Payment Services Directive 2
–
(Cyber) Security for Payment Services Providers

Stéphan Hellmann

S1727923

Correspondence Address:
Cyber Security Academy, Wilhelmina van Pruisenweg 104, 2595 AN, The Hague.
THE NETHERLANDS

info@csacademy.nl

Abstract

One of the objectives of the European Union is to foster competition within its borders in order to e.g. create more choice for the consumers and reduce costs. To this end, the revised Directive on Payment Services (PSD2) allows many new, non-banks parties – third party payment services providers (TPPs or PSPs) – to enter the European payment market and access consumers' sensitive data, with the aim to offer new, convenient and secure payment services leveraging on new technologies. This research analyses the regulatory technical standards of strong customer authentication (RTS on SCA&SC), issued by the European Banking Authority (EBA) in order for these new non-bank parties to ensure a pre-required level of (cyber) security. The immediate objective of the research is to address some of the missing or unclear cyber security related definitions in the RTS and provides recommendations about some of the missing or unclear cyber security requirements, in order to help PSPs and banks identify an appropriate trade-off. In the end, balancing security and convenience will prove key to one of the objectives of PSD2 – the adoption by all Europeans of a digital payment market to contribute to the broader adoption of the European digital single market, a second EU-objective –, as consumers will not embrace a solution too cumbersome nor will they accept a payment service they cannot trust.

Keywords

PSD, PSD2, Authentication, Authorisation, Consumer, Convenience, Cyber Security, Payments, Directive, RTS, Risk-Based, ASPSP, AISP, PISP, Banks, Payment Service Providers, Mobile Payments, Smartphone, Wearable, Single Digital Payment Market, European Commission, ECB, EBA.

To Aurélie and Naèle, whom I love unconditionally.

Acknowledgment

This research would not have been possible without the support of many people. I would like to express special thanks to my advisers, Prof. dr.ir. J. (Jan) van den Berg and drs. Dennis de Geus, who read my drafts, challenged them and helped make sense of this report. Thanks to all the colleagues who offered guidance and support, in particular Steven Maes, for the many hours spent to explain the implications of PSD2 for a.o. Belgian banks, always in a comprehensive way. Thanks to ING Belgium, in particular to Johan Kestens (Chief Technology Officer) and Philippe Tasset (Chief Information Security Officer), for sponsoring my study and providing with the valuable time to take the courses. Thanks to the Cyber Security Academy's professors and lecturers for the knowledge and the many insights shared regarding the complex matter that is cyber security, and to my fellow students for the support and fun during the past two years. And finally, the most special thanks to my partner, family, and friends who endured this long process with me, always offering true support and love.

Table of Contents

1. Introduction

The official introduction of the Euro currency in 2002 made cash payments more convenient anywhere in the European Union (EU). The burden of exchanging currencies while travelling abroad was replaced with easy cash payments in Euro in each member state of the EU. The burden remained though for electronic payments: at the time, it was rarely possible to pay a restaurant bill in France with e.g. a Dutch bank debit card. And transferring money between accounts in different European countries proved time-consuming and often problematic.

To address these problems and to further harmonize the retail payment landscape within its borders, the EU, by means of its European Parliament and European Council, adopted the Payment Services Directive (PSD) in 2007[1]. The directive, turned into law in 2009, ensured that each EU member state abides by the same rules regarding electronic payments. From then on, it became easier to use a banking debit card issued in a EU country to buy goods in another EU country. The introduction of Single Euro Payment Area (SEPA)[2] a few years later – the key deliverable of PSD – enabled more than five hundred million European citizens, businesses and European public authorities to experience electronic payments or money transfers throughout Europe as easy and safe as in-land transactions or cash payments. The PSD has been the fundament for the creation of a EU single market for payments, introducing the concepts of fair and open access to payments markets and increase of consumer protection. Developing further this integrated internal market for safe and easy electronic payments proves vital for the growth of the EU economy[3]. To this end, an updated PSD has been adopted in April 2016: the Payment Services Directive 2 (PSD2), which member states of the EU must transpose into their national law before January 2018.

PSD2[4] has for objective to further standardize, integrate and improve the payment efficiency in the European Union in order to move towards a EU single digital payment market. One key feature in the revised directive is the promotion of innovation – such as new mobile payment services – in the payment environment, aiming at harmonizing prices, reducing costs and creating convenience for customers. PSD2 seeks also to open up the European payments market to new (innovative) players – new third party providers of (new) payment services – thus creating more competition by ensuring an equal playing field for all payment service providers. A third important feature in PSD2 is the incorporation of new and emerging payment services and methods in the regulation, thus providing more clarity on the use of e.g. mobile payments and online payments. A fourth key feature aims at offering a better protection to customers by improving and standardizing the security of payment processing across the EU.

While the different regulations were so far seeking to harmonize the payments environment in the EU, PSD2 shows many differences that will lead to major, more radical changes[5]. Information about customers' payment accounts is essential for any companies willing to develop new, innovative financial products and services. Until now, the only companies having access to this information were the customers' own banks, which house, a.o., their payment accounts. PSD2 allows for a whole new group of payment service providers – (PSPs) or third party payment providers (TPPs) – to access these data in order e.g. to aggregate them into one

[1] Directive 2007/64/EC of the European Parliament and of the Council, Official Journal of the European Union, November 2007
[2] Regulation (EU) No 260/2012 of the European Parliament and of the Council, Official Journal of the European union, March 2012
[3] Skinner, C., *The Future of Finance After SEPA*, The Wiley Finance Series, 2008
[4] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015, on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, Official Journal of the European Union, November 2015
[5] Rohan, P., PSD2 in Plain English, Rohan Consulting Services Limited, 2016

single overview – Account Information Service Providers (AISPs)[6] – or to initiate a payment transaction for her/him – Payment Initiation Service Providers (PISPs)[7] –, provided the customer gave her/his consent.

Although fostering competition and innovative services in a conservative payment market is a legitimate objective, allowing PSPs to process sensitive information and personal data is likely to offer many risks when these parties lack adequate security measures. Besides convenience, new payment methods will also provide malicious actors with new opportunities to access these data so far highly protected by banks, to enrich themselves at the expense of the consumers – end customer and merchants – by plundering their bank accounts. If e.g. new methods of mobile payments offered by PISPs prove unsecure, the consumers will refrain from adopting their services and fall back on the more conservative bank services, thus hampering the very objective of PSD2: have all European to partake to the digital payment market.

Methodology

The purpose of this *exploratory* research is to contribute to the enhancement of (cyber) security regarding the upcoming account information and payment transaction activities that third party providers will offer. A better understanding of these PSPs' needs regarding (cyber) security will be sought through a *qualitative analysis* of open answers of a survey submitted by the European Banking Authority (EBA) to all stakeholders forming the payment landscape, after publishing a consultation paper on the draft Regulatory Technical Standards on Strong Customer Authentication an Secure Communication[8] (RTS on SCA & SC) EBA was mandated to develop, – together with the European Central Bank (ECB) – for PSPs. Once the (cyber) security needs were identified, relevant *scientific and professional literature* has been reviewed in order to provide well-founded recommendations.

Structure

While chapter 1 introduces the research's topic and motivation, along with the applied methodology, chapter 2 sets the scene of the European payment landscape since 2000, introduces PSD2 and its radical changes. Chapter 3 reports on the different mandates related to PSD2, summing-up the five guidelines and four RTS EBA was tasked to develop and identifying which of this mandates are relevant to cyber security and motivating further enquiry on the RTS on Strong Customer Authentication and Secure Communication only. In chapter 4, first a short description of the twenty-two articles of these RTS is given, followed by a qualitative analysis of the hundred forty-six responses to an EBA survey where cyber security related issues are identified. Recommendations on some of these issues are motivated in chapter 5, emphasizing on the need for clear, common definitions for important topics (e.g. authentication and authorisation) and on allowing ASPSPs and PSPs to perform essential risk-based approaches, a subject facing reluctance from EBA. Chapter 6 concludes the research. Subjects for future researches are shortly recommended in chapter 7, coming forth from the qualitative analysis. References to literature reviewed are provides in chapter 8. Three addendums are completing the report: one relating to the main PSD2 nomenclature, one reporting the list of respondents and the last describing the reconstruction of Europe after world war II and the premises for one integrated EU market, constituted amongst other of the digital payment market.

2. The European payment landscape since the early 2000s

[6] www.mint.com
[7] www.ideal.nl
[8] Consultation Paper on the Draft Regulatory Technical Standards specifying the requirements on strong customer authentication and secure communication under PSD2, European Banking Authority, EBA/CP/2016/11, page 6, 12 August 2016

At the turn of the millennium, the European Union (EU) can rely on a European Single Market without borders – and its related freedom of circulation – and on the Euro as a single currency – in an introduction phase – to support the internal market (see a detailed research in addendum). Seeking further harmonization within its borders, the EU aimed at creating a single market for payments, by standardizing payment methods and enabling more competition. In 2007, the Directive on Payment Services I (PSD) was adopted, establishing a set of rules for financial institutions – seeking to increase competition between them – and allowing new entrants on the payment market, with as key achievement the introduction of Single European Payment Area (SEPA). In 2015, a revision of the PSD was adopted (PSD2), with an extra focus on increasing competition and innovation by opening the payment market to new players and removing legislatively remaining obstacles – mainly formed by the financial institutions themselves, afraid of losing market shares –.

A. Directive on Payment Services (PSD)

In 2007, all 30 countries of the European Economic Area (EEA) – constituting the European Single Market – adopted the Directive on Payment Services[9] (PSD) – originally known as New Legal Framework for Payments[10] –, committing to transpose the directive into national legislation before November 2009. This directive, administered by the European Commission, provided the legal foundation for the creation of a European single market for payments, with a set of rules to regulate payment services and (future) payment services providers and users within the EU and beyond.

Main focus points

Concretely, PSD's main focus points were:

a. Establishing a single EU market in payment services and consistency between national rules
b. All types of payment services carried out in EU currencies within the EU
c. Creating transparency of conditions and information requirements for payment services
d. Clear description of the respective rights and obligations of payment service users and payment service providers in relation to the provision of payment services
e. Consumer protection

The aim was three-fold: striving to make cross-border payments as easy, efficient and secure as in-border payments (e.g. establishing maximum execution times for payments in euro and other EU/EEA currencies and harmonizing customer protection); increasing competition by opening up the payment market to new entrants (e.g. introducing a new licensing regime to encourage non-banks to enter the payment market); and establishing the legal foundations for the most important requirement of PSD: the Single Euro Payments Area initiative[11] (SEPA).

SEPA

SEPA is an initiative aiming at simplifying bank transfers done in euro, improving the efficiency of cross-border payments and grouping all the different national payment markets of the EU member states into one single domestic one, thus creating one payment area within the

[9] Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC

[10] *Communication from the Commission to the Council and the European Parliament on a New Legal Framework for Payments in the Internal Market*, COM(2003) 718 of 2nd December 2003; 2. *New Legal Framework for Payments in the Internal Market* - BEUC position on the Communication, Bureau Européen des Unions de Consommateurs (BEUC), BEUC/065/2004, 15 February 2004

[11] Regulation (EU) No 260/2012 of the European Parliament and of the Council of 14 March 2012 establishing technical and business requirements for credit transfers and direct debits in euro and amending Regulation (EC) No 924/2009

European borders, in which credit transfers, direct debits and card payments occur in a same, standardized way. A concrete achievement of SEPA is the fact that a Dutch citizen can now use her/his payment card issued by a Dutch bank to pay electronically in France in a same way she/he would perform the electronic payment in the Netherlands. Another concrete achievement is the fact that an Italian citizen working in Germany can still use her/his Italian payment account – which under SEPA became an International Bank Account Number (IBAN) – to receive her/his German salary. These two achievements were not possible in the early 2000s.

Toward a revision of the directive

Although many goals have been achieved with PSD to integrate retail payments in the EU – e.g. cross-border payments are now as easy and safe as in-border payments – some ambitions still remained unanswered, the most important one being the increase of competition. In its assessment of the PSD implementation in 2012[12], the European Commission (EC) concluded that many gaps remained between the goals sought to be achieved and the actual embedment of the directive. For example, one aim was to increase the collaboration between payment institutions and banks, as the formers are highly dependable of the latters to offer their services. The assessment showed that many banks were still reluctant to share information about customers' bank account with the payment institutions. Another issue found by the EC was that all payment services are still mainly provided by banks and are far too similar, leaving a very few choices for the payment service users (consumers or merchants). In other words: banks do not innovate enough and rely on their 'comfort-zone' business model. The EU also sought (and still does) to leverage on innovative technologies to improve the efficiency of payments and make electronic payments safer[13].

Therefore, the European Commission proposed in 2013 a revision[14] of the PSD, which aimed at creating a competitive level playing field on the electronic payments market – encouraging new providers of card, Internet and mobile payments; increasing the efficiency, transparency and choice of payments instruments for payment services users; fostering the digital economy – one of the objective of the Single Market Act II –; and ensuring a high level protection of the consumers and merchants. This revision was adopted by the European Parliament and the Council of the European Union in the fall of 2015 and became law in January 2016, requesting all member states to transpose the revised directive (also named PSD2) into national laws before January 2018.

B. Revised Directive on Payment Services (PSD2)

The revised directive on Payment Services [15] (PSD2), although building further on its predecessor, is also very different. Where PSD harmonized the traditional way in which payments are made, PSD2 is creating a legal framework for new type of payments services and non-banks players – called third party payment service providers (TPP or PSP) – to access bank customer account information, making it mandatory for banks to provide this information. Information from a customer's payment account is very useful, as it is a vital ingredient for developing financial products. For many years, only the bank that managed the customers'

[12] Impact Assessment, Commission Staff Working Document, European Commission, Vol. 1/2, SWD (2013), 24 July 2013

[13] *PSD2 Guidance – Guidance for implementation of the revised Payment Service Directive*, European Banking Federation, September 2016

[14] Proposal or a Directive of the European Parliament and of the Council, on payment services in the internal market and amending Directives 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC, European Commission, COM(2013) 547, 24 July 2013

[15] Directive (EU) 2015/2366 Of The European Parliament And Of The Council, on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, 25 November 2015

accounts had this information, which never shared it with other banks, let alone with new players. As more providers will be allowed to retrieve this information, innovation and competition will increase, leading banks to fear for the persistence of their conservative business models and to urgently redefine them. PSD2 allows many service providers – with a specific authorization – to initiate payments and access information from an account, if authorized by the customer.

Main changes

Concretely, PSD2 brings the following changes:

a. Scope extension beyond Europe and of the definition of a "Payment Institution." While the original PSD applied only to transactions occurring within the EU – the so-called two-leg transactions, where both the payer and the payee are based in the EU – and in EEA currencies (including e.g. the British pound and the Danish krone), PSD2 extends this scope to "one leg out" transactions – when either the payer or the payee is based out of the EU – and to payments in all (non-EEA) currencies (including e.g. the US dollar and the Chinese yen). The directive also extends the 2007 PSD definition of "Payment Institution" to include new categories of third-party payment providers.
b. Strong focus on electronic payments: cards, online and mobile payments.
c. Third-party payment initiation. PSD2 encourages competition in European payments by regulating payment initiation service providers (PISPs, one of the two most important new players). These services operate using a "push" payments process unlike the traditional, card-based "pull" payments flow.
d. Third-party account access. PSD2 also regulates account information service providers (AISPs, the second most important new players). These providers act as aggregators of customer payment account information.
e. Strong emphasis on transparency and customer protection. One of the main goals is to encourage lower prices for payments. Therefore, the current card charges on merchants – standard practice in EU – will be banned and these merchants will not be allowed to surcharge customers – now a common practice in order to compensate for the card charges imposed by the card's issuers (e.g. bank or credit card company) – for using their payment cards. PSD2 seeks to standardize the different approaches to surcharges on card-based transactions, which are currently applied across EU.
f. Strengthening of the security of online payments and account access. PSD2 introduces and defines the concept of strong customer authentication as new security requirements for electronic payments and account access, along with new security challenges relating to AISPs and PISPs.

Levelling the playing field

In its quest to foster more competition in the payment landscape, the EU introduces with PSD2 a legal framework for a new type of players: thirst party providers (TTP). Willing to invest in new payment technologies, PSD2 is encouraging new – non-banks – companies to enter the payment (services) market in order to break the bank's monopoly and diversify the very conservative product offer. PSD2 seeks also to provide more clarification by defining a new nomenclature regarding payment services: the directive introduces the concepts of a.o. Payment Service Providers (PSP) consisting on the one side of Account Servicing Payment Services Providers (ASPSP, e.g. the banks holding the customers' accounts and credit card companies), and on the other side of the TPP: Account Information Servicing Providers (AISP) and Payment Information Services Providers (PISP). In this regard, PSD2 enables access to customers' bank accounts not only to financial but also non-financial institutions – called Access to Accounts (XS2A) – resulting in security concerns not clearly answered by the directive,

relying on the Regulatory Technical Standards on security, authentication and communication – currently under development by the European Banking Authority (EBA) on the request of the EU – to provide with a detailed "how-to".

AS PSP

An Account Servicing Payment Service Provider is any '*financial institution that offer payment accounts (e.g. current accounts, credit cards) with online access (internet banking), and under this legislation will be obliged to open up an interface to allow authorised and registered third parties to initiate payments and access account information*'[16]. Most of the ASPSPs are the banks, managing their customers' banking accounts. But other financial institutions, recognized and authorized as payment institutions, are also ASPSP (e.g. credit card companies).

PISP: how payments information service will work with PSD2

A payment initiation service is "*a service to initiate a payment order at the request of the payment service user with respect to a payment account held at another payment service provider*"[17]. In other words, payment initiation services providers help consumers to make online credit transfers and inform the merchant immediately of the payment initiation, allowing for the immediate dispatch of goods or immediate access to services purchased online. For online payments, they constitute an alternative to credit card payments as they offer an easily accessible payment service, as the consumer only needs to possess an online payment account.

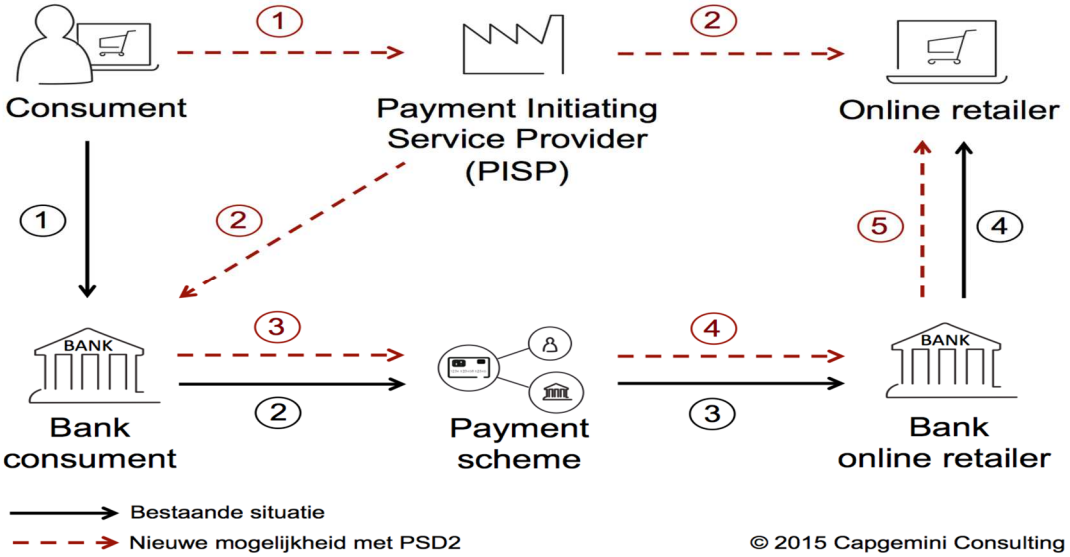

Figure 1 – Current vs. post-PSD2 process of online payment with debit/credit card[18]

Payment initiation services providers allow consumers that shop online to pay for their purchases through a simple credit transfer from their payment account. In some countries, these services are already in use (55% of internet payments in the Netherlands). By providing a proper legal framework in which these services can be offered, PSD2 opens possibilities for providers of these services to operate across the EU and to compete on an equal basis with other regulated players in the market, such as banks.

[16] Boden, A., Hipperson, M., Sawyer, J., Williams-Gardener, S., McParlane, T., Explaining PSD2 without TLAs is tough!, white paper, Starling Bank, 2015

[17] *Preparing for PSD2 : exploring the business and technology implications of the new payment services directive*, white paper, Finextra Research, March 2016

[18] Capgemini Consulting, 2015

AISP: how account information service will work with PSD2

An Account Information Service Provider is '*any online provider that wishes to aggregate online information on one or more payment accounts held with one or more other payment service providers who typically presents the information in a single dashboard for a customer*'[19]. Account information services "*provide consolidation information on one or more payment accounts held by the payment service user with one or more other payment services providers*"[20]. In clear, account information services allow consumers and businesses to have a global view on their financial situation, for instance, by enabling consumers to consolidate the different current accounts they may have with one or more banks and to categorise their spending according to different typologies (food, energy, rent, leisure, etc.), thus helping them with budgeting and financial planning. Mint.com[21] is the most famous example, providing balance sheet services to consumers in the U.S. and Canada.

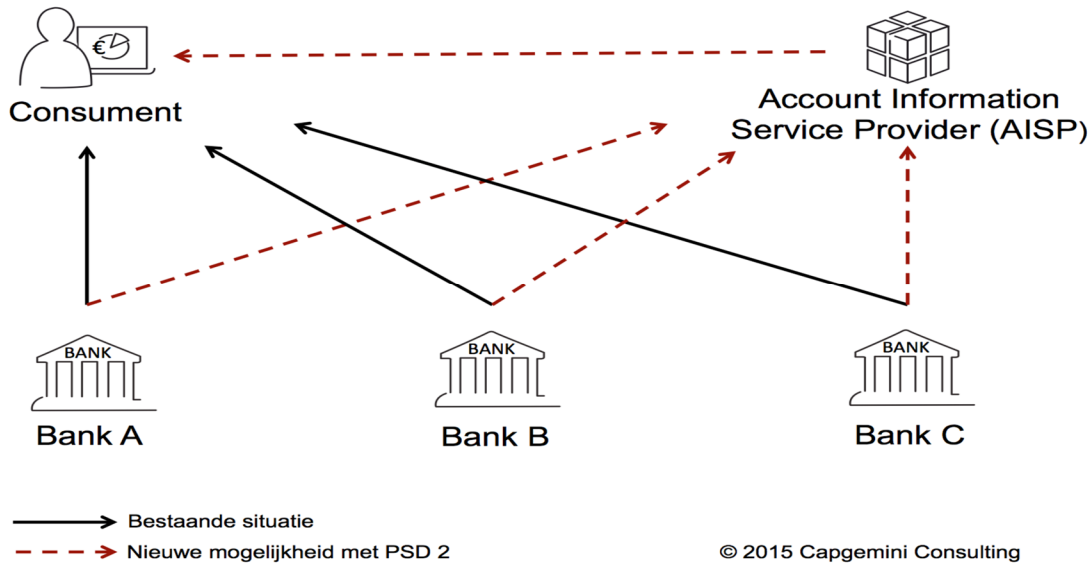

Figure 2 - Current vs. post-PSD2 process of online checking of multiple bank information[22]

Account information service providers already exist today and offer tools that allow companies and consumers to have a consolidated view of their financial situation. Not yet being regulated, PSD2 provides a common legal framework setting the rules and conditions under which these providers can access the financial information on behalf of their clients. The services providers will be able to operate without obstacles and reach a broader audience, not used yet to such account managing services.

