BANKING & FINANCE
CAPITAL MARKETS

NR. 1/2016

Newsletter

Open Access (XS2A) – EBA publishes Discussion Paper on Strong Customer Authentication and Secure Communication!

On 12 January 2016 the revised Payment Services Directive ("**PSD2**")[1] came into force. The new law shall give third party payment providers ("**TPPs**") full access to their customers' bank accounts, commonly known as XS2A. The European legislator aims to facilitate internet-related payment transactions triggered at the customer's request. In turn, TPPs must submit to the supervision of national bank regulators. The new law is expected to lead to a fundamental shake-up of the European payment industry as it deprives traditional credit institutions from their most valuable asset, the data of their customers.

1. TPPs

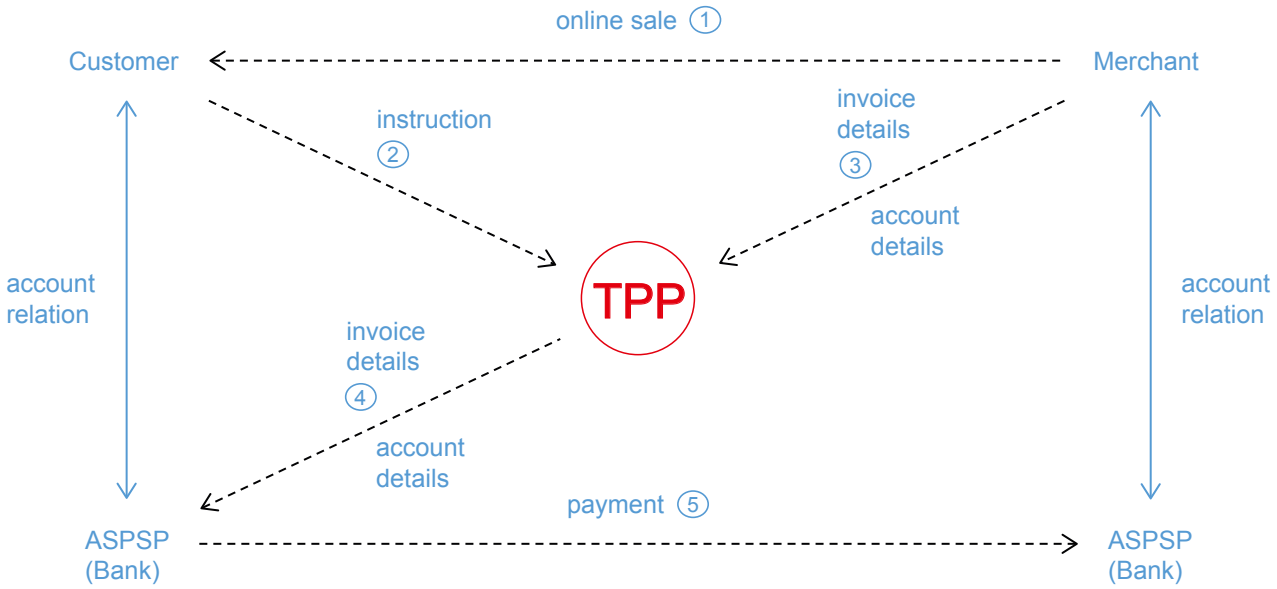
TPPs provide payment account services for payment accounts, for which they are not the account-servicing payment service provider ("**ASPSP**"). Account services are usually provided by credit institutions.

TPPs offer so-called payment initiation services ("**PIS**") or account information services ("**AIS**") to payment service users, often without entering into the possession of the funds to be transferred.

TPPs may also provide both payment initiation and account information services. The services may be offered as proprietary solutions by individual TPPs, or the services are organised in the form of payment schemes, with one or more TPPs – and usually also several ASPSP – as participants.[2]

(see chart below)

Payment Initiation Service



[1] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015.

[2] Final recommendation of the European Forum on the Security of Retails Payments for the security of payment account access services following the publication consultation/May 2014 ("**SecuRe Pay Recommendations**").

