CUSTOMER AUTHENTICATION FOR CASHLESS TRANSACTIONS:

Impact of the new RTS (Regulatory Technical Standards) within the context of PSD II

Holger Friedrich
Dr. Waldemar Grudzien

18. August 2016
COREtechmonitor | Blogpost

Key Facts

- The European Banking Authority (EBA) publishes Regulatroy Technical Standards (RTS) with requirements for strong customer authentication and secure communications for cashless transactions
- The main contents concern the regulation of strong customer authentication, including rules regarding exemptions, the use of biometry and the clarification of aspects such as channel separation and risk analyses
- Requirements have numerous impacts on security, processes and the business potential of credit institutions

Report

1. Rationale

The regulator urges various initiatives for financial institutions to create access to data and information by third parties, whose seclusion is not justified. Details of this market opening in the financial industry, fostered by the Payment Service Directive PSD II, have been specified in two major points recently published as “RTS” (Regulatory Technical Standards) by the EBA: strong customer authentication and secure communication for electronic payment services. These regulations have major consequences on the current standards and established processes with cashless transactions.

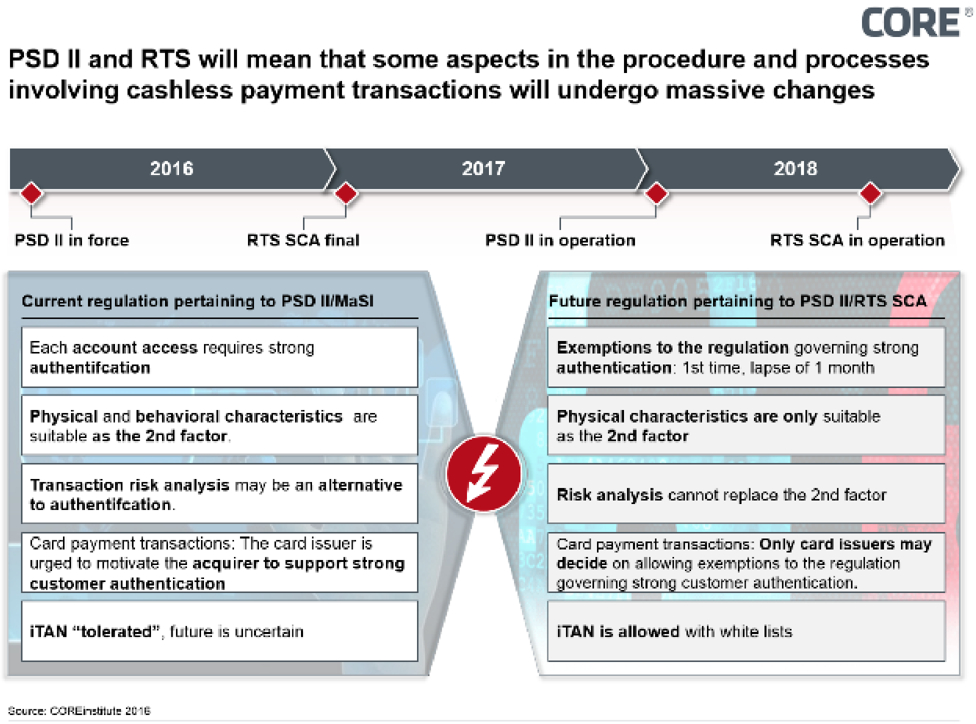
The document is comprised of two main parts; “Background and rationale” in Chapter 3 and also 23 articles featured in Chapter 4, which represents the final version of the actual RTS. Indeed, only the articles will ultimately be binding as RTS, nevertheless, the EBA takes a stance on specific aspects and commits to an opinion in Chapter 3. It remains to be seen what views of the EBA are ultimately reflected in the articles of the RTS. The following pages give an insight into the main concerns and consequences of RTS regarding PSD II. References are given for text passages that have been analysed.

2. Analyses

2.1 Framework

The PSD II lays out, that in-house banking services concerning the bilateral relationship with the customer by means of internal APIs, will have to be provided by public third-party interfaces by January 2018. This took effect on January 12, 2016, and must continue to be applied until January 13, 2018. The PSD II consults 11 mandates of the EBA to specify certain aspects of payment transactions. On August 12, 2016, the EBA published the consultation document detailing the requirements for strong customer authentication and secure communications for electronic payment services – RTS specifies the requirements on strong customer authentication (SCA) and common secure communication under PSD II.

The consultation document in question illustrates the implementation of Article 98 (Regulatory Technical Standards on Authentication and Communication) of PSD II. The published version is based on the discussion paper published on December 8, 2015, in which the comments of 118 respondents have been included.



