CORE®

EBA PUBLIC HEARING

On Strong Customer Authentication and Secure Communication under PSD II

Holger Friedrich
Dr. Waldemar Grudzien

30. September 2016
COREtechmonitor | Blogpost

Key Facts

- The EBA is strengthening the major aspects of RTS (Regulatory Technical Standards) in terms of strong customer authentication and secure communication for cashless transactions
- Discussion I: SCA (strong customer authentication) occurs only once a month with AISPs (Account Information Service Providers)
- Discussion II: Strengthening SCA
- Confirmation: the use of PSD II interface is mandatory for TPPs (Third-Party Providers) (screen scraping prohibited)
- Conclusion: strengthening SCA does not generate any momentum for RBA technologies, even if reference is made to synergies in other application scenarios (e.g. digital identity under eIDAS)

Report

1. Context

The EBA public hearing on Regulatory Technical Standards, specifying the requirements on strong customer authentication and common secure communication under PSD II, took place on September 23. The public hearing is an integral part of the consultation phase and regularly provides a summary of the initial consultation phase, as well as an insight into how the RTS are likely to shape up. Starting with the main points of development concerning RTS, which are reflected in the Consultation Paper [compare "Customer Authentication for Cashless Transactions: Impacts of the New RTS (Regulatory Technical Standards) under PSD II" post], the major points of discussion during the hearing are detailed below.

The key development items and discussion points can be deemed as the preliminary status of PSD II in terms of (1) strong customer authentication and (2) secure communication for cashless transactions, as responses to the RTS published on August 12 can be submitted by October 12, 2016. The EBA is planning to publish the final draft of RTS in the first quarter of 2017. Nonetheless, statements made by the EBA during the procedure represent a strong opinion, which might be included in the final RTS. The most important statements are detailed below, together with an initial assessment of each.

2. Details of Statements Made by the EBA

The EBA will not change the basic elements of PSD II, as was made clear several times during the hearing. The mandate conferred on the EBA which applies to the development of regulatory and technical guidelines for selected aspects regarding the implementation of PSD II.

The current discussion concentrates mainly on procedures concerning strong customer authentication and securing the trust and integrity of user credentials, as well as requirements governing exemptions from strong customer authentication. Up until now, the rule was that SCA (Strong Customer Authentication) could always be applied and requested when account information was being accessed. This would now change as a result of the discussion, as of right now it would only be permitted to request SCA again after a one-month period. Applying SCA earlier in

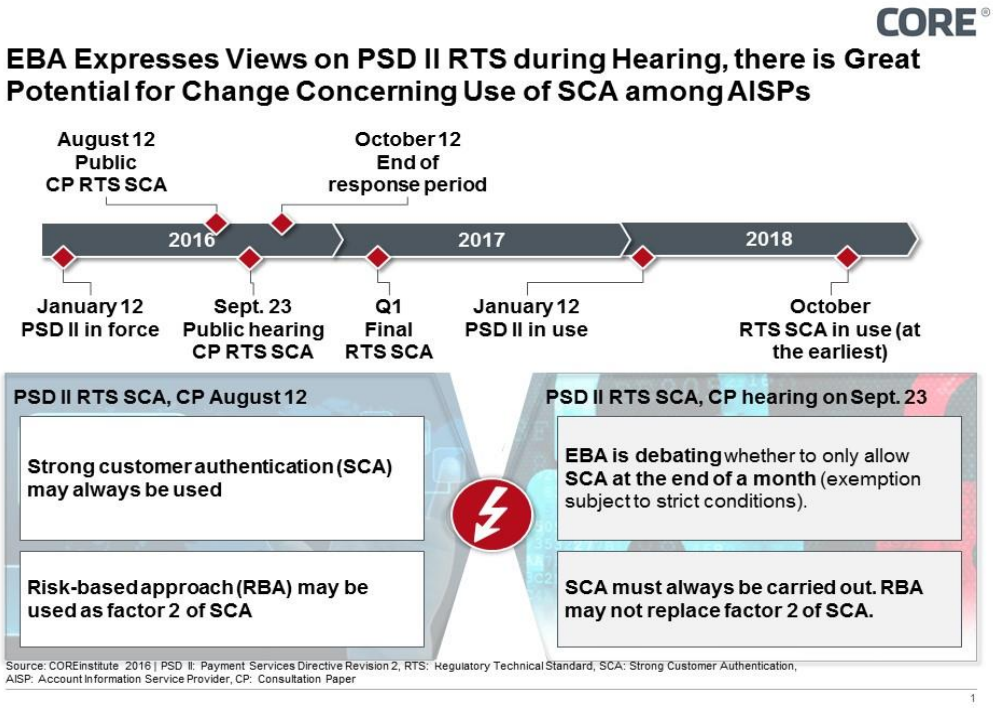

Fig. 1: The EBA's views on applying exemption rules to SCA for AISPs following the hearing on September 23 in conjunction with the RTS SCA draft dated August 12