BANKING & FINANCE

2. EBA's Mission

The European legislator refrained from implementing a complete set of rules detailing open access to TPPs. Rather, the European Banking Authority ("**EBA**") was mandated to work out the technical standards for the implementation of secure authentication and communication processes. The EBA shall develop, in close cooperation with the ECB, draft regulatory standards ("**RTS**") addressed to payment service providers ("**PSP**") specifying:

(a) the requirements of the strong customer authentication when the payer accesses the payment account online, initiates an electronic payment transaction or carries out any action, through a remote channel, which may imply a risk of payment fraud or other abuses;

(b) the exemptions from the application of strong customer authentication;

(c) the requirements security measures have to meet in order to protect the confidentiality, and the integrity of the payment service users' ("**PSU**") personalised security credentials; and

(d) the requirements for common and secure open standards of communication for the purpose of identification, authentication, notification, and information, as well as for the implementation of security measures.

To get sufficient input from all relevant stakeholders, the EBA published a discussion paper ("**Discussion Paper**") which (i) addresses the challenges of its mission and (ii) invites all stakeholders to submit by 8 February 2016 responses to the questions raised by EBA in such paper.[3]

3. Timeline

The EBA is required to publish the RTS by January 2017. The European Commission shall then adopt the RTS, after which the PSD2 provides that another 18 months pass until the RTS shall be applied.[4] The exact date of said application is unknown as it depends, inter alia, on the extent to which the EU Parliament and the EU Council exercise their scrutiny rights during the adoption process. However, the date will certainly not be earlier than September 2018, but is likely to fall into calendar year 2019, and thus definitely after the transposition and application date of all other PSD2 provisions on 13 January 2018.

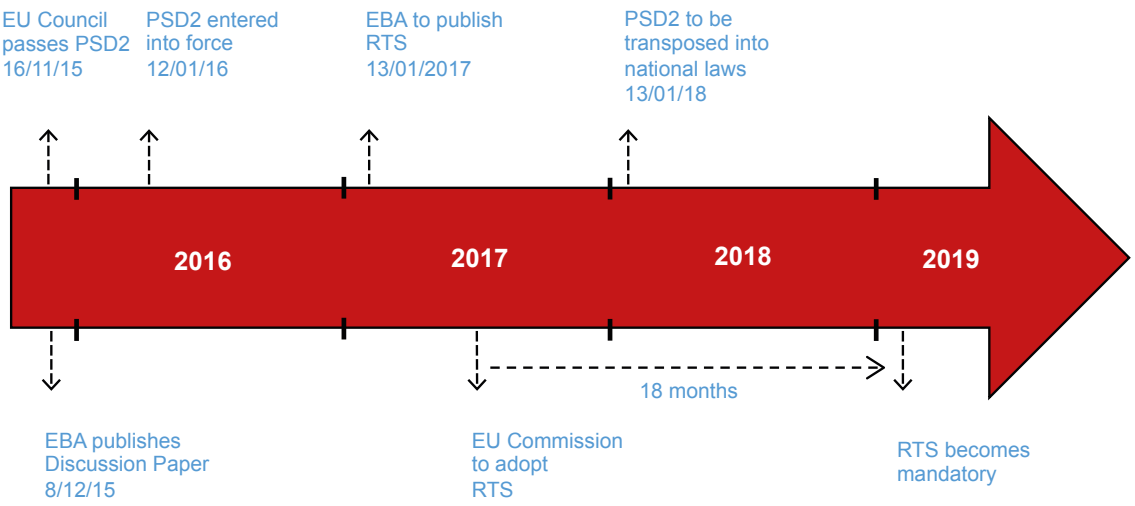
(see chart below)

4. Challenges of Open Access

Pursuant to Article 36 PSD2 the Member States shall ensure that payment institutions have access to credit institutions' payment account services on an objective, non-discriminatory and proportionate basis. Such access shall be sufficiently extensive as to allow payment institutions to provide payment services in an unhindered and efficient manner.

