CORE®

EBA PSD2 RTS Comment

Clarification of uncertainties raises new questions

Dominik Siebert
Dr. Waldemar Grudzien
Benedikt von Hake

July 2019
Blogpost
Copyright © CORE SE

Key facts

- EBA publishes final position paper on Strong Customer Authentication (SCA) in the context of the PSD2 final RTS
- Numerous queries amongst affected parties reveal uncertainty about the interpretation of the RTS and, for the first time, the EBA granted the possibility of a transitional period for the implementation of the SCA requirements for both issuers and merchants
- Behaviour-based biometric features will be granted as authentication element, as long as quality of implementation is given – verification of said quality, however, is not specified
- Possible interpretation: Use of biometrics with 3-D Secure 2.0 as currently observable in the market, is incompliant with RTS
- Clarification from the EBA to be obtained swiftly; development of a PSD2 compliant industry standard in the midterm.

Background

On September 14th 2019, the PSD2 will become applicable national law. The obligations of strong customer authentication under Article 97 of the PSD2, which are specified in the "Regulatory Technical Standards (RTS) on strong customer authentication and secure communication in cashless payment transactions" drawn up by the EBA, will thus also take effect.

During the iterative process of the RTS development, there were frequent queries and comments from market participants, which were reflected by the EBA in the course of the final report on the final RTS in February 2017. However, to date not all questions seem to have been conclusively clarified for those affected, as can be seen, for example, with the EuroCommerce trade association's letter to the EBA published at the beginning of June.

In response to the remaining uncertainties, the EBA published a further position paper, on June 21st 2019 - not even three months before the RTS came into force - which, according to its own statement, was final (https://eba.europa.eu/documents/10180/2622242/EBA+Opinion+on+SCA+elements+under+PSD2+.pdf).

As stated in the introduction of the document, this statement is primarily addressed to the national regulatory authorities (CAs), but is also intended to provide guidance for payment service providers (PSPs), payment systems and payment service users (PSUs), including merchants, in view of the prudential expectations involved.

The EBA divides its comments into "general" and "specific". The majority of the comments either answer very specific questions addressed to the EBA, or rather serve as a supplementary specification of individual RTS requirements which, however, do not affect the generally perceivable interpretation of the RTS in the market.

Nevertheless, some of the EBA comments are likely to correct at least some areas of the market participants' prevailing interpretation to date and will therefore be briefly explained below.

Unexpected EBA interpretations and their significance for the market

Article 13 and 14: EBA opens up the possibility of transition periods

While even after the publication of the final RTS, a number of aspects were still under discussion on the market side, it has so far been quite undisputed that from 14 September 2019 onwards all market participants concerned will have to have implemented the RTS mandatorily, whereby non-compliance could potentially result in sanctions being imposed by the national authorities (CAs). According to the provisions of the PSD2, there was no scope for individual assessments.

Articles 12 and 14 of the EBA paper now recognise that, in exceptional cases, CAs may decide "to avoid unintended negative consequences for some payment service users" to allow limited additional time to implement SCA requirements. This flexibility of the supervisory authorities explicitly requires, however, that the PSPs[1] in question must draw up a migration plan, coordinate it with the CAs and implement it in accordance with the CAs' specifications. The CAs in return are required to monitor the implementation of these plans in order to ensure rapid compliance with the technical standards of the PSD2 and the EBA. This would also include the need for adequate communication with the PSUs.

Nontheless, the EBA notes in paragraph 15 that it will monitor the adequate use of these margins and, if necessary, take action in the event of non-compliance.

In summary, however, this EBA model can be considered ambivalent: The statement itself can be seen as a possible relief for PSPs that are unlikely to be able to comply with the initial forced timeline for RTS implementation, or rather it gives the supervisory authorities the opportunity to decide on further action depending on the situation. However, since the EBA explicitly refers to a "large number of queries" in this context, a possible interpretation would be that this would probably apply to more PSPs than currently communicated. The fact that the European Trade Association EuroCommerce warned Adam Farkas, Executive Director of EBA, in an urgent letter at the beginning of June that the retail industry was not yet far enough with the implementation of the SCA requirements and that fatal consequences for retail and consumer confidence were to be expected, further illustrates this. In the letter, EuroCommerce explicitly calls for precisely this transitional period that is now granted. It remains to be seen, however, to what extent the new scope will actually be exploited.

