CORE®

Security in card-based payment

Convergence of TRA/RBA and 3-D Secure 2.0 as a challenge and opportunity for issuer banks

Dominik Siebert
Benedikt von Hake

June 2019
Blogpost

Key facts

- Obligations for strong customer authentication (SCA) from the final RTS of PSD2 law in force as of 14th September 2019
- "3-D Secure 2.0" reflects increased security requirements for card payments
- RTS has been in the focus of financial institutions for some time - 3-D Secure 2.0 has been less noticed so far
- Adequate risk scoring system central component of both 3-D Secure 2.0 and the RTS of PSD2
- Increase issuers' willingness to take risks in order to maximise the user convenience of card schemes and competition - to avoid a downward spiral is to establish qualitative risk scoring early on

Background

On 14 September 2019, the PSD2 will become applicable national law. Along with it the obligations for strong customer authentication according to Art. 97, which are specified in the "Regulatory Technical Standards (RTS) for strong customer authentication and secure communication in cashless payment transactions", also become effective.

For transactions initiated by the payer, "Strong Customer Authentication" (SCA) must be carried out using two independent factors, unless one of the exceptions shown in Figure 1 applies. (https://core.se/techmonitor/final-version-of-rts-under-psd-ii-eba-urges-technological-competition).

Exemption	Article	Description
Account Information	Article 10	▪ Account balance ▪ Transaction history of the last 90 days ▪ No disclosure of confidential payment info ▪ Not at the first instance ▪ Not if last SCA more than 90 days ago
Contactless POS Payments	Article 11	▪ Single payments ≤ EUR 50 ▪ Cumulated amount ≤ EUR 150 or 5 consecutive single payments without SCA
Transport and parking fees	Article 12	▪ Unattended payment terminals, e.g. for toll and parking
Known recipients and recurring payments	Article 13	▪ Recipient Whitelist ▪ Payment series with the same amount to the same recipient ▪ Not when applying changes to the Whitelist ▪ Not at the first instance
Payments to oneself	Article 14	▪ Payments to oneself where both accounts are with the same bank
Small value payments	Article 15	▪ ≤ EUR 30 ▪ Payment series ≤ EUR 100 or 5 consecutive single payments without SCA
Transaction Risk Analysis (TRA)	Article 16	▪ Threshold value ETW depending on loss rate per payment method

Figure 1: Exemptions to the use of strong customer authentication

In the case of the "Transaction Risk Analysis" (TRA) exemption according to Article 16 (see Figure 1) risk factors are to be explicitly included and assessed in real time. These include amongst others the historical spending behaviour of the user, the location of payer and payee or possible abnormal use of an access device or the software used.

The applicability of the exception according to TRA depends on the Exemption Threshold Value (ETV). Depending on the payment system provider's loss rate, the ETV can be 100, 250 or 500 Euros. Strong customer authentication must only be requested once the ETV has been exceeded. The EBA distinguishes between card-based payments and transfers. The exact numerical values are shown in Figure 2.

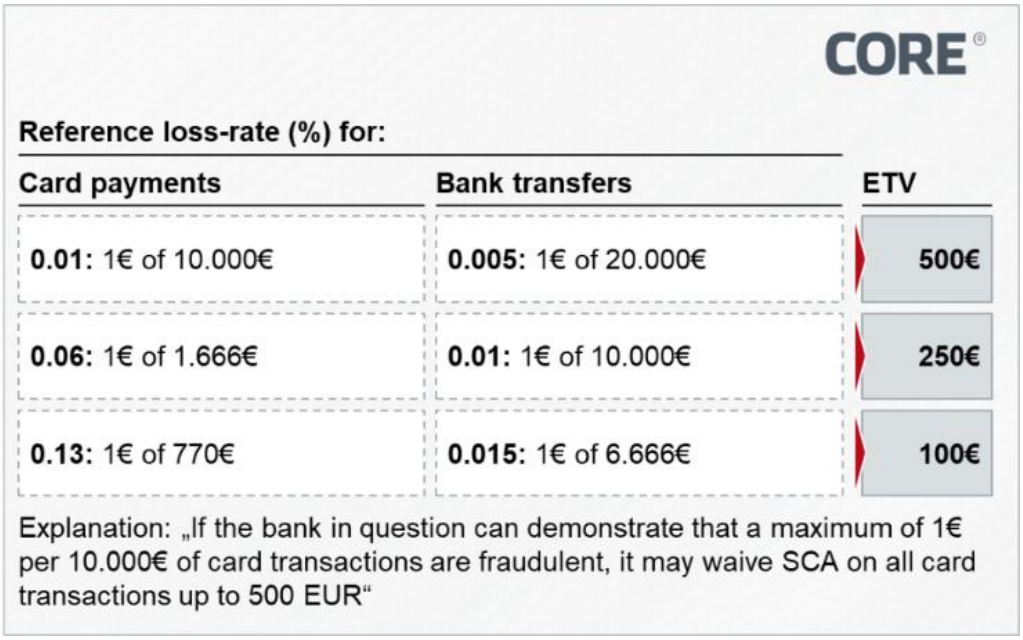

Figure 2: ETV depending on loss rate and payment instrument

SCA has been established for years with the 3-D Secure protocol for card-based remote payments: If a merchant has secured a transaction by 3-D Secure customer authentication, the risk of fraud is transferred to the card-issuing bank. In principle, a transaction secured via 3-D Secure meets the SCA requirements of the RTS.

