CORE®

FINAL VERSION OF RTS UNDER PSD II

EBA urges technological competition

Dominik Siebert
Holger Friedrich
Dr. Waldemar Grudzien

27. February 2017
COREtechmonitor | Blogpost

Key Facts

- The EBA has finalized the Regulatory Technical Standards (RTS) on strong customer authentication and secure communication for cash-free transactions
- Final confirmation of the compulsory version of the PSD II interface for third-party payment service providers (TPPs) – meaning screen scraping is no longer necessary and will be prohibited
- Regulation on mandatory strong customer authentication (SCA) have been adjusted in response to feedback from the market. The limit for the exemption applying to remote payments has been raised from €10 to €30. SCA will now only need to be repeated for account information services every 90 days instead of the original 30, and biometric methods can be used for SCA without restriction.
- Two new exemptions to be made for SCA for transaction risk analysis (TRA) and unattended terminals
- Overall, the EBA is creating balanced, market-oriented regulations. Banks are encouraged yet again to compete technologically by means of introducing an exemption based on TRA.

Context

In August 2016, the EBA published the draft RTS for consultation, and spelled out the details in a public hearing on 23 September 2016, especially regarding the points on "Use of strong customer authentication for account access (one-month discussion)" and "Using a risk-based approach as a replacement for the second factor". On 23 February 2017, after taking account of 224 comments received back from the market, the EBA published the final version of the RTS. This means that depending on approval by the European Parliament, the RTS will come into force from November 2018 at the earliest.

The EBA has classified the feedback received into three main areas

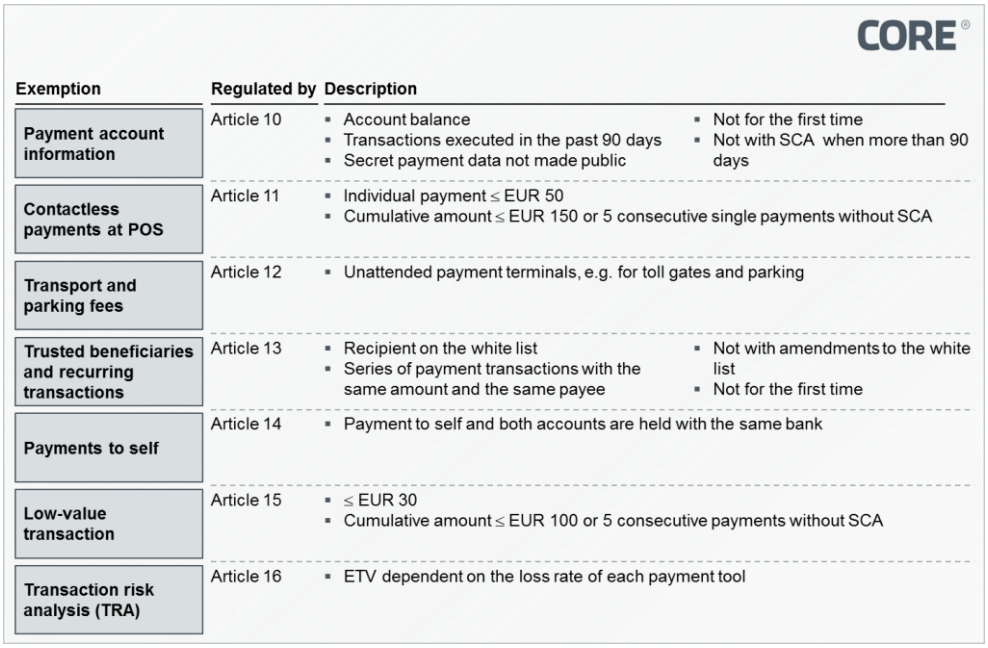
a) Scope of RTS and technological neutrality
b) Access to the payment account for third party payment service providers (TTPs), and communication requirements
c) Exceptions for minor risk payments based on transaction risk analysis

Comments on topic areas

Scope and technological neutrality

The EBA has explained that the scope of applicability is specified by PSD II, not by RTS. This means that the user makes remote payments using online payment accounts which can also be attacked online, leading to possible losses for the user. Further, the RTS apply to transfers and card payments, as well as payments where an electronic debit authorization is issued as part of the process – but not to direct debits as such. Moreover, the EBA sees scope of validity applied to corporate as well as private customers.

In order to ensure neutrality in relation to technology and business models, mention of the ISO standard 27001 and HTTPS over TLS was removed in the final RTS draft. However, reference to ISO standard 20022 was retained because in the view of the EBA, a standardized message format for transaction data is a prerequisite for the success of PSD II.



