CORE®

“AUTHENTICATE!” – RTS UNDER PSD II IS INTENDED TO PROMOTE COMPETITION AND INNOVATION

Holger Friedrich
Marcus Nasarek
Dr. Waldemar Grudzien

December 2017
COREtechmonitor | Blogpost

Key Facts

- Final requirements for strong customer authentication have been published without the requested clarity concerning implementation
- Regulations combine different security paradigms
- Generalization of banking access for Internet payment services does not meet the requirements of digital ecosystems
- Requirements benefit card-based payment tools as well as payment service providers with huge revenue
- Applying the regulations to innovative developments is a challenge to the regulatory authority and market participants alike

Basically a compromise

The new regulations concerning strong customer authentication and secure communication (RTS SCA & SC) under PSD II were published by the EU Commission on November 27, 2017. At first glance two points, in particular, come to mind: On the one hand, the requirements have been worded very generally, meaning that applying these rules to concrete payment processes will prove a major challenge to many market participants. On the other, the underlying security paradigms all appear to be inconsistent with one another. Even though these points were continually debated during the long consultation phase – including consultations, public hearings, numerous meetings involving market participants and the European Banking Authority (EBA), the final version of the RTS still does not provide sufficient clarity on the subject.

Consequently, the published final version of the RTS still does not satisfy the claims made on it. Following the longstanding struggle concerning the legal wording of the PSD II, the EU Commission had hoped to achieve clarity by delegating the task to the EBA. SCA, the key element in implementing the objectives of the PSD II, is intended to support the following demands in equal measure:

1. To create a level playing field
2. To promote innovation in the market place
3. To break down rigid structures by creating incentives for improved collaboration between banks

With its detailed regulatory requirements regarding SCA, RTS is intended to create prerequisites in order to encourage new players to enter the market and ensure security at the customer interface. In actual fact, the RTS has, however, merely reworded the statement of the problem and provides very little guidance for actually implementing the topic. This vagueness will have a significant impact on market development.

Thus, for example, the concept of an authentication code was introduced in order to protect

authorization data when it is transmitted by way of a third party. Nevertheless, embedding this code has been neglected in the overall concept: Is the authentication code still to be treated as a secret and protected as if it were a personal security feature? Or will the authentication code become public property as a result of being tied to a concrete transaction and the fact that there is no trace back to the personal security features as a result of the code? Then an authentication code can also readily be passed onto a third party without any qualms. These are merely transmitting the authorization as they themselves cannot issue one. A concrete answer to this frequently posed question during the consultation phase is particularly significant for risk management and questions regarding liability. However, there is no mention of it in the final version of RTS.

Similarly, the issue of the dynamic link of authentication with transaction data remains very vague. A significant aspect is what is exactly meant by “link”. Is this a technical or an organizational aspect, or is it a cryptographic process? Many producers of authentication processes, as well as payment service providers, are attempting to implement processes at their own discretion. Consequently, they run a huge risk of having to adapt them at a later stage. This fact also poses the question as to who is responsible if the roles are ambiguous. In Article 5, for example, a payment service provider is mentioned in the final version who is responsible for implementing the security measures involved in authorizing a payment. This may mean the account-holding bank, or it may also mean the payment service triggering the payment which is a payment service provider in terms of the Payment Services Directive (PSD). Does this then mean that the service triggering the payment is also given access to personal login data of the person using the payment service? Or not? This, too, is a pertinent question, which was asked during the final revision of the RTS and which needs to be clarified during the course of the implementation.

The most surprising aspect is, nevertheless, preference for the card-based systems. In the report by ECB concerning fraud with Internet payments – the original trigger of the EBA guidelines on security of Internet payment procedures and presenting the RTS on SCA – were card payments made on the Internet which represented the lion’s share of payment fraud. Card systems, of all things, are now being given better conditions (higher limit for small payment amounts, significantly higher thresholds for fraud rates) compared with transfer-based payment procedures. There is not even a mention in the RTS as to the justification for this different risk pattern. This would, nevertheless, help to apply the requirements to the procedure, which are based on new rules of procedure – not card-based and not SEPA-based.