Since the additional necessary interaction for customer authentication – for example, a one-time password sent by SMS – reduces the convenience of the checkout process, retailers often tend to disregard 3-D Secure authentication in order to avoid aborted purchases and increase the conversion rate accordingly.

Taking this circumstance into account, the major Card Scheme Association EMVCo launched a new version of the 3-D Secure Protocol ("3-D Secure 2.0"[1]) in 2015, which, among other adjustments, permits the so-called "Risk Based Approach" (RBA). The RBA enables the card-issuing bank to do without additional customer interaction in the authentication process on the

[1] The current version of the protocol is 3-D Secure 2.2.0 (link to specification below), but the wording "3-D Secure 2.0" is still common

basis of risk scoring. The scoring is based primarily on new data elements, which are transferred to the issuer or its service partner in the course of the 3-D Secure 2.0 transaction request, e.g. information on the retailer or shopping cart. The resulting increase in convenience is intended to prevent cancelled purchases caused by 3-D Secure and thus increase merchant implementation of the 3-D Secure protocol.

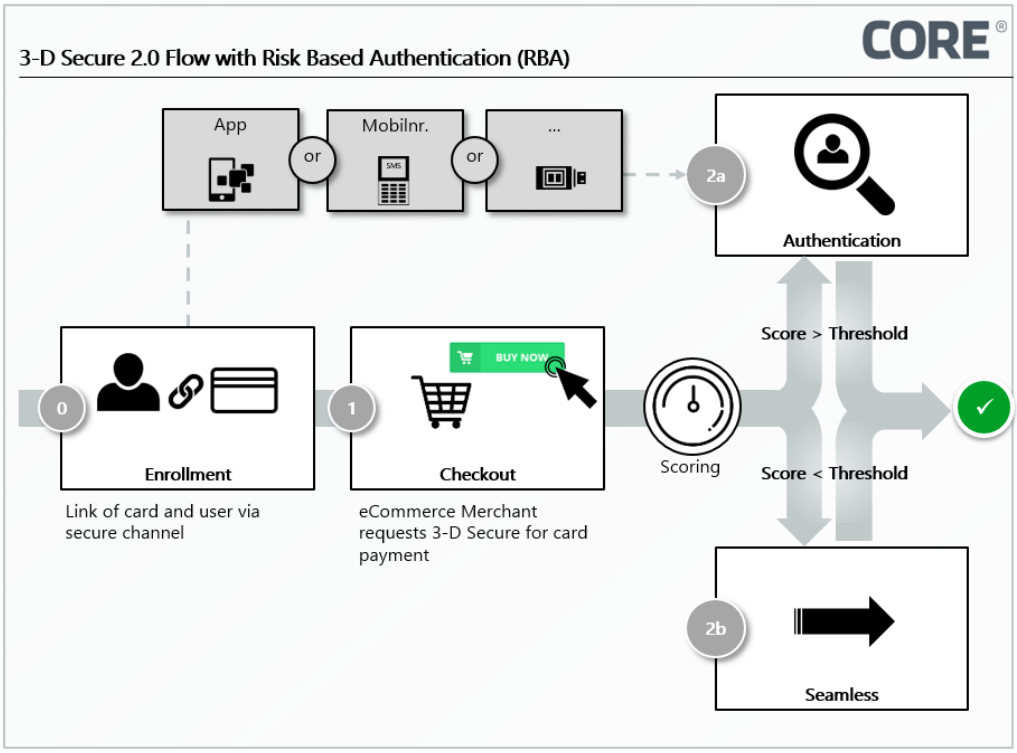

Figure 3: Simplified Userflow with 3-D Secure 2.0

Logically the TRA exemption of the RTS and the RBA from 3-D Secure 2.0 seem like a perfect fit: If the card-issuing bank implements a sufficient risk scoring, it can enable the cardholder to conveniently shop in e-commerce without any additional authentication steps and still is in compliance with the requirements of SCA under PSD2.

More security, greater convenience and thus potentially more transactions – those please customers, regulators, merchants, issuing banks and card schemes. At least that's the theory. While banks have already anticipated the PSD2 RTS, the market's attention to the topic of 3-D Secure 2.0 is comparatively low and, accordingly, its adaptation is still in its infancy.