Payment service provider issuing card-based payment instruments

Any authorised payment service provider, be it a bank or a payment institution, can issue payment instruments – e.g. debit and credit cards –. PSD2 allows payment service providers that do not manage the account of the payment service user to issue card-based payment instruments to that account and to execute card-based payments from that account. Such third party payment service provider – e.g. a bank not servicing the account of the payer – will be able, with the customer or merchant's consent, to receive from the financial institution where the account is held, a confirmation – a simple yes/no answer – as to whether there are sufficient funds on the account for the payment to be made.

---

[19] Boden, A., Hipperson, M., Sawyer, J., Williams-Gardener, S., McParlane, T., *Explaining PSD2 without TLAs is tough!*, white paper, Starling Bank, 2015

[20] *Preparing for PSD2 : exploring the business and technology implications of the new payment services directive*, white paper, Finextra Research, March 2016

[21] source: www.mint.com

[22] Capgemini Consulting, 2015

API to enable XS2A

PSD2 and the Regulatory Technical Standards on security, authentication and communication – under development by the EBA –, are promoting account access by third parties providers (XS2A, the most debated part[23] of PSD2), in order to foster competition on the payment services market. APIs are foreseen to allow all Payment Initiation Service Providers (PISPs) and Account Information Service Providers (AISPs) to connect to Account Servicing Payment Service Providers (AS PSP) in a secure and effective manner.

Application Programming Interfaces (API) – are a means for accelerating digital transformation. APIs, in a technical sense, are simply '*a mechanism that allows the capabilities of a computer program to be used by other computer programs*'[24].
APIs have been used in the past decade by many organizations that hold large amounts of data to become platforms for third party innovation and share these data. Large platforms such as Google, Twitter and Facebook offer APIs to third parties, e.g. for login or for initiating messages. In the payment space, PayPal[25] was the first to introduce external APIs in 2010, later to be followed by others (e.g. iDEAL in The Netherlands).

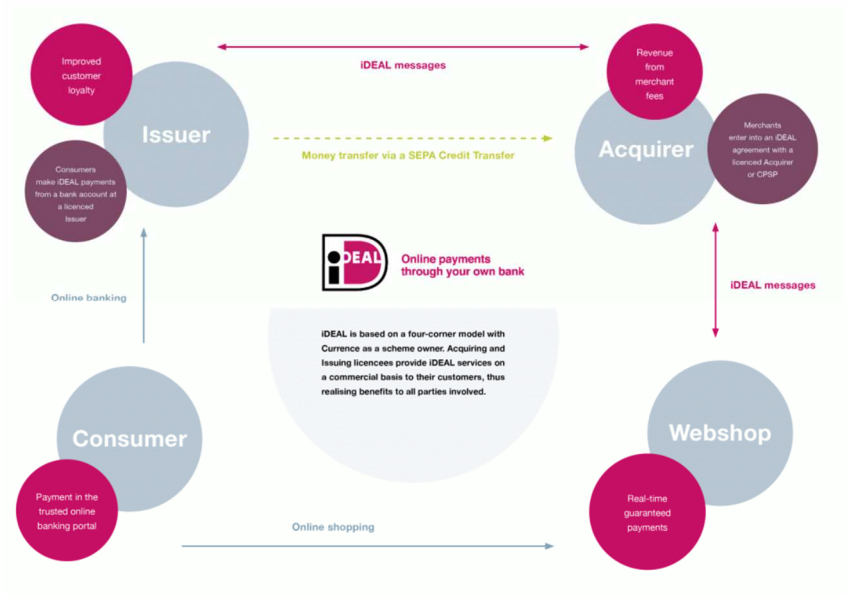

Figure 3 - iDEAL payment process and roles[26]

Emphasized upon in PSD2, external APIs are becoming a hot topic within the European payment landscape. APIs will provide customers with more options to interact with their bank, next to usual online and mobile banking applications. Fostering XS2A, APIs will open up banks' accounts and associated data to TPPs – AISPs and PISPs, if authorized by the payment service user (the bank account holder, either the customer or the merchant) –, impacting the traditional business model of banks and the way they conduct payments.

[23] Lycklama, D., *PSD2 'Access to account' (XS2A) – forcing a marriage between banks and Fintech, romance still to be discovered*, Interview, 24 June 2015
[24] Woods, D., *Don't Get Ubered: APIs Hold Key To Digital Transformation*, Blog-post, Forbes Tech, 19 October 2015
[25] source : www.paypal.com
[26] source : www.ideal.nl

Customer protection

In PSD2, updated definitions ensure a level playing field between different – new – providers and address more efficiently the level of consumer protection needed concerning the use of payment services.

PISPs, AISPs and providers issuing payment instruments will only be allowed to provide the services that the payer wants to use, and only have access to the payer account part needed to provide the service. The providers offering payment instruments or payment initiation services will only be able to receive information from the payer's bank on the availability of funds – a yes/no answer – on the account before initiating the payment – with the explicit consent of the payer –. Account information service providers will receive the information explicitly consented by the payer and only to the extent they are necessary for the service provided to the payer.

Improved security measures will allow consumers to be better protected against fraud – or other abuses – and payment incidents. Harmonised liability rules will cover eventual consumers losses in case of unauthorised transactions, ensuring enhanced protection of the legitimate interests of payment users – both customers and merchants –. Except in cases of fraud or gross negligence by the payer, the maximum amount a payer could, under any circumstances, be obliged to pay in the case of an unauthorised payment transaction will decrease from €150 to €50 – the so-called unconditional refund right[27] –. In such cases, payers can request a refund even in the case of a disputed payment transaction.

Consumers will also be better protected when the transaction amount is not known in advance – e.g. car rentals and hotel bookings. The payee will only be allowed to block funds on the account of the payer if the payer has approved the exact amount that can be blocked. The payer's bank shall immediately release the blocked funds after having received the information about the exact amount and at the latest after having received the payment order.

PSD2 increases consumer rights when sending transfers and money remittances outside the EU or paying in non-EU currencies, by including 'one-leg' transaction in the scope of the PDS2 rules on transparency, hence covering payment transactions to persons outside of the EU.

Finally, the new directive obliges EU Member States to appoint competent authorities to handle complaints of payment service users and other interested parties, such as consumer associations. Payment service providers should also put in place a complaints procedure for consumers that they can use before launching court proceedings. The new rules will oblige payment service providers to answer in written form to any complaint within 15 business days[28].

Conclusion

In its quest to foster more competition in the payment landscape, the EU introduces with PSD2 a legal framework for a new type of players – thirst party providers (TTP) –, encouraging non-banks players to enter the market with innovative ideas and technologies. PSD2 also emphasizes on the protection of payment services and the consumers using it, as allowing many more parties to access their sensitive data can alter the security of payments now offered by banks. One of the nine mandates that EBA was granted with for the implementation of PSD2, is the development of regulatory technical standards specifically linked to payment security and customer protection.

[27] Boudewijn, G., *PSD2 : Almost final – a state of play*, European Council Blog and Discussion Board, 18 June 2015
[28] Current EU Directives & Regulation, Payment Talk, VeriFone, August 2015

3. PSD2 governance

While PSD2 is setting the scene towards a digital single market by encouraging new innovative – and potentially disruptive – competitors to enter the payment landscape and fostering access to customers' accounts (XS2A) to non-banks, it also aims at a better protection of customers when performing online (cross-border) payments. In this sense, the directive proves somewhat paradoxical at first sight, as it seeks to ensure more security while allowing new players to provide payment services (AISP and PISP), which do not have the long experience and heavy

regulation on a.o. security that banks and credit card companies – ASPSPs representing most of the payment institutions so far – have[29].

PSD2 defines the rules for an increased payment security, which forms a key issue for many payment users – e.g. consumers and merchants – when doing electronic payments. As of 2018, all payment service providers, including banks, payment institutions or third party providers (TPPs), will need to prove yearly that they have specific security measures in place – ensuring safe and secure payments – based on – external or internal – audit of the operational and security risks at stake and the mitigating measures in place. PSPs issuing payment instruments are subject to various obligations such as ensuring that a payment service user's personalised security credentials are not accessible to other parties and not sending unsolicited payment instruments (except as a replacement).

In order to ensure that all payment service providers play by the same rules, the European Parliament and the Council of the European Union have mandated the European Banking Authority – in close collaboration with the European Central Bank – to develop a set of Regulatory Technical Standards (RTS) and guidelines (GL) – see figure 6 –, consolidating all needed requirements for the enhancement of consumer protection, promotion of innovation and improvement of the security of payment services across the European Union.

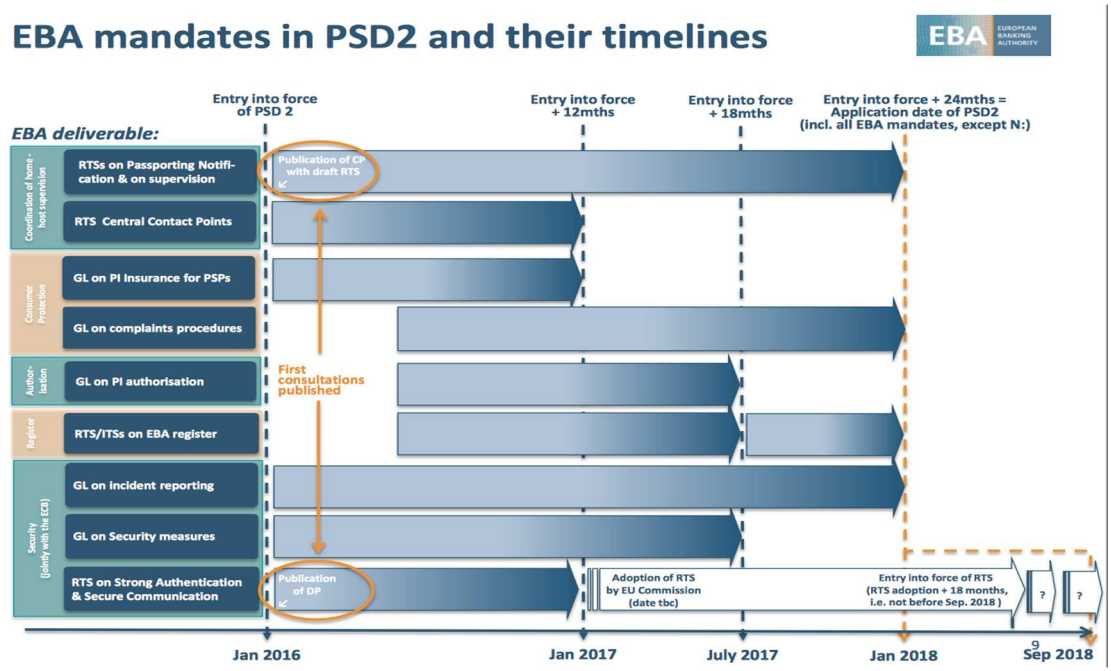

Figure 4 - EBA mandates in PSD2 and their timelines[30]

Governance and timelines

Many governance bodies are involved, at different levels and for different purposes.

As already described in chapter 2, the European Commission (EC) – after evaluating the implementation of the first Payment Service Directive in 2012 – came to the conclusion that the directive needed some adaption to close unforeseen gaps, in order for instance to foster competition on the market for payment services. Therefore, the EC proposed a revised text for the directive (PSD2), which was adopted in 2015 by the European Parliament and the Council

[29] S. Mansfield-Devine, Open banking : opportunity and danger, Computer Fraud & Security, October 2016.

[30] Goffinet, G., EBA mandate on the RTS on strong customer authentication & secure communication – Status update, EBA, European Payments Gateway Conference, Brussels, 9 June 2016

of the European Union and entered into force in January 2016. EU member states' local government must transpose PSD2 into national law before January 2018.

The European Banking Authority (EBA), created in 2011[31], has been mandated by the EU Parliament and the Council to develop a set of Regulatory Technical Standards and guidelines for the different stakeholders, including the needed requirements to ensure a rightful implementation of PSD2. When using the abbreviation 'EBA', no confusion should be made with the European Banking Association (also abbreviated as EBA) that reports to the European Central Bank (ECB). The directive and its implementation are under the supervision of the European Parliament and the Council of the European Union, not the ECB.
The national banks (such as the Belgian National Bank for Belgium) are mandated by the national governments to supervise and audit the implementation of PSD2 and its RTS and guidelines by the financial sector. The financial sector (in Belgium represented by Febelfin, the Federation for the Belgian Financial sector) is appointed with the task to review both PSD2, RTS and guidelines texts and provide advices to the EBA about feasibility and adaptation – via a task force populated by the four biggest banks and two smaller banks –.

Regulatory Technical Standards (RTS) vs guidelines

Under PSD2, payment institutions are required to fulfil a variety of requirements in order to obtain an authorization to provide payment services, very similar to the requirements issued under the first PSD. The main changes relate to the enhanced levels of payment security under PSD2. Entities that wish to be authorised as a payment institution must provide with their application a security policy document, as well as a description of security incident management procedure, contingency procedures, etc.
While the EU introduces through PSD2 new legal terminologies to clarify the payment (service) landscape, the European Banking Authority (EBA) – an independent authority whose goal is to maintain financial stability in the EU, continuously on the watch for eventual new risks in the EU banking sector – has been entitled by the European Parliament and the Council of the European Union with the task to develop – in close collaboration with the ECB – Regulatory Technical Standards (RTS, mainly for the players in the payment services market) and to design guidelines (mainly for regulators). The RTS are different from what payment professionals understand under the term 'technical'[32]. The RTS are more of a set of rules and principles than a specific technical description of how PSD2 needs to be implemented.

Five categories

The RTS and Guidelines are classified in different five categories[33]: coordination of home-host supervision, consumer protection, authorisation, register and security (the governance documents for the latter category is developed in collaboration with the European Central Bank).

Category I: Coordination of home-host supervision

[31] Goffinet, G., *EBA mandate on the RTS on strong customer authentication & secure communication* – Status update, EBA, European Payments Gateway Conference, Brussels, 9 June 2016
[32] Lycklama, D., *PSD2 'Access to account' (XS2A) – forcing a marriage between banks and Fintech, romance still to be discovered*, Interview, 24 June 2015
[33] Goffinet, G., *EBA mandate on the RTS on strong customer authentication & secure communication* – Status update, EBA, European Payments Gateway Conference, Brussels, 9 June 2016

RTS on passporting notification and on supervision[34]

PSD2 aimed at creating more competition in the provision of payment services in the EU internal market, by authorising new players to become payment institutions (PI) and to provide payment services to local and cross-border customers. Collaboration between the relevant authorities of the different member-states involved – the home member-state where the PI has been authorised and the "host" member-state(s) where the PI offers its payment services – is key to ensure a smooth and uniform, transparent processing of the PI by the different authorities. Therefore, the EBA (pursuant to Article 28(5) of the Directive), was mandated to develop Regulatory Technical Standards, specifying a harmonised framework – standard forms, templates and procedures – for competent authorities (CAs) to exchange information about a PI's (defined as a PI's passport), to inform the PI about the information exchange and to provide clarity to the PI about the regulatory requirement in force in the host member state. The deadline for this RTS is set on 12 January 2018[35].

RTS Central Contact Points

Although listed in the June 2016's EBA press newsletter reporting all upcoming EBA publications[36], to date (08 January 2017) no information is available on this RTS. Enquiry at EBA learned that the need of central contact points is still under investigation. As this topic is not relevant for cyber security and this research, the author did not investigate further.

Category II: Consumer protection

Guidelines on Professional Indemnity Insurance (PII) for Payment Service Providers (PSPs)[37]

Third party providers (TPP), bringing new type of payment services to customers – such as payment initiation services and account information services – were not in the scope of the former payment directive (PSD). Therefore, the few already existing Payment Information Service Providers (PISPs) and Account Information Service Providers (AISPs) were not subject to supervision by the competent authorities – as were payment institutions –, while having access to customers' payment information. As a result, many issues rose regarding customer protection, security, liability and data protection. PSD2 adapts the status of these payment service providers (PSPs), by defining specific conditions and requirements they have to address in order to be authorised as a payment institution, needed to provide payment services. One of these requirements addresses the amount of money a PSP must set aside to ensure a.o. the coverage of legal costs and customer compensation in the case something goes wrong (called professional indemnity insurance, PII). Article 5(4) of PSD2 mandated the EBA with the development of guidelines to help competent authorities calculating this PII. The due date of this guideline was set on 13 January 2017[38] and will apply as of January 2018[39]

[34] EBA final draft Regulatory Technical Standards on the framework for cooperation and exchange of information between competent authorities for passport notifications under Directive (EU) 2015/2366, European Banking Authority, EBA/RTS/2016/08, 14 December 2016

[35] Osborne Clark, *Payments regulatory timeline, Payment Service Directive 2 (PSD2),* Osborne Clark, February 2016

[36] European Bank Authority, *Upcoming EBA publications (June 2016 – September 2016),* Newsletter EBA Press, June 2016

[37] Consultation paper on the Draft Guidelines on the criteria on how to stipulate the minimum monetary amount of the professional indemnity insurance or other comparable guarantee under Article 5(4) of Directive (EU) 2015/2366, European Banking Authority, EBA/CP/2016/12, version 2, 22 September 2016

[38] Payments regulatory timeline, Payment Service Directive 2 (PSD2), Osborne Clark, February 2016

[39] Consultation paper on the Draft Guidelines on the criteria on how to stipulate the minimum monetary amount of the professional indemnity insurance or other comparable guarantee under Article 5(4) of Directive (EU) 2015/2366, European Banking Authority, EBA/CP/2016/12, version 2, page 28, 22 September 2016

Guidelines on complaints procedures

These guidelines, about the requirement for adequately handling complaints, are still work in progress and due 12 January 2018[40]

Category III: Authorisation

Guidelines on Payment Institution (PI) authorisation[41]

PSD2 allows new type of players (TPPs) to become payment institutions. Article 5(5) of the directive mandated the EBA to develop guidelines about the standard information (a.o. business plan, initial capital, internal control mechanisms, security measures in place to safeguard customers' funds, security incidents and customer complaints procedure in place, PII, etc.) TPP need to provide to competent authorities in order to be authorised and registered as payment institutions. This guideline is due on 13 July 2017[42].

Category IV: Register

Implementing Technical Standards (ITS) on EBA register

Articles 15 mandates the EBA with the development, operating and maintenance of a digital central register to store all PI information compiled by the competent European authorities. Therefore, the EBA is asked to develop an ITS about the information it needs to be provided with by these competent authorities as well as the procedures. The finalized ITS must be submitted to the European Commission by 13 January 2018[43]. So far, no ITS have been issued and proposed for review.

Category V: Security

Guidelines on major incident reporting[44]

Article 96(3) of PSD2 mandates the EBA to develop – in close collaboration with the European Central Bank (ECB) – guidelines for PSPs and competent authorities on the management, classification and (the relevance of) reporting of major operational and/or security incidents. Criteria, thresholds and methodology – incident reporting template, reporting process, time frame, etc. – are defined for the PSPs to assess if an incident is major and needs notification to competent authorities or not. The guidelines also allow the PSPs to outsource incident reporting obligations to a third party meeting strict defined conditions and address the level of transparency competent authorities should ensure when sharing information regarding a major incident with other domestic authorities. These guidelines are to be published by 18 January 2018[45].

Guidelines on security measures

The EBA and the ECB developed in close collaboration guidelines regarding the security of Internet payments[46] that were published in December 2014, to answer the increasing amount

[40] Payments regulatory timeline, Payment Service Directive 2 (PSD2), Osborne Clark, February 2016
[41] Consultation paper on the Draft Guidelines on the information to be provided for the authorisation as payment institutions and e-money institutions and for the registration as account information service providers, European Banking Authority, EBA/CP/2016/18, 03 November 2016
[42] Payments regulatory timeline, Payment Service Directive 2 (PSD2), Osborne Clark, February 2016
[43] Payments regulatory timeline, Payment Service Directive 2 (PSD2), Osborne Clark, February 2016
[44] Consultation paper on the Draft Guidelines on major incidents reporting under the Payment Services Directive 2, European Banking Authority, EBA/CP/2016/23, 07 December 2016
[45] Payments regulatory timeline, Payment Service Directive 2 (PSD2), Osborne Clark, February 2016
[46] Final guidelines on the security of internet payments, European Banking Authority, EBA/GL/2014/12_Rev1, 19 December 2014

of frauds online payments were facing. They set the minimum-security requirements for payment services providers across the EU, seeking to provide confidence to online payment service users by increasing their protection against payment fraud on the Internet. These guidelines remain in force until the security requirements under the PSD2 apply from 2018/9 onward[47]. Although article 95(3) of the PDS2 directive mentions that the EBA and the ECB are to issue updated security guidelines by 13 July 2017[48] – e.g. to address XS2A –, no guidelines have yet been drafted and proposed for review[49]. An important point to mention is that these guidelines are convertible into a RTS if requested by Commission.

RTS on strong authentication & secure communication[50]

PSD2 aims at giving a more prominent place to electronic payment services in the EU internal market. These services and the adoption of the supporting (new) technologies need to prove secure, e.g. by ensuring safe authentication of the customer and reducing as much as possible the risk of fraud. Considered as most crucial to achieving the PSD2 objective of *'enhancing consumer protection, promoting innovation and improving the security of payment services across the Union'*[51], Article 98 of the directive mandates the EBA and the ECB to develop together RTS specifying the security requirements needed to ensure confidentiality and integrity of the payments services users' – e.g. customers or merchants – 'private credentials'. Strong customer authentication (SCA) is covered as well as the cases where SCA application can be exempted. The RTS also address the requirements for standards to allow secure communication between account servicing payment service providers (ASPSPs, e.g. the banks), PISPs, AISPs, payers, payees and other PSPs.

The goal of these RTS is to design a uniform framework ensuring the needed level of security for customers to use and for PSPs to provide new payment services, thus allowing competition amongst all PSPs and fostering the development of innovative means of payments. The deadline was set on 13 January 2017[52] but a final draft is now expected in February or March 2017[53].

