BRIEFING

Scrutiny papers

European Parliament

# EBA Draft Regulatory Technical Standards on Strong Customer Authentication and Secure Communication

**Committee on Economic and Monetary Affairs**

**Scrutiny Session of 27 March 2017**

This briefing supports **ECON's work on scrutiny** of delegated acts, in particular the discussion of **27 March 2017** on the *final* draft Regulatory Technical Standards (**RTS**) on **Strong Customer Authentication and Secure Communication (SCA**) submitted by the European Banking Authority (EBA) to the Commission for endorsement under Article 98 of the revised *Payment Services Directive* (**PSD2**) 2015/2366. ECON has already held a Scrutiny Session on the consultation paper (see briefing for the 28 November 2016 session)[1].

**In brief**

PSD2 aims at, inter alia, harmonisation, innovation and security with regard to payment services. Concerning security, Article 98 of PSD2 mandates the EBA to prepare *draft Regulatory Technical Standards on strong customer authentication and secure communication* (RTS SCA) in close cooperation with the ECB. On the basis of a Discussion Paper published in 2015, the EBA issued, in August 2016, a Consultation Paper containing a draft RTS text, which was **finalised in the light of the feedback received** and was submitted to the Commission on 23 February 2017. The RTS balances, on the one hand, the possibility (also for new market entrants) to provide the new services regulated by PSD2, to enhance existing payment services and users' experience, as well as to allow for innovation and, on the other hand, to introduce a framework that ensures common, as well as specific, approaches which ensure a high level of security, e.g. by proper authentication (confirming that the person giving the payment instruction is the right person). The issue to discuss now is whether the RTS text gets the balance right between access and SCA requirements.

When assessing the responses to the Consultation Paper, the EBA 'has had to make difficult trade-offs between the various, at times competing, objectives of PSD2, including enhancing security, promoting competition, ensuring technology and business-model neutrality, contributing to the integration of payments in the EU, protecting consumers, facilitating innovation and enhancing customer convenience' (Final Report, p. 6, paragraph 4). The **key issues** of this final draft EBA RTS are:

- the **scope** and **technological neutrality** of the requirements of the draft RTS;
- the **exemptions**, including scope, **thresholds** and the request made by numerous respondents to add an exemption for transactions identified as low-risk as a result of what some respondents referred to as **'transaction-risk analysis**' (TRA - previously referred to as 'risk-based authentication', RBA), and
- **access to payment accounts for third-party providers** (TPPs) and the requirements pertaining to the **information communicated**.

[1] The ECON PSD2 Negotiating Team commented on the EBA consultation text in its letter to the EBA of 24 October 2016.

Authors: D. Kolassa, A. Krischel - ECON Secretariat
Committee on Economic and Monetary Affairs
Directorate-General for Internal Policies of the Union

On 24 October 2016 the **ECON PSD2 Negotiating Team (NT) raised a number of issues on the consultation draft RTS** in a letter to the EBA, namely:

- business model neutrality;
- conflicting limits to the use of risk-based authentication (RBA); and
- direct and indirect access possibilities for Payment Service Providers (PSPs).

The NT wanted to ensure that direct access to payment accounts remains possible for TPPs when a bank's interface is used, and that banks will ensure that authentication as required by Article 65(2)(c), Article 66(3)(d) and Article 67(2)(c) PSD2 is technically possible for both, indirect and direct access.

## MAIN CHANGES BETWEEN CONSULTATION PAPER AND FINAL DRAFT RTS

The EBA agreed with some of the ca. 300 proposals by respondents, and made a substantial number of changes to the RTS as a result. The detailed, 100-page 'feedback table' at the end of the report summarises all comments and explains in its last column whether and how the provisions of the RTS were changed.

### When is SCA required? Scope of the draft RTS, as determined by Article 97(1) PSD2

PSD2 states that the PSP must apply SCA where **the payer** choses to *access the payment account online*, initiates an *electronic payment*, or engages in an action through a *remote channel which may imply a risk of payment fraud* or other abuses. Therefore, the EBA sees e-money transfers as covered, while electronic transactions initiated **only by the payee** (e.g. direct debits) are not. In consultation with the Commission on the discussion of the (continued) application of Article 74(2) PSD2, the EBA determined that the payee's PSP may forgo SCA until the RTS is in force, but afterwards only where an exemption contained in the RTS applies. When third-country payment instruments are used for cross-border transactions within the EU, the EU PSP shall make every reasonable effort to avoid fraud, but not necessarily applying SCA as this might not be possible (Final Report, p. 8, paragraph 16). However, such cross-border transactions are not taken into account for calculating fraud rates under the new Article 16 RTS SCA.

