Strong Authentication for e-Banking: A Survey on European Regulations and Implementations

Federico Sinigaglia[1,2], Roberto Carbone[1] and Gabriele Costa[2]

[1]*Security & Trust Unit, FBK-Irst, Trento, Italy*

[2]*DIBRIS, University of Genova, Genova, Italy*

Keywords: Strong Authentication, e-Banking, Internet Payments, Mobile Payments.

Abstract: The modern, smart society needs a reliable and trustworthy access to the internet of services. *Strong authentication* mechanisms promise to rise the bar of security and they are polarizing the attention of both institutional and industrial stakeholders. In this survey, we take stock of the strong authentication mechanisms used by e-Banking services in terms of regulations and implementations. To this aim, we reviewed the EU regulations and their evolution in the last decade and we analyzed the strong authentication mechanisms implemented by 26 major EU and non-EU banks.

1 INTRODUCTION

In the modern society, the citizens rely on their digital identity to interact with many critical services. Among them, e-banking, e-health and e-voting are just few examples. Clearly, these services must prevent illegal accesses that might have dramatic effects.

Strong authentication (SA) mechanisms aim at preventing unauthorized users from logging in a system. In particular, SA mechanisms extend traditional authentication ones in order to guarantee a higher level of security, e.g., through the adoption of multiple authentication factors. Moreover, due to the social implications, one would expect that the adequate levels of security are stated by the national authorities.

Due to the enormous interest toward SA, many initiatives flourished in the last years. As a consequence, there has been a rapid development of SA and its exploitation in many application scenarios. Unfortunately, this generated a scattered landscape where many proprietary, scarcely documented implementations exist. Concurrently and perhaps consequently, the national and international stakeholders did not release precise regulations and propositions on how SA must be achieved. The result is a lack of parameters for classifying, comparing and evaluating the existing SA solutions in terms of security.

The goal of this paper is to provide a general overview of the state of the art of SA. We aim at identifying common factors that can lead to a classification of the SA mechanisms. To do that, we consider two perspectives, i.e. *regulations* and *implementations*. In the last years, the lawmakers faced the problem of characterizing the SA so to establish the acceptable level of security. Clearly, the service providers have to comply with laws and directives. However, they can achieve that in many different ways.

In this paper we focus on the following aspects.

1. *EU regulations*. Among the involved stakeholders, EU is certainly a very active one and its laws about SA are constantly evolving.
2. *Mobility*. Smartphones and tablets play several roles in SA, including: client application (via web browsers or mobile apps), secure hardware (e.g., relying on the SIM card) or second channel endpoint (e.g., for SMS or voice calls).
3. *E-Banking*. Banks are strongly motivated in implementing SA mechanisms as part of their online services.

Related Work. Although SA mechanisms are receiving attention from both the academia and the industry, at the best of our knowledge, no authors carried out a systematic review of the existing implementations.

In (Haupert and Müller, 2016), the authors classify the SA mechanisms used by four German banks. In particular, they focus on SA implementations based on mobile apps. Our paper follows a similar line, but with a new classification approach and by extending it to banks of different countries.

Sinigaglia, F., Carbone, R. and Costa, G.
Strong Authentication for e-Banking: A Survey on European Regulations and Implementations.
DOI: 10.5220/0006438504800485
In *Proceedings of the 14th International Joint Conference on e-Business and Telecommunications (ICETE 2017) - Volume 4: SECRYPT*, pages 480-485
ISBN: 978-989-758-259-2

Many authors focus on the problem of defining SA protocols and verifying their security properties. For instance, in (DeFigueiredo, 2011) the authors carry out a security evaluation of two-factor authentication on mobile devices. A similar reasoning is presented in (Hagalisletto, 2007), but explicitly considering phishing attacks. In (Armando et al., 2013), the authors use model checking to automatically verify SA protocols.

The FIDO (Fast Identity Online) Alliance (FIDO, 2017) is a prominent initiative for the standardization of the SA mechanisms. Several important stakeholders, e.g., Google, Paypal and Bank of America, joined the initiative. Interestingly, however, no EU banks participate in the FIDO alliance.

Methodology. Our goal is to identify and discuss the key concepts related to the SA mechanisms and their features. To do that, we proceeded from abstract to concrete. In particular, we started from the analysis of EU directives and recommendations. As a matter of fact, these documents provide the general definitions and social requirements of the SA mechanisms. Our presentation follows the temporal evolution of the key concepts appearing in the documentation.