the month would not be permitted. High hurdles would be placed on financial institutes who wish to undertake SCA at an earlier stage. The EBA is asking for responses to this idea.

A basic change has come about concerning the assessment of the risk-based approach during customer authentication. Before the hearing took place, an account-holding bank was able to request strong authentication for each access request, but was also able to waive SCA and only apply RBA for factor 2. The EBA made it quite clear during the discussions held at the hearing, that factor 2 can no longer be achieved by means of RBA. The EBA cites the following two arguments to back up its view:

1. Breaching the level playing field: a possible scenario would be that the account-holding bank only carries out checks in line with RBA, whereas it would request SCA from TPPs (third-party providers), thereby putting them at a disadvantage.
2. Loss ratio in online banking: according to the EBA, the risk-based approach isn't enough to reduce or keep losses to a minimum in online banking over the long term. The EBA only refers to a "few small retailers and some countries" as evidence of this assessment.

The EBA confirmed its opinion in regards to the mandatory use of a bank's interface for TPPs. Accordingly, TPPs have to use an interface provided by the bank for PSD II functions PISP, AISP and PIISP, and may not use any other means of access, such as screen scraping. The interface must provide the same functions and data as offered by Web browser-based online banking.

3. CONSLUSION

The EBA's latest hearing on RTS for SCA brought about two major changes to the discussion, beyond strengthening PSD II: SCA can not to be carried out prior to the end of a one-month period, no application of RBA for factor 2 of SCA.

Should banks not be allowed to use exemption rules regarding SCA for account information services, this would, in our view, have implications on the convenience and security of banking and cashless transactions.

The loss of significance regarding RBA may not only result in a drop in use, but also adversely affect research into RBA in Europe. This would mean that pioneering technologies such as device fingerprinting, behavioral analytics and biometrics would suffer too. Strengthening SCA compared with RBA does not generate any direct momentum for RBA technologies, even though the EBA points out synergies for other application scenarios (for instance under eID).

Sources

EBA, 2016

https://www.eba.europa.eu/news-press/calendar?p_p_auth=5HgT-FilL&p_p_id=8&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&_8_struts_action=%2Fcalendar%2Fview_event&_8_eventId=1548209

EBA, 2016

https://www.eba.europa.eu/-/eba-consults-on-strong-customer-authentication-and-secure-communications-under-psd2

COREtechmonitor, 2016
http://www.coretechmonitor.com/de/auswirkungen-rts-psd-ii/

Holger Friedrich is Managing Director of CORE. Prior to founding CORE, Holger built up a consulting firm, held a senior role at a market-leading technology provider, and was a partner at a leading international strategy consulting agency. Throughout his career his work has mainly focused on technology-driven transformations in the banking and financial services sector.

Mail: holger.friedrich@coretransform.com

Dr. Waldemar Grudzien is Transformation Engineer at CORE and focused on the security regulations of the financial industry and their technological effects on IT infrastructures. During his work at a national federation of the financial industries he was a specialist for retail banking and banking technologies. He graduated in electrical engineering at the TU Berlin.

Mail: waldemar.grudzien@coretransform.com

COREinstitute
Am Sandwerder 21-23
14109 Berlin | Germany
www.coreinstitute.org
Phone: +49 30 16344 020
office@coreinstitute.org

COREtransform GmbH
Am Sandwerder 21-23
14109 Berlin | Germany
www.coretransform.de
Phone: +49 30 26344 020
office@coretransform.de

COREtransform GmbH
Limmatquai 1
8001 Zürich | Helvetia
www.coretransform.ch
Phone: +41 442 610 143
office@coretransform.ch

COREtransform Ltd.
One Canada Square
London E14 5DY | Great Britain
www.coretransform.co.uk
Phone: +44 203 319 0356
office@coretransform.co.uk