Scope limitation

The author was assigned with the task to perform a research on the needed (cyber) security requirements related to PSD2. Therefore, only category V applies for the scoping of this research. Other categories – e.g. Customer Protection – might sporadically touch the topic of cyber security, but they are about remediation – e.g. amount to compensate a customer by e.g. fraud –. To address security, all the documents will refer to category V. A deep-dive in the guidelines on major incident reporting shows that this document is only about common governance and procedures around the handling of operational and security incidents: it defines criteria for incident classification, reporting templates to be used and indicators to be addressed by competent authorities when assessing the relevance of the incidents. In the guidelines, the EBA and the ECB compile already existing (mandatory) reporting procedures for payment-related incidents in a common framework[54] and seek to leverage on the standards, specifications and expertise of the European Union Agency for Network and Information

[47] Upcoming EBA publications (June 2016 – September 2016), European Bank Authority, Newsletter EBA Press, page 3, June 2016
[48] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015, on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, Official Journal of the European Union, November 2015
[49] Feedback from Belgian banks task force represented in Febelfin
[50] Consultation Paper on the Draft Regulatory Technical Standards specifying the requirements on strong customer authentication and secure communication under PSD2, European Banking Authority, EBA/CP/2016/11, 12 August 2016
[51] Upcoming EBA publications (June 2016 – September 2016), European Bank Authority, Newsletter EBA Press, page 3, June 2016
[52] Payments regulatory timeline, Payment Service Directive 2 (PSD2), Osborne Clark, February 2016
[53] Feedback provided by Febelfin (Federation of Belgian Financial institutions) in November 2016 to the Belgian banking task force working on RTS on strong authentication & secure communication
[54] Consultation paper on the Draft Guidelines on major incidents reporting under the Payment Services Directive 2, European Banking Authority, EBA/CP/2016/23, page 6, article 8, 07 December 2016

Security (ENISA) on the subject. Although Febelfin - through its task force of Belgian banks – will provide an answer on the consultation paper as required by the EBA, the task force representatives as well as the direct management of the author acknowledge that these guidelines should be kept out of scope of this research, bringing forward the reason already elaborated above: these guidelines are about the compiling of existing documentation and procedures into one common framework to ensure an uniform governance regarding operational and security incident reporting. Therefore, no further attention will be paid to these guidelines during the research.

As already mentioned, although updated guidelines on security measures are due by 13 July 2017, to date no consultation paper or other documentation provided to Febelfin or published on the EBA website. An official EBA document[55] confirms that the guidelines on the security of Internet payments from December 2014 (enforced in April 2015) remain applicable until the publication of the final PSD2 security requirements (enforcement expected in 2018/2019). As no documentation can be assessed, these guidelines are also kept out of the scope of this research.

Considering the elaboration above, this research focuses only on recommendations for the Regulatory Technical Standards on Strong Customer Authentication and Secure Communication, which are also recognised by the EBA[56], the European financial sector and related – who together provided one hundred forty-six responses on the consultation paper for these RTS[57] – and the Febelfin task force representatives[58] as the most important regulatory text regarding the (cyber) security objectives of PSD2.

Conclusion

In order to ensure that PSD2 will achieve its key objectives – encouraging new innovative (and potentially disruptive) competitors to enter the payment landscape and fostering access to customers' accounts (XS2A) to non-banks –, the European Bank Authority (EBA) has been mandated to develop Regulatory Technical Standards (for the payment service providers) and guidelines (for the competent authorities) to address different key subjects. This research will focus further on the RTS on Strong Customer Authentication and Secure Communication, as it is seen as the most important regulatory text regarding the (cyber) security challenges of PDS2.

[55] Upcoming EBA publications (June 2016 – September 2016), European Bank Authority, Newsletter EBA Press, page 3, June 2016
[56] Upcoming EBA publications (June 2016 – September 2016), European Bank Authority, Newsletter EBA Press, page 3, June 2016
[57] www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2/-/regulatory-activity/consultation-paper.
[58] The revised Payment Service Directive (EU) 2015/2366 – Objectives and Scope (slide 7: 3 mandates EBA to ensure the establishment of adequate security measures for electronic payments – Focus RTS on Strong Customer Authentication), presentation of a not to be named Belgian financial institution to Febelfin, 15 November 2016.

4. Analysis of the draft RTS on Strong Customer Authentication (SCA) & Secure Communication (SC)

One of the objectives of the revised Directive on Payment Services (PSD2) is to offer consumers the possibility to access their account information and funds through third – non-banking – parties. This must of course occur in the same secure way as when the account information is accessed through the customer's bank. Protection of the consumer when performing online payment activities is a second objective of PDS2, therefore calling for '*a harmonized framework aimed at ensuring an appropriate level of security for consumers as well as payment service providers (PSPs)*'[59].

To answer Article 98 of PDS2, the European Banking Authority (EBA) has been provided the task – in close collaboration with the European Central Bank (ECB) – to develop Regulatory Technical Standards on Strong Customer Authentication & Secure Communication, considered as the most crucial[60] regulatory text on (cyber) security challenges to achieving the PSD2 objectives. Following the 118 responses[61] to a first discussion paper published by EBA in December 2015[62], a draft of these RTS – consisting of four chapters and twenty-two articles – has been published on 12 August 2016 as a consultation paper on the EBA website[63], where all relevant stakeholders to the payment market – financial institutions, third party (payment service) providers, consultancy organisations, etc – were given the possibility to provide comments. The consultation process consisted of a ten questions-survey to which a total of one hundred forty-six companies[64] responded within a period of three months (deadline for response was set on 12 October 2016).

A. Sum-up draft RTS on SCA & SC (4 chapters, 22 articles)

Five PSD2 objectives[65] form the essence of these RTS: a)*'ensuring an appropriate level of security for PSUs and PSPs, through the adoption of effective and risk-based requirements'*; b)*'ensuring the safety of PSUs' funds and personal data'*; c)*'securing and maintaining fair competition among all PSPs'*; d)*'ensuring technology and business-model neutrality'* and e)*'allowing for the development of user-friendly, accessible and innovative means of payment'*.

High-level requirements

During the elaboration of the SCA requirements, the EBA struggled[66] with the balancing of consumer protection – meaning very detailed security requirements – and consumer convenience – less detailed security requirements –. Answering the call of the majority of the respondent to the discussion paper of 2015, the EBA defined principle-based, high level, solution-agnostic requirements for strong customer authentication (SCA), arguing that a too granular level of detail would be an obstacle to e.g. the (quick) adaptation of PSP to new fraud

[59] www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2/-/regulatory-activity/consultation-paper
[60] Upcoming EBA publications (June 2016 – September 2016), European Bank Authority, Newsletter EBA Press, page 3, June 2016
[61] www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2/-/regulatory-activity/consultation-paper
[62] Discussion Paper on future Draft Regulatory Technical Standards on strong customer authentication and secure communication under the revised Payment Services Directive (PSD2), European Banking Authority, EBA/DP/2015/03, 8 December 2015
[63]www. eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2/-/regulatory-activity/consultation-paper
[64] www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2/-/regulatory-activity/consultation-paper
[65] Consultation Paper on the Draft Regulatory Technical Standards specifying the requirements on strong customer authentication and secure communication under PSD2, European Banking Authority, EBA/CP/2016/11, page 6, 12 August 2016
[66] Consultation Paper on the Draft Regulatory Technical Standards specifying the requirements on strong customer authentication and secure communication under PSD2, European Banking Authority, EBA/CP/2016/11, page 9, 12 August 2016

scenarios. The RTS also clarify the relationship between authentication factors, the definition of personalised security credentials (PSCs) and the SCA procedure.

The RTS are specifically addressed to payment service providers (PSPs) – such as Payment Information Service Providers (PISPs) and Account Information Service Providers (AISPs) – and provide the following high-level requirements:

a) *'The requirements for strong customer authentication (SCA) when the payer accesses his 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'.* These requirements are laid down in chapter 1 of the RTS.

b) *'The exemptions from the application of Article 97 on strong customer authentication and adequate security measures to protect the confidentiality and integrity of personalised security credentials (PSCs), based on the level of risk involved in the service provided; the amount, the recurrence of the transaction, or both; or the payment channel used for the execution of the transaction.* These exemptions are laid down in chapter 2 of the RTS

c) *'The requirements with which security measures have to comply in order to protect the confidentiality and the integrity of the payment service users' (PSU) personalised security credentials (PSCs)'.* These requirements are laid down in chapter 3 of the RTS

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, between ASPSP, PIS providers, AIS providers, payers, payees and other payment service providers'.* These requirements are laid down in chapter 4 of the RTS

Chapter 1 – Requirements on Strong Customer Authentication (SCA)[67]

Seven articles define the requirements on Strong Customer Authentication. Article 4(30) of PSD2[68] forms the basis, stating that strong authentication relies on the use of independent multiple factors related to knowledge (something only the user knows; e.g. user name and password), possession (something only the user possesses; e.g. smartphone with a one-time password token) and inherence (something the user is; e.g. finger scan). Confidentiality and integrity of authentication data must be guaranteed at all time.

Article 1 – Authentication procedure and authentication code

This article puts forward the requirement that a generated authentication code may only be accepted once (article 1.1) by the Payment Service Provider (PSP), for the same Payment Service User (PSU). Each payment activity of the user should generate a new authentication code. The article describes also a set of rules to which the authentication code must comply (article 1.2) – such as the protection of the PSU's personal security credentials (no element of the multi-factor authentication can be derived from the code) – and the mechanisms that a SCA procedure must include (article 1.3) – e.g. time limitation of an online session, maximum

[67] Consultation Paper on the Draft Regulatory Technical Standards specifying the requirements on strong customer authentication and secure communication under PSD2, European Banking Authority, EBA/CP/2016/11, page 29, Chapter 1 – Strong Customer Authentication, 12 August 2016

[68] Directive (EU) 2015/2366 Of The European Parliament And Of The Council, on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, 25 November 2015

amount of failed authentication attempts and prevention, detection and blocking mechanisms – to minimize as much as possible the risk of fraudulent payment transaction–.

Article 2 – Strong customer authentication procedure with dynamic linking

This article refers to article 97(2) of PSD2 and requires that a transaction must be dynamically linked to a specific amount and a specific payee, of which the payer must be aware at all times (article 2.1). It also states that the confidentiality, authenticity and integrity of the transaction regarding amount and payee and transaction information displayed to the payer must at all remain unaltered (article 2.2). The article addresses also card-based transactions (article 2.3) – specifying that a generated authentication code must be linked to the maximum amount that the payer has agreed with the payee and has given consent to be blocked when initiating the transaction – and the rules for authentication code regarding batches of remote electronic payments to many payees (article 2.4).

Article 3 – Requirements related to elements categorised as knowledge

This article refers to one of the three categories commonly used for multi-factor authentication (something only the user knows). It specifies the rules for ensuring the security of knowledge elements used in SCA in order to prevent uncover or disclosure to unauthorised parties – such as the use of complexity and expiration time features (article 3.1) and the use of mitigation measures (article 3.2) –.

Article 4 – Requirements related to elements categorised as possession

This article refers to the second of the three categories commonly used for multi-factor authentication (something only the user possesses). It specifies the rules for ensuring the security of possession elements used in SCA in order to prevent use by or disclosure to unauthorised parties – such as the use of algorithm specifications and information entropy (article 4.1) and the use of measures to prevent replication – e.g. forging or cloning – of the elements (article 4.2) –.

Article 5 – Requirements related to devices and software to read authentication elements categorised as inherence

This article refers to the last of the three categories commonly used for multi-factor authentication (something only the user is). It specifies the rules for ensuring the security of inherence elements used in SCA in order to prevent disclosure of sensitive information related to these elements to unauthorised parties and to reduce the risk as much as possible that an unauthorised party could be authenticated as legitimate payment service user. Security measures mentioned are algorithm specification, biometric sensor and template protection features (article 5.1), in order to guarantee resistance against unauthorised access (article 5.2) –.

Article 6 – Requirements related to the independence of the elements

This article focuses on the procedures (article 6.1) – e.g. technology, algorithms and parameters – that can guarantee independence of the different elements – mentioned in article 3, 4 and 5 – used in multi-factor authentication. The aim is to guarantee the reliability of the strong customer authentication in place, so that one compromise element does not alter the integrity of the others. When using a multifunctional device – e.g. smartphone or tablet –, security measures must be included in the authentication procedure in order to mitigate the risk of compromise of the device (article 6.2), such as segregation of environment within the device and (mitigating) mechanisms to ensure non-alteration of the device or software.

Article 7 – Review of the strong customer authentication procedure

This article explains that the effectiveness of the SCA procedure in place must be periodically – according to the PSP's audit framework – tested, assessed and audited by internal and external certified auditors (article 7.1), and reported (article 7.2). Reports will be fully available when requested by competent authorities (article 7.3).

Summary

PSPs must ensure the use of at least a two-factor authentication (a combination of knowledge, possession and inherence elements). These factors must be independent from each other, in order to ensure the reliability of the others if one should be compromised. Security measures must be implemented in order to guarantee the integrity of the different elements of the multi-factor authentication procedure. The ensuing generated authentication code may only be accepted once by the PSP for the same PSU. The same procedure is applicable for the payer's PSP in the case of electronic remote payment transactions, with the extra requirement that the issued authentication code must also address the specific amount of money the payer and the payee agreed upon when initiating the transaction. The effectiveness of the strong authentication procedure in place at the PSPs must be audited periodically.

Chapter 2 – Exemptions from Strong Customer Authentication (SCA)[69]

While PDS2 introduces the obligation for PSPs to apply strong customer authentication for online payments, it also fosters more convenient – user-friendly – payment means for low-risk payments[70]. As such, recital 96 of PSD2[71] requires the EBA to define criteria for PSPs to be exempted from Strong Customer Authentication (SCA). These criteria, based on a) the level of risk involved in the service provided, b) the amount, the recurrence of the transaction or both and c) the payment channel used for the execution of the transaction, are translated into one article in the RTS.

Article 8 – Exemptions to strong customer authentication (SCA)

The application of SCA is exempted when a user is only accessing the (consolidated) information of her/his account(s) online for consulting purposes without disclosure of sensitive payment data – except when the user is accessing this functionality for the first time or more than one month after the last logon, in which case SCA is applicable – or when the user is initiating a non-remote contactless payment (e.g. RFID technology) that does not exceed 50 EUR – 150 EUR cumulated since the last application of SCA – (article 8.1).

SCA is also not mandatory when payments are performed to payees included in the payer's trusted list of beneficiaries (at ASPSP level), when the payer initiates a series of online payments with a same amount to a same payee – except for the first time –, when the payer is transferring money to another of her/his own account within the ASPSP (e.g. bank) or when a remote online payment is initiated for an amount of 10 EUR – 100 EUR cumulated since the last application of SCA – (article 8.2).

[69] Consultation Paper on the Draft Regulatory Technical Standards specifying the requirements on strong customer authentication and secure communication under PSD2, European Banking Authority, EBA/CP/2016/11, page 35, Chapter 3 – Exemption from Strong Customer Authentication, 12 August 2016

[70] Consultation Paper on the Draft Regulatory Technical Standards specifying the requirements on strong customer authentication and secure communication under PSD2, European Banking Authority, EBA/CP/2016/11, page 14, 12 August 2016

[71] Directive (EU) 2015/2366 Of The European Parliament And Of The Council, on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, page L337/50, 25 November 2015

Chapter 3 – Protection of the Confidentiality and Integrity of the Payment Service Users' Personalised Security Credentials (PSUs' PSCs)

Eight articles define the security measures required of PSPs to implement in order to ensure the protection of the confidentiality and integrity of users' security credentials, as PSD2 allow them to access this information, providing the user has given her/his consent.

Article 9 – Requirements for security measures

This article states that PSCs' confidentiality and integrity must be guaranteed at all time during the authentication procedure – e.g. display, transmission and storage – (article 9.1). Security measures must ensure that data on PSC are masked and not readable when displayed, data related to the PSC and its encryption is not stored in plain text and all secret encryption material (related to the encryption of the PSC) is stored on secured devices and environments.

Article 10 – Security measures for transactions initiated by or through a payee in the context of a card-based payment transaction

This article is covering pull (or mutual) payments[72] (e.g. credit card or cheque payment), when the payee (credit card company or merchant) initiates the funds transfer from the payer – thus pulling the money from the payer –. In this case, the payee (or its PSP) needs to have security measures in place in order to protect data related to the payer's personalised security credentials.

Article 11 – Creation of personalised security credentials (PSCs)

This principle-based article addresses the secure creation of PSCs in order to ensure the protection of their confidentiality and integrity and mitigate the risk of unauthorised use should PSCs, authentication devices and/or software be lost, stolen or duplicated before delivery to the payer.

Article 12 – Association of the payer with personalised security credentials, authentication devices and software

This article describes how security measures must ensure the secure, exclusive association of the payer with her/his PSCs, authentication devices and software. The link between the payment service user's identity and her/his PSCs, authentication devices and software must occur in a secure environment – under the responsibility of the PSP (e.g. Internet environments or secure websites serviced by PSP and ATMs – where customer and PSP authentication is assured. The PSP is not responsible for risks related to the use of devices and underlying components needed for the association process. Strong customer authentication must be applied when association process occurs via a remote channel.

Article 13 – Delivery of personalised security credentials, authentication devices and software

This article aims at the same protection as article 11, addressing now security measures needed to ensure a secure delivery of PSCs to the payment service user, such as a. o. secure mechanisms ensuring the delivery to the right user and guaranteeing that authentication software delivered through Internet is digitally signed by the PSP.

Article 14 – Renewal of personalised security credentials

The same procedures as described in article 11, 12 and 13 are applicable.

[72] Ward, A. *The four types of payments*, in2payments.com, post, 08 March 2011

Article 15 – Destruction, deactivation and revocation of personalised security credentials, authentication devices and software

Dedicated processes with relevant security measures must protect the confidentiality and integrity of PSCs when destroying, deactivating or revoking PSCs – or its related information stored in the PSPs' systems and databases –, authentication devices and software. When authentication devices and software are to be reused, the secure re-use must be implemented, assessed and documented by the PSP prior to re-distribution to another user.

Article 16 – Review of the security measures to protect the confidentiality and integrity of payment service users' personalised security credentials

This article is about the periodic testing, evaluating and auditing of effectiveness of the security measures in place to ensure that the confidentiality and integrity of users' PSCs are not altered. As in article 7 (SCA), the periodicity is dependable of the audit framework applicable at the PSPs. Results must be duly reported and made available if required by the competent authorities.

Summary

PSPs must implement the necessary security measures to ensure that the confidentiality and integrity of the payment service users' personal security credentials are protected at all times. This accounts for the authentication procedure (e.g. PSC data not to be displayed in plain text), the creation, delivery, renewal and revocation of the PSCs, authentication devices and software as well as for their re-use, and for card-based payment transaction process where the payee (and its PSP) must have security measure in place to protect the payer's PSCs.

Chapter 4 – Requirements for common and secure open standards of communication[73]

All stakeholders – account servicing payment service providers (ASPSPs), payment initiation service providers (PISPs), account information service providers (AISPs), payment services users (PSUs, the payers and payees, both customers and merchants) and other payment service providers (PSPs) – involved in the payment service process must be able to communicate with each other in an effective and secure way.

Therefore, the EBA was tasked with the development of requirements for the adoption of common and secure open standards of communication regarding identification, authentication, notification and information. As a result, eight articles were drafted in the RTS, of which two are defining generic principle-based requirements for communication standards. These requirements will be complemented further by the upcoming guidelines major incident reporting under PSD2 (discussed briefly in chapter 3 of this research), as required by article 95 of PSD2. The four remaining articles contain more dedicated requirements for specific communication between ASPSPs and AISPs/PISPs, and between PSPs themselves regarding the confirmation of availability of funds (conform article 65 of PSD2).

Article 17 – Requirements for identification

Article 17.1 states that *'Payment services providers shall ensure secure bilateral identification when communicating between the payer's device and the payee's acceptance devices for electronic payments, including but not limited to payment terminals'.* In addition, article 17.2 sets out that *'Payment services providers shall ensure that mobile applications and other*

[73] Consultation Paper on the Draft Regulatory Technical Standards specifying the requirements on strong customer authentication and secure communication under PSD2, European Banking Authority, EBA/CP/2016/11, page 39, Chapter 4 – Common and Secure Open Standards of Communication, 12 August 2016

payment services users interfaces offering electronic payment services are protected against misdirection of communication to unauthorised third parties'.

Article 18 – Traceability

PSPs must ensure that all their payment service related interactions with payment service users and other PSPs are at all time traceable and knowledgeable. PSPs must ensure that all communication sessions rely on a unique identifier of the session (so that all parties can easily be identified), on security mechanisms enabling detailed logging of the transaction (e.g. transaction number and other relevant data) and on timestamps using the standard – but not limited to – NTP protocol for clock synchronization.

Article 19 – Communication interface

ASPSP (e.g. the banks offering and managing a user's payment accounts) must provide at least one communication interface – such as an Application Programming Interface (API) – that allows AISPs, PISPs and PSPs issuing card-based payment instruments to identify themselves towards the ASPSP and to communicate in a secure way with the ASPSP for payment account information requests, payment initiation and confirmation of sufficient funds available on the user's account to execute a card-based payment transaction. The interface must also enable the AISPs and PSIPs to rely on the ASPSP's authentication procedures (article 19.1). AISPs and PISPs must be allowed to rely on ASPSPs' authentication procedures (article 19.2). To this end, the communication interface must enable instruction from the PISPs or AISPs to the ASPSP to start authentication procedures, during which communication sessions between the mentioned providers and the payment service user are ensured and maintained. The interface must also ensure that transmission of the PSCs and authentication codes by AISPs and PISPs occurs in a secure way, so that these data cannot be altered.

The use of international or European standards of communication is promoted (article 19.3), as well as the use of ISO 20022 elements – a standard for financial messaging (electronic data exchange) between financial institutions created by the International Standards Organisation[74] – to ensure a secure communication interface. The synergy between the TPPs' (AISPs and PSIPs) and the ASPSPs' systems must be ensured through well-documented technical specifications – e.g. needed protocols and tools – of the interface by the ASPSPs; these specifications must be published on the ASPSPs' website, free of charge (article 19.4). Changes in these specifications must be documented, communicated and published at least three months before the changes are implemented – except in the case of emergency changes – (article 19.5). The ASPSPs must ensure – and monitor – that the interface's performance and availability provided to TPPs do not differ from the performance and availability of the own online platform used by the ASPSPs' customers in order to directly access their payment accounts (article 19.6). Statistics must be provided to the competent authorities when requested. A test environment – including support – must be made available by the ASPSPs, in order for the TPPs to perform connection and functional testing on their software and applications.

Article 20 – Identification

The starting point here (article 20.1) is the use of qualified certificates for website authentication – as defined in article 3(39) of Regulation (EU) No 910/2014[75] –, issued by a qualified trust service provider and meeting the specific requirements addressed in Annex IV[76]

[74] Paper on the Strategies for Improving the U.S. Payment System, United States Federal Reserve System, 16 January 2015

[75] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, Official Journal of the European Union, page L257/86, 28 August 2014

[76] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, Official Journal of the European Union, page L257/114, 28 August 2014

of the same Regulation – e.g. a qualified certificate must contain a unique certificate identity code and the certificate's period of validity –. Website certificate issuers must verify registration number of the legal person to whom the certificate has been issued – either the ASPSP or the PSP issuing card-based payment instrument and the AISP and/or the PISP – (article 20.2). Although additional attributes must also be included in the qualified certificates – the PSP's role (ASPSP, AISP, PISP or PSP issuing card-based payment instruments) and name of the competent authority where the PSP is registered – (article 20.3), this must not alter the reliability of the certificates (article 20.4).