In practice, the new law will force banks to make account information accessible to third parties via standardised application programming interfaces ("**APIs**"). This revision is remarkable as

Timeline



[3] See www.eba.europa.eu.

[4] Article 115 para 4.

it removes the proprietary ownership banks currently have over the data of their customers. The new law is expected to spur new account related applications in the internet payment industry, providing the costumers with new analysis and information services.[5]

In enabling open access, the EBA will have to make difficult compromises between competing demands such as:

(a) high security requirements versus facilitation of the development of innovative security solutions in years to come;

(b) high security requirements versus customer convenience; and

(c) very detailed requirements for common and open standards of communication to be implemented by all banks to avoid a scenario where, in practice, the implemented solutions are so divergent that these become an obstacle for TPPs.[6]

The latter holds particularly true with respect to the highly fragmented German banking market with roughly 1,700 banking groups.[7]

5. Strong Costumer Authentication

Pursuant to Article 4 (30) PSD2 strong costumer authentication must be based on the use of two or more elements categorised as

- "**knowledge**" (something only the user knows, such as passwords, PINs and TANs);
- "**possession**" (something only the user possesses such as token, chip card or mobile telephone); and
- "**inherence**" (something the user is such as fingerprints or geometrical devices).

According to the Discussion Paper strong customer authentication requires either that the personalised security credentials are a valid combination of these elements themselves, or something which is only generated when all the elements have been provided (e.g. an algorithm in a chip produces a one-time password or cryptogram, based on a challenge response where the costumer is asked for a PIN).[8]

In light of these requirements, the Discussion Paper provides an overview of the considerations the banking authority has made so far. Finally, the EBA addresses certain questions where the authority would like to get the input from the stakeholders. Inter alia, the EBA wants to get comments on (i) the "possession" element (physical form or are data sufficient?), (ii) the "inherence" elements (are behaviour-based characteristics appropriate?), (iii) the independence of the authentication elements used (e.g. for mobile devices) and (iv) dynamic linking (which challenges do you identify?).

Notably, the EBA does not address the liability regime foreseen in PSD2. During the lawmaking process credit institutions strongly opposed to a provision[9] according to which the ASPSP will be held liable for payments triggered by TPPs without observing the rules of strong costumer authentication. The banks (unsuccessfully) argued that they cannot be held liable for services of third parties which they cannot control.

6. Possible Synergies with e-IDAS Regulation?

At the end of the Discussion Paper EBA raises the question whether the determinations of the e-IDAS Regulation[10] could help to define the requirements for strong costumer authentication under PSD2.[11] e-IDAS Regulation (i) sets out a supervisory regime to enable qualified trust service providers to deliver qualified trust services with a high level of assurance for electronic transactions and (ii) establishes a legal framework for electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services and certificate services for website authentication.

The EBA wonders whether the e-IDAS regulation might offer one (of possibly many) suitable solution(s) on which PSPs could rely for ensuring strong authentication of payments, for protecting the confidentiality and the integrity of the payment service users' personalised security credentials. In addition, the authority states that the "qualified trust services" provided by "qualified trust service providers" under e-IDAS can also be of relevance for the identification between the TPPs with the account servicing payment service providers (i.e. banks).

[5] For example, the new law will put TPPs in the position to compile the balances from all costumer accounts to provide the customer with on overall status on the basis of which certain analysis services can be offered.

[6] However, in doing so the EBA does not want to limit future innovations in communication standards (Discussion Paper, page 9).

[7] The 19 member states of the Euro zone host roughly 3,500 banking groups.

[8] Discussion Paper, page 13, note 31.

[9] Now Art. 73 para 2 PSD2.

[10] Regulation (EU) N 910/2014 on electronic identification and trust services for electronic transactions in the internal market.

[11] Chapter 4.5.

