EBA - Request to issuing PSPs

26 July 2019

EBA request for input on the preparedness to meet the requirements on strong customer authentication

1. The European Banking Authority (EBA) contributes to improving the functioning of the internal market, including, in particular, a sound, effective and consistent level of regulation and supervision. One of the EU Directives that fall within the scope of action of the EBA is Directive (EU) 2015/2366 on payment services in the internal market (PSD2).

2. Among other rules for payment services, PSD2 sets outs strict security requirements for electronic payment transactions that protect consumers' financial data, ensure safe authentication and reduce the risk of fraud. In particular, PSD2 introduced the concept of strong customer authentication (SCA) that requires payment service providers (PSPs) to verify the identity of payment services users or the payment instruments the latter use based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is).

3. In addition, the PSD2 conferred 12 mandates to the EBA – six Technical Standards and six set of Guidelines. One of these 12 mandates is the Regulatory Technical Standard on strong customer authentication and common and secure communication (EBA/RTS/2017/02) (RTS SCA&CSC), which underpin the new security requirements under PSD2. These RTS specify, among others, the requirements of SCA, the exemptions from SCA and the requirements to protect the confidentiality and the integrity of the payment service users' personalised security credentials. The RTS on SCA&CSC were published in the Official Journal (OJ) of the EU in March 2018 as a Commission Delegated Regulation (EU) 2018/389 and apply from 14 September 2019.

4. To fulfil its statutory objective of contributing to supervisory convergence in the EU and to address queries that the EBA and national competent authorities (CAs) have received from market participants on the application of SCA, the EBA published a number of additional clarifications on the implementation and application of the RTS, which include the Opinion on the implementation of the RTS on SCA&CSC (EBA-Op-2018-04) published in June 2018, an Opinion on the elements of strong customer authentication under PSD2 (EBA-Op-2019-06) published in June 2019, and a number of Q&As in the EBA's Single Rulebook Q&A tool.

5. In the Opinion on the elements of SCA under PSD2, paragraph 12 and 13 in particular, the EBA acknowledged:

   - the complexity of the payments markets across the EU and the necessary changes required to enable the application of SCA, in particular by actors that are not PSPs, such as e-merchants, which may be challenging and may lead to some actors in the payments chain not being ready by 14 September 2019; and

   - that a key component for the successful application of SCA is to explain and make customers aware of such changes and that it is paramount for customers to be able to continue making payments, including online.

6. To avoid unintended negative consequences for some payment service users after 14 September 2019 in the area of electronic e-commerce payment transactions carried out with payment cards, the EBA therefore clarified that it would accept supervisory flexibility where CAs may decide to work with PSPs and relevant stakeholders, including consumers and merchants, to provide limited additional time to allow issuers to migrate to authentication approaches that are compliant with SCA and acquirers to migrate their merchants to solutions that support SCA. This supervisory flexibility is available under the condition that PSPs have set up a migration plan, have agreed the plan with their NCA, and will execute the plan in an expedited manner.

7. In order to fulfil the objectives of PSD2 and the EBA of achieving consistency across the EU, the EBA will later this year communicate deadlines by which the aforementioned actors will have to have completed their migration plans. The EBA wants to reiterate that the application date of the RTS by which all PSPs have to comply with the requirements of SCA is 14 September 2019 and therefore said supervisory flexibility should be as short as possible. Nevertheless, in order for the EBA to be in a position to set the deadlines based on robust information from a wide range of stakeholders, the EBA decided to carry out a fact-finding exercise with relevant stakeholders, including issuing PSPs.

8. In that regard, you are kindly requested to provide responses to the questions set out below and to return one form.

9. We would be grateful if you could complete and return the questionnaire to janis.matevics@fktk.lv **by 21 August 2019, cob**.