Article 21 – Security of communication session

Strong, recognised encryption techniques must be used to ensure secure data exchange between the different parties involved (article 21.1). Sessions between TPPs and ASPSPs must be kept as short as possible and TPPs must immediately close the session when the requested action related to a payment service has been completed by the ASPSP (article 21.2). The same goes for parallel network sessions, where the TPP must ensure a secure link to sessions with the payment service users (PSU), so that no data exchanged between the parties (ASPSP-TPP-PSU) can be compromised (article 21.3). Messages or information exchanged between ASPSPs and TPPs must always contain a) '*the payment service user and the corresponding communication session in order to distinguish several requests from the same payment service user*', b) '*for payment initiation services, the uniquely identified payment transaction initiated*' and c) '*amount necessary for the execution of the card-based payment transaction*'.
Regarding the transmission of PSCs and authentication codes, the TPP's staff must not be able to access them at any point. By eventual breach or loss of confidentiality under their premises, TPPs must inform the user and the PSCs' issuer at once (article 21.5). TPPs must ensure that the processing and routing of PSCs and authentication codes occur in ISO 27001[77] – a standard addressing the requirements for information security management systems – certified secure environments (article 21.6).

Article 22 – Data exchanges

ASPSPs are not allowed to make any differentiation in the information richness provided to the AISPs. The same information, about payment accounts and related transactions, made available to the ASPSPs' customers must be accessible for the AISPs – providing customer's consent has been given – (article 22.1). The same goes for PISPs – regarding information related to payment transaction initiation and execution – and PSP issuing card-based payment instruments – regarding information related to account provisioning of a customer in order to perform e.g. a contactless payment –.
A notification message must be sent by the ASPSP to the TPPs in case identification, authentication of exchange of data could not take place explaining the reason – e.g. of the error or unexpected event – (article 22.2). AISPs must limit the request of information related to payment accounts and transactions to what the user provided consent for (article 22.3). Requests for information are allowed each time the user is actively requesting it or no more than twice a day when not specifically requested by the user (article 22.5). PISP must provide ASPSPs with the same information they requested the user to provide them when initiating a payment transaction (22.4).

[77] ISO/IEC 27001, Information technology — Security techniques — Information security management systems — Requirements, International Standards Organisation, September 2013.

Summary

PSPs must at all time ensure that the information exchanged between the different parties occurs via a secure, well-maintained and well-documented ISO 20022 certified communication interface (e.g. API) made available by the ASPSPs – including a testing environment –, enabling the reliance on the ASPSPs' authentication procedures. Identification must occur through qualified certificates – conform the requirements laid down in the existing EU regulation on electronic identification related to electronic transactions – and strong encryption techniques must be used to protect the confidentiality and integrity of the data exchanged. The duration of established secure sessions must be kept as short as possible and AISPs/PISPs must ensure that the processing and routing of personalised security credentials (PSCs) and authentication codes occurs in secure ISO 27001 certified environments. No differentiation is allowed between the information provided to the payment service user (PSU), the TPPs (AISPs, PISPs and PSP issuing card-based payment instruments) and the ASPSPs. AISPs must refrain from frequent information requests to strictly service the activity the user provided her/his consent for.

B. EBA's ten questions-survey

Following the publication of the draft RTS on Strong Customer Authentication and Secure Communication on the EBA's website, all EU en non-EU payment services stakeholders – e.g. TPPs, banks, and Credit Cards companies – and related – consultancy companies – were invited by the EBA to provide comments via an Internet form[78] on the proposals set out in these RTS by means of answering a ten questions-survey (see figure 7), which covered the twenty-two articles composing the four chapters of the draft RTS (see A.).

Chapter 1. Requirements on Strong Customer Authentication
Q1: Do you agree with the EBA's reasoning on the requirements of the strong customer authentication, and the resultant provisions proposed in Chapter 1 of the draft RTS?
Q2: In particular, in relation to the "dynamic linking" procedure, do you agree with the EBA's reasoning that the requirements should remain neutral as to when the "dynamic linking" should take place, under the conditions that the channel, mobile application, or device where the information about the amount and the payee of the transaction is displayed is independent or segregated from the channel, mobile application or device used for initiating the payment, as foreseen in Article 2.2 of the draft RTS.
Q3: In particular, in relation to the protection of authentication elements, are you aware of other threats than the ones identified in articles 3, 4 and 5 of the draft RTS against which authentication elements should be resistant?
Chapter 2 – Exemptions from Strong Customer Authentication
Q4: Do you agree with the EBA's reasoning on the exemptions from the application of Article 97 on strong customer authentication and on security measures, and the resultant provisions proposed in Chapter 2 of the draft RTS?
Q5: Do you have any concern with the list of exemptions contained in Chapter 2 of the draft RTS for the scenario that PSPs are prevented from implementing SCA on transactions that meet the criteria for exemption?
Chapter 3 – Protection of the Confidentiality and Integrity of the Payment Service Users' Personalised Security Credentials
Q6: Do you agree with the EBA's reasoning on the protection of the confidentiality and the integrity of the payment service users' personalised security credentials, and the resultant provisions proposed in Chapter 3 of the draft RTS?
Chapter 4 – Requirements for common and secure open standards of communication
Q7: Do you agree with the EBA's reasoning on the requirements for common and secure open standards of communication for the purpose of identification, authentication, notification, and information, and the resultant provisions proposed in Chapter 4 of the draft RTS?
Q8: In particular, do you agree that the use of ISO 20022 elements, components or approved message definitions, if available, should be required to ensure the interoperability of different technological communication solutions

[78] www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2/-/regulatory-activity/consultation-paper

implemented between PSPs for the provision of AIS, PIS or for the confirmation on the availability of funds? Do you see any particular technical constraint that would prevent the use of such industry standards?
Q9: With regards to identification between PSPs, do you agree that website certificates issued by a qualified trust service provider under an e-IDAS policy would be suitable and allow for the use of all common types of devices (such as computers, tablets and mobile phones) for carrying out different payment services?
Q10: With regards to the frequency with which AIS providers can request information from designated payment accounts when the payment service user is not actively requesting such information, do you agree that the proposed limit of no more than two times a day achieve an appropriate balance between allowing AISP to provide updated information to their users while not negatively impacting the availability of the ASPSP's communication interface? If not, please indicate what would be in your view the appropriate frequency and rationale for such frequency.

Figure 3 - EBA's ten questions-survey and their relation to the RTS on SCA & SC

C. Responses

1.046 answers disclosed by one hundred forty-six respondents

One hundred forty-six respondents – mostly European – from diverse backgrounds (see figure 8) submitted their answers to (part of) the 10 questions[79] - representing a total of 1.046 answers –. As the form contained a non-disclosure option, it is not possible for the author to provide any information about the actual response rate.

Background

It must also be mentioned that the grouping shown below might be subject to discussion, as the result is an appreciation of the author after a ground desk research of each respondent. For instance, some respondents stated in the EBA form – where the respondents' company background is requested – that they were operating as ICT service providers while these companies' core business is actually the processing of payment transfers or aggregation of customers' account information for the sake of a service to either the merchants or the customers themselves (end-consumers). For consistency reasons, the author chose to integrate these cases in the category of payment service providers (PSPs), given the fact that an ICT service provider – established or FinTech start-up[80] – in this research is considered by the author as a provider of either the generic infrastructure and/or the software needed by PSPs to offer their payment services to users, not as a provider of a final PSP-service. Also, as this research is focusing on the (cyber) security aspects inherent to the new opportunities enhanced by PSD2, the author created a specific 'security-related' category, populated by established ICT companies – e.g. Gemalto – offering generic multi-sector solutions and FinTech start-ups – e.g. Token[81] –, newly born to address the new directive's (cyber) security requirements for the specific electronic payment sector. Whatever the category the few cases described above are included in, does not affect the end-result.

Background of the disclosed respondents	#	%
Banks (and related, e.g. associations or federations)	35	24%
TPP/PSPs (AISPs and/or PISPs related)	25	17%
(Cyber) security related FinTechs (e.g. SCA)	20	14%
ICT service providers/ FinTechs	15	10%
(Credit) card related	10	7%
Non-bank PI & CI related	10	7%
(E)-commerce	6	4%
Consultancy	6	4%
Government	6	4%
Retailers	3	2%

[79] www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2/-/regulatory-activity/consultation-paper
[80] PwC Financial Service Institute, What are FinTechs ?, Q&A PwCFinTech, April 2016
[81] Founded in 2015. http://token.io/company

Academia	3	2%
Consumer organisations	2	1%
Payment systems related	2	1%
Marketing	1	1%
Telco	1	1%
Food industry	1	1%
Total	**146**	**100%**

Figure 4 - Diversity of respondents

Even considering that not all responses might not have been disclosed on the EBA site, the fact that Account servicing payment service providers – ASPSPs e.g. banks –, payment, credit and credit card institutions, (third party) payment service providers – PSPs acting as e.g. AISPs and/or PISPs – and ICT/FinTech companies represent 79% of the respondents (115/146) shows that the game around the conquest of the European digital single market[82] is being played by the established financial institutions on the one hand and by FinTech companies on the other. The European Commission, by means of the PSD2, wants to ensure a greater adoption of online payments by merchants and customers. Electronic transactions need therefore to become more secure[83], hence why the payment market is also being opened to technology and security companies for which online security – e.g. authentication and identification, elements of strong customer authentication – is the core business.
All feedback is deemed valuable by the EBA, which is currently consolidating the responses in order to finalize the RTS it has been mandated to develop – expected in February or March 2017 –. The RTS will then become applicable eighteen months later (Q3 2018). The table shows the amount of responses provided per question by the different respondents, as assessed by the author.

Sector	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10
Banks (+ related, e.g. federations)	31	31	26	33	34	28	31	30	30	31
PSPs (AISPs and/or PISPs related)	23	12	12	23	12	14	17	16	13	15
(Cyber) security related (e.g. SCA)	19	14	12	14	12	13	15	12	11	8
ICT service providers/FinTechs	13	11	11	12	11	13	12	12	12	12
(Credit) card related	10	9	5	10	9	4	8	3	1	-
Non-bank PI & CI related	10	9	8	9	10	10	9	8	8	8
(E)-commerce	6	5	1	5	5	2	5	-	-	1
Consultancy	4	3	4	5	4	4	4	3	3	5
Government	6	3	3	4	3	4	2	2	4	2
Retailers	2	2	2	2	2	2	3	2	1	1
Academia	3	1	3	2	1	3	2	1	2	1
Consumer organisations	1	1	2	2	1	2	1	-	-	-
Payment systems related	2	2	1	2	2	1	2	2	2	2
Marketing	1	1	-	1	1	-	1	-	-	-
Telco	1	1	1	1	-	1	1	-	-	1
Food industry	1	1	1	1	1	1	1	-	-	-
Total	133	106	92	126	108	102	114	91	87	87
Response rate	91%	73%	63%	86%	74%	70%	78%	62%	60%	60%

Figure 5 – Total response rate per question

Competing interests

All in all, the analysis of the different answer proves further the resulting 'power' play between e.g. banks – the ASPSPs once PSD2 is enforced in January 2018 – and the FinTechs companies – most of them future AISPs or PISPs –, the formers in order to ensure that sufficient security measures will be requested of the PSPs to avoid fraud as much as possible, as the PSD2

[82] A Digital Single Market for Europe, Jean-Claude Juncker's address to the State of the Union – European Parliament, European Commission, 14 September 2016
[83] Stavins, J. & Schuh, S., How Consumers Pay: Adoption and Use of Payments, Working paper, Consumer Payments Research Center, Federal Reserve Bank of Boston, page 17, 12 December 2011

stipulates that the final liability lies by the ASPSPs – and the latter in order to make sure that their planned payment market acquisition will not be tampered with. The customers seem to occupy a less preponderant place in the rhetoric: they are only referred to by PSPs, when it comes to the too strict SCA requirements issued in the RTS, arguing that they would surely hamper the customers' convenience when using new electronic payment services coupled to too many security measures.

Considering the total response rate per question (figure 5), the first and the fourth questions clearly seem the most relevant to the respondents. The interest in addressing question 1 – about the requirements of strong authentication (SCA) in general – can be explained by the fact that this question is the most open. As such, the majority of the respondents (91%) provides general feedback about their different vision on strong customer authentication, questioning (e.g. PSPs) or validating (e.g. ASPSPs) its requested application to all parties – as the final liability lies by the ASPSPs, why should some of the PSPs also apply SCA? –, preferring other solutions (e.g. ICT providers) and requesting modification of (part of) some of the articles laid down by the EBA in the RTS (all of the mentioned). The ASPSPs doubt that PSPs will give the needed focus to payment security when developing new solutions, prioritizing instead on disruption and customer acquisition. On the other hand, PSPs' recurring fear is that ASPSPs will not give the same priority to the communication interface's quality and availability as they do for their own channels directly accessible by their customers.
Question 4 – about the exemptions from the application of SCA and security measures – is again source for (counter)-argumentation from ASPSPs and PSPs. In the RTS, the EBA proposes clauses[84] describing in which situations strong customer authentication is not needed. ASPSPs seek – rightfully – to remove from the RTS the mandatory aspect regarding the application of exemptions, advocating instead – supported by non-bank payment or credit institutions, credit card and security related companies and few PSPs – a transactional risk-based approach, through which the ASPSPs could decide to apply SCA (e.g. in the case of fraud suspicion) even if the situation allows a exemption in the regulatory text (e.g. the payer initiates an electronic credit transfer to a payee included in the payer's beneficiary list). Most of the PSPs urge to keep the mandatory aspect, in order to prevent ASPSPs from security over-engineering, which would translate in loss of convenience for the customer – directly impacting PSPs' business model –.

Broader look

In order to avoid the pitfall of this research being caught in the power play described above because of considering question 1 and 4 only, a broader approach is sought in the analysis of the answers – relevant for (cyber) security, which show a response rate of more than 80% and which are provided by sectors represented by at least ten respondents (figure 6). As a result, six sectors – ASPSP, PSP security and ICT related – as well as twenty-three out of the sixty possible groups of responses qualify (marked in yellow), ensuring that all questions provided by EBA are covered in this research, providing the answers are relevant to (cyber) security –. Given the extent of the responses, only (cyber) security relevant issues are reported. Based on the principle that quality of the answers prevails above quantity, the responses of the remaining sectors – represented by less than ten respondents – are also in scope of the below analysis when relevant.

Sector	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10
Banks (+ related)	89%	89%	74%	94%	97%	80%	89%	86%	86%	89%
PSPs	92%	48%	48%	92%	48%	56%	68%	64%	52%	60%
(Cyber) security related	95%	70%	60%	70%	60%	65%	75%	60%	55%	40%

[84] Consultation Paper on the Draft Regulatory Technical Standards specifying the requirements on strong customer authentication and secure communication under PSD2, European Banking Authority, EBA/CP/2016/11, page 33, Chapter 3 – Exemptions from strong customer authentication, 12 August 2016

ICT providers/FinTechs	87%	73%	73%	80%	73%	87%	80%	80%	80%	80%
(Credit) card related	100%	90%	50%	100%	90%	40%	80%	30%	10%	-
Non-bank PI & CI	100%	90%	80%	90%	100%	100%	90%	80%	80%	80%

Figure 6 - Response rate per respondent per question

Responses to question 1

As already mentioned above, the very open character of this question invites to feedback, hence the high response rate noted by each of the represented sector. Besides the many demand for text adaptation, Another common argument is that the EBA confounds authentication with authorisation (a.o. Informed Risk Decisions Ltd), arguing that more reliance should be sought on the existing eIDAS regulation[85] (a.o. Luxembourg Government IT Center) and NIST publication (a.o. Icon Solutions Ltd) to provide clear definitions. It is also not clear what is meant by 'digital signature' (a.o. Iden Trust). Less common arguments are the considering of a) identity assurance (Government Digital Service UK), – as '*SCA without verifying identity ensures only that the same entity is returning to services, not that the entity is the right person or a valid entity*' – and b) end-user psychology (Kontomierz.pl S.p.) as a complement of strong customer authentication. As authentication, authorisation and digital signature are essential to strong customer authentication, these topics will be subject to further development and recommendations in the next chapter.

Responses to question 2

Although many respondents welcome the flexibility that the RTS offer regarding the application of dynamic linking (a.o. AFEC), there is a general call for clarification regarding the required independence of channels (o.a. IBM). Some feedbacks prove reticent (a.o. Italian Banking Associaton), as this requirement would remove for example the possibility of managing the generation of a token via embedded functionalities in the payment apps – technology currently considered as the state of the art regarding security and user experience, according to IBA –. One respondent (Token) disagree completely with the concept of channel separation, arguing that if the dynamic link occurs through electronic signatures – in which validation of the amount and the payee are signed by multiple private keys of the payer –, *'use of different channels is unwarranted and leads to unnecessarily poor user experience'*. Clarification is needed, therefore this topic qualifies for further enquiry in the next chapter.

Responses to question 3

Mainly, respondents advocate that PSPs should have a strong password management policy in place, to ensure an adequate level of protection, warn for too much reliance on inherence (IBM), and refer to the Global Data Protection Regulation[86] (GDPR) in order to ensure data privacy (Intercede Ltd). Strong password management is essential to SCA, so it qualifies for further enquiry, as does data privacy, as more parties will be allowed to process personal data after the enforcement of PSD2.

Responses to question 4 & 5 (related, also in the responses)

As already mentioned, a very supported feedback is that although exemptions should not be made mandatory for ASPSPs or a clause should be added allowing transactional risk-based assessment for ASPSPs, to be performed in specific cases – e.g. suspected fraud – (a.o. Klarna). Many respondents also call for a clear definition of sensitive data related to payments (Fintonic Servicios Financieros), as none is included in the draft RTS. Both topics will be further developed

[85] Regulation (EU) No 910/2014 of the European Parliament and the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, Official Journal of the European Union, 28 August 2014

[86] Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 4 May 2016 (Text with EEA relevance)

in the next chapter, as a risk-based approach can prove a game changer for mobile banking adoption – generally speaking, (cyber) security can rarely generate convenience – and a clear definition of sensitive payment data is essential to implement adequate SCA measures on the right data.

Responses to question 6 (about personalised security credentials)

Most relevant feedbacks mention the omission in the draft RTS of Trusted Execution Environment (TEE) for mobile device – as a means to protect the content once stored on the device – (o.a. Notakey) and standards for the PSCs (Payment UK & Co). The standards for PSCs exist[87] and should indeed be referred to. This topic will not be enquired further in the next chapter. TEE is an obvious component of cyber security, as it allows protecting e.g. user credentials and encrypted key. Although this topic is not going to be further enquired in this research – TEE qualifies for a whole research on itself –, EBA should address TEE in the RTS and seek understanding – if needed – in de scientific[88][89][90], academic[91] and professional[92][93] literature.

Responses to question 7

The main issue here is that PSPs want to ensure – make it mandatory – that ASPSPs will provide high quality APIs, with a structural availability of 99,999% such as there is the norm for ASPSPs' own channels. The second main finding is the lack of requirements for a standardisation of communication interfaces (API). As the former is mostly a juridical issue – mandate in the RTS the obligation for ASPSPs to maintain the interface for PSPs with the same quality as their own –, it is not really relevant for further development in the next chapter. Requirements for standardisation of communication interface are indeed relevant, but a too broad a subject for this research. It earns an own research, which is also requested by some respondents to EBA. Both these subjects will not be considered further in the next chapter.

Responses to question 8

By far most of the respondents were referring to expected interoperability issues (o.a. IdenTrust) and the fact that ISO 20022 is not commonly used (Gemalto). Given the many aspect of the subject, it disserves an own research and will therefore not be enquired further.

Responses to question 9 (about the relevancy eIDAS recognised web certifcates)

Many respondents validate the use of e-IDAS-recognised web certificates as an identification means (o.a. Finect) but note that other alternatives must also be made possible (o.a. Intessa Sanpaolo). One respondent argues that web certificates are not the right tools for the required identification (GBIC). Respondents also mention that there are no Certificate Authority (CA) yet created to distribute these certificates, not helping in adopting eIDAS qualified website authentication certificates (QWAC). This subject might also qualify for an own research; therefore it will not be developed further.

---

[87] www.pcisecuritystandards.org/document_library

[88] Jang, J.S. et al., SeCRet : Secure Channel between Rich Execution Environment and Trusted Execution Environment, NDSS, 2015

[89] Ekberg, J. E., Kostiainen, K., Asokan, N., Trusted execution environments on mobile devices. In Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security (pp. 1497-1498). ACM, November 2013

[90] Ekberg, J. E., Kostiainen, K., Asokan, N., The Untapped Potential of Trusted Execution Environments on Mobile Devices, IEEE Security & Privacy, July-Aug. 2014, Vol.12(4), pp.29-37

[91] Murdoch, S.J., presentation on Introduction to Trusted Execution Environments (TEE) – IY5606, Computer Laboratory, University of Cambridge

[92] www.globalplatform.org/mediaguidetee.asp

[93] Gullberg, P., Trusted Execution Environment – TrustZone and Mobile Security, OWASP Götebrog: Security Tapas, 20 October 2015

Responses to question 10 (request information frequency from AISPs)

Most of the discussions – in the few responses on this question – are focusing on the one hand about the need to access the data frequently (AISPs representatives and related) and on the other hand about the data exchange overload that could saturate the network (ASPSPs). Considering the few answers compared to other issues – such as a clear definition of authentication and authorisation, which is critical to SCA –, and the relevancy of the subject for (cyber security) – besides a Denial of Service because of saturated network (no attack) and potentially on privacy (addressed by the fact that an AISP may not perform any activity for which the user has not given any consent), the daily frequency that an AISP should be allowed to request customer information has no real impact on cyber security. There the topic does not qualify for further enquiry.

D. Generic issues

Besides the issues related to the ten EBA questions, more global issues have been identified during the research, such as the fact that PSD2 will become applicable as of 18 January 2018, but the its RTS are only expected to be enforced in somewhere in October 2018 at the soonest. An issue will be that PSPs will not be obliged to apply SCA during this transitional period. On the other hand, ASPSPs will be free to provide an API with a minimum quality and availability rate.

Yet another issue is the apparent distrust and competition between ASPSPs (e.g. banks) and PSPs (e.g. AISPs and PISPs). Banks, so far enjoying a monopolist leadership in the payment market, have become aware that a significant share of their – for the most somewhat conservative – business model can vanish, providing they miss the opportunity to adapt quickly. On the other hand, PSPs – represented by a booming number of FinTechs – are conscious of the fact that they can – and are willing to – potentially disrupt a market long undisputed. This competition, although applauded by the EU law-makers, can also have repercussions on the consumers if the power play mentioned above goes on too long. Both need each other, and collaboration[94] will deliver more benefits[95] on the long term than avoiding each.

Although both relevant more or less relevant for (cyber) security, they will not be addressed in the next chapter, as the former issue lies within the jurisdiction of EBA and the later qualifies for a whole research on itself.

E. Conclusion

The analysis of the many – disclosed – responses report many issues or demands for more clarity regarding the (cyber) aspect of PSD2. Some of these issues will be addressed in the next chapter. As a general comment, competing interests left aside, the balancing between security measures and convenience of payment transactions will prove a key success factor. Too much of one will be on the expense of the other, either creating unsecure electronic payments or non user-friendly, unpractical payment solutions. Both cases would lead to the non-adoption of the new digital means by the consumers – either the end customers or the merchants –, which would hamper the very objective of PSD2: one single digital EU payment market.