Article 18 – 20: Use of Inherence Authentication Factors

In accordance with Article 4 (30) of the PSD2 , strong customer authentication (SCA) requires at least two elements from the three categories: Knowledge (something that only the user knows), possession (something that only the user possesses) or inherence (something that the user is), which are independent of each other insofar as the non-fulfilment of one criterion does not call into question the reliability of the others.

In Article 18-20 of the Paper, the EBA now specifies the applicability of inherence authentication factors: On the one hand, the EBA clearly states that in addition to physiological also behaviour-based biometric features such as, for example, keyboard touch dynamics can be used as

[1] PSPs as defined by RTS include both payment service providers in the classic sense as well issuers

authentication factors, which contradicts many previously prevailing interpretations of the RTS. Furthermore, with reference to Article 8 of the RTS, it is relativized that it is not the factor itself, but the (quality of) implementation that determines the applicability for strong customer authentication, i.e. from the perspective of the EBA, no biometric feature per se is excluded, as long as the implementation ensures a "*very low probability of an unauthorized party being authenticated as the payer*". However, the extent to which such a quality can and must be validated is not further specified. Thus, the EBA's comments open up a subsequent discussion, since, for example, in contrast to PIN Pads, biometric authentication systems within the finance industry have no regulated approval procedures. Nevertheless, the EBA's statements are to be welcomed, as they open up biometrics to the large field of technical supervision that it needs in order to enforce market standards and establish biometrics for transactions as well. These market standards should be developed by the industries affected and a rapid accreditation in cooperation with the EBA should be secured.

EBA's classification of the usability of inherence factors can be interpreted as technically liberal and pro-competitive, not least because EBA itself notes in paragraph 18 that biometrics has the most "*innovative*" and "*dynamic*" market environment in terms of the technical potential for secure customer authentication. Since, due to the large range of RTS requirements, most issuers have only focused on minimally invasive implementation so far, innovative solutions that exploit this potential are unlikely to be found in mass use soon.

Article 21 – 23: Inherence with 3-D Secure 2.0

Driven by Visa, Mastercard and Co, cardholder authentication via 3-D Secure 2.0 is increasingly becoming the market standard in card-based payment transactions, whereby in the prevailing market perception the procedure fully covers the SCA requirements of PSD2 (https://core.se/de/techmonitor/sicherheit-im-kartenbasierten-zahlungsverkehr). EMVCo, the

Non-exhaustive list of possible inherence elements CORE®

Element	Compliant with SCA?*
Fingerprint scanning	Yes
Voice recognition	Yes
Vein recognition	Yes
Hand and face geometry	Yes
Retina and iris scanning	Yes
Keystroke dynamics	Yes
Heart rate or other body movement pattern identifying that the PSU is the PSU (e.g. for wearable devices)	Yes
The angle at which the device is held	Yes
Information transmitted using a communication protocol, such as EMV® 3-D Secure	No (for approaches currently observed in the market)
Memorised swiping path	No

Figure 1: Overview of potential inherence elements according to EBA Position Paper

originator of the 3-D Secure Protocol, emphasizes that this new version is in particularily intended to simplify the integration of biometric procedures for cardholder authentication.

Consequently, it is surprising that the EBA has classified the currently in the market observable implementations for the use of biometrics in the context of 3-D Secure as not meeting the formulated requirements of an inheritance factor. The reason given for this is that the data points used for biometric authentication themselves (e.g. fingerprints) are not part of the protocol, with reference being made to Article 8 of the RTS. This means that in order to use an inherence authentication factor, it must be ensured that the respective terminal device and the associated software must be resistant to unauthorised use of this inherence factor for authentication even if it is accessed. This refers indirectly to the necessity of "template protection", which has been discussed in expert circles for some time (cf. https://core.se/publications/blog-posts/default-title-1). However, the EBA does not further elaborate on this point.

It seems that the EBA could see Article 8 of the RTS as potentially violated, since the biometric factor of the established biometric functions of smartphones and tablets (TouchID, FaceID, etc.) can be overridden or re-initialized when the respective device PIN is accessed.

Currently, however, these solutions are advancing to best practice for the implementation of 3-D Secure 2.0: The user receives a push notification in the transaction flow on an app previously bound to the device (possession factor), opens it via TouchID/FaceID (supposed inheritance factor) and only has to release the transaction in the app itself. Since the latter authentication factor is not permitted as such, in accordance with the EBA paper, a static password (knowledge factor) would have to be added in order to comply with the minimum requirements for a SCA.