PSD II and RTS will mean that some aspects in the procedure and processes involving cashless payment transactions will undergo massive changes

Current regulation pertaining to PSD II/MaSI

- Each account access requires strong authentifcation
- Physical and behavioral characteristics are suitable as the 2nd factor.
- Transaction risk analysis may be an alternative to authentifcation.
- Card payment transactions: The card issuer is urged to motivate the acquirer to support strong customer authentication
- iTAN "tolerated", future is uncertain

Future regulation pertaining to PSD II/RTS SCA

- Exemptions to the regulation governing strong authentication: 1st time, lapse of 1 month
- Physical characteristics are only suitable as the 2nd factor
- Risk analysis cannot replace the 2nd factor
- Card payment transactions: Only card issuers may decide on allowing exemptions to the regulation governing strong customer authentication.
- iTAN is allowed with white lists

Source: COREinstitute 2016

Figure 1: Compared with the current situation, major changes as a result of PSD II are in conjunction with RTS SCA.

The consultation stage for the RTS will end on October 12, 2016, after which the EBA will publish the final RTS no later than January 12, 2017. In accordance with PSD II, the RTS has to be applied by the market participants within 18 months, after the approval of the EU Commission. Consequently, they have at least until October 2018 in order to implement the requirements.

Detailed regulations pertaining to RTS will have a major impact on the current standards and established processes for cashless transactions, either in regards to the (non-) use of strong customer authentication when accessing the account and for starting the payment process, or for the use of risk-based analyses.

RTS addresses the following aspects in terms of payment service providers:

- Strong customer authentication for accessing the account, for carrying out a payment and for any action relating to a remote channel which may result in loss of money or any other misuse.
- Exceptions of the use of strong customer authentication and of security measures, in order to protect confidential security data of the payment service user, such as PIN and TAN.
- Measures to protect confidential security data.
- Requirements for a uniform, secure and open communication interface between account servicing payment service providers (ASPSP), payment initiation service providers (PISP), AISP, PIISP, payers, payees and other payment service providers.

2.2 Details

According to Article 1, the EBA incorporates three highly recognizable elements of knowledge, possession and inherence (biometric characteristics) in order to calculate the authentication code (to access an account or to initiate a payment). None of these elements may be traced back to the authentication code. Furthermore, Article 1 states mechanisms of strong authentication which might cause some challenges primarily to the account-holding institute. Consequently, in line with Article 1 No. 3(e), governing for the prevention, detection and stopping of fraudulent transactions during a banking session, viruses with malware are to be recognized which includes damage scenarios (ii.) that are already known. It still remains to be seen what exactly the EBA expects. Will a PSP be able to recognize a virus on a customer's private computer? If found to be positive, what can the bank do about it? Merely stop the transaction to contact the customer and make sure that the computer is decontaminated? Even the requirement for information concerning the customer device used (iv.) needs to be provided with further information. Does this refer only to the device issued by the bank such as a TAN generator, or does this also include the user's private smartphone? Questions are also likely to arise concerning taking the user's risk profile into account as well as his or her end device (v.). According to what criteria and thresholds must an account-holding institute refuse the transaction requested by a user? Measures such as including blocked bank cards (i.) and the user's payment history (iii.) in the risk analysis may then be classed as "known".

Article 2 comprises of the clarification of "channel separation", jargon used by the German credit industry, meaning that payment preparation and payment initiation may take place on an end device with a given independence/separation of channel, end device or by means of an app.

In Article 8 concerning exceptions to the use of strong authentication, the RTS lists an elementary deviation to the rules of PSD II governing access to an account (PSD II Article 97(1)): In line with PSD II, any access to an account requires strong authentication. So in accordance with RTS, first-time access to an account and the initial account access after a period of one month, where account access was granted without strong authentication on behalf of the customer, will mean that once again strong authentication is required. On the one hand, this simplification represents a concession to those countries which have always worked primarily with a static customer authentication – such as Germany. On the other hand, this regulation harbors the strong likelihood of confusing customers, as they will sometimes have to provide strong authentication and sometimes not. It will be interesting to observe how the account-holding institutes active on the market will decide; for reasons of convenience, some could be in favor of the permanent strong authentication of account access. This regulation surely represents a concession on behalf of the EBA towards the European Commission as a competitive authority wishing to protect account information services. Here, it remains to be seen how the competition watchdogs, at a European and national level, behave if banks were to count on strong authentication without exception for reasons of convenience concerning account access.