Review: Motivation for SCA

The different requirements of RTS seem to be like a patchwork of various security paradigms when seen in the context of the aforementioned examples. This view can be explained against the background of the origins of RTS and, especially concerning the requirements of SCA: The

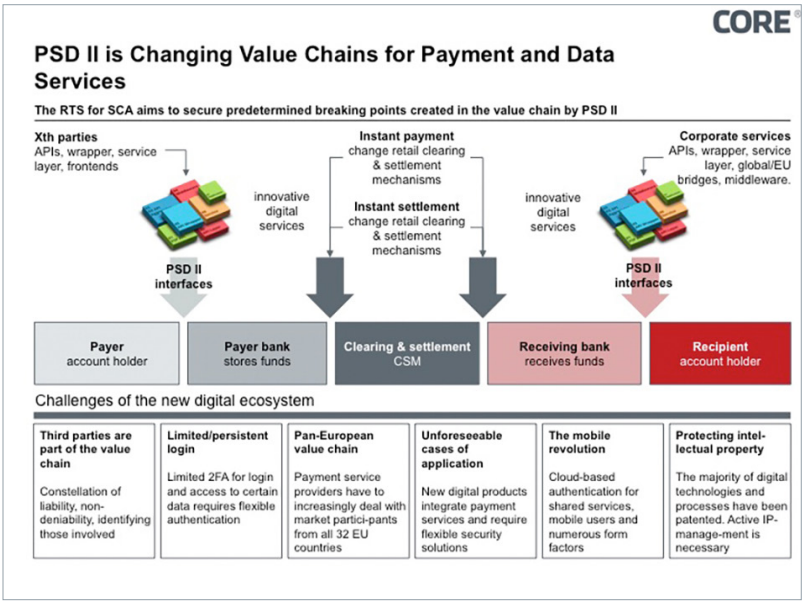

Figure 1: EBA RTS secures new predetermined breaking points

optional guidelines drawn up under the helm of the ECB in the preceding years concerning security of payments on the Internet were initially translated into compulsory guidelines by the ECB and were then supposed to be universally worded under PSD II into legal provisions for all payment services. PSD II was also intended to solve the problem of third parties having access to a customer's account by means of new legal parameters. This legal parameter was intended to ensure more security for the customer interface despite bank accounts giving access to third parties.

The problem concerning access to an account by third-party service providers goes back almost 15 years. The problem back then: German credit institutes, which were then acting as a Central Credit Committee, were confronted with the question at the turn of the millennium as to whether and how to respond to emerging online payment services. These services fill in the customer's bank transfer forms for them with the retailer's data as the recipient during online transactions. As the German banking industry had great difficulty in responding for a variety of reasons, first and foremost due to security concerns, it was originally the German banking authority, followed by the European one, which took up the issue. The rigid and insufficiently innovative market of retail payments was about to be broken down. Against the background of the new SEPA system, the European Commission saw the opportunity in assisting the EU's Digital Agenda with a program to stimulate the market. Digital payment processes were intended to support the digital domestic market.

Bank transfer services came just at the right time in order to break down rigid bank structures. Nevertheless, the key question was how a third party is able to access an account without endangering security. Since then, the concept of Strong Customer Authentication (SCA) has been a core element of PSD II. However,

even though it was considered to be a fundamental pillar in regulating new services under PSD II, it was virtually impossible to unite the radically different positions of the market participants. Consequently, the reconciliation of interests is particularly a challenge as PSD II must not be too concrete regarding the technical organization for regulatory reasons. It was due to this that the problem was handed over to the European Banking Authority. The European Banking Authority intends to safeguard the predetermined breaking points in the value chain of banks as defined under PSD II in the form of open bank interfaces. These predetermined breaking points are intended to create favorable prerequisites for new ecosystems (see Fig. 1). New services now actually emerge at these interfaces which complement each other, build on each other and mutually enrich each other (mash-ups). Individual value chains emerge based on payment data and payment-triggering services – and all of this long before the new regulations take effect.

