modalities (e.g. card transaction limits, real purchase power of money, etc.).

Q6
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?

In Poland, ASPSPS and, in particular, the banking sector treat user login data protection principle in a very serious way, and has applied, for many years, the requirement and practice of preventing the user from disclosing such data to third parties. The above principle is both reflected in the documents attached to agreements with customers and has been repeatedly communicated to customers through educational efforts, which have lasted for many years. We consider the change proposed in RTS, i.e. absence of an explicit ban on providing login details outside the ASPSP, to be very negative. As it appears, this would be a clear invitation to criminals and would increase in a very significant way the likelihood of success of criminal activities targeted at customers, in particular phishing attacks. We believe that existing practical solutions which do not require login data to be provided to third parties are capable of satisfying the regulator's expectations expressed in PSD2.

We agree with the solutions proposed in Chapter 3 of RTS.

It must be stressed that, over the years, Polish PSPs, with the support of regulators, have developed and propagated appropriate standards among PSUs, and we believe that it would be unacceptable to allow these rules to be relaxed in a way likely to lead to disclosures or consent to disclosures of such data to third parties.
In this context, we would like to draw your attention to the pay-by-link solutions used in Polish e-commerce (redirecting the client to their bank's website, where, after log-on, a completed fund transfer form will appear) – EBA should closely analyse this solution with a view to the potential application of such an approach when implementing PSD2 and the RTS in question.

Q7
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?

Applying generally acceptable standards to the greatest possible extent will ensure all market participants a basis for stable growth of their business. A solution based on an open and standardised API allowing third parties to access customers' bank accounts seems more secure than the very risky model which involves sharing authentication data with third parties (screen scraping).

However, it must be observed that introducing a new category of interfaces for the needs of communication with AISs/PSPs, PiSs/PSPs, PSPs issuing card-based payment instruments will certainly be a major and costly implementation-related challenge for ASPSPs, most of which have complex payment processing infrastructures, based also on standards other than those proposed in RTS, especially with respect to cards.

As regards EBA's proposal to develop communication standards on the basis of requirements of international or European standardisation organizations, we would like to emphasise that some

countries (including Poland) already have solutions supporting communication between ASPSPs and TPP. That is why we strongly believe that it should be possible to develop standards also based on ISO 20022. However, it is important to ensure that there will be a pan-European API solution capable of functioning between local country markets. Currently, there are several initiatives in European countries to implement country standards (e.g. CAPS, CSI, UK Open Banking Group, Berlin Group). Those initiatives differ significantly in terms of technical, operational and business models.

Furthermore, it must be clarified who will be responsible for ensuring sufficient funds to cover the transaction cost and assuming the risk of their absence: the account servicing payment service provider (ASPSP), the card issuer (PSP), or the payment service user (PSU)? The above question is not answered by the provisions of PSD2, which explicitly ban account servicing payment service providers from blocking funds on the account – Article 65(4) of PSD2. Therefore it should be clarified, when the RTS is issued or PSD2 is implemented in national law, whether the costs of transactions initiated by PSPs issuing card-based instruments will be covered with funds available on accounts managed by ASPSPs.

We believe, however, that the RTS lacks provisions protecting ASPSPs against unexpected consequences of increased numbers of queries and communication from AISs/PISs, which may, in the first place, affect the quality of services provided to the overall customer base. We think that in this respect regulations should explicitly provide for extraordinary procedures whereby the ASPSP could take protective actions in such situations. The RTS insufficiently defines the responsibilities and liability of third party providers (AISs/PISs) in the event of failures or security incidents, leaving much room for interpretation and arbitrariness, which is, as we believe, highly inadvisable in the context of the security issues discussed here.

Q8

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?

The proposed harmonisation of the standards through the use of ISO 20022 elements, components or approved message definitions is to be welcomed. From this perspective, they will certainly improve the interoperability between payment service providers, notwithstanding the different technologies and solutions used, because most providers have already implemented ISO 20022. We also support the references to security standards established by ISO 27001.

However, in addition to specifying the security standards, it would be advisable to determine – when defining the RTS and specifying the rules for the different market actors and regulators – the method for verifying and auditing the implementation of the security standards (in particular, implementation of ISO 27001 by TPPs), the results of risk analysis, and classification of information on which TTPs rely when accessing sensitive information.

Furthermore, RTS clearly favour the existing recognised communication standards. RTS do not precisely determine when a given new standard may be treated as an international/European

standard compliant with RTS requirements. It will be hard to consider any standard developed in one country as RTS-compliant before it is applied outside that country. If these conditions are not clearly defined, it will not be possible for the new domestic standard to be considered as an international standard compliant with RTS.

Q9

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 ?

We agree with EBA that there is a need for certifying account access intermediaries by dedicated offices established in accordance with the e-IDAS directive. In our view, this will improve the verification of PSPs in registers before the certificate is issued and before the responsibility is assumed by the certifying body. This should also ensure efficient protection and stability of services provided pursuant to PSD2. The principle of basing information exchange security on qualified certificates is commendable and will not hinder device use.

In addition to using qualified website certificates, consideration should also be given to the possibility of using qualified electronic stamp certificates (compliant with e-IDAS), considering, in particular, that this would be more appropriate for API-based communication.

At the same time, we would like to point out that, as yet, there is no established e-IDAS certification practice on the Polish market, and to the best of our knowledge, there are no qualified trust service providers. Therefore, the effectiveness of ensuring security based on e-IDAS certificates is yet to be proven in practice in the future.

Q10

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.

Experts are not unanimous when it comes to the question of using information from payment accounts when such information is not actively requested by the payment service user. They have expressed opposing views in this respect, with some of them pointing to the need of unrestricted access to account information, subject to no additional strong customer authentication. Having considered all the arguments, we definitely support the opposite solution, namely excluding, for security reasons, the possibility of retrieving information from the customer's account when it is not specifically requested by the customer.

Modern technology allows all details necessary to reply to a customer's request to be retrieved sufficiently fast with no need to generate automatic queries with no customer involvement.

Retrieving account data at regular time intervals, and not at the user's request, will allow checking the account balance and operations, gathering behavioral data, and in certain

situations, may also lead to spoofing. If obtained by criminals, such information would be a perfect source of knowledge about persons worth stealing from and would indicate the best ways of doing it. Therefore the purposefulness of AIS should be reconsidered and the risk associated with its functioning should be assessed.

We believe that as regards customer account access (AIS services), such access should be, each and every time, consciously initiated by the customer. As a consequence, we think that there is no need to define the number of automatic requests.

At the same time, it needs to be clarified whether requesting information from an account by AIS providers – if it is actually allowed – will be subject to strong user authentication, i.e. at least once a month (as is envisaged by the draft RTS). Including no such explicit requirement in the draft RTS may lead to inconsistencies of the security procedures related to accessing account information directly by the user and through AIS providers. In our opinion, authentication rules should be common, and at the same time, the service provider keeping the account should be able to force the use of strong authentication in line with internal risk management policies.