It is also worth mentioning regarding Article 8 that amount thresholds for contactless card payments at the PoS do not require strong authentication card transactions for amounts of 50 euros for single transactions and 150 euros as the maximum amount, meaning that the current threshold reigning on the market of 30 euros for each transaction will be raised significantly.

Furthermore, the exemption regulation for initiating payments when using white lists for payees in accordance with Article 8 No. 2 is very interesting. As strong customer authentication is no longer prescribed as its no longer deemed safe enough, banks could continue to use iTANS as a means of legitimation because customers are used to them. The authors do not agree with this.

In regards to biometry, the EBA has stated that (Rationale No. 29) they do not recognize characteristics based on behavior as the sole 2nd factor. Nevertheless, these characteristics may be part of an element in risk analyses for damage prevention. Biometric characteristics based on behavior include how the person uses their keyboard, the speed and the movement pattern of their computer mouse. By contrast, the EBA feels that physical characteristics are secure enough for a sole 2nd factor, meaning that, for example, the fingerprint method which is already widely used, can remain as the 2nd factor for accessing accounts as well as for initiating payments. Other physical characteristics, largely used in banking, include the face, eyes, voice and veins (surface of the hand, finger). Furthermore, the statement in Article 5 concerning the provision of devices and software needs to be more detailed, as it is not generally payment service providers which deliver devices featuring biometric sensors, but rather telecommunications companies, or in the broadest sense, technology providers. Neither the RTS nor PSD II will include these suppliers of customer end devices into the regulation, hence the responsibility for secure biometry will ultimately remain with the bank concerned.

In accordance with Rationale No. 41, it is only the card issuer who can make a decision on strong authentication for card payment transactions by applying the exemption regulations. In regards to MaSI, the card issuer is encouraged to motivate the card acceptor (retailer) into supporting strong customer authentication. It is now entirely up to the card issuer to decide. This raises the security in the overall card payment transaction system on the internet.

For safer communications between the account-holding bank and the three market participants introduced as part of PSD II (notably PISP, AISP and PIISP), account-holding banks need to provide an interface (Article 19 No. 1). This must support the identification of the three participants (Article 19 No. 1(a)) as well as the basic services they provide (Article 19 No. 1(b)). Further instructions, some of which are very detailed, are given in Article 19. For instance, the interface must provide exactly the same functions and service qualities as the customer would experience if s/he were accessing online banking directly (Article 19 No. 6). Furthermore, the interface must have test possibilities for the three payment service providers (Article 19 No. 7). Overall, the requirements of the interface, which is to be set up and the costs to be accepted solely by the bank in question, are generic but still challenging as they need to guarantee the same service level (e.g. availability, security) as provided by online banking.

In accordance with Rationale No. 69g, account information services ought to be in a position to access accounts as requested by the payment service user, and in the case of no activity, no more than twice each day. This rule is to be seen as a concession for account-holding credit institutes in order to take the pressure of their IT infrastructures.

In its Rationale No. 79 and No. 80, the RTS reinforces the statements made by PSD II concerning outsourcing of IT services by payment service providers in which no negative consequences are allowed to occur regarding operation, security, monitoring and supervisory ability. As such, payment service providers remain fully responsible for their outsourcing; this view of the RTS fully corresponds to the opinion of the national regulatory boards, as BaFin views IT outsourcing as a normal case of application (regulated by Section 25b of the KWG (Credit Services Act) and General Section of AT 9 of the MaRisk (Minimum Risk Requirements)).

3. Conclusion

It appears that the regulator will achieve his aim of opening up the market by creating account access for third parties by means of the regulations governing PSD II. With the help of more detailed information contained in RTS, access to an account will be implemented securely for customers, banks and third parties. Firstly, the reactions from the market mentioned in the text will have to be waited on as well as, secondly, the possible counter-reactions by competition authorities and regulatory boards. Thirdly, it remains to be seen how criminality directed against bank customers will develop.

Nowadays in the bilateral relationship between the customer and his/her bank, the attack vectors and damage patterns are, for the main part, “fully developed” and are only further developed on a reactionary basis. The PSD II will open up the bilateral basis by introducing a third party. The potential opportunities for attack and damage will increase as is the case with every IT system which is expanded to this extent. Only then can it be judged whether RTS has achieved its goal of providing secure payment services or not. Regardless, this regulation will have a major impact on current security standards and established processes with account-holding banks apart from opening up the market. Starting with the interface, which needs to be set up to include new risk models, business opportunities formed as a result of account access for banks, will also have to understand how to use them.

Sources

INTERNET:

EBA, 2016

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

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 electricial 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