[94] www.febelfin.be/nl/fintech-bedrijven-willen-samenwerken-met-financiele-instellingen

[95] Berger, R., *FinTechs in Europe – Challenger and Partner*, Roland Berger Study (with Belgian key points), November 2016, page 2(4)

5. Recommendations

The analysis of more than thousand responses performed in the previous chapter reported many (cyber) security relevant issues relating to the different articles of the draft Regulatory Technical Standards on Strong Customer Authentication and Secure Communication (RTS on SCA & SC) published by EBA. Some of the identified issues – e.g. API specifications and interoperability under ISO 20022 – are too large to be addressed in this report and require an own research. Others – e.g. allowed daily frequency of information request – are less relevant to (cyber) security or SCA. The remaining issues – e.g. clarification of the definition of authorisation vs. authentication and sensitive payment data – will be addressed below, through a short explanatory element followed by a recommendation. One addressed topic – transaction-based risk analysis – will show that a sound security can indeed generate

convenience, contributing to the balancing between of security of payment and easy-to-use services.

Recommendation 1

Authentication vs. authorisation (related to question 1)

As reported in the previous chapter, many respondents believes that the EBA, in its draft RTS, seems to confuse authentication with authorisation. Article 4(29) of the PSD2 limits the definition of 'authentication' to a "procedure which allows the PSP – payment service provider – to verify the identity of a PSU – payment service user – or the validity of the use of a specific payment instrument, including the use of the user's personalised security credentials", while article 1 (1) of the RTS speaks of an "authentication procedure – that –shall result in the generation of an authentication code that is accepted only once by the PSP each time that the payer [PSU] making use of the authentication code accesses its payment account online, initiates an electronic transaction or carries out any action through a remote channel which may imply a risk of payment fraud or other abuses" and article 1(3) is clearly referring to 'authorisation' while speaking of the same use of authentication codes. It might prove relevant to clarify the two definitions.

In the literature, one clear definition[96] refers to 'authentication' as a procedure 'verifying the claimed identity of a client or service'. To illustrate, when client A initiates a money transfer to someone else's account, the bank wants to be certain that client A is really the person she/he claims to be – authentication – and that no one else is using client A's identity for malicious purposes –called "spoofing" –. 'Authorisation' is defined[97] as a procedure 'allowing an authenticated client to use a particular service'. Using the same example as above, when the bank is certain that client A is the person she/he claims to be, she/is allowed – authorised – to use her/his account services (in this case the transfer of money).

The National Institute of Standards and Technology (NIST) – referred to by some respondents – supports these two definitions, by describing[98] 'authentication' as the process of *'verifying the identity of a user, process or device, often as a prerequisite to allowing access to resources in an information system*'. Although no specific definition is provided for 'authorisation', NIST refers to this process in the above definition as a sequel of the authentication phase. The ECB's definition[99] of 'authorisation' – although focused on payments – could be referred to as a complement, explaining that 'authorisation' is '*a procedure that checks whether a customer or PSP has the right to perform a certain action, e.g. the right to transfer funds, or to have access to sensitive data'*.

Some of the respondents refer to the eIDAS regulation[100] – which forms the governing regulation on electronic transactions in the European Union –, where – in their understanding – 'authentication' is considered as 'electronic identification' and defined in article 3(1) as a '*process using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person'*. This proves a

[96] Miller, S.P., Neuman, B.C., Schiller, J.I. and Saltzer, J.H., *Kerberos authentication and autorisation system*, Section E.2.1, Project Athena Technical Plan, 1987

[97] Miller, S.P., Neuman, B.C., Schiller, J.I. and Saltzer, J.H., *Kerberos authentication and autorisation system*, Section E.2.1, Project Athena Technical Plan, 1987

[98] Kissel, R., *Glossary of Key Information Security Terms*, NISTIR 7298, Revision 2, NIST, US Department of Commerce, May 2013, page 17

[99] European Central Bank, Recommendation For The Security Of Mobile Payments – Draft Document For Public Consultation, November 2013, page 23

[100] Regulation (EU) No 910/2014 of the European Parliament and the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, Official Journal of the European Union, 28 August 2014

misperception, as 'authentication' and '(electronic) identification' are two different processes composing the process allowing access to a system (authentication procedure). In computer systems, 'identification' is *'the process of ascribing a user identitfier (ID) to a human being or to another computer or network component'*[101], while 'authentication' is *'the process of binding an ID to a specific entity'*[102]. Using our example, 'identification' occurs when client A types her/his username in the login screen of the bank system – she/he "presents" the system with her/his user identifier linked to her/him when becoming the bank's client – while 'authentication' occurs after client A entered her/his password and hit the "login" button – the bank's system then "validates" – or not in case of fraud attempts – that the username is indeed of client A –. Once authenticated, she/he is authorised to access the bank system and the specific services included in client A's authorisation.

The use of above identified definitions is recommended to clarify the concept and definition of 'authentication' – composed of 'identification' and 'authentication' processes – and 'authorisation' in the RTS, in order for all parties involved to have a common and shared understanding on the topics, allowing for a consequent and secure application of strong customer authentication. A particular accent is laid on the eIDAS regulation defintions, as it has been designed specifically to enable the Single Digital Market by a.o. ensuring that electronic signatures and website authentication are recognised and workable across borders[103].

Recommendation 2

Logical independency of the channels (linked to question 2)

For many respondents, the RTS were not clear about the requirements for independency of the elements of strong customer authentication – knowledge, possession and inherence – (article 6) when performing a mobile payment transaction.

First, a common understanding of how a mobile device – e.g. smartphone or tablet – works might prove useful. Reference is made to the very clear and rich explanation provided by GSMA – a London based association representing the interests of mobile operators around the world[104] – in its feedback[105] to EBA on the draft RTS, where it explains the *'differentiated view'* of a mobile device, consisting of three elements – the mobile device itself, the *'mobile business process'*, and the mobile network –, which are all interlinked but work fully independently from each other – ensuring a high level of security –. A short sum-up is provided below.

While always under the control of its owner – thus qualifying for an SCA element categorised as possession –, the mobile device, when lost or stolen, is the only element that actually *'disappears'*: although the owner cannot use it anymore, the mobile network operator (MNO, triggering the second element (see below)) can access the device remotely – e.g. to disable it – as long as its subscriber identity module (SIM) is *'active and attached to the network'*.

The business process is *'the mobile network operator's ability to interact'* with the device. In the case of theft or loss, business processes can still access the device to disable its use. The loss of a mobile device being generally detected and reported sooner than the loss of a

[101] Sandhu, R., Hadley, J., Lovaas, S. and Takacs, N. (2012) *Identification and Authentication*, in Computer Security Handbook, Sixth Edition (eds S. Bosworth, M. E. Kabay and E. Whyne), John Wiley & Sons, Inc., Hoboken, NJ, USA. ch28

[102] Sandhu, R., Hadley, J., Lovaas, S. and Takacs, N. (2012) *Identification and Authentication*, in Computer Security Handbook, Sixth Edition (eds S. Bosworth, M. E. Kabay and E. Whyne), John Wiley & Sons, Inc., Hoboken, NJ, USA. ch28

[103] www.ec.europa.eu, Trust Services and eID, *Digital Single Market*, Digital Economy and Society, European Commission, 29 June 2016

[104] www.mobileworldcongress.com/about/about-the-gsma

[105] www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2/-/regulatory-activity/consultation-paper/GSMA

wallet[106], GSMA considers the *'interactions between device and network'* as key for an enhanced security, as *'risk situations can be dealt with appropriately'*. Besides disabling the device, MNOs can also access other data such the device's location and *'restore the payment capability remotely'*, when applicable.

The mobile device, the SIM and the phone number (Mobile Station Integrated Services Digital Network, MSISDN) are connected together by the mobile network, the resulting interlinking being '*stored very securely in the mobile network, which'* – according to GSMA – *'is not penetrable from the outside'*. Each time the mobile device accesses a network – e.g. when the phone is switched on –, this network recognises the combination phone/SIM/phone number. Attempts to use the device with another SIM are detected by the network and immediately acted upon accordingly – e.g. block the account in case of suspected fraud –. Moreover, a mobile device labelled as "stolen" by a MNO is also labelled as such by all other mobile operators worldwide – according to GSMA, a proven security process for the mobile industry – .

GSMA motivates that an identical level of independence – as described above and as required in the RTS – regarding mobile payment transactions can be achieved – '*with beneficial impact on security' – 'by ensuring that the consumption and the authentication channels* remain *two independent channels'* through out-of-band authentication – two-factor authentication –, where the consumption channel (e.g. a banking application on a smartphone) is used by customers or merchants to access payment services while the authentication channel is used by the smartphone app or SIM applet to authenticate the interaction of the user with PSPs (e.g. through a PIN). Although both present on a same device, the channels are independent of each other.
In the end, *'the fundamental independence between the mobile device (something the consumer has) and the PIN (something the consumer knows) remains intact even when the mobile device is lost or stolen'*, thereby addressing and complying to article 3 and 4 of the RTS.

Although this topic would be suitable for a whole research on itself – e.g. are mobile network indeed not penetrable? What about unprotected WiFi-connections? –, the explanation and argumentation provided above should be food for thoughts for EBA, in order to either formulate an end objective and leave it up to market – where the knowledge lies – to come up with solutions (e.g. GSMA's Mobile Connect, a new standard in digital authentication[107] that links users directly to mobile phone they own[108]), thus removing the need of passwords when accessing websites and apps) or to refer to existing standards and proven solutions, addressing specific, uniform and industry-relevant requirements still needed to be defined in the RTS. Moreover, EBA should also consider the growing diversity of mobile devices that do not require a mobile phone network to access the Internet – e.g. wearable such as Apple Watch –. PSPs will likely offer payment services accessible from these devices too. The Apple Watch, for instance, can either connect to a smartphone via Bluetooth or directly to the Internet via connection to a Wi-Fi network, which both proved easy to compromise[109][110][111][112] – e.g.

[106] Herbert, C., Crain, T., Smith, C., Low power apparatus for preventing loss of cell phone and other high value items, Google Patents, 11 November 2010, [0005]
[107] www.gsma.com/personaldata/mobile-connect
[108] Mobile Connect fact sheet, GSMA, 15 June 2015
[109] Wong, L.W., Potential Bluetooth Vulnerabilities in Smartphones, School of Computer and Information Science, Edith Cowan University, 2005
[110] Browning, D., & Kessler, G. C. (2009, January). Bluetooth hacking: A case study. In Proceedings of the Conference on Digital Forensics, Security and Law (p. 115). Association of Digital Forensics, Security and Law.
[111] Reddy, S. V., Ramani, K. S., Rijutha, K., Ali, S. M., & Reddy, C. P. (2010, June). Wireless hacking-a WiFi hack by cracking WEP. In Education Technology and Computer (ICETC), 2010 2nd International Conference on (Vol. 1, pp. V1-189). IEEE.
[112] Bradbury, D. (2011). Hacking wifi the easy way. Network Security, 2011(2), 9-12.

malicious parties can use special tooling to scan for vulnerable devices with an active Bluetooth connection or tapping Internet traffic through unsecure Wi-Fi networks[113]. A recommendation would be to require stronger authentication means – transaction authorisation code sent on another device (e.g. mobile phone) – when seeking to perform mobile payment transactions using a Bluetooth or (free) Wi-Fi connection.

Recommendation 3

Strong password policy (linked to question 3)

Some respondents stated that PSPs should have a strong password policy in place (e.g. forcing strong password, providing password-handling recommendations to the users and password blacklist to block weak passwords). Beside security measures [114] ensuring information entropy[115] (increasing the length, complexity and unpredictability of a password and therefore its strength, such as with passphrases) against guessing attacks (brute force), the maximum number of erroneous trials must additionally be limited (e.g. 3 times as generally used by banks) by the implementation in order to exclude exhaustive trial attacks.

NIST issued a draft of new guidelines [116] addressing password policies in 2016. Although primarily designed for the US government – like all NIST standards –, the guidelines define requirements to address four levels of assurance (LoAs)[117] regarding e.g. registration – where identity proofing (validating that the person is who she/he claims she/he is) is separated from authentication – and authentication of a user. After defining as a common standard what the terms "shall", "should", "may" and "can" imply, NIST recommends e.g. to put the burden as much as possible on the identity verifier – and to stop asking the user to do things that are not increasing security[118] –, a maximum length of at least sixty-four characters (more is possible for more sensitive accounts) and the use of a dictionary to disallow common passwords. Moreover, the use of printable ASCII characters[119] – including spaces – must (!) be allowed and all Unicode – including emoji – should be accepted. On the other hand, password hints[120] and knowledge-based authentication (KBA) – when users have to choose from a list of questions (e.g. what is the name of your first pet) as a security check when e.g. password is lost – must be banished, and no more rules forcing the use of (a combination of) specific characters – called 'composition rules' – nor routine password expiration should be use. If users are to comply to the use of long passwords with many difficult characters, they should not have to change these passwords unnecessarily. Requirements for user verifiers (PSPs) are also defined for password storage (e.g. all passwords must be hashed – keyed HMAC hash using SHA-1, SHA-2 or SHA-3 – , salted – 32 bits or more – and stretched – PBKDF2 algorithm with at least 10.000 iterations –).

The NIST guidelines on digital identities could be referred to by PSPs and other relevant parties as a template when developing new payment service applications, as there is a strong emphasis on user experience. The increase of the maximum characters and the inclusion of non printable ASCII will allow the use of passphrases and the emoji acceptance will be very welcome for the somewhat younger part of the users. Granted, a sixty-four characters password on a mobile phone screen will not prove adequate and the entropy-level of a ASCII space character is

[113] Henn, S., Here's One Big Way Your Mobile Phone Could Be Open To Hackers, NPR, Privacy & Security, 13 June 2014 (blog)
[114] Cyber Security Tip ST04-002, *Choosing and Protecting Passwords*, US CERT, 01 October 2016
[115] Schneier, B., *Choosing Secure Passwords*, blog, Schneier on Security, 03 March 2014
[116] Grassi, P. A., Garcia, M.E. and Fenton, J., *Digital Identity Guidelines*, Draft NIST Special Publication 800-63-3, Computer Security, NIST, US Department of Commerce
[117] Office of Management and Budget, *E-Authentication Guidance for Federal Agencies*, Executive Office of the President, 16 December 2003
[118] Fenton, J., Toward Better Password Requirements, PasswordsCon address, Las Vegas, 2 August 2016
[119] www.jupiner.net, *Reference: Nonprintable and Printable ASCII Characters*, TechLibrary, Jupiner Networks, 8 February 2011
[120] Ducklin, P., *Anatomy of a password disaster – Adobe's giant-sized cryptographic blunder*, Naked Security by Sophos, www.nackedsecurity.sophos.com, 4 November 2013

questionable; they also oppose somewhat the – unclear – requirement of article 3(1) of the RTS defining non-repeatable characters (supposedly for a password) as a measure to ensure resistance against disclosure to malicious parties, which is also arguable. Nonetheless, official security standards guidelines issued, by a globally recognised institute, focusing on user-friendly passwords may not be neglected by PSPs, as user experience will be key to their payment services' adoption.

Recommendation 4

Privacy (linked to question 3)

Although confidentiality is mentioned in the RTS, some respondents feel that the requirements are mostly focusing on the protection of the authentication elements' integrity and on their non-repudiation aspect, omitting privacy. As the Global Data Protection Regulation (GDPR regulation (EU) 2016/679)[121] will apply as of March 2018, it is indeed necessary to consider the privacy aspect of the RTS, considering that post-PSD2 many more PSPs will become either data controllers (article 4(7) of GDPR) or data processors (article 4(8)). Personal (security) data (article 4(1)) will be stored and/or exchanged; account data will be process (article 4(2)) for profiling reason (4(4)) by AISPs and PISPs; and biometric data (article 4(14)) are likely to be involved as security measures for mobile payment transaction. All these activities must occur with the user's consent (4(11)). It is not clear yet what personal data must be included in the user personal security credentials or in other authentication elements (e.g. user name or account number). No matter the personal data used, the user's privacy needs to be protected when exchanging sensitive data online (in this case via mobile device) or else privacy lawyers will have plenty of suing cases on their shelves. As a solution, one respondent proposes to anonymise e.g. a user's personal data by linking e.g. user account(s) and name an anonymous identifier known only by bank. While technically not correct – the process described is about pseudonymisation, anonymised data are not re-linkable to the owner[122] –, the idea is worth giving it some thoughts.

The GDPR does not apply to anonymous data but does consider pseudonymous data (article 4(5)). Privacy enhancing techniques[123] (PETs) allow to amend sets of data in such a way that no user can be (directly or indirectly) identified from those data without a "key" that allows the data to be re-linked to the owner. This re-identification is the reason why pseudonymous data are still treated as personal data. However, pseudonymous data brings along an extra security layer – provided that the "re-identification key" is kept separate and secure –, which results in a lower risk of unauthorised use, meaning that a lower level of protection is required for those data (as privacy is ensured by default). The GDPR explicitly encourages data controllers to consider pseudonymisation as a security measure (recital 29).

Recital 94 of the PSD2 states that EBA *'should systematically assess and take into account the privacy dimension'* when developing the RTS on SCA & SC. The Consultation Paper[124] on the RTS does refer to data protection – the official EU name for privacy[125] –, explaining that the *protection of individuals with regard to the processing of personal data by the EBA is based on Regulation (EC) N° 45/2001 of the European Parliament and of the Council of 18 December*

[121] Regulation (EU) No 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 4 May 2016 (Text with EEA relevance)

[122] Neubauer, T. and Riedl, B., *Improving Patients Privacy with Peudonomisation*, Studies in health technology and informatics 136 (2008): 691, page 693 – figure 1

[123] www.enisa.europa.eu, *Privacy enhancing technologies*, Data Protection, ENISA Publications,

[124] Consultation Paper on the Draft Regulatory Technical Standards specifying the requirements on strong customer authentication and secure communication under PSD2, European Banking Authority, EBA/CP/2016/11, page 33, Chapter 3 – Exemptions from strong customer authentication, 12 August 2016, page 3

[125] www.enisa.europa.eu, *Privacy by Design*, Data Protection, ENISA Publications,

2000[126]*'*. Recital 17 of the GDPR requires an adaptation of Regulation (EC) N°45/2001 and all *'other legal acts applicable to processing of personal data'* to the principles and rules defined in the GDPR, in order to create a strong data protection framework in the European Union.
As such, the RTS should anticipate and base data protection requirements on the now adopted Global Data Protection Regulation (GDPR) rather than an aged Regulation. Coherence between the legal texts will help create uniformisation on data protection. EBA should seek leverage on the implementation requirements defined in the GDPR, as they are applicable in Q1 2018, at least a half year before the enforcement of the RTS on SCA & SC. It would avoid reinventing the wheel and allow – in this case – the payment sector to go further with the application of the GDPR requirements regarding data protection, which eventually will serve the PSD2 and RTS purpose.

Recommendations 5

Transactional risk analysis (linked to question 4)

Many respondents argue that exemptions from applying strong customer authentication should not be made mandatory for ASPSPs (and eventually for PSPs, when more mature and using own SCA means), as they should be able to perform risk assessments based on specific transactions is specific situation, such as by fraud suspicion.
ECB defines[127] transaction risk analysis as an evaluation of the risk related to a specific transaction taking into account criteria such as customer payment patterns (behaviour), the value of the related transaction, the type of product and the payee profile.

EBA motivates in recital 54 the exclusion of transactional risk analysis from the RTS as the will to ensure fair competition among all PSPs by reducing the security investment needed. Considering the end customer segment, the structural application of the exemptions will certainly ensure a level playing field for PSPs, as all customers can be considered as equal, allowing PSPs to start with a same security investment budget. However in case of fraud (suspicion) – based e.g. of customer behaviour analysis –, ASPSPs must be able to apply SCA. Applying SCA on high-risk transactions is often better than blocking them: it avoids extra traffic that comes from re-initiation of the transaction – in case of false-positive – and is more customer friendly, while maintaining a high level of security.
On the other hand, mandatory exemptions are not suitable for merchants, as many of them have implemented authorisation matrixes directly integrated in the authorisation procedures/SCA of the ASPSP, which apply to all of the payments they initiate and the accesses they require to electronic channels, with as objectives security enhancement and protection against internal and external fraud. As a consequence ASPSPs (and later PSPs) should always be able to apply strong customer authentication to facilitate the authorisation procedures in place.
Moreover, risk analysis of payment transactions can help improve the customer experience and the payment services. Although users seek payment security, they are also looking for convenient ("one-click[128]") payment services and products. Allowing ASPSPs to invest in risk analysis on recurring transactions would result in an improvement of the payment services – linked to these transactions – offered to the users: if e.g. an analysis of Dutch credit transfers up to 50 euro returns a fraud probability of e.g. 0,01%, the residual risk might be accepted by the ASPSPs – liable for customers' financial losses – and therefore chose not to apply SCA, make it more convenient for customers to use all the services related to this transaction. Risk analysis

[126] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12 January 2001).
[127] European Central Bank, Recommendation For The Security Of Mobile Payments – Draft Document For Public Consultation, November 2013, page 23
[128] www.oneclickpay.be

could occur on the users (both payers and payees) themselves, by assessing their profiles, behaviour - e.g. past behaviour but also tracking user behaviour in the communication session to detect anomalies before the payment transaction is initiated –, transactions data – e.g. amount and recurrence – but also on the devices and the software used, the location, etc.
One respondent proposes to measure biometric security performance according to ISO/IEC 19795[129] and to use the results as base for risk assessments, which might prove relevant in a digital payment landscape more and more focused on mobile transactions.

EBA should reconsider its position and include transaction risk analysis as security measure in the RTS, as a thorough comprehension of the risk linked to transactions will result in more convenient payment services for users and contribute to an increase adoption of the digital payment market. A risk-based approach can prove essential and a game changer for the ASPSPs (and PSPs) – to identify transactions were residual risks can be accepted, resulting in lower security investments – as well as for the payment service users' experience and adoption of the new payments means – less security measures means a greater user friendliness of products and services –. Regarding PSPs, minimum SCA requirements must be defined in the RTS in order to avoid differences in applied levels of security that could certainly make the payment service user vulnerable. EBA needs to understand that requesting PSPs to offer a minimum of security to customers would not necessarily hamper fair competition, provided this minimum is clearly defined – based e.g. on scenario analysis – and made mandatory to all AISPs and PISPs in specific cases.

Recommendations 6

Definition of sensitive payments data (linked to question 4)

Many respondents reported the lack of (clear) definition in the RTS regarding sensitive payment data. EBA states in recital 50 of the Consultation Paper on the RTS that neither definition nor list of sensitive payment data will be provided in the RTS to not hamper technology neutrality and innovation. Although this motivation is comprehensible, it remains a fact that uniform application of the RTS will only occur if the rules are clearly laid down so that no (mis)interpretation is possible. As these data need extra protection, new – and even old – players on the payment market need to know what those data are in order to take all the measures necessary to protect the data and its owner.

The European Central Bank (ECB) provided in 2013[130] a very comprehensive and rich definition of sensitive payments data still actual for payments transactions: *'data which could be used to carry out fraud, excluding the name of the account owner and the account number, including data enabling a payment order to be initiated (e.g. PAN, card expiry date, CVx2), data used for authentication (customer identifiers, birth date, passwords, codes, PIN, secret questions, passwords/codes for reset, telephone number, certificates), data used for ordering payment instruments or authentication tools to be sent to customers (customer's physical address, telephone number, e-mail address), as well as data, parameters and software which, if modified, may affect the legitimate party's ability to verify payment transactions, authorise e-mandates or control the account (such as "black" and "white" lists, customer-defined limits), and browser plug-ins and java applets provided by PSPs to their customers'*.