The analysis of the EU regulations allowed us to analyze the actual SA implementations and critically discuss their features against the directives. Thus, we carried out a systematic review of the SA implementations used by 26 important international banks chosen among the world top 100 in terms of asset (Relbanks, 2016). Banks were selected by considering their (*i*) turnover, (*ii*) number of customers and (*iii*) geographical distribution. In particular, we privileged EU banks (17 out of 26) in order to understand how they met the EU directives. For each of these banks we parsed the available documentation referring to the SA mechanisms, e.g., used for online payments. Such a documentation included specifications, handbooks and guidelines. The full list of considered documents is available at https://sites.google.com/fbk.eu/strong-auth-banks-survey/.

This paper is structured as follows. In Section 2, we discuss the main EU regulations related to SA and online payments. In Section 3, we present the data collected about the implementations of SA mechanisms. In Sections 4, we provide an overview of the lesson learned. Section 5 concludes the paper.

2 EU REGULATIONS

In this section we present the history and evolution of the EU directives and recommendations referring to SA and related topics, e.g., online payments.

Payment Services Directives in the European Community (PSD). PSD (EBA, 2007) was published by the European Central Bank (ECB) in 2007, with the aim of creating the basis for a unique area of payment in the whole EU (the so-called Single Euro Payments Area). Among those definitions, the PSD presented the first proposal for EU rules concerning the *Payment Services* which are defined as business activities that allow people

> **(D1 – PS)** to deposit or withdraw cash on or from a payment account, as well as the operation of that account; execute payment transactions (e.g., standing orders, direct debits, etc.) both on payment accounts or by electronic means; issue and/or receive payment instructions; execute money remittance [...].

Noticeably, no distinction between traditional payments (e.g., through a point of sale) and online payments (i.e. only using the internet) is provided.

Recommendations for the Security of Internet Payments (RSIP). RSIP (ECB, 2013a) was released in 2013 and officially became law in 2015. Interestingly, it was the first document with a clear definition of *Internet Payments* (IPs). Indeed, they are defined as

> **(D2 – IP)** the execution of card payments on the internet, including virtual card payments, the execution of credit transfers (CTs) on the internet, the issuance and amendment of direct debit electronic mandates and the transfers of electronic money between two e-money accounts via the internet.

The document also states that IPs should be protected through a mechanism of *Strong Customer Authentication* (i.e. SA applied to banking customers). In this context, SA is defined as

> **(D3 – SA)** a procedure based on the use of two or more of the following elements—categorised as knowledge, ownership and inherence: i) something only the user knows, e.g., static password, code, personal identification number; ii) something only the user possesses, e.g., token, smart card, mobile phone; iii) something the user is, e.g. biometric characteristic, such as a fingerprint. In addition, the elements selected must be mutually independent [...].

It is worth noticing that this definition explicitly defines the three types of *elements* (hereafter *Authentication Elements*, AEs in short) that one can adopt to achieve SA. In addition, the definition states that the adopted AEs must be mutually *independent*, i.e. two AEs cannot be compromised by a single action.

According to RSIP, customers can access the PS after a registration procedure called *enrolment*. A successful enrolment leads to the activation of the AEs (used to grant SA in the IP). This phase is called *provisioning*. About them, the document says that the Payment Services providers

> **(D4 – P)** should ensure that customer enrolment for and the initial provision of the authentication tools required to use the internet payment service and/or the delivery of payment-related software to customers is carried out in a secure manner.

Although generic, this is the first official statement about the enrolment and provisioning phases and their roles in the SA.

Recommendations for the Security of Mobile Payments (RSMP). A similar approach was used for RSMP (ECB, 2013b) released in the end of 2013. Briefly, RSMP applies the concepts of RSIP to the context of IPs involving mobile technologies. More precisely, *Mobile Payments* (MPs) are described as

> **(D5 – MP)** payments for which the payments data and the payment instruction are transmitted and/or confirmed via mobile communication and data transmission technology through a mobile device between the customer and his/her payment service provider in the course of an online or offline purchase of services, digital or physical goods.

Moreover, RSMP extends the definitions and requirements already proposed in RSIP by considering the specific aspects related to the mobile technologies. In particular, mobile enrolment and mobile provisioning are defined and new constraints are added about the distribution of mobile software through reliable/trusted channels/vendors.

Payment Services Directives in the Internal Market (PSD2). In 2015, the ECB released PSD2 (EBA, 2015). PSD2 refines the definitions of PSD by introducing some concepts presented in RSIP and RSMP. To do that, PSD2 combines the two notions of IP and MP in a single one: *remote payment transaction*. Moreover, PSD2 is the first directive that states where SA must be employed, i.e. when the user (i) accesses its account online, (ii) initiates an electronic remote payment transaction and (iii) carries out any risky action through a remote channel.