Respondent's identification

Member State: Latvia

Issuing PSPs: Finance Latvia Association Payments Subcommittee on behalf of retail banks licenced in Latvia

Name of the person: Edgars Pastars

Position: Chief Legal Officer

Email: edgars.pastars@financelatvia.eu

Tel. no: +371 29213847

Survey questions on the preparedness to meet the requirements on SCA with regard to electronic e-commerce payment transactions carried out with payment cards

1. **How likely is it that you will be fully compliant with the SCA requirements under PSD2 and the RTS on SCA&CSC with regard to electronic e-commerce payment transactions carried out with payment cards? If not fully compliant, what is the estimated level of preparedness to meet the requirements by 14 September 2019?** ***(please indicate (i) the number of SCA-compliant authentication approaches to the total number of authentication approaches supported by you and (ii) SCA-compliant payment transactions to the total number of these transactions)***

Retail banks service approx. 89%, specialized banks service approx. 11% of all bank customers in Latvia.

In terms of processing card payments all banks are compliant with SCA on the base of 3DS protocol #1. None of the banks comply with protocol #2.

All banks have **~ 20%** SCA compliant payment transactions / **80%** SCA-non-compliant payment transactions on issuing side (initiated without 3DS from merchants' side).

At this juncture, as coordinated with CAs, card payments initiated on merchants side without SCA (*especially in other EU member states, because most of the payments initiated in Latvia are SCA compliant on the base of 3DS protocol #1*) are accepted by banks with the condition that payments comply with banks' risk policy and pass fraud prevention measures.

In terms of SCA authentication methods, situation differ in retail banks and specialized banks.

Retail banks' clients* already can choose between **different SCA compliant authentications methods**:

- Smart ID /https://www.smart-id.com/about-smart-id/;
- Pin-calculator /hard token/;
- National ID-card /https://www.pmlp.gov.lv/en/home/services/personal-certificates-(eid)/;
- Mobile SCAN (https://www.citadele.lv/en/customer-support/faq/mobilescan/);
- SMS OTP and login name (if it is not just a person's name/surname) or password for TAN card users.

** One of the retail banks who recently formed in result of the merger of two retail banks, in addition SCA PSD2 compliant method, use also OTP delivered via SMS.*

There are no SCA-non-compliant authentication methods used in retail banks.

Instead, some of specialized banks already comply with SCA two-factor authentication by offering PIN + hardware token, **but most of the specialized banks provide 3DS protocol #1 with 1 factor (SMS OTP) authentication, which is not compliant with** SCA approach.

2. **What are the main obstacles/issues that prevented you from being compliant with the SCA legal requirements? In your view, how can these obstacles/issues be overcome now?**

Industry need more time to implement 3DS protocol #2.

Banks as issuers receive majority of e-commerce transactions without cardholder authentication being requested by acquirer/merchant.

Banks understand concerns of other industry actors about deficiency of existing 3DS protocol #1 which makes SCA process less attractive from them.

Taking into consideration global substance of the changes and complexity of payment market industry banks need more time for proper implementation of new protocols and authentication approaches / RTS exemptions, risk-based authentication and etc/ for purpose or improve security and consumer user experience in a natural way.

If Issuer banks are required to decline SCA-non-compliant transactions starting from September 14, it will become as an issue for the bank, merchants and their customers as it will result in a substantial increase of declined transactions and abandonment rates.

Several banks are running huge other IT development projects. Several banks are intending start implementing protocol #2 in March 2020, some of them are about it to start as soon as **VISA/MasterCard deliver final technical specifications.**

The main obstacle mentioned by every bank was that card system vendors late readiness based on late technical requirement specification availability.

3. What are the SCA-compliant authentication approaches you intend moving towards (based on the non-exhaustive list of potential SCA elements as specified under Tables 1, 2 and 3 of the EBA Opinion on the elements of SCA under PSD2)? (*please describe the two authentication factors that will be used for each SCA compliant approach by indicating also the category of the element – knowledge/inherence/possession, as well as the 3DS protocol you intend using)*

See Section 1 for already existing methods. **Retail banks**, being already compliant in this respect**,** look forward to introducing even more advanced approaches, like biometric authentication.

Speaking of **specialized banks**, they are currently moving forward with the 2 following factors:

1) possession of a device evidenced by an OTP generated by, or received on, a device (software token generator, SMS OTP).

2) knowledge element – password or login name (if it is not just a person's name/surname).