The EBA working "closely" with ECB on the RTS for SCA & SC, this definition should be included in the RTS, to provide at least a good base for PSPs to start implementing security measures (e.g. tokenisation of the sensitive payment data).

[129] ISO/IEC 19795 series 1-6, Information technology - Biometric performance testing and reporting, ISO, 2006 - 2012
[130] European Central Bank, Recommendation For The Security Of Mobile Payments – Draft Document For Public Consultation, November 2013, page 25

Conclusion

The analysis in chapter 4 of more than thousand answers reported structural issues of the lack of (uniform) definitions – and consequently clarity – concerning authentication, authorisation and sensitive payment data. Referring to existing standard of NIST and eIDAS, clear, unambiguous definitions were provided for the two first processes (recommendation 1) while the definition of the ECB – from 2013 but still actual for payments – was provided and is recommended (recommendation 6) as a starting point for PSPs that will evolve along with the new services they will offer. More importantly, the concept of risk-based analysis is introduced, demonstrating that sound security risk assessment do not necessary lead to unfriendly services or products and therefore requesting the EBA to reconsider its position on the subject (recommendation 5). Evidences were also given that independency of the customer and the authentication channels can be achieved while using only one mobile device (recommendation 2), describing first how a mobile phone works – thanks to a very clear explanation of the topic by GSMA – and applying the model to mobile payment. Reference was again made to the new NIST standard – still in draft form – to define strong password policies, as requested by the respondents (recommendation 3). This new standard is focusing on user convenience – *'stop asking the users to do things that do not improve security!'* –, put the burden of security by the identity verifier and set a basis to allow e.g. more complex passphrases – although these might not prove suitable on a smartphone screen –. Finally, the privacy-risk issue was addressed (recommendation 6) by referring to the Global Data Protection Regulation that will be enforced in Europe as of March 2018, which issues many requirements regarding the protection of the user during the processing of her/his personal data, such as advocating data pseudonomisation, as proposed by a respondent.

As a general comment, chapter 5 clearly demonstrated that although the European Union is seeking a common and uniform framework for e.g. privacy and security to achieve a single digital market, it seems that the different EU instances mandated to develop and implement policies fail to align with each other, as in the draft RTS on SCA & SC – published in August 2016 –, data protection is said to be based on a regulation from 2000, which was referred to as out-dated by the GDPR, a text adopted in April 2016 but which requirements were defined years before already.

6. Conclusion

The European Union spent decades to create one internal single market common to all its member states – and some exceptions –, removing the borders and regulatory obstacles to allow free movement of European citizens, capital, goods and services, thus e.g. fostering competition and employability and improving quality and efficiency of products and services. At the turn of the millennium, the EU – aware of increasing use of Internet and new digital technologies – is seeking to upgrade the internal market into one digital single market, willing to remove online regulatory barriers and bring the digital market of its twenty-eight member states into one.

As good functioning payment mechanisms prove vital for an economy, the payment market was the very first to be addressed post-2000, with the enforcement of the Payment Services Directive (PSD) in 2009 and the creation of Single Euro Payments Area (SEPA), which allowed a.o. debit cards issued in one European country to be used in all other countries being part of the EU and money transfers to be performed with the same convenience as domestic transfers. Nonetheless, one specific objective sought by the EU – the increase of competition – could not be achieved with PSD, as banks were still protecting their leadership in the market for payments and PSD lack the legal ground to prevent it. In 2013, a revision of PSD started, which final text – known as the revised directive on Payment Services (PSD2) – was amended in 2016. PSD2,

although building further on its predecessor, is also very different. Where PSD harmonized the traditional way in which payments are made, PSD2 is introducing new types of payments services and non-banks players – called third party payment service providers (TPP or PSP) – to access bank customer account information needed for them to offer new – disruptive – payment services, making it mandatory for banks to provide this information, even if doing so can cost them their leadership in payment services.

As often, new opportunities come with – new – risks. Allowing many more parties to access consumers' sensitive – payment – data is likely to create genuine interest of malicious parties. While banks have greatly invested in a heavily regulated and audited security, questions are raised around the capacity and willingness of the new parties to invest so much in security. When a new digital payment service proves unsafe, consumer will refrain from using it and the greater adoption of the digital – payment – market as sought by the EU will fail to be achieved. Therefore, the European Bank Authority (EBA) was mandate by the European Commission (EC) to develop a set of guidelines and standards addressing security, specifically the regulatory technical standards (RTS) on strong authentication and secure communication (RTS on SCA & SC). The two other security-related guidelines still being work in progress, this research addresses the RTS only.

The analysis of the RTS – through the feedback of more than a hundred of respondents invited to answer a ten-questions survey developed by EBA – shows that a greater alignment is needed between all parties involved, if the objectives of PSD2 are to be achieved. For instance, common definitions are required on e.g. authentication, as EBA uses this term to also describe an authorisation process in the RTS, leading to question the EBA's ability to understand the subject. To this regard, an attempt to clarification is made in Recommendation 1, referring to definitions in the scientific literature but also in the more professional texts of the National Institute of Standards and Technology (NIST), the European Central Bank (ECB) and the eIDAS regulation. Many questions also raised regarding the logical independency of the customer and the authorisation channels while using one single – mobile – device. Using GSMA' process description of a mobile device, Recommendation 2 demonstrates that the issue can be answered even if the channels are included in only one device. Recommendation 3 refers to the newest NIST's guidelines – still in draft – to set a basis on which PSPs' strong password policies could best be created, as often requested by respondents. These new guidelines focus on users' convenience, putting the burden by the identity verifier. Although not every aspect applies to mobile payment – the possibility to enter a passphrase of sixty-four characters might not prove handy on a mobile screen –, many of the NIST requirements seem relevant, such as the use of printable ASCII and Unicode (e.g. emoji), not possible so far. Issues regarding privacy – or data protection – are addressed in Recommendation 4, where guidance is sought in the Global Data Protection Regulation (GDPR) that will be enforced in 2018. GDPR defines clear requirements – e.g. data pesudonomisation, as requested by a respondent – concerning the processing of sensitive data, which can effectively be re-used in the RTS. Strangely, the RTS refer to a regulation of 2000, described as outdated in the GDPR. Recommendation 5 covers the aspect of risk-based approach that lacks in the RTS, as EBA does not consider it as relevant for a good implementation of PSD2. The research, although high-level, argues that the ability of Account Servicing Payment Services Providers (ASPSPs) and PSPs to – continuously – evaluate risks of payment transactions will prove essential in addressing the convenience of new players' products and services, as low-risk transactions will not be subject to strong authentication mechanisms, often synonym of burden for users. It will also allow ASPSPs and mostly PSPs to identify the areas where they shall invest in security, to ensure revenues for themselves and payment safety and data protection for the consumers. Finally, Recommendation 6 refers to ECB to provide a clear definition of sensitive payments data, which

the RTS lack. The RTS being a joint effort between EBA and ECB, it is difficult to understand why such an essential – and existing! – definition is not included in a document that is supposed to become law for all payment stakeholders as of end of 2018. How can PSPs invest in protection of sensitive payment data *'at all time'* if it is not clear what these data are?

Finding the right balance between security and convenience will prove key for the adoption by consumers – the payment services users (PSUs) – of new payments services and means offered by PSPs. In the end, PSD2 will only achieve its objectives when these new services and means are perceived as – at least – as secure as the services provided by banks (the ASPSPs of post-PSD2) today, and more convenient. Too much security will be obtained at the expense of new services' user-friendliness while too few security will prove detrimental to the users' trust in these same new services. Risk-based approaches are very well suited to address this problem, allowing the ASPSPs and PSPs to identify the best trade-off per type of transactions or services, thus limiting their security investments, resulting in lower costs for the consumers. Transactional and service risk analysis will prove a continuous exercise, as (cyber) threats and malicious means to perform fraudulent activities are evolving daily. The only way to address this rapidly changing threat landscape is by reassessing risks on a regular basis, as a risk consider as benign today can prove genuine tomorrow, and vice-versa.

This report seeks to contribute to the implementation of PSD2 and its RTS in a convenient and secure way, by helping PSPs – and EBA – understand some essential aspects of cyber security. Only common definitions, uniformly used by all parties, will enable fair competition and secure new payments means. Only a common and continuous understanding of the (cyber) threats involved will allow ASPSPs and PSPs to define their risk appetite, key to service and product convenience offered to the end users. It could be helpful for PSPs when EBA would build on the elements highlighted in the recommendations as well as on the cyber security specific literature offered this research. The current RTS being too high-level, EBA will need to deep-dive in many (security) elements to come to a clear understanding of what is actually at stake. Only then will it be able to take a clear position, based on the security level of payments it seeks to achieve in the European Union instead of – seemingly – market penetration and adoption of new payments means at all costs. When the RTS were to stay as ambiguous as they are today, market fragmentation would be achieved rather than standardisation. And it has already started, as the lack of requirements for a standard API have brought Belgian banks to decide against a single bank API, meaning that PSPs will have to adapt their software to each Belgian bank they will require customer information of.

In the end, EBA was mandated by the European Commission to develop RTS – meant as a legal document – that will become mandatory to all parties involved in the payment market. For these standards to be enforced, they need to define clearly what is expected of these parties, or else different interpretations will lead to different implementation, which might result in unfair competition, unsecure payment and, eventually, non-adoptive consumers.

7. Food for further research

Short reflection on some (cyber) security issues that are not further enquired in the research, which the author wishes to share with the audience, for further research purposes.

Rush on certificate authorities

A certificate authority issues digital certificates, meant to create assurance regarding secure connections by certifying that the subject mentioned in a certificate owns a given public key. Parties (clients) can then rely on this certificate each time the public key is used to sign – authentication – before launching a secure connection. PSD2 allowing more parties and more digital solutions to perform payments transactions, new certificates – likely eIDAS – will be used specifically for these purposes. As certificates are now directly linked to money transfers, these will be a prey for malicious parties. Therefore, once the governing bodies – e.g. ENISA – have defined which instances are to become certificate authorities and empowered to issue eIDAS certificates, it is likely that a rush on these parties by the aforementioned malicious parties will occur, as money has never be closer. A research of the success chance of such attacks might prove useful for risk-based analysis (e.g. Diginotar's case).

Governance

Regarding the RTS on SCA&SC, there are so many organisms – at EU- but also at national level, with new ones created specifically to 'mirror' already existing entities and make sure they have a saying in the matter – involved in the review and addressing the subject that decision-making and -taking proves cumbersome. In a rapidly changing cyber threat landscape, research might prove useful in how to address new EU-security legislation at national level.

Data sovereignty

PSD2 allows PSPs to access customer data and store them on own severs. While these PSPs will be subjects – either directly if link to GDPR is made in the RTS or indirectly – to the Global Data Protection Regulation (GDPR), how to ensure that the data protection requirements for data processors defined in GDPR will be respected if a PSP stores the data on a US server? How to ensure that the European sovereignty of data will remain even if the US parties seek to access these data, relying on the Patriot Act?

API requirements

The RTS on SCA&SC state that ASPSPs (banks) are obliged to provide PSPs with a communication interface – likely an API –, free of charge, to access to customers' data securely and every time the customer provides her/his consent to do so. Requirements are needed to ensure a high level of security and an availability of 99,999% as is the case fro ASPSPs' own channels. EBA has been requested by the respondents to provide with the requirements, which disserve a research to ensure a European standard. Note that banks have recently decided to not provide at least a national standard. Research on a European API standard will oblige uniformity and counter fragmentation, as will occurred if banks are allowed to go further with an own API.

Security vs. customer acceptance

As identified during the research, balancing between security and convenience of services will prove essential for customers' adoption of the digital payment market. Not much research could be found on the subject and one respondent supported this assessment. Research on high security enabled (payment) solutions vs their acceptance by the consumer could help fine-tuning the trade-off to which ASPSPs and PSPs are seeking to identify.

Collaboration between FinTechs and financial institutions

This research reports about the power play between PSPs – mainly FinTechs – and banks, the former afraid that banks will do anything in their power to slow down their business while the latter fear a downsizing of their – conservative – business model. A first research[131] shows that 86% of the FinTech companies want to collaborate with financial institutions, identifying themselves as technology enablers with superior digital capacities rather than future leader of the payment market. Research is needed on how collaboration could prove key for both, as they would leverage on each other's core business to address new consumer needs.

[131] https://www.rolandberger.com/publications/publication_pdf/roland_berger_fintech.pdf

8. References

i. *20 Years That Changed Europe* - The Copenhagen Criteria and the Enlargement of the European Union, Conference Report, Copenhagen, 14 May 2013

ii. *A Digital Single Market for Europe*, Jean-Claude Juncker's address to the State of the Union – European Parliament, European Commission, 14 September 2016

iii. *Accession criteria* (Copenhagen criteria), Treaty on European Union, Articles 6(1) and 49, established by the Copenhagen European Council (1993) and strengthened by the Madrid European Council (1995)

iv. *Agreement on the European Economic Area*, OJ No L 1, 3.1.1994, p. 3; and EFTA States' official gazettes

v. Behrman, Greg, *The Most Noble Adventure: The Marshall Plan and the Time When America Helped Save Europe*, Simon & Schuster, 2007

vi. Berger, R., *FinTechs in Europe – Challenger and Partner*, Roland Berger Study (with Belgian key points), November 2016, page 2(4)

vii. Boden, A., Hipperson, M., Sawyer, J., Williams-Gardener, S., McParlane, T., *Explaining PSD2 without TLAs is tough!*, white paper, Starling Bank, 2015

viii. Bordo, M.D., Eichengreen, B., *A Retrospective on the Bretton Woods System: Lessons for International Monetary Reform*, University of Chicago Press, p. 461-494, January 1993

ix. Boudewijn, G., *PSD2 : Almost final – a state of play*, European Council Blog and Discussion Board, 18 June 2015

x. Bradbury, D. (2011). *Hacking wifi the easy way*. Network Security, 2011(2), 9-12.

xi. Browning, D., & Kessler, G. C. (2009, January). *Bluetooth hacking: A case study*. In Proceedings of the Conference on Digital Forensics, Security and Law (p. 115). Association of Digital Forensics, Security and Law.

xii. *Charter of the Community* (Europe Declaration), signed at Paris, 18 April 1951

xiii. Communication from the Commission to the Council and the European Parliament *on a New Legal Framework for Payments in the Internal Market*, COM (2003) 718 of 2nd December 2003; 2. *New Legal Framework for Payments in the Internal Market - BEUC position on the Communication*, Bureau Européen des Unions de Consommateurs (BEUC), BEUC/065/2004, 15 February 2004

xiv. Communication from the Commission: *Single Market Act: Twelve levers to boost growth and strengthen confidence: Working together to create new growth*; COM(2011)206/4

xv. Communication from the Commission: *Single Market Act II: Together for new growth*; COM/2012/0573

xvi. Consultation paper *on the Draft Guidelines on major incidents reporting under the Payment Services Directive 2*, European Banking Authority, EBA/CP/2016/23, 07 December 2016
xvii. Consultation paper *on the Draft Guidelines on the criteria on how to stipulate the minimum monetary amount of the professional indemnity insurance or other comparable guarantee under Article 5(4) of Directive (EU) 2015/2366*, European Banking Authority, EBA/CP/2016/12, version 2, 22 September 2016
xviii. Consultation paper *on the Draft Guidelines on the information to be provided for the authorisation as payment institutions and e-money institutions and for the registration as account information service providers,* European Banking Authority, EBA/CP/2016/18, 03 November 2016
xix. Consultation Paper *on the Draft Regulatory Technical Standards specifying the requirements on strong customer authentication and secure communication under PSD2*, European Banking Authority, EBA/CP/2016/11, 12 August 2016
xx. *Current EU Directives & Regulation*, Payment Talk, VeriFone, August 2015
xxi. Cyber Security Tip ST04-002, *Choosing and Protecting Passwords*, US CERT, 01 October 2016
xxii. Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015, *on payment services in the internal market*, *amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC,* Official Journal of the European Union, November 2015
xxiii. Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 *on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC,* Official Journal of the European Union, November 2007
xxiv. Discussion Paper *on future Draft Regulatory Technical Standards on strong customer authentication and secure communication under the revised Payment Services Directive (PSD2*), European Banking Authority, EBA/DP/2015/03, 8 December 2015
xxv. Dr. Cohen, B., *Bretton Woods System*, prepared for the Routledge Encyclopedia of International Political Economy
xxvi. Ducklin, P., *Anatomy of a password disaster – Adobe's giant-sized cryptographic blunder*, Naked Security by Sophos, www.nackedsecurity.sophos.com, 4 November 2013
xxvii. EBA final draft Regulatory Technical Standards *on the framework for cooperation and exchange of information between competent authorities for passport notifications under Directive (EU) 2015/2366*, European Banking Authority, EBA/RTS/2016/08, 14 December 2016
xxviii. EFTA Bulletin, EFTA Free Trade association, July-August 2006
xxix. Ekberg, J. E., Kostiainen, K., Asokan, N., *Trusted execution environments on mobile devices*. In Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security (pp. 1497-1498). ACM, November 2013
xxx. Ekberg, J. E., Kostiainen, K., Asokan, N., T*he Untapped Potential of Trusted Execution Environments on Mobile Devices*, IEEE Security & Privacy, July-Aug. 2014, Vol.12(4), pp.29-37
xxxi. Eichengreen, B., Braga de Macedo, J., *The European Payments Union: History and Implications for the Evolution of the International Financial Architecture. Fragility of the International Financial System - How can we prevent new crises in emerging markets*, 2001, pp. 25-42.
xxxii. European Bank Authority, *Upcoming EBA publications (June 2016 – September 2016),* Newsletter EBA Press, June 2016
xxxiii. European Central Bank, *Recommendation For The Security Of Mobile Payments* – Draft Document For Public Consultation, November 2013
xxxiv. Fenton, J., *Toward Better Password Requirements*, PasswordsCon address, Las Vegas, 2 August 2016
xxxv. *Final guidelines on the security of internet payments*, European Banking Authority, EBA/GL/2014/12_Rev1, 19 December 2014
xxxvi. Furth, J.H., *The European Monetary Agreement*, Board of Governors of the Federal Reserve System, 6 September 1955 (public as of 01 January 2009)
xxxvii. Goffinet, G., *EBA mandate on the RTS on strong customer authentication & secure communication – Status update*, EBA, European Payments Gateway Conference, Brussels, 9 June 2016
xxxviii. Grassi, P. A., Garcia, M.E. and Fenton, J., *Digital Identity Guidelines*, Draft NIST Special Publication 800-63-3, Computer Security, NIST, US Department of Commerce
xxxix. Gruhn, I. V.,*The Lomé Convention: Inching Toward Interdependence*, International Organization 30 (Spring 1976): 240–262.
xl. Gullberg, P., *Trusted Execution Environment – TrustZone and Mobile Security*, OWASP Götebrog: Security Tapas, 20 October 2015
xli. Henn, S., *Here's One Big Way Your Mobile Phone Could Be Open To Hackers*, NPR, Privacy & Security, 13 June 2014 (blog)
xlii. Herbert, C., Crain, T., Smith, C., *Low power apparatus for preventing loss of cell phone and other high value items*, Google Patents, 11 November 2010, [0005]
xliii. Heuser, B., O'Neill, R., *Securing Peace in Europe, 1945–62: Thoughts for the post-Cold War Era*, Palgrave MacMillan, 1992
xliv. Hoopes, T., Brinkley, D., *FDR And The Creation Of The U.N.*, Yale University Press, 27 March 1997

xlv. *Impact Assessment*, Commission Staff Working Document, European Commission, Vol. 1/2, SWD (2013), 24 July 2013
xlvi. ISO/IEC 19795 series 1-6, *Information technology – Biometric performance testing and reporting*, ISO, 2006 - 2012
xlvii. ISO/IEC 27001, *Information technology — Security techniques* — Information security management systems — Requirements, International Standards Organisation, September 2013.
xlviii. Jang, J.S. et al., *SeCRet : Secure Channel between Rich Execution Environment and Trusted Execution Environment*, NDSS, 2015
xlix. Kaplan, J.J., Schleiminger, G., *European Payments Union: Financial Diplomacy in the 1950s*. Oxford: Clarendon Press, 1989.
l. Kissel, R., *Glossary of Key Information Security Terms*, NISTIR 7298, Revision 2, NIST, US Department of Commerce, May 2013, page 17
li. Lycklama, D., *PSD2 'Access to account' (XS2A) – forcing a marriage between banks and Fintech, romance still to be discovered*, Interview, 24 June 2015
lii. *Making the best use of the flexibility within the existing rules of the Stability and Growth Pact*, Communication from the Commission to the European Parliament, the Council, the European Central Bank, the Economic and Social Committee, the Committee of the Regions and the European Investment Bank, European Commission, 13 January 2015
liii. Miller, S.P., Neuman, B.C., Schiller, J.I. and Saltzer, J.H., *Kerberos authentication and autorisation system*, Section E.2.1, Project Athena Technical Plan, 1987
liv. Mobile Connect fact sheet, GSMA, 15 June 2015
lv. Moussis, N., *Access to European Union: law, economics, policies*. The ultimate textbook on the European Union, 19th updated edition, Rixensart, 2011
lvi. Murdoch, S.J., presentation on Introduction to Trusted Execution Environments (TEE) – IY5606, Computer Laboratory, University of Cambridge
lvii. Neubauer, T. and Riedl, B., *Improving Patients Privacy with Peudonomisation*, Studies in health technology and informatics 136 (2008): 691, page 693 – figure 1
lviii. Office of Management and Budget, *E-Authentication Guidance for Federal Agencies*, Executive Office of the President, 16 December 2003
lix. *One currency for one Europe – The road to the Euro*, Economic and Financial Affairs, European Commission, Publications Office of the Eurpean Union, 2015
lx. *Payments regulatory timeline*, Payment Service Directive 2 (PSD2), Osborne Clark, February 2016
lxi. Paper *on the Strategies for Improving the U.S. Payment System*, United States Federal Reserve System, 16 January 2015
lxii. *Payments regulatory timeline*, Payment Service Directive 2 (PSD2), Osborne Clark, February 2016
lxiii. *Preparing for PSD2 : exploring the business and technology implications of the new payment services directive*, white paper, Finextra Research, March 2016
lxiv. Proposal for a Directive of the European Parliament and of the Council, *on payment services in the internal market and amending Directives 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC*, European Commission, COM(2013) 547, 24 July 2013
lxv. PSD2 Guidance – *Guidance for implementation of the revised Payment Service Directive*, European Banking Federation, September 2016
lxvi. PwC Financial Service Institute, *What are FinTechs ?,* Q&A PwCFinTech, April 2016
lxvii. Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 *on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data* (OJ L 8, 12 January 2001).
lxviii. Regulation (EU) No 2016/679 of the European Parliament and the Council of 27 April 2016 *on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation*), 4 May 2016 (Text with EEA relevance)
lxix. Regulation (EU) No 260/2012 of the European Parliament and of the Council of 14 March 2012 *establishing technical and business requirements for credit transfers and direct debits in euro and amending Regulation (EC) No 924/2009*
lxx. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 *on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC*, Official Journal of the European Union, 28 August 2014
lxxi. Report of the Monetary Committee *on the problem of the European Unit of Account*. II/703/74. Monetary Committee. Brussels: European Communities, 4 October 1974
lxxii. Rich, B., *Mortgaging the earth: The World Bank, environmental impoverishment, and the crisis of development*. Island Press, 2013.
lxxiii. Rohan, P., *PSD2 in Plain English (Payments Landscape for Non-Specialists)*, Vol. 1, 07 April 2016
lxxiv. S. Mansfield-Devine, *Open banking : opportunity and danger*, Computer Fraud & Security, October 2016.