Implicit challenges and resulting dilemma

First of all, it should be noted that both banks and providers of 3-D Secure solutions, must first implement the new 3-D Secure 2.0 protocol and thus a corresponding risk scoring system, and then parameterise it to suit their own risk appetite. This must be issuer and market-specific in each case. It will probably take some time before the improvement in convenience and rising authentication request rates become noticeable in merchants checkout processes.

In order to accelerate this development, the card schemes are trying to put pressure on the issuing banks: Visa demands the implementation of RBA explicitly for newly issued, remote-capable cards, Mastercard indirectly via mandatory conversion rates in e-commerce, which can de facto only be achieved with the use of RBA.

As a result, issuing banks tend to be urged to act in a risk-affine manner and parameterize their thresholds for waiving customer authentication accordingly – furthermore fueled by the fact that the RTS regulations now make convenience in e-commerce a differentiating factor from competitors: If, for example, the cardholder at Bank A has to authenticate himself at high frequency during e-commerce purchases, but Bank B can usually do without a further authentication step, while still providing adequate security, it is very likely that the customer will no longer use Bank A's card in the short to medium term.

On the other hand, a risky RBA parameterization means that a bank could exceed the fraud thresholds as outlined in the RTS and thus is less often allowed to surppress a strong customer authentication with 3-D Secure.

Since there are currently no broad empirical values for either the RTS or the 3-D Secure 2.0 implementations, it is difficult for banks to anticipate the ideal value for their own risk appetite. Moreover, there is a lack of data bases for the corresponding parameterizations, and since very few merchants have adapted the 3-D Secure 2.0 protocol to date, there is almost no historical data for risk scoring on the basis of the new data elements – all issuers and 3-D Secure service providers are therefore in the same starting position.

In the worst case, issuers who miss out on this trend could thus enter a downward spiral as a result of the potential development described below:

1. The issuer must implement RBA and, due to competition and card scheme requirements, tends to parameterize in a risk-affine manner.
2. The issuer thereby exceeds the TRA thresholds and, in accordance with the RTS, must request SCA more frequently.
3. Customer dissatisfaction and shopping abandonment increases due to limited convenience.
4. Instead, customers use alternative payment methods (possibly also from competitors), which reduces the number of transactions and the smaller database limits the optimization potential for risk scoring.
5. More fraud and/or purchase cancellations result in a decline in sales, loss of reputation and ultimately even put the issuer in risk of sanctions from the regulator or the schemes.

Conclusion

Firstly, it should be noted that the PSD2 RTS regulations concerning SCA strengthen card-based payment transactions in e-commerce in terms of security, which is in the interest of consumers and ultimately also of card-issuing banks. The SCA derogations added in the final version of the

RTS, under the premise of correct implementation on the part of the banks, make it possible to keep convenience at a moderate level whereby the latter is an important factor in asserting the card as a means of remote payments. However, as in many other situations, issuers must balance security and convenience. The described threat of a "downward spiral" puts pressure on issuers, which makes the short-term implementation of an efficient risk scoring tool for RBA/TRA indispensable: Waiting for market developments is not an option and issuers should prioritize and, accordingly, proactively act. After all, superior handling of RBA/TRA can become a competitive advantage when played out correctly. Effective risk scoring tools live from the constant supply of data, which postulates once again: The sooner the issuer implements a risk scoring, the more likely it is that it will stand out qualitatively. Buying the risk scoring as a service from a 3-D Secure Provider can potentially outsource the challenge for issuers. However, in contrast to an individual approach, the best possible outcome is a scoring model at competition level, but no positive differentiation can be achieved. Additionally, the risk scoring for the RBA should ideally be linked to the risk scoring for transaction authorization that is already implemented almost everywhere and mostly internally in the card business today, since this can also be further optimized through the expanded data scope. Depending on the strategic thrust and their own architecture, issuers should therefore rather evaluate the internal implementation of risk scoring.

Regardless of whether the scoring is sourced externally or implemented internally: In the early stages of the implementation of RTS and 3-D Secure 2.0, banks need to take advantage of the transition phase and actively shape the market before risk scoring mutates from a potential differentiation factor to a mere hygiene factor.

Sources

1. **EMV 3-D Secure**
   Protocol and Core Functions Specification
   https://www.emvco.com/terms-of-use/?u=/wp-content/uploads/documents/EMVCo_3DS_Spec_v220_122018.pdf
2. **Apple Card Uncovered - Top 10 Q&A**
   https://medium.com/rivero-ag/top-10-questions-about-apple-card-9bf458649d03
3. **Commission Delegated Regulation (EU) 2018/389 of 27 November 2017**
   https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R0389
4. **Figure 1: Exemptions to the use of strong customer authentication**
   CORE
5. **Figure 2: ETV depending on loss rate and payment instrument**
   CORE
6. **Figure 3: Simplifies Userflow with 3-D Secure 2.0**
   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

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