### Technology- and business model neutrality of the draft RTS

The EBA's consultation text included references to the mandatory use of ISO standards and technologies with the aim of achieving the integrated EU payments market envisaged by PSD2. As some respondents were concerned that these references may stifle innovation, the EBA amended the description of the three SCA elements (user's knowledge, possession, and inherence, see Article 4(3)(a) RTS) in a more neutral way to allow for future developments. The references to ISO 27001 and HTTPs were removed. But the EBA kept the reference to ISO 20022 - the international standard that defines the development of financial messages which is also specified in the SEPA Regulation - 'as it believes having a standardised message format is essential to the good functioning of the interface between the different PSPs.'[2] It is clarified that the standard applies only to the financial messaging structure (not to the communication technology used, e.g. XML), and only where banks offer a dedicated interface.

### Exemptions: new possibility for *transaction-risk analysis (*TRA), Article 16

The EBA has substantially amended and clarified the text on exemptions to SCA (Articles 10-18 = ex-Article 8). The most important change is the insertion of a new Article 16, which makes it possible to waive SCA when transaction-risk analysis (TRA) is used – previously often referred to as *risk-based authentication*

[2] Final Report, p. 8, paragraph 18. See also EPC on ISO 20022: 'In the world of payments processing, the role of the data format used to exchange information between banks can be compared to the role of language in communication between people […] SEPA data formats are based on the global ISO 20022 message standards'.

*(RBA)*[3]. TRA/RBA is not defined and the sophistication of TRA varies greatly across the industry. It may, for example, consist of automated background checks verifying the plausibility of the payment to prevent fraud by using fraud indicators such as IP address, device used, location of user, shop frequented, etc., in order to decide if a transaction is low-risk and can continue (without further authentication requests to the consumer), or whether too many flags have been raised and the transaction must be challenged. The new Article 16 allows utilisation of this tool to prevent fraud, albeit only in clearly defined circumstances and subject to objective criteria: it sets reference fraud rates below which the PSP has to remain for payments between EUR 100 and EUR 500. The lower the fraud rate, the higher are both the exempted threshold in EUR and the number of payments to which the exception can apply. Fraud rates and the performance of TRA must be monitored and independently assessed by qualified auditors, and must be reported to national competent authorities.

Thus, under the final draft RTS:

- some currently performed services would no longer qualify (e.g. Amazon 1-Click, *single* authentication with background TRA for credit card payments) **unless they are exempted** via Articles 10 to 18, in particular meaning that they would have to meet the requirements for fraud rates;
- account aggregation services (AISPs) would require the SCA - including a single-use code - to be repeated for each login where sensitive payment data (as defined in Article 4(32) PSD2) are disclosed.

### Exemptions: raised thresholds and exemption for unattended transport or parking terminals

A new exemption from SCA for unattended transport/parking terminals has been added, and one **threshold** for SCA exemption has been raised; however, corporate payments remain covered:

| Type of payment | Consultation RTS on SCA | New final draft RTS on SCA |
|---|---|---|
| **Contactless payment at a point of sale** if<br>i. individual amount does not exceed…<br>ii. cumulative amount does not exceed … | **Article 8(1)(b)**<br>EUR 50<br>EUR 150 | **Article 11**<br>EUR 50<br>EUR 150 (**or 5 consecutive payments**) |
| **Low-value transaction**<br>i. individual amount does not exceed…<br>ii. cumulative amount does not exceed … | **Art 8(2)(d)**<br>EUR 10<br>EUR 100 | **Article 15**<br>**EUR 30**<br>EUR 100 (**or 5 consecutive payments**) |
| **New:** no SCA for payments at unattended terminals... | -/- | ...for paying transport or parking fees |

### Extent and means of access to payment accounts

The **scope** of access is set by PSD2 because banks (or *account servicing payment service providers* - ASPSPs) provide not only payment accounts for their customers, but also savings accounts, securities accounts, mortgage services, etc., so it must be clear in the RTS which type of information is to be communicated. Other issues debated were the frequency of requests and the means to be used for access.