lxxv. Sandhu, R., Hadley, J., Lovaas, S. and Takacs, N. (2012) *Identification and Authentication*, in Computer Security Handbook, Sixth Edition (eds S. Bosworth, M. E. Kabay and E. Whyne), John Wiley & Sons, Inc., Hoboken, NJ, USA. ch28
lxxvi. Schneier, B., *Choosing Secure Passwords*, blog, Schneier on Security, 03 March 2014
lxxvii. *Single European Act*, Official Journal of the Communities, L 169/1, 29 June 1987
lxxviii. Skinner, C., *The Future of Finance After SEPA*, The Wiley Finance Series, 2008
lxxix. *Special Drawing Rights (SDR)*, Fact sheet, IMF, 01 October 2016
lxxx. Stavins, J. & Schuh, S., *How Consumers Pay: Adoption and Use of Payments*, Working paper, Consumer Payments Research Center, Federal Reserve Bank of Boston, page 17, 12 December 2011
lxxxi. *Stockholm Convention*, Stockholm, 4 January 1960
lxxxii. *The end of the Bretton Woods system (1972-81*), IMF, imf.org
lxxxiii. *The euro*, ec.europa.eu, 2 November 2015
lxxxiv. *The Marshall Plan and the establishment of the OEEC*, CVCE, 08 July 2016
lxxxv. *The revised Payment Service Directive (EU) 2015/2366 – Objectives and Scope* (slide 7: 3 mandates EBA to ensure the establishment of adequate security measures for electronic payments – Focus RTS on Strong Customer Authentication), presentation of a not to be named Belgian financial institution to Febelfin, 15 November 2016.
lxxxvi. *The Schengen acquis - Agreement between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders,* Official Journal, L 239, 22 September 2000, P. 0013 - 0018
lxxxvii. *The Schuman Declaration of 9th May 1950*, Foundation Robert Schuman, European issue no.204, 10 May 2011
lxxxviii. *The Units of Account as a Factor of Integration*, Commission of the European Communities, 87/75
lxxxix. *Traité instituant la Communauté Européenne de Charbon et De l'Acier*, signé à Paris, 18 April 1951
xc. *Treaty establishing a Single Council and a Single Commission of the European Communities*, signed in Brussels, 8 April 1965
xci. *Treaty establishing the European Atomic Energy Community (Euratom Treaty)*, signed at Rome, 25 March 1957
xcii. *Treaty establishing the European Economic Community (EEC Treaty)*, signed at Rome, 25 March 1957
xciii. *Treaty of Alliance and Mutual Assistance (Treaty of Dunkirk),* signed at Dunkirk, 4 March 1947
xciv. *Treaty of Amsterdam amending the Treaty on the European Union, the Treaties establishing the European Communities and certain related acts*, Official Journal C 340 , 10/11/1997 P. 0001 - 0144
xcv. *Treaty of Economic, Social and Cultural Collaboration and Collective Self-Defense (Treaty of Brussels),* Brussels, 17 March 1948
xcvi. *Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community*, signed at Lisbon, 13 December 2007, Official Journal of the European Union, C 306, Vol. 50, 17 December 2007
xcvii. *Treaty of Nice amending the Treaty on European Union, the Treaties establishing the European Communities and certain related acts*, signed at Nice, 26 February 2001, Official Journal C 080, 10 March 2001, P. 0001 - 0087
xcviii. *Treaty on the European Union (Treaty of Maastricht),* Official Journal of the European Communities, C 191, Vol. 35, 29 July 1992
xcix. Ungerer, H., *A concise history of European monetary integration: From EPU to EMU*. Greenwood Publishing Group, 1997.
c. *Upcoming EBA publications (June 2016 – September 2016)*, European Bank Authority, Newsletter EBA Press, page 3, June 2016
ci. Ward, A. *The four types of payments*, in2payments.com, post, 08 March 2011
cii. *What is the euro area?,* ec.europa.eu, 11 November 2016.
ciii. Wong, L.W., *Potential Bluetooth Vulnerabilities in Smartphones*, School of Computer and Information Science, Edith Cowan University, 2005
civ. Woods, D., *Don't Get Ubered: APIs Hold Key To Digital Transformation*, Blog-post, Forbes Tech, 19 October 2015
cv. www.eba.europa.eu, consultation paper *on regulatory technical standards on strong customer authentication and secure communication under psd2*, regulation and policy, payment services and electronic money, regulatory activity
cvi. www.ec.europa.eu, *Trust Services and eID*, Digital Single Market, Digital Economy and Society, European Commission, 29 June 2016
cvii. www.enisa.europa.eu, Privacy by Design, Data Protection, ENISA Publications,
cviii. www.enisa.europa.eu, *Privacy enhancing technologies*, Data Protection, ENISA Publications,
cix. www.febelfin.be/nl/fintech-bedrijven-willen-samenwerken-met-financiele-instellingen
cx. www.globalplatform.org/mediaguidetee.asp
cxi. www.gsma.com/personaldata/mobile-connect
cxii. www.ideal.nl

cxiii. www.jupiner.net, *Reference: Nonprintable and Printable ASCII Characters*, TechLibrary, Jupiner Networks, 8 February 2011
cxiv. www.mint.com
cxv. www.mobileworldcongress.com, about the GSMA
cxvi. www.oneclickpay.be
cxvii. www.origins.osu.edu
cxviii. www.paypal.com
cxix. www.token.io/company

Addendum I – Nomenclature

Term	Definition	Existing brands/*potential new examples*
Access to Accounts (XS2A)	Access to Accounts (XS2A) basically entails that financial institutions but also non-financial market players may obtain access to the bank account of European consumers. These businesses would be positioned between the consumer and banks and are referred to as Third Party Payment Service Providers (see below).	n/a
Account Information Service Provider (AISP)	Any online provider that wishes to aggregate online information on one or more payment accounts held with one or more other payment service providers who typically present the information in a single dashboard for a customer.	Yodlee Money Dashboard Mint First Direct *Price comparison sites e.g Money Supermarket* *Banks e.g Starling*
Account Servicing Payment Service Provider (ASPSP)	All financial institutions that offer payment accounts (e.g. current accounts, credit cards) with online access (internet banking), and under this legislation will be obliged to open up an interface to allow authorised and registered third parties to initiate payments and access account information.	Banks e.g. HSBC, Santander Building Societies e.g Nationwide, Yorkshire BS
Card scheme	Card schemes are payment networks linked to payment cards, such as debit or credit cards, of which a bank or any other eligible financial institution can become a member.	MasterCard Visa AMEX
European Banking Authority (EBA)	The European Banking Authority (EBA) is a regulatory agency of the European Union headquartered in London, United Kingdom. Its activities include conducting stress tests on European banks to increase transparency in the European financial system and identifying weaknesses in banks' capital structures.	n/a
Merchant acquirer	An acquiring bank (or acquirer) is a bank or financial institution that processes credit or debit card payments on behalf of a merchant (e.g. retailer). The term acquirer indicates that the bank accepts or acquires credit card payments from the card-issuing banks within a card scheme.	WorldPay First Data Elavon

Open Application Programme Interface (API)	An API is a set of commands, functions, and protocols which programmers can use when building software for a specific operating system. The API allows programmers to use predefined functions to interact with the operating system, instead of writing them from scratch. An open API is an interface that has been designed to be easily accessible by the wider population of web and mobile developers. This means an open API may be used both by developers inside the organisation that published the API or by any developers outside that organisation who wish to register for access to the interface.	n/a
Payment Initiation Service Provider (PISP)	Any organisation (traditionally retailers, but could be utilities or any other category of business that takes online payments) that initiates a payment, needing a software bridge between the website of the merchant and the online banking platform of the payer's bank in order to initiate internet payments on the basis of a credit transfer.	*Amazon* *John Lewis* *British Gas*
Payment Institute	A category of payment service provider that came into being as a result of the enactment of the original Payment Services Directive (PSD1). They can offer their customers the following services: - Executing payment transactions (including credit transfers, direct debits, through payment cards or a similar device); - Issuing and/or acquiring of payment instruments; - Money remittance; - Foreign exchange services; - Ancillary services; - Credit can be granted for a maximum of 12 months if this credit is closely linked to a payment service provided.	PayPal First Data WorldPay VocaLink ConCardis BVZI
Payment Services Directives 1 & 2 (PSD1 & PSD2)	Two pieces of legislation handed down from the European Parliament and the council of the European Union. These directives provide the legal foundation for the initial creation and subsequent widening of scope, of an EU wide, single market for payments.	n/a
Regulatory Technical Standards (RTS)	A set of detailed compliance standards that will be set for all parties to meet covering things such as data security, who is accountable if something goes wrong, and what is the compensation process.	n/a
Single Euro Payments Area (SEPA)	SEPA is a payment-integration initiative of the European Union with the objective to simplify bank transfers denominated in Euro. As of 2015, SEPA consists of the 28 member states of the European Union, the four member states of the European Free Trade Association (Iceland, Liechtenstein, Norway and Switzerland), Monaco and San Marino. Andorra will become part of the area in 2016.	n/a
Third Party Payment Service Providers	In this context, the third party payment service providers are the AISPs and PISPs that are the third parties alongside the banks and the customer in the payment process.	As above

Addendum 2 – List of respondents (disclosure enabled)

1	AB SEB bankas	74	Intesa Sanpaolo S.p.A.
2	ABN AMRO Bank N.V.	75	Intive
3	Accenture	76	Intuit, Inc.
4	Adyen	77	iSignthis
5	AFEPAME	78	ITALIAN BANKING ASSOCIATION
6	AFTE - French association of corporate treasurers	79	JACCOO
7	Air Bank a.s.	80	Payments UK, Financial Fraud Action UK and The UK Cards Association
8	American Express	81	Klarna AB (Sofort)
9	ASF	82	KOBIL Systems
10	Association of Consumer Credit Information Suppliers (ACCIS)	83	Kontomierz.pl Sp. z o.o. (Kontomatik)
11	Association of Credit Card Issuers Europe (ACCIE)	84	Korala Associates Limited (KAL)
12	Association of Foreign Banks in Germany	85	LSc LifeScience Consult GmbH
13	Austrian Federal Economic Chamber, Division Bank and Insurance	86	Lufthansa AirPlus Servicekarten GmbH
14	Avanza Bank AB	87	Luxembourg Government IT Center
15	Bank of Cyprus	88	MAIF
16	Banking & Payments Federation Ireland	89	MIDAS Alliance
17	Banking Stakeholder Group	90	Ministry of Finance of the Slovak Republic
18	BEUC, The European Consumer Organisation	91	Ministry of Industry
19	bevh - German Distance Sellers Association	92	Mobysign
20	Bitkom e.V.	93	Mooverang
21	British Retail Consortium	94	MRC Fraud & Payments EU Ltd.
22	Callcredit Information Group	95	MYPINPAD LTD
23	Citibank Europe plc	96	Nets A/S
24	Crédit Agricole S.A.	97	Norwegian University of Science and Technology (NTNU)
25	crown holdings	98	Notakey
26	Currence iDEAL B.V.	99	NTT DATA
27	CyberSource Ltd	100	OP Financial Group
28	DeBarra Innovations Limited	101	Optima Consultancy
29	Deutsche Bank AG	102	PAN-Nordic Card Association
30	Dutch Payments Association	103	paydirekt GmbH
31	Ecommerce Europe	104	PayPal
32	Electronic Money Association	105	PaySquare SE
33	EMOTA European eCommerce and Omni Channel Trade Association	106	Polski Standard Płątności sp.
34	EMVCo LLC (Europay, Mastercard and Visa)	107	Portuguese Banking Association (APB)
35	EPSM - European Association of Payment Service Providers for Merchants	108	Prudentiz
36	ESBG	109	Quali-Sign Ltd
37	Eurobits Technologies	110	Rabobank
38	EuroCommerce	111	Raiffeisenbank a.s., Czech Republic
39	European Association of Co-operative Banks	112	Romanian Banking Association
40	European Banking Federation	113	RSA
41	European Cards Stakeholders Group	114	SAS NUMERICOMPTA
42	European Financial Congress	115	SlimPay
43	European Payment Institutions Federation	116	Slovak Banking Association
44	European Payments Council (EPC)	117	Slovenská sporiteľňa, a.s.
45	EUROSMART	118	Societe Generale Group
46	Febelfin	119	SPA
47	Federal Office for Information Security (Germany)	120	Svensk Handel
48	FEDMA	121	Swedish Bankers' Association
49	FIDO Alliance (Fast Identity Oline)	122	The Association of Foreign Exchange and Payment Companies
50	figo GmbH	123	The Bank Association of Slovenia
51	Finance Norway	124	The Danish Bankers Association
52	Financial Data and Technology Association	125	The European Card Payment Association
53	Finect	126	The Federation of Finnish Financial Services
54	Finical API Working Group - Open ID Foundation	127	The German Federal Association of Payment Institutions (BVZI)
55	Finnish Federation for Telecommunications and Teleinformatics, FiCom	128	The Ministry of Finance of the Czech Republic
56	Fintonic Servicios Fincieros, SL's	129	The Royal Bank of Scotland plc
57	French Banking Federeration	130	Tink AB
58	FUGAM	131	Token
59	Galitt	132	Transpact.com
60	Gemalto	133	Trustonic
61	German Banking Industry Committee (GBIC)	134	UL TS BV
62	GLEIF	135	UniCredit
63	Government Digital Service, UK Cabinet Office	136	University College London
64	Groupement des Cartes Bancaires CB	137	van den Berg AG
65	GSMA	138	VASCO Data Security
66	IBM	139	Vendorcom
67	Icon Solutions Ltd	140	Federation of German Consumer Organisations
68	IdenTrust	141	Visa Europe
69	IKEA Group	142	VocaLink
70	Informed Risk Decisions Ltd	143	Vodafone Group PLC
71	ING Bank NV	144	worldline
72	Intercede Ltd.	145	Yodlee, Inc.
73	Interessengemeinschaft Kreditkartengeschäft	146	Związek Banków Polskich (Polish Bank Association)

Addendum 3 – Evolution of the European landscape after 1945

In the aftermath of World War II, Europe was facing three challenges: ensuring (together with its allies) a long lasting peace, rebuilding its continent and undertaking the integration of its economy[132]. The first challenge was answered – amongst others – by the endorsement of the U.N. Charter establishing the United Nations organization in October 1945[133] and, specifically for European countries, the adoption of the Treaty of Brussels in March 1948[134] by France, the United Kingdom, Belgium, Luxemburg and The Netherlands, which tended to improve the mutual defense pledge signed between France and the United Kingdom in the Treaty of Dunkirk in 1947[135]. Eventually, the Treaty of Brussels led to the creation of the Western European Union in 1954. The second and third challenges took longer to shape, some European leaders willing to 'upgrade' the continent towards one integrated European economy, with a harmonized European market enabled by free circulation.

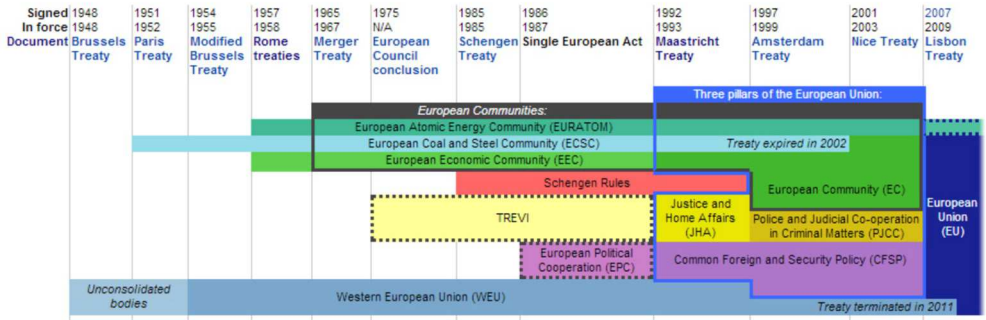

Figure 7 - Timeline of the creation of the European Union[136]

A. Shaping one Single European market

The Organisation for European Economic Cooperation

In April 1948, the Organisation for European Economic Cooperation[137] (OEEC) was established in order to formalize the economic help of the United States and Canada – in the framework of the Marshall Plan[138], – for the reconstruction of Western Europe after World War II. The Marshall Plan, seen by the US as a device for fostering the integration of Europe with a funding reaching eventually thirteen billion dollars until it stopped in 1952, was to be implemented only if strict – US – conditions were met: the dismantling of intra-European trade restrictions, a central coordination of national recovery plans and a reviewed agreement on how to allocate payments from a recipient perspective. The OEEC's role was to supervise the implementation of the Plan and to ensure that each participating country complied with the strict conditions. The OEEC translated these conditions into a set of working principles[139], such as the promotion of cooperation between participating countries and their national production programs for the reconstruction of Europe, the development of intra-European trade by reducing tariffs and other barriers to the expansion of trade, and the study of the feasibility of creating a customs union or free trade area – which can be seen as the premises for the foundation of the modern European Union –. The OEEC, originally composed of eighteen participants[140], was renamed

[132] *The Schuman Declaration of 9th May 1950*, Foundation Robert Schuman, European issue no.204, 10 May 2011
[133] Hoopes, T., Brinkley, D., *FDR And The Creation Of The U.N.*, Yale University Press, 27 March 1997
[134] *Treaty of Economic, Social and Cultural Collaboration and Collective Self-Defense* (Treaty of Brussels), Brussels, 17 March 1948
[135] *Treaty of Alliance and Mutual Assistance* (Treaty of Dunkirk), signed at Dunkirk, 4 March 1947
[136] Source: origins.osu.edu
[137] Ungerer, H., *A concise history of European monetary integration: From EPU to EMU*. Greenwood Publishing Group, 1997.
[138] Behrman, Greg, *The Most Noble Adventure: The Marshall Plan and the Time When America Helped Save Europe*, Simon & Schuster, 2007
[139] Heuser, B., O'Neill, R., *Securing Peace in Europe, 1945–62: Thoughts for the post-Cold War Era*, Palgrave MacMillan, 1992
[140] *The Marshall Plan and the establishment of the OEEC,* CVCE, 08 July 2016

the Organisation for Economic Cooperation and Development (OECD) in 1961, a worldwide body counting thirty-five members today.

European Communities/ European Union

In the wake of the US conditions to the implementation of the Plan Marshall and to comply with one of the OEEC principle, a French Foreign Minister named Robert Schuman proposed in May 1950 to bring the Franco-German coal and steel production under the authority of a community of European countries that would be willing to participate[141]. The proposal was either economical – coal and steel being the basis of the industry and power of the two countries – and political – to further reinforce Franco-German solidarity (while the world was still mostly associating the 'Germans' to the atrocities 'they' committed during a war 'they' started) and to set the premises for European integration –. This text is considered to be the starting point of the European Union, as it led to the adoption in 1951 of the Treaty of Paris[142] by six countries – France, West-Germany, Italy, Belgium, Luxemburg and The Netherlands, known as the 'inner six' –. This Treaty established the European Coal and Steel Community (ECSC), which goal was to create a common market for coal and steel – by means of free movement of coal and steel and free access to sources of production – contributing to economic expansion, employment generation and a better living standard. During the signing of the Treaty of Paris, the six countries also adopted the Europe Declaration[143] – known as the Charter of the Community –. The Declaration recognized the creation of the ECSC as the birth of Europe as a political, economic and social entity, '*open to all European countries that have freedom of choice'* whether to participate or not.

The signing of the Treaty of Rome[144] in 1957 by the 'inner six' led to the creation of the European Economic Community (EEC), aiming at a common European market and customs union – a European free trade area with a common tariff for its member states –. The very same day, the six countries also ratified the Euratom Treaty[145], creating the European Atomic Energy Community (EAEC or Euratom), founded with the aim to develop and distribute nuclear energy to its member states and selling the surplus to non-member states. The ECSC, EEC and Euratom formed the European Communities (EC) and share the same members (if a country became member of one community, it became automatically also member of the two others). The adoption of the Merger Treaty[146] in 1965 allowed the aggregation of the ECSC, EEC and Euratom into one single institutional structure, proclaiming the Commission of the EEC and the Council of the EEC as the sole governing body for all three communities, although each community remained legally independent.

The 'inner six' remained the sole members of the EC until 1973, when the United Kingdom and Denmark left the European Free Trade Association (see later in this chapter) to become members of the European Communities, together with Ireland. Greece became the tenth member in 1981, Spain and Portugal followed suit in 1986, year when the Single European Act[147] (SEA) – a major revision of the Treaty of Rome – was signed by the EC, setting as objective the establishment of a European Single Market by the dawn of 1993. Since 1987, Turkey is applying for membership but has yet to fulfil the needed requirements[148]. In 1989, the Berlin

[141] *The Schuman Declaration of 9th May 1950*, Foundation Robert Schuman, European issue no.204, 10 May 2011
[142] *Traité instituant la Communauté Européenne de Charbon et De l'Acier*, signé à Paris, 18 April 1951
[143] *Charter of the Community (Europe Declaration),* signed at Paris, 18 April 1951
[144] Treaty establishing the European Economic Community (EEC Treaty), signed at Rome, 25 March 1957
[145] *Treaty establishing the European Atomic Energy Community* (Euratom Treaty), signed at Rome, 25 March 1957
[146] *Treaty establishing a Single Council and a Single Commission of the European Communities*, signed in Brussels, 8 April 1965
[147] *Single European Act*, Official Journal of the Communities, L 169/1, 29 June 1987
[148] Accession criteria (Copenhagen criteria), Treaty on European Union, Articles 6(1) and 49, established by the Copenhagen European Council (1993) and strengthened by the Madrid European Council (1995)

Wall fell, along with the Iron curtain, opening the door for Eastern European countries to apply for membership if meeting the Copenhagen criteria[149].

In 1985, the Schengen Agreement[150] was signed by five of the – then – ten member states of the EU – France, Belgium, Luxemburg, The Netherlands and West Germany –, aiming at abolishing internal border checks and harmonizing visa policies, thus allowing their citizens to travel between the countries without any passport control at the frontiers. Supplemented by the Schengen Convention in 1990, the Agreement was only enforced first in 1995 by seven countries – France, reunified Germany, Belgium, Luxemburg, The Netherlands, Portugal and Spain – and in 1997 by the remaining member states of the EU – except the United Kingdom and Ireland –, when they all signed the Agreement during the Amsterdam Intergovernmental Conference, which eventually led to adoption of the Treaty of Amsterdam (see below) and the incorporation of the Schengen Agreement into the European Union law.