7. Exemptions for Strong Customer Authentication

Pursuant to Article 98.3 PSD2 exemptions for strong customer authentication shall be based on the following criteria:

(a) the level of risk involved in the services provided;

(b) the amount and/or the recurrence of the transaction;

(c) the payment channel used for the execution of the transaction.

With respect to (a) and (b) the EBA could imagine that exemptions could apply for:

(i) low value payments as defined in the PSD2, provided that the risks for cumulative transaction are monitored;

(ii) outgoing payments to trusted beneficiaries included in previously established white lists by a PSU;

(iii) transfers between two accounts of the same PSU held at the same PSP;

(iv) low-risk transactions based on a transaction risk analysis;

(v) purely consultative services, with no display of sensitive payment data, taking into account data privacy laws. [12]

With respect to (c), the EBA has so far not identified circumstances that would justify considering exemptions based on the payment channel used for the execution of the transaction.

8. Protection of the Payment Service Users' Personalised Security Credentials

Pursuant to Article 97 (3) PSD2 the Member States shall ensure that payment service providers have in place adequate security measures to protect the confidentiality and integrity of payment service users' personalised security credentials. To address this requirement, the EBA considers providing clarification on the following:

(i) the creation, issuance, modification and re-issuance of the credentials needs to be secured to guarantee (a) the confidentiality, and the integrity of the enrolled personalised security credentials and (b) their delivery to, or possession by, the intended costumer;

(ii) all communication channels and technical components hosting, providing access to or transmitting the personalised security credential (e.g. via a mobile device, storage in a cloud, hardware or software) need to be resistant to tampering and unauthorised access. The EBA could then also clarify how such communication channels and technical components should be certified or evaluated by independent third parties to ensure such resistance.

(iii) the security measured to protect the confidentiality and the integrity of the payment service users' personalised security credentials should be proportionate to the risks related to a fraudulent use of the PSCs to carry out fraud or to access sensitive payment data. [13]

Notably, the EBA does not mention the ECB's [14] and BaFin's [15] opposition to the sharing of personalised security credentials. These regulators raised severe security concerns with respect to the sharing of such information and the ECB came up with an alternative proposal which does not foresee any sharing. [16] Given the strong position of the ECB with respect to the practical implementation of banking law in the Euro zone, we would not exclude that such discussion re-emerges in the upcoming implementation process.

9. Requirements on Common and Secure Standards of Communication

Article 98 (d) PSD2 confers on the EBA the mandate to define the requirements for the common and secure open standards of communication for the purpose of identification, authentication, notification, and information between account servicing payment service providers, TPPs, payers, payees and other payment service providers. These requirements will also apply for the confirmation of availability of funds between issuing card-based payment instruments' PSP and account-servicing payment service providers.

To address this issue, EBA considers to clarify the following aspects:

(i) define what makes a standard "common" and "open";

(ii) the way TPPs will have to identify themselves towards the ASPSP for access to payment account information (see

[12] Discussion Paper, page 16.

[13] Discussion Paper, page 19 et seq.

[14] See SecurRe Pay Recommendations, page 5 (see footnote 2 above): "*There should be no sharing of credentials between the TPPs and the account-servicing payment service provider; the TPP should either redirect the payer in a secure manner to its account-servicing payment service provider or issue its own credentials. Both options should form part of a standardised European interface for payment access that needs to be developed.*"

[15] Payment Services Directive II: Risks and serious consequences for users and banks, 16 June 2014 ("**BaFin Paper**").

[16] Compare figure 3 of BaFin Paper (see footnote 15).

sections 5 and 6 above) and every time a payment is initiated including the purpose for which the TPP is authorised by the costumer and requesting access to the account-servicing payment provider upon each connection;

(iii) the way TPPs and ASPSPs communicate between themselves and with the costumer in a secure manner;

(iv) the minimum functionalities requirements that the future common and secure open standards of communication will have to provide;

(v) the minimum security controls that the future common and secure open standards of communication will have to provide related to the potential unauthorised or fraudulent access to payment accounts or initiation of a payment transaction;

(vi) the minimum technical requirements that could apply to the common and secure open standards of communication, the minimum reachability requirements for each ASPSP to provide at least one interoperable interface, servicing all requirements of the RTS and compliant with PSD2 regulation, while TPPs would have to adapt their services to the respective standardised interfaces used.