Exemption	Regulated by	Description
Payment account information	Article 10	▪ Account balance ▪ Transactions executed in the past 90 days ▪ Secret payment data not made public ▪ Not for the first time ▪ Not with SCA when more than 90 days
Contactless payments at POS	Article 11	▪ Individual payment ≤ EUR 50 ▪ Cumulative amount ≤ EUR 150 or 5 consecutive single payments without SCA
Transport and parking fees	Article 12	▪ Unattended payment terminals, e.g. for toll gates and parking
Trusted beneficiaries and recurring transactions	Article 13	▪ Recipient on the white list ▪ Series of payment transactions with the same amount and the same payee ▪ Not with amendments to the white list ▪ Not for the first time
Payments to self	Article 14	▪ Payment to self and both accounts are held with the same bank
Low-value transaction	Article 15	▪ ≤ EUR 30 ▪ Cumulative amount ≤ EUR 100 or 5 consecutive payments without SCA
Transaction risk analysis (TRA)	Article 16	▪ ETV dependent on the loss rate of each payment tool

Figure 1: Exemptions from the use of strong customer authentication

Overall, security requirements in relation to strong customer authentication (possession, knowledge and inherence) and authentication data were made less specific, and tied to technological progress in the formulation "as long as the security requirements are fulfilled".

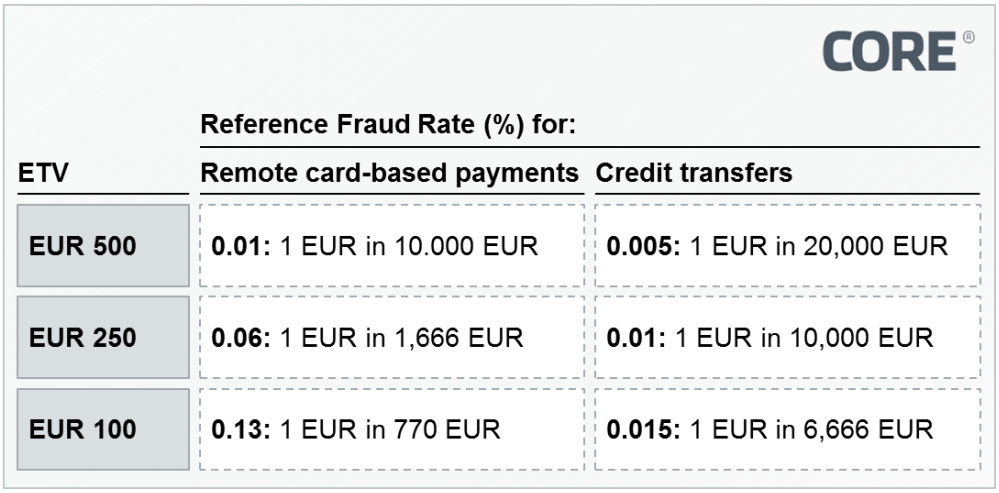
Access to payment accounts for TPPs

Account information services are now only allowed to aggregate the accounts four times a day without this being initiated by the account holder. In addition, instead of every 30 days as initially envisaged, strong customer authentication will only need to be repeated for the authorization of account information services after every 90 days. Once the RTS come into force, third parties will no longer be allowed to use screen scraping; instead they will have to base their services on the PSD II interface provided by the bank where the account is held. On the other hand, the banks must offer third-party service providers the same level of access and range on functions over this interface as their own customer has when managing the account online. The interface requirements in relation to this are specified in Article 28.

Exceptions for minor risk payments according to transaction risk analysis

The EBA generally takes the view that exceptions must not go against its essential purpose, since if exemptions were permitted for a majority of payments, this would undermine the aim of increasing transaction security. Furthermore, the EBA views the RTS as preparing the way for the post-PSD II world, where every transaction is based on strong customer authentication (SCA). Articles 10 to 18 describe exceptions to the use of strong customer authentication.

The EBA has created two new exemptions for TRA (transaction risk analysis, Article 16) and unattended terminals (Article 12). Article 16 aims to reduce losses in cash-free transactions by using an incentive model on the principle "the lower the losses, the



ETV	Reference Fraud Rate (%) for: Remote card-based payments	Credit transfers
EUR 500	**0.01:** 1 EUR in 10.000 EUR	**0.005:** 1 EUR in 20,000 EUR
EUR 250	**0.06:** 1 EUR in 1,666 EUR	**0.01:** 1 EUR in 10,000 EUR
EUR 100	**0.13:** 1 EUR in 770 EUR	**0.015:** 1 EUR in 6,666 EUR

Figure 2: ETV subject to the fraud rate and payment tool

higher the monetary threshold for SCA". Unattended terminals (attended terminals are, for example, POS terminals in retail) for transport (e.g. road tolls) and car parks make up the second exemption.

In addition, the exception for remote payments of low amounts was raised from 10 euros to 30 euros, and the total threshold for consecutive payments stays at 100 euros or five payments without SCA. For contactless payments at the POS, these limits are 50 euros, or a cumulative total of 150 euros, and also five transactions. Transactions in the same amount to the same recipient are now included in the exemption whatever the form of payment.