In 1992, the Treaty of Maastricht[151] was signed by all member states of the European Communities. The treaty was a major milestone, setting clear rules for five key goals: strengthening the democratic legitimacy of the institutions, improving the effectiveness of these institutions, developing the Community social dimension, establishing an economic and monetary union – leading to the creation of the Euro as single European currency – and establishing a common foreign and security policy. The purpose was mostly to prepare for European Monetary Union and to introduce elements of a political union – e.g. European citizenship –, by establishing the European Union, introducing co-decision procedure, giving the European Parliament more decision-making power, fostering new forms of cooperation between EU-governments – e.g. defense and justice affairs – and implementing a standardized system of laws that apply in all member states.
In the Treaty of Maastricht, the member states agreed to rename The European Economic Community as the European Community (EC) – renaming its founding treaty as the Treaty establishing the European Community (TEC) – while the European Communities (consisting of the ECSC, EEC and Euratom) became the European Union (EU), with the newly formed European Community as most constituent part and the ECSC and Euratom as subordinate parts.

In 1993, the integrated, single European Single Market (or Internal market) was established – objective set in the SEA of 1986 –, along with four freedoms: the free movement of goods, services, people and capital. Many laws have been agreed upon since – e.g. tax policy and business regulation – to remove barriers and open the frontiers. In 2011 and 2012, the European Commission adopted the Single Market Act I[152] and the Single Market Act II[153], a series of measures to address the missing legislation, administrative obstacles and lack of enforcement preventing the full exploitation of the European Single Market opportunities, with as goal to give a fresh impetus to the internal market.

[149] *20 Years That Changed Europe - The Copenhagen Criteria and the Enlargement of the European Union, Conference Report*, Copenhagen, 14 May 2013
[150] *The Schengen acquis* - Agreement between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders Official Journal, L 239, 22 September 2000, P. 0013 - 0018
[151] *Treaty on the European Union* (Treaty of Maastricht), Official Journal of the European Communities, C 191, Vol. 35, 29 July 1992
[152] Communication from the Commission: *Single Market Act: Twelve levers to boost growth and strengthen confidence: Working together to create new growth*; COM(2011)206/4
[153] Communication from the Commission: Single Market Act II: Together for new growth; COM/2012/0573

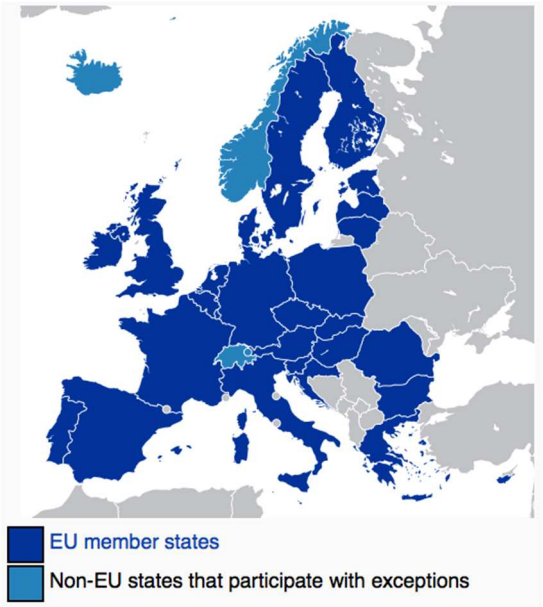

Figure 8 - European Single Market (or Internal Market) as of 1993 (SEA requirement)

In 1995, Austria and Sweden left the European Free Trade Association (EFTA, see below) to become member state of the EU, together with Finland.
In 1997, all EU member states ratified the Treaty of Amsterdam[154], agreeing to reform the EU institutions – e.g. devolvement of certain national government powers to the European Parliament –, to give Europe a stronger international voice and to invest in employment and the rights of citizens. Negotiations started with ten countries of Central and Eastern Europe, which expressed their desire to become member states of the EU after the fall of the Iron Curtain. They would eventually become EU-members. In 2001, the EU member states adopted the Treaty of Nice[155], which purpose was to agree to reform further the EU institutions – methods for changing the composition of the Commission and redefining the voting system of in the European Council – to ensure efficient functioning of the EU after reaching 25 member states.

In 2007, the EU member states signed the Treaty of Lisbon[156], approving a.o. to give more powers to the European Parliament and to appoint a permanent president of the European Council with the goal to make the EU more democratic and more efficient and able to address global problems such as climate change. While making the Union's bill of rights – the Charter of Fundamental Rights – legally binding, the Treaty also gave member states the explicit legal right and the related procedures to leave the EU – right used by the United Kingdom in 2016 after a national referendum favoured a 'Brexit' – or rejoin it. The Treaty of Lisbon also saw the Treaty establishing the European Community (TEC) being renamed as the Treaty on the Functioning of the European Union (TFEU), resulting in the merging of the two remaining communities (EC and Euratom) into the reformed European Union. The ECSC had already ceased to exist in 2002, when its founding treaty expired. The EC was dissolved in the EU, Euratom remained as a distinct entity, governed by the European Union institutions.
Today, the European Union is composed of 28 member states and 510 million inhabitants.

[154] *Treaty of Amsterdam amending the Treaty on the European Union, the Treaties establishing the European Communities and certain related acts*, Official Journal C 340 , 10/11/1997 P. 0001 - 0144
[155] *Treaty of Nice amending the Treaty on European Union, the Treaties establishing the European Communities and certain related acts*, signed at Nice, 26 February 2001, Official Journal C 080, 10 March 2001, P. 0001 - 0087
[156] *Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community*, signed at Lisbon, 13 December 2007, Official Journal of the European Union, C 306, Vol. 50, 17 December 2007

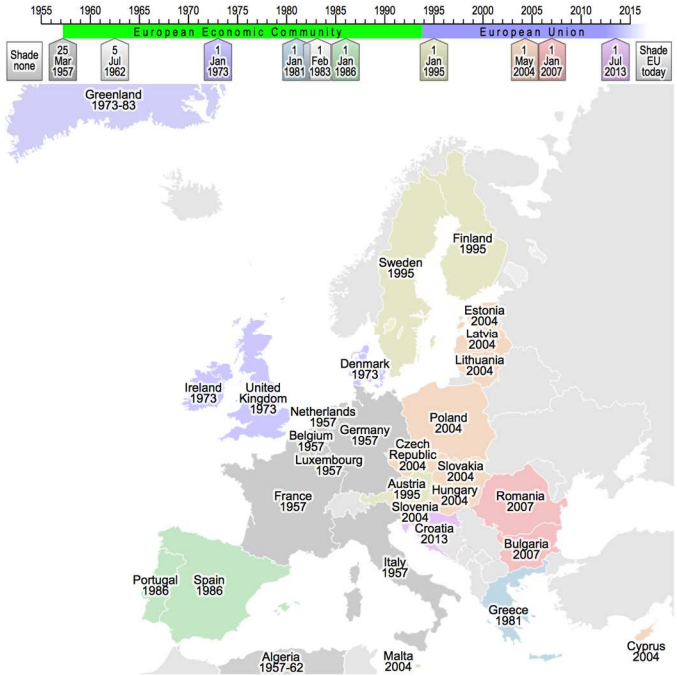

Figure 9 - Timeline of countries becoming member states of the European Union

European Free Trade Association

In 1960, seven European countries unable or unwilling to join the European Economic Community – Norway, Switzerland, Austria, Denmark, Portugal, Sweden and the United Kingdom, known as the 'outer seven' as opposed to the 'inner six' that created the EU – founded the European Free Trade Association[157] (EFTA) by signing the Stockholm Convention, based on the premise of free trade among its member states to achieve the very same goals as the ECSC. In 1967, full free trade in industrial products was achieved within the EFTA; ten years later, full free trade was achieved with the EEC member states. In 2006, EFTA was covering 50 countries and territories, servicing 850 million inhabitants on four continents[158]. Today, only Switzerland and Norway remain as founding members, plus Liechtenstein and Iceland. The organization is operating in parallel with the European Union, participating to the European Single Market – through the European Economic Area Agreement (EEA, see below) – without being member state.

European Economic Area

In 1994, the European Economic Area[159] (EEA) was created as an agreement in response to the establishment of the European Single Market (ESM) – or Internal Market –, guaranteeing the EFTA member states (non-EU) willing to use the EU Internal Market free movement of goods, services, people and capital – the same conditions as for EU member states –. Today, twenty-eight EU members and three of the four EFTA members constitute the EEA. The fourth EFTA member – Switzerland –, although not part of the EEA, is allowed to participate to the Internal Market through a series of bilateral agreements with the European Union.

[157] *Stockholm Convention*, Stockholm, 4 January 1960
[158] EFTA Bulletin, EFTA Free Trade association, July-August 2006
[159] *Agreement on the European Economic Area*, OJ No L 1, 3.1.1994, p. 3; and EFTA States' official gazettes

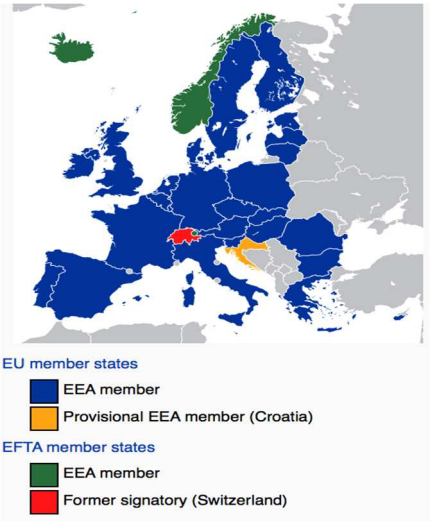

Figure 10 – The European Economic Area in 2016

B. Shaping one Monetary and Payment Union

Gold parity of account

Since the mid-1940s, the rules for commercial and financial transactions between Western Europe, the United States, Canada, Australia and Japan were set out by the Bretton Woods system[160], the first monetary system aiming at governing the monetary relations among the nation-states having negotiated the system. Participating countries were obliged to comply with the Bretton Woods system's monetary policy by coupling their currency to gold – called the gold parity unit of account – which was itself valued against the US dollar, as the United States were controlling two thirds of the world's gold reserve. As of then, gold was used as a unit of account to value goods and services and to record debts. Tying gold to the dollar currency meant that values of these goods, services and record debts were priced or expressed in dollars[161], also in Europe.

With the intend to rebuild the international economic system damaged by World War II, dozens of allied nations signed the Bretton Woods agreement in July 1944, committing to comply to the strongly US-derived Bretton Woods rules. The agreement created at the same time the International Monetary Fund (IMF) – a supervisory body which goal was to bridge eventual temporary imbalances of payments of a participating nation-state – and the International Bank for Reconstruction and Development (IBRD) – which goal was to provide loans to developing countries –. Today, both are part of the World Bank Group, the world's largest and most famous development bank[162].
The European Coal and Steel Community (ECSC) started to use the gold parity unit of account upon its creation in 1958, the European Economic Community following suit in 1962, until the Bretton Woods system collapsed in the early 1970s[163], due to the increase of the United States' domestic – e.g. US Great Society programs – and military – e.g. the Vietnam war – spending in the 1960s, which caused an overvaluation of the dollar, leading to the suspension of the US

[160] Dr. Cohen, B. *Bretton Woods System*, prepared for the Routledge Encyclopedia of International Political Economy
[161] Ungerer, H., *A concise history of European monetary integration: From EPU to EMU*. Greenwood Publishing Group, 1997.
[162] Rich, B., *Mortgaging the earth: The World Bank, environmental impoverishment, and the crisis of development*. Island Press, 2013.
[163] *The end of the Bretton Woods system* (1972-81), IMF, imf.org

currency's convertibility into gold. Since then, major currencies have never again been coupled to gold, floating instead against each other[164].

The European Payments Union

Shortly after the end of World War II, Europe was facing an economic depression. Bilateral payments agreements were signed between European countries to foster intra-European trade. Trade and payments could only be made in US dollars – the only acceptable reserve currency at the time –. As many of the European countries were in full recovery, they lacked US dollar reserves to pay for the import of goods from either other European countries or the United States. At one point, many intra- or extra-European transactions occurred through barter – meaning that goods were exchanged against other goods. European countries needed to answer strict requirements if they were to receive US funding through the Marshall Plan[165], such as enforcing stability-oriented policies – e.g. currency convertibility –.

Created in September 1950 by the Organisation for European Economic Cooperation members, the European Payments Union (EPU) was a peer pressure instrument used by the OEEC – and the US – to multilateralize the bilateral agreements upon which intra-European trade was occurring shortly after the war[166]. All participating countries needed to abide by the EPU code of conduct. The EPU acted as a clearing union that replaced the bilateral (direct) payment agreements by multilateral, (monthly) settlement – introducing also loans as a financing mechanism –, the whole aimed at improving the payment landscape in order to ensure a sustainable liberalization of trade[167]. Among the intended improvements, transferability and convertibility of European currencies – as stability policies – were key objectives. The transferability issue was tackled when the EPU introduced a unit of account as a way to express a transaction, based on gold and the US dollar – the gold parity of account –. The measure proved highly effective, as European US dollar reserves started to increase – also helped by the Marshall Plan funding, as Europe was meeting the US requirements –, bringing the financing of intra-European payments back in balance all the way until December 1958, when article 8 of the IMF Articles of Agreements was signed by the majority of the EPU members. This article introduced external convertibility – the ease with which a country's currency can be converted into gold or another currency – of the members' currencies, answering the second objective of the EPU. With the restoration of currency transferability and convertibility, the EPU had no reason to linger. Although full convertibility would not be achieved until the 1980s, the EPU was dissolved at the end of 1958.

The European Monetary Agreement

In August 1955, OEEC members signed the European Monetary Agreement (EMA)[168] to put in place a structural multilateral settlement system – introduced by the EPU – and to establish a European Fund, in order to maintain a high level of stable trade and liberalization between the OEEC members. The Fund aimed at granting the OEEC members loans – repayable within two years – in order for them to withstand temporary balance and payment difficulties. The EMA was the successor of the EPU and lasted until 1972, when its objectives were taken over by the International Monetary Fund (IMF).

---

[164] Bordo, M.D., Eichengreen, B., *A Retrospective on the Bretton Woods System: Lessons for International Monetary Reform*, University of Chicago Press, p. 461-494, January 1993

[165] Kaplan, J.J., Schleiminger, G., *European Payments Union: Financial Diplomacy in the 1950s*. Oxford: Clarendon Press, 1989.

[166] Eichengreen, B., Braga de Macedo, J., *The European Payments Union: History and Implications for the Evolution of the International Financial Architecture.* Fragility of the International Financial System – How can we prevent new crises in emerging markets, 2001, pp. 25-42.

[167] Ungerer, H., *A concise history of European monetary integration: From EPU to EMU*. Greenwood Publishing Group

[168] Furth, J.H., *The European Monetary Agreement*, Board of Governors of the Federal Reserve System, 6 September 1955 (public as of 01 January 2009)

Special Drawing Rights

In the late 1960s, the Bretton Woods – fixed exchange rate – system became unstable, as the conservative monetary policy of the US – due to the increase in US domestic and military spending – could no longer guarantee sufficient international supply of the two preferred foreign exchange reserves – gold and the US dollar – to support the expansion of the worldwide trade. For this reason, the IMF-members created in 1969 a new, supplementary international exchange reserve, called the Special Drawing Rights (SDR or XDR)[169], which value was not coupled to one currency but to a basket of five international currencies with adjusted weights – depending on the currency prominence with regard to international trade and national foreign exchange reserves –, reviewed by IMF every five years. This proved highly effective when the Bretton Woods system collapsed in 1973 – a few year after the SDR creation –, moving the major international currencies from a fixed exchange rate system towards mere floating exchange rate regimes. The SDR, still used today, are not a currency but form a unit of account, allocated to the IMF members essentially when the US dollar comes under pressure.

European Unit of Account

After the fall of the Bretton Woods system and the abandonment of its coupled gold parity unit of account, a growing amount of units of accounts were used in Europe for different purposes. In 1975, the European Communities decided to leverage on the IMF's work and created the European Unit Account[170] (EUA), linked to more stable SDR. The EUA used the same mechanism as the SDR did, but at European level, being a basket of European currencies aiming at easing the trade between the European Union and other continents[171]. First used only by the European Economic Community and seventy-one Third World nations – from the African, Caribbean and Pacific (ACP) countries – within the framework of the Lomé Convention[172] – the EUA was later also introduced to the two other communities until March 1979, when the European Currency Unit (ECU) replaced it.

European Currency Unit

In March 1979, the European Economic Community (EEC) took a series of measures to further foster monetary and political stability and paved the way for a common European currency. The European Monetary System (EMS) was established as an arrangement between – in a first stage – eight European member states of the EEC who linked their currencies to reduce exchange rate variability among the EMS countries. While the EMS countries' currencies were floating against other currencies, the newly introduced European Exchange Rate Mechanism (ERM) acted as a pegged exchange rate system – a combination of variable currency exchange rates within fixed currency exchange rate margins – for the EMS countries' currencies, forcing the changes in EMS currencies to be within an interval of +/– 2.25 percent. The aim of ERM was to minimize the fluctuation between member states' currencies and the European Currency Unit (ECU)[173], a newly introduced unit of account – as a replacement of the EUA – to which EEC member states' currency were linked. Although used in some international financial transactions, the ECU was not seen as a currency, as member states inhabitants could not used it. The ECU would be replaced by the Euro as a true European currency in 1999.

---

[169] *Special Drawing Rights (SDR),* Fact sheet, IMF, 01 October 2016

[170] *Report of the Monetary Committee on the problem of the European Unit of Account*. II/703/74. Monetary Committee. Brussels: European Communities, 4 October 1974

[171] *The Units of Account as a Factor of Integration*, Commission of the European Communities, 87/75

[172] Gruhn, I. V.,*The Lomé Convention: Inching Toward Interdependence*, International Organization 30 (Spring 1976): 240–262.

[173] Ungerer, H., *A concise history of European monetary integration: From EPU to EMU*. Greenwood Publishing Group

The European Monetary Union

To further integrate the different European countries into one full economic unity, The European Monetary Union (EMU) program[174] was launched in 1989 and would eventually consist of three stages[175]: stage 1 (1990) focused on completing the internal market – the European Single Market was came to full life in 1993 – and removing restrictions to allow further financial integration, ensuring complete freedom for capital transactions, an increased cooperation between the different central banks, free use of the European Currency Unit (ECU, the forerunner of the Euro) and improvement of the economic convergence between the member states – mandatory criteria for member states stated in the Treaty of the European Union (Maastricht) seeking to use the single currency; stage 2 (1994) established the European Monetary Institute, to strengthen further the cooperation between the European central banks and prepare for the European System of Central Banks (ESCB), increase the coordination of monetary policies and prepared for the transition to the Euro as one European single currency in 1999; stage 3 (1999) definitively fixed the exchange rates for conversion between the different European currencies and the newly adopted Euro, set a.o. the responsibility of independent single monetary policy-making at the European Central Bank (ECB) and ESCB and enforced the Stability and Growth Pact[176], a set of rules designed to ensure that countries in the European Union pursue sound public finances and coordinate their fiscal policies.

Where the U.S. had encouraged acceptance of the EPU code of conduct through a system of rewards and sanctions administered by the OEEC, the success of EMU depended (and still depends) on the members of the EU alone.

The Euro: a single currency as a complement to a single market

In 1999, the Euro (€) was introduced as a replacement of the ECU and came into full force in 2002 in twelve EU countries[177]. The euro is introduced in eleven countries (joined by Greece in 2001) for commercial and financial transactions only. Notes and coins came only in 2002. The Euro allowed a.o. a cost reduction for travellers – no need for currency exchange (and related transaction costs) anymore when travelling in a Euro Area country – and price comparison and transparency between countries – increasing competition between suppliers, one eternal goal of the EU –.

To date, nineteen of the twenty-eight EU member states are using the Euro as their currency, forming the Euro area. The remaining nine members have kept their own national currencies, but trades with the Euro area occur in Euro. Also non EU-members, such as Montenegro and Kosovo, are using the Euro as national currency. In 2015, the Euro was used daily by some 337 million Europeans[178], exchanging over 15.7 billion euro banknotes with a value of over €930 billion.

[174] Eichengreen, B., Braga de Macedo, J., *The European Payments Union: History and Implications for the Evolution of the International Financial Architecture*. Fragility of the International Financial System – How can we prevent new crises in emerging markets, 2001, pp. 25-42.
[175] *One currency for one Europe – The road to the Euro*, Economic and Financial Affairs, European Commission, Publications Office of the Eurpean Union, 2015
[176] *Making the best use of the flexibility within the existing rules of the Stability and Growth Pact*, Communication from the Commission to the European Parliament, the Council, the European Central Bank, the Economic and Social Committee, the Committee of the Regions and the European Investment Bank, European Commission, 13 January 2015
[177] *What is the euro area?*, ec.europa.eu, 11 November 2016.
[178] *The euro*, ec.europa.eu, 2 November 2015

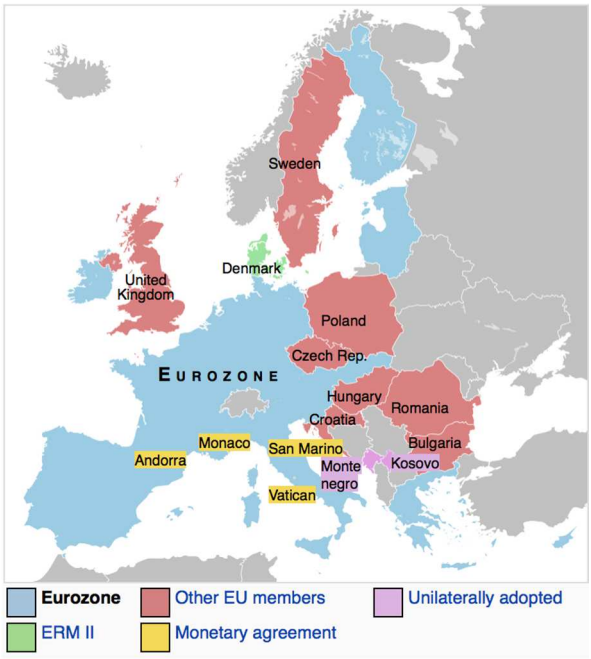

Figure 11 – The Euro area

Starting with the reconstruction of its continent and its economy after the chaos of World War II, Europe has spent more than seventy years signing many treaties to ensure an efficient integration of the European countries in a harmonized European landscape. The creation of the European Communities (1950-1967), as forerunners of the European Union, was a first step, followed by the European Single Market – or internal market – in 1993 and the introduction of the Euro as a single currency in 1999. The single market allowed – and still does – a.o. free circulation of goods, capital, services and people. The Euro as a single currency removed in a very first stage the need for currency exchange – and the costs linked to the transaction – and has gradually allowed an increased competition in different sectors, as prices could now be easily compared and payment methods standardized everywhere within EU. The fostering of competition is essential for the maintenance of the single market and forms as a result one of the most important European Union's flagship[179]. Therefore, many regulative adaptations have taken place since the introduction of the single market and the single currency, to ensure that competition on *equal terms* is possible on the markets of all EU member states. The Directive on Payment Services (PSD) I and II are such adaptations that seek to increase the competition within the financial sector, opening the Payment services market for other entities than banks.

[179] Moussis, N., *Access to European Union: law, economics, policies*. The ultimate textbook on the European Union, 19th updated edition, Rixensart, 2011