Banks who are not fully compliant with SCA (and they cover the smallest part of all bank customers, see Section 1, are in the progress to implement SCA-compliant authentication approaches. Compliance to SCA will be delivered by **the end of 2019 or mid-2020.**

4. Taking into account the limited supervisory flexibility that CAs can provide, what is the most expedient timeline for you to migrate to each of the SCA authentication approaches referred to in your answer to question 3? *(Please indicate the readiness date – e.g. SCA approach X: expected to be available on 'dd/mm/yyyy')*

Retail banks do not need transitional time to migrate customer to other SCA tools as those solutions are already in place and used by customers.

For those banks grace period is needed for "not to be obliged to decline SCA-non-compliant transactions initiated and send from merchants without 3DS after September 14". Grace period is needed to ensure SCA compliance and merchant readiness throughout all EU. The end date of the grace period should be aligned

with deadline given to acquirers and merchants for implementation of protocol #2.

Specialized banks who use SMS OTP authentication will add the knowledge element (see section 3) as the second factor element. Timeline varies from the end of 2019 to March 2020. 3DS protocol #2 adoption – 18 months.

5. **What main tasks (e.g. analysis, development, test and implementation/deployment) do you intend to carry out to meet the timeline specified in your answer to question 4?** ***(please elaborate on each task and specify the time needed for their execution)***

There are two separate tasks:

1. Specialized banks by mid-2020 will add the knowledge element as the second factor element in order to provide SCA compliant authentication tools for their customers;

2. All banks, when VISA/MasterCard deliver technical specifications in due time, preferably by the end of this year, will implement 3DS protocol #2, especially to be able use SCA exemptions. Estimated time needed – 18 months.

6. **To the best of your knowledge, do the SCA authentication approaches you offer or intend moving towards impact the configurations implemented by acquirers, merchants or acceptance systems?**

Latvian card issuing banks SCA authentication is operational only if both merchant and acquirer are supporting 3DS protocol.

7. **How are you going to support the use of the exemptions from SCA, including those originating from acquirers/merchants? (*If 'Yes', please specify which one, the date when they will be available and the version of 3DS used for authenticating the transactions)***

Answers from retail banks differ. Some of them will apply no exemptions at this juncture. Some of them instead are going to support acquirers/merchants' exemptions. The implementation of issuer exemptions is under investigation (particularly, low value payments and transaction risk analyses).

8. **What is the level of readiness to recognise transactions that are not subject to the requirement to apply SCA, such as payee-initiated transactions[1]?**

At this juncture banks recognize recurring transactions.

9. **What is the percentage of payment service users that already use SCA approaches you make available?** ***(please indicate the number of payment service users that use SCA-compliant authentication approaches to the total number of payment service users)***

[1] Payee initiated transactions meeting the conditions specified in Q&A 4031.

Retail banks: 100% of banks with their authentication approaches are SCA compliant

Specialized banks: 30% of banks with their authentication approaches are SCA compliant.

All banks support 3DS protocol #1.

10. Taking into account the limited supervisory flexibility that CAs can provide, how much time do you consider necessary for raising awareness to consumers about the new SCA-compliant authentication approaches referred to in your answer to question 3?

1. Customers have used to SCA compliant authentication methods mentioned in Section 1 for a while, changing the protocol from #1 to #2 (internal technical matter) should not create visible impact. Therefore, no additional time needed for raising customer awareness.
2. Communication toward consumers becomes essential if Issuers start to decline SCA non-compliant transactions and other market actors are not supporting any of 3DS protocols (usually in other EU countries). If this indeed will be the case, 6 months is a minimum period to prepare communication toward consumers to warn of expected inconvenience and to give a time to find other payments solutions.
3. Bank will assess should customer awareness be raised in regards of wider SCA usage in e-commerce environment.

11. What main tasks do you intend to carry out to raise awareness to consumers about the new SCA-compliant authentication approaches? *(please elaborate on each task, specify the time needed for their execution and indicate the major milestones needed)*

Referring to Section 10.3, Banks in upcoming 4 months intend to raise awareness to consumers about significant shift in e-commerce payment environment in order to prepare consumers for changes they are about to face.

Information to customers, depending on the size of the bank, will be delivered in several ways, for example:

1. via home page;
2. via internet banking platform;
3. via mail;
4. individually;
5. placing information in branches;
6. with the help from local banking association (Finance Latvia Association).

Thank you for your cooperation.