Against this background the European Banking Authority has the task of formulating the requirements more specifically, but must nevertheless remain largely neutral in terms of the technological aspect. As a result, the requirements are worded such that basic questions remain unanswered: Is an authentication token confidential? What are sensitive payment data? Is the transmitter of payment data to the bank already a payment-triggering service? May a payment-triggering service obtain access to secret access data? How are payment data linked to the authentication tokens in technical terms? In spite of the long-term debate concerning these questions, the final version of the regulations does not provide any clear answers. Nevertheless, this vagueness was accepted, in order to open up the widest possible scope for new developments and competition.

Regulatory mechanisms and their impact

Accordingly, the development of RTS was a process of generalizing a concrete problem of competition as well as the difficulty of increasing card fraud as a result of Internet payments. The solution to these problems in the form of SCA is nevertheless tightly geared to whoever initiates the bank transfer. As regards Internet payments, the main industry is not the banking industry but rather e-commerce. The transfer of the payment in the banking system is merely a small intermediary step in this value chain.

A payment transaction starts when goods have been selected and ends in the retailer's merchandise information system. Online bank transfer services, which basically concentrate on simplifying this intermediary step, are only one in a host of payment processes and merely account for a one-digit percentage point in Internet revenue 15 years after being introduced to the market. Payment tools which offer other services surrounding payment transactions and respond to the needs of both the retailers and buyers make up a much greater percentage. These payment tools are not explicitly addressed by RTS in the same way as for card systems or bank transfers. Nonetheless, they must also implement the regulatory requirements. These include the following payment tools:

1. Card-based payment tools (e.g. credit card, debit card)
2. Transfer-based payment tools (e.g. SEPA credit transfer)
3. Direct debit-based payment tools (e.g. SEPA direct debit)
4. E-money-based payment tools (e.g. PayPal)

The respective payment tools have different starting positions thanks to the inconsistencies surrounding RTS. For instance, direct debit-based transfers do not have to include SCA. Unless, of course, the customer's bank plays an active role in preparing the direct debit mandate, and the recipient of the amount incorporates this banking procedure when issuing the mandate. Internet retailers will hardly wish to make the effort as the conversion then also depends on the bank. And if a bank offers an e-mandate solution, this will be different for every single bank. This is virtually a knock-out criterion for e-mandates or for a bank to take part in electronic direct debit solutions with e-commerce. Having said this, payment processes based on direct debiting are significantly more flexible in the choice of funds, and will therefore become the preferred choice without direct involvement by the bank. As direct debits can be reversed, retailers do not, however, generally have any payment guarantee.

The retailer can choose between either a card-based, bank transfer-based or e-money-based payment process in order to receive guaranteed payment. Although these processes have to adopt SCA, there is a different amount of scope for each one of these processes. Card-based systems are able to make use of higher limits in order not to have to implement SCA. For exceptions to SCA regarding payments up to 250 euros, a transfer-based payment system must have, for example, six times less fraud rates in order to be on the same footing as for card systems. A payment-triggering service, which has to assert itself against a card service on the market, will probably always be at a disadvantage due to conversion aspects as a result of the SCA which is required. After all, customer authentication is an extremely sensitive step in conjunction with the conversion rate. In turn, the conversion rate is a critical parameter for Internet retailers. If a transaction is canceled, the business associated with it is lost. If additional steps are required for certain payment procedures and the conversion suffers as a result, the retailer will generally motivate his customers to use a different payment system. Consequently, SCA tips the scales as regards what payment process is used. The shopping cart size and exemptions to rules concerning limits will be decisive as to whether a certain payment process is even used. It is very likely that there will be a shift in revenue among the various payment tools.

Furthermore, it is very probable that there will be a move from small to large payment service providers. This correlation stems from the introduction of exemption threshold values of a payment service provider. The lower the payment service provider's fraud rate, the more flexible it will be regarding the use of SCA exemptions. Initially, small amounts of 30 euros are generally exempt from SCA irrespective of how high or low the fraud rate is. With a card payment fraud rate of under 13

base points (= 0.13%), amounts of up to 100 euros are considered to be low-risk transactions. By the way, debit-based services can only allow themselves a fraud rate of 1.5 base points for the same limit. Nevertheless, if this limit is adhered to, a cart with a median share of 65 euros (= 50% of payments are less or no higher than 65 euros) is granted for risk-based exemptions for the overwhelming majority of payments. If the fraud rate is less than 1 base point – the limit is 500 euros for card payments and 250 euros for transfers, SCA is generally only applied under exceptional circumstances.