If this interpretation of the EBA paper actually corresponds to the regulatory perspective, this will probably require a reassessment of the situation for card schemes such as Mastercard and Visa, 3-D Secure Providers and Card Issuers. Moreover, various other banks and payment transaction participants would also be affected, as many implementations of 2-factor authentication (e.g. for e-banking access) are designed similarly.

Conclusion

The EBA's statements allow conclusions to be drawn in various dimensions about the current market situation and future development:

For one, the facts that there were numerous queries, that bank and commercial representatives repeatedly asked for additional time to implement the obligations, and that the EBA published this interpretation paper less than three months before the RTS comes into force, make it clear that some of the parties affected by the RTS have not yet built up the necessary expertise in many areas to adequately implement the demanded requirements. The fact that these questions will not be discussed until more than two years after the publication of the final RTS suggests that the market has partially addressed the challenges from the PSD2 too late. Moreover, it seems that the competitive potential of SCA implementations has not yet been fully anticipated by the market (https://core.se/techmonitor/security-in-card-based-payment). Issuers and PSPs should therefore

be urged all the more to devote the necessary attention to the subject of SCA and to establish conventional solutions not only in accordance with the regulator's minimum requirements, but also proactively and in a way that shapes the market - e.g. through the use of biometrics now explicitly envisaged by EBA.

However, in particular the EBA classification of 3-D Secure 2.0 as inherence in particular still allows for different interpretations and could therefore still cause some tensions in the market. In spite of, or precisely because of the EBA's statements, some of which cannot be interpreted in a one-to-one way, a discussion is opened on the use of biometrics in banking, which is fundamentally positive and was possibly even intended by the EBA.

Although the EBA affirms in paragraph 11, that, beyond the existing Q&A process, it does not wish to publish any further remarks of this kind before the RTS comes into force, it is now necessary for all parties concerned to engage in the discussion and demand short-term clarity from the EBA, particularly in view of the timely effectiveness of the RTS. In the dynamic environment of biometrics in particular, it seems necessary to establish general market standards and corresponding approval and testing procedures for biometric authentication solutions in order to create clear framework conditions and thereby enable the widespread use and consequently the exploitation of the security potential of these technologies.

Sources

1. **EBA Comment on Strong Customer Authentication under PSD2**
   https://eba.europa.eu/documents/10180/2622242/EBA+Opinion+on+SCA+elements+under+PSD2+.pdf
2. **Final EBA Report on the RTS Draft**
   https://eba.europa.eu/documents/10180/1761863/Final+draft+RTS+on+SCA+and+CSC+under+PSD2+%28EBA-RTS-2017-02%29.pdf
3. **Letter from the EuroCommerce trade association to the EBA**
   https://www.bargeldlosblog.de/4773-2/
4. **Figure 1: Overview of potential inherence elements according to EBA Position Paper**
   CORE

Dominik Siebert is an Expert Director at CORE and looks back on a wealth of experience in the financial industry with complex transformation projects, from strategic conception to implementation control. At CORE, Dominik focuses on projects for the development and strategic positioning of digital payment solutions.

Mail: dominik.siebert@core.se

Benedikt von Hake is Transformation Manager at CORE. As a graduate economist with an international degree, he gained his first professional experience in the development of a digital sales platform. At CORE, Benedikt uses his knowledge to support the banking and payment industry in complex IT transformations, especially in the areas of platform IT and innovative payment systems.

Mail: benedikt.hake@core.se

Dr. Waldemar Grudzien is a Expert Director 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@core.se

CORE SE
Am Sandwerder 21-23
14109 Berlin | Germany
https://core.se/
Phone: +49 30 263 440 20
office@core.se

COREtransform GmbH
Am Sandwerder 21-23
14109 Berlin | Germany
https://core.se/
Phone: +49 30 263 440 20
office@core.se

COREtransform GmbH
Limmatquai 1
8001 Zürich | Helvetia
https://core.se/
Phone: +41 44 261 0143
office@core.se

COREtransform Ltd.
Canary Wharf, One Canada Square
London E14 5DY | Great Britain
https://core.se/
Phone: +44 20 328 563 61
office@core.se

COREtransform MEA LLC
DIFC – 105, Currency
House, Tower 1
P.O. Box 506656
Dubai I UAE Emirates
https://core.se/
Phone: +97 14 323 0633