Details of the new regulations

The newly created Article 2 requires that transactions be monitored to spot unauthorized and fraudulent transactions and emphasizes the importance of monitoring against risks and fraud. Transaction monitoring must operate on the basis of the user's normal behavior. At a minimum, the risk analysis must cover compromised and stolen account identities, the amount of the transaction, known loss scenarios and signs of infection with malicious software. This implies a complete risk analysis system, though nothing like this seems likely to be in place in the world of online banking as yet compared to the world of cards. In cases of exemption in line with TRA (Article 16), risk factors to be taken into account and evaluated in real time are mentioned explicitly. These include the user's historical spending patterns, the location of the payer and recipient, and even possible abnormal use of the access device or the software employed.

In Article 5 on dynamic linking, the draft removes the technical limitations included in the August 2016 version relating to the number of devices and channels. These requirements have been replaced by a demand for secure procedures to guarantee confidentiality, authenticity and integrity. In the view of the authors, it is worth emphasizing that this technology-independent regulation guarantees a high degree of future-proofing. Finally, Article 16 introduces a new exemption for transaction risk analysis (TRA) building on the exemption threshold value (ETV).

Depending on the payment system provider's fraud rate, the ETV may be 100, 250 or 500 euros. Strong customer authorization only needs to be brought to bear once this value has been exceeded. The EBA makes a distinction between card-based payments and credit transfers. Figure 2 shows the exact figures. The risk analysis system must operate in real time.

In addition to the security factors mentioned in Article 2, the risk analysis must take six factors into account. For example, a check must be made for unusual spending behavior on the part of the payer or an unusual location. The fraud rate as a comparison measure for the ETV is derived from the total of non-authorized and fraudulent transactions for each payment instrument per 90 days. No account is taken of whether the payments were successfully recovered. The regulator must be informed on request of the calculation method and the actual fraud rates. Articles 17 and 18 describe further details regarding the RTA exemption.

PSD II itself makes it perfectly clear that the bank where the account is held must give access to third parties free of charge via an interface, but this is explicitly stated again in the RTS. Article 27 no. 4 states that access must be free of charge, and Article 28 lays out in detail requirements for the dedicated interface. The bank where the account is held is also required to monitor the availability and range of functions of the interface, and to provide the regulator with statistics on this if so requested. Third-party providers, too, are to report deficiencies in the interface to the regulator.

Evaluation and conclusion

The EBA has shown its openness to constructive adaptation, and its vision, by avoiding narrow technical requirements on end devices and communication channels, and by finally placing even behavior-based biometry on a truly equal footing with possession and knowledge. It also put to one side the superfluous speculations about "mandated exceptions" still seen at the public hearing in September 2016.

The authors feel that the final RTS represents a good compromise between the demands of all stakeholders. The EBA has managed to produce a balanced, market-oriented set of regulations for strong customer authentication and communication for the services as required by PSD II.

Even when PSD II was first published, it was clear that the entry of third-party services into the bilateral relationship between banks and customers is going to lead to "convenience competition" between third parties and banks. The TRA exemption now included in the RTS paves the path for banks to offer customer-friendly services, making it the favored means to shape competition for customers in a positive way for banks. If banks wish to take advantage of this exemption, they must monitor losses and transaction risks, and have these evaluated by independent auditors.

The additions to the RTS might be interpreted by banks as an attack on the last bastion of non-reporting of losses. But the reporting volume called for in ongoing ECB regulations means this is a price worth paying for the supposedly new freedoms granted by the final RTS. This obligation, like the now "inevitable" implementation of extensive fraud scoring systems in online be

and mobile banking channels, should not seen by banks as a burden. It is an opportunity for a new service role with the client, for cooperation between banks and with TTPs with an open mind, and for a true culture of innovation. If they do not take it, the bilateral bank/customer relationship may be replaced by a bilateral third-party/customer relationship before too long.

Sources

https://www.eba.europa.eu/documents/10180/1761863/Final+draft+RTS+on+SCA+and+CSC+under+PSD2+%28EBA-RTS-2017-02%29.pdf

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

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

Dominik Siebert is a Transformation Associate at CORE. He already gained some work experiences in process optimization regarding automotive manufacturing, as well as development and evaluation of advanced driver assistance systems. At CORE Dominik supports the development of digital payment systems.

Mail: dominik.siebert@coretransform.com

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@coretransform.com

Dr. Waldemar Grudzien is a Transformation Engineer at CORE. With a doctorate in electrical engineering and a degree in Business Administration, he has been a manager in a national banking association. A particular focus of Waldemar's is on security regulation and its technological effect on IT infrastructures.

Mail: waldemar.grudzien@coretransform.com

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

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
office@coretransform.ae