- **Scope**: The revised Art. 31 RTS envisages the communication to AISPs of the same information as the client may obtain, but limited to 'designated payment accounts and associated payment transactions'.
- Access **frequency**: Banks demanded a limited number of access requests per day, while TPPs requested multiple/hourly access. But in reality, banks employ different approaches/times for updating payment accounts. So, 'in line with the domestic clearing cycle in some EU Member States', the **EBA doubled TPPs'** independent (from customers') access requests to **4 times per day,** Article 31(5)(b) RTS.
- **Screen scraping**[4]: Consulting with the Commission and in view of PSD2's new requirements on TPPs' identification, SCA, and access to payment accounts restrictions, the EBA's interpretation of PSD2 is that once the RTS is applicable, screen scraping will no longer be allowed (EBA report, p. 11, para. 32.).

[3] The change in terminology – **from RBA to TRA** - stems from the fact that using TRA justifies an exception, i.e. a reason not to apply SCA, but it is not a means of '*authentication*' within the meaning of the PSD2 and the RTS on SCA.

[4] According to the EBA, screen scraping is 'also sometimes erroneously referred to as "**direct access**"', see report, p. 11, para. 31.

- **Access through a 'dedicated' or the customer's interface:** the EBA clarifies in the revised Article 28 that for online payment accounts, **banks must have at least one interface in place,** Article 27(1). This interface can either be one specifically established for the access of TPPs, or banks may provide access for TPPs via the (existing) interface they provide to their customers, Article 27(2). Then, most likely the customer's interface will have to be supplemented by a means to identify the TPP. Banks must provide technical information on the interface to the TPPs for free, Article 27(4). The RTS also foresees testing facilities, a three-month notification period for interface changes, and emergency documentation.

  In order to adequately meet TPPs' concerns regarding the proper functioning of the dedicated interface, the EBA has added a new Article 28, which stipulates a set of obligations with which dedicated interfaces must comply, in particular providing the same level of availability and performance, as well as support and contingency measures, at the same level as is offered by the banks to their own customers.

### Timeline of RTS on Strong Customer Authentication

| | |
|---|---|
| **25 November 2015** | PSD2 adopted (published 25 December 2015, in force as of 12 January 2016)<br>EBA tasked to develop six RTS and five guidelines. Article 98 PSD2 states that EBA shall develop, together with the ECB, draft RTS on SCA addressed to PSPs. |
| **8 December 2015** | EBA publishes discussion paper, to which it receives 118 responses. |
| **12 August 2016** | EBA publishes Consultation Paper |
| **12 October 2016** | End of consultation period |
| **23 February 2017** | EBA publishes *final* draft RTS SCA and submits it to the Commission.<br>Commission to endorse the RTS within three months (*23 May 2017*); Article 10(1) EBA Regulation. Scrutiny of European Parliament and Council (scrutiny period: 1+1 month, if 'the same' as the final draft EBA RTS, 3+3 months if not 'the same') |
| ***13 January 2018*** | **PSD2** becomes **applicable**. |
| *At the earliest: November 2018* (EBA estimate): | the **RTS** to become **directly applicable** in the EU, see Article 115(4) PSD2: 'The RTS will be applicable 18 months after its entry into force' |

### ABBREVIATIONS

| | |
|---|---|
| **AISP** | account information service provider (Article 4 (16) PSD2) |
| **ASPS** | account servicing payment service |
| **ASPSP** | account servicing payment service provider (Article 4 (17) PSD2), e.g. a bank |
| **PIS** | payment initiation service (Article 4 (15) PSD2) |
| **PISP** | payment initiation service provider |
| **PSP** | payment service provider (PSD2/SEPA context) |
| **RBA** | risk-based authentication |
| **SCA** | strong customer-based authentication (Article 98 PSD2) |
| **TPP** | third party payment (service provider) |
| **TRA** | transaction-risk analysis |

### CONTACTS


➢ ECON Secretariat
econ-secretariat@ep.europa.eu

➢ ECON Committee webpage
http://europarl.europa.eu/econ


➢ All ECON Scrutiny papers can be found on the ECON Policies pages

**Disclaimer:** The content of this document is the sole responsibility of the author and any opinions expressed therein do not necessarily represent the official position of the European Parliament. It is addressed to Members and staff of the EP for their parliamentary work. Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the European Parliament is given prior notice and sent a copy.