10. First Comments

The mere fact that the EBA published a 'discussion paper' and not a 'consultation paper' (which already suggests specific regulatory solutions) indicates that the EBA team led by Dirk Haubrich does not feel fully comfortable with the assignment conferred on it by the European legislator. The questions directed by the Discussion Paper to the stakeholders are often of very basic nature, leaving the reader with the impression that the regulator is still at the beginning of its considerations. Therefore, market observers are more than sceptical whether the EBA will work out a reliable and practical solution within the remaining time frame.

Further, the London based authority is more and more shadowed by the ECB which assumed in 2014 important supervision competences for the banks of the 19 Euro member states. Although the ECB's supervisory mandate does not extend to the supervision of payment services, we expect a strong involvement of the Frankfurt based regulator in the upcoming RTS setting process. The ECB already issued a legal opinion on PSD2[17], providing firm views on many aspects of the new law. And even if the EBA would try to keep the ECB out of the RTS setting process, the Central Bank would definitely re-access the PSD2 arena, if it comes to the practical implementation of the new law in 2019. The experience with other RTS issued by the EBA shows that such standards are always subject to the practical implementation of the competent bank regulators.

Further, certain member states[18] and consultancies[19] are already pushing forward in setting up API standards. This will make it difficult for EBA to develop and establish own independent standards. To keep control of the entire process, EBA obviously needs to beef up its efforts to deliver a persuasive solution in January 2017.

Dr. Christof Aha,
Lawyer,
BEITEN BURKHARDT
Rechtsanwaltsgesellschaft mbH,
Frankfurt am Main

Dr. Andreas Lober,
Lawyer,
BEITEN BURKHARDT
Rechtsanwaltsgesellschaft mbH,
Frankfurt am Main

Dr. Christoph Schmitt,
Lawyer,
BEITEN BURKHARDT
Rechtsanwaltsgesellschaft mbH,
Frankfurt am Main

Please note

[17] See http://www.ecb.europa.eu/ecb/legal/opinions/html/act_13000_amend.en.html. Despite the fact that such opinions are formally issued by the Directorate General Legal Services we assume that it was primarily drafted by the Oversight Division of the Directorate General Market Infrastructure & Payments.

[18] See for example the paper "Banking for the 21st Century: driving competition and choice, March 2015, issued by the UK's Treasury Department.

[19] See www.openbankproject.com.

BANKING & FINANCE

Imprint

This publication is issued by
BEITEN BURKHARDT Rechtsanwaltsgesellschaft mbH
Ganghoferstrasse 33, D-80339 Munich
Registered under HR B 155350 at the Regional Court Munich/
VAT Reg. No.: DE811218811

For more information see:
www.beitenburkhardt.com/imprint

Editor in charge

Dr. Christof Aha,
Lawyer

You will find further interesting topics and information about Banking & Finance on our website.

BEITEN BURKHARDT · RECHTSANWALTSGESELLSCHAFT MBH
FRANKFURT AM MAIN · WESTHAFEN TOWER · WESTHAFENPLATZ 1 · 60327 FRANKFURT AM MAIN · TEL.: +49 69 756095-0 · FAX: +49 69 756095-512
HEINRICH MEYER · HEINRICH.MEYER@BBLAW.COM · DR. CHRISTOPH SCHMITT · CHRISTOPH.SCHMITT@BBLAW.COM
MUNICH · GANGHOFERSTRASSE 33 · 80339 MUNICH · TEL.: +49 89 35065-0 · FAX: +49 89 35065-123
DR. DIRK TUTTLIES · DIRK.TUTTLIES@BBLAW.COM · MICHAEL ZIEGLER · MICHAEL.ZIEGLER@BBLAW.COM

01/2016