The law of large numbers then takes effect. A single fraud case involving the limit has a lesser impact on large amounts than it does on small sums. In addition, established payment service providers with large revenues and large customer payments are better able to hone their risk systems and are significantly preferred in two ways. Incidentally, e-money payments are generally considered here to belong to transfer-based transactions. These will then attempt to optimize their risk systems to their threshold limits, in order to keep up with the competition concerning card systems, as they have the potential in terms of major databases. However, it is doubtful whether banks, too, will forgo SCA for a 500-euro transfer in favor of conversion.

Conclusion

It is indeed apparent that RTS is intended to unite various problems and solutions. From a regulatory point of view, there would be two ways to approach this: Objectives are set, similar to that of the exhaust emission standard in the automotive industry or contaminant thresholds in the foods industry, and it is up to the manufacturers as to which route they adopt in order to achieve their goal. Or, however, procedural guidelines are drawn up, and very little scope is granted to the service provider. The EBA has attempted to combine both approaches with the RTS, and has merely achieved a compromise.

Furthermore, the RTS is geared to a problem dating back 10 years, which has since been replaced by new technological trends and their respective impact on payment procedures. Besides new value chains in digital ecosystems where the problem is one of how authorizations and role models are passed on among themselves, the mobile market has developed rapidly. Interactive customer authentication, as required by RTS using SCA, plays a subordinate role in current-day security systems due to the constraints placed on end devices. Modern processes take into account a payment, and rely on multiple data points as well as their intelligent combination, in order to securely identify the customer.

In the aforementioned case, the RTS creates an enormous challenge for the national regulatory bodies, conveying a message to market participants from a different era. On the one hand, very detailed guidelines have been set on SCA, but on the other hand the application is once again relativized due to exemptions, and, finally, systemic differences are introduced in terms of payment tools. The implementation of RTS as part of current applications is extremely time-consuming in light of the above and hardly meets its own objectives when all is said and done.

Sources

Internet:

http://ec.europa.eu/finance/docs/level-2-measures/psd2-rts-2017-7782_en.pdf
https://www.ecb.europa.eu/pub/pdf/other/4th_card_fraud_report.en.pdf

Previous posts in this series:

@COREinsitute:

https://www.coretechmonitor.com/de/public-hearing-der-eba-zu-starker-authentifizierung-und-sicherer-kommunikation-im-rahmen-der-psd-ii/
https://www.coretechmonitor.com/de/auswirkungen-rts-psd-ii/

https://www.coretechmonitor.com/impact-of-the-new-rts-regulatory-technical-standards-of-psd-ii/

Authors

Holger Friedrich has been in charge of our consulting unit since 2010. He was one of the founding members of the Institute for Theoretical Computer Science at the University of Potsdam (HPI). Before founding CORE, he set up a technology company and was a partner in a leading international strategic consulting firm.

Mail: holger.friedrich@core.se

Holger Friedrich

Marcus Nasarek is an expert in the DACH region in the field of payments. During his many years in the financial industry, he has managed projects for the e-SEPA process and designed and implemented complex security architectures. Today Marcus uses this experience and supports financial institutions in optimizing the IT security of all relevant payment systems.

Mail: mn@marcus-nasarek.de

Marcus Nasarek

Dr. Waldemar Grudzien is a Transformation Engineer at CORE and focused on the security regulations of the nancial industry and their technological effects on IT infrastructures. During his work at a national federation of the nancial 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

Dr. Waldemar Grudzien

COREinstitute
Am Sandwerder 21-23
14109 Berlin | Germany
https://institute.core.se
Phone: +49 30 26344 020
office@coreinstitute.org

CORE SE
Am Sandwerder 21-23
14109 Berlin | Germany
https://www.core.se
Phone: +49 30 26344 020
office@core.se

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

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

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

COREtransform MEA LLC
DIFC – 105, Currency House, Tower 1
Dubai P.O. Box 506656 I UAE
https://www.core.se
Phone: +971 4 3230633
office@coretransform.ae