Regulatory Technical Standards (RTS). Together with the PSD2, the ECB released RTS (EBA, 2016), with the purpose to map the abstract indications of PSD2 into concrete technical solutions. For instance, a list of key features is provided for the precise characterization of the features of the AEs. Furthermore, the independence of the elements is specifically targeted, requiring dedicated measures in the case that the SA or part of it is executed through multi-purpose devices (e.g., mobile phones and tablets). Regarding the AEs provision, moreover, the RTS refers to the contributions given in RSMP, losing the specification of possible distribution channels but introducing new requirements regarding the elements activation (acknowledging the risks of remote distribution). Finally, the concept of Exemption is introduced, presenting some low-risk situations in which the usage of SA mechanisms may be avoided.

Table 1: Key concepts in EU regulation.

		Definition	**Application**	**Exemption**	**Internet**	**Mobile**	**Definition**	**Independence**	**Features**	**Provisioning**	**Enrolment**
Source	**Year**	**SA**			**Pay**		**AE**			**Phases**	
PSD	2007	–	–	–	–	–	–	–	–	–	–
RSIP	2013	●	◑	–	●	–	●	–	–	●	●
RSMP	2013	●	◑	–	●	●	●	–	–	●	●
PSD2	2015	●	●	–	◑	◑	●	●	–	–	–
RTS	2015	●	●	●	◑	◑	●	●	●	●	◑

2.1 Considerations

Some facts arise from the comparison of the documentation mentioned above.

SA. The notion of SA evolved over time and new concepts were defined. As a matter of fact, PSD2 also introduced a precise description of the cases where SA must be applied. Moreover, in RTS some exemption cases were introduced.
Pay. As a refinement to RSIP, in RSMP IPs and MPs have a precise and distinct characterization. Such distinction disappears in PSD2 and RTS where the IPs and MPs are combined under the same term, i.e. *remote payment transaction*.
AE. The definition of AEs also evolved over time. In particular, more attention was dedicated to the definition of independence and the identification of desired features. These aspects have a crucial role for establishing reliable criteria for the evaluation of the AEs.
Phases. A rather precise definition of the provisioning and enrolment phases is present in RSIP and RSMP. Surprisingly enough, they do not appear in the official directives (PSD and PSD2). However, a technical description is provided in the RTS.

Table 1 summarizes how the regulations deal with the key concepts relevant for SA. For the sake of presentation, we use ●, ◑, and – when a concept is clearly, partially (e.g., contextually to another definition or without a dedicated statement), and not defined in the document, respectively.

3 SA IMPLEMENTATIONS

We analyzed the SA mechanisms adopted by 26 banks for their online payment services. Table 2 summarizes the collected information (EU banks only).[1] Each row describes the relevant aspects of the SA implementation of the corresponding bank. For instance, the first row refers to Deutsche Bank from DE: the bank offers four distinct AEs (col. AE); each AE is provisioned in a different way (and the provisioning of ▣ depends on 🖩); four different IP procedures are supported (one for each AE), aiming at providing the user with an OTP that she can use to confirm the operation on the web browser; two MP procedures are in place: 🖩 and ▣ cannot be used for the MPs (the – symbol means that the corresponding AE is not involved in any authentication procedure)[2] while the process for 📱 changes by replacing otp$_h$ with otp$_i$. The meaning of each column and the corresponding notation is detailed below.

3.1 Authentication Elements (AE)

Below we list the AE used by the selected banks. Among them, we do not include access credentials, e.g., username & password, as they are common to every service. Instead, we focus on AEs that are requested at each payment. For each AE, in brackets we report the category (Ownership, Knowledge or Inherence), following the definition D3 in Section 2.

💳 **Smart Card (O).** It is a magnetic card, with a unique card code, that also embeds high-security electronic circuits, dedicated to cryptographic operations. Since the Smart card is usually given when the customer applies for the bank account and it is always used in combination with other AEs, we omit it in the AE and P columns of Table 2. It is only considered in the IP and MP columns.

🖩 **HW OTP Generator (O).** It is a hardware devoted to the generation of one-time passwords (OTP). The features of these AEs may vary significantly. For instance, a simple generator provides the user with an OTP when she performs a single operation (e.g., pressing a button, inserting a PIN). On the other hand, with a card reader, the user has to employ an associated smart card in order to obtain the OTP.

Table 2: SA implementations (EU banks).

Bank name	C	AE	P	IP	MP
Deutsche B.	DE	🖩 ⊞ ▣ 📱	🏛/✉ 🏛 🌐🖩 🌐💬	opid$_o$ » 🖩 » **op ?** » otp$_h$ (x,y) » ⊞ » otp$_h$ otp$_m$ » ▣ » otp$_h$ opid$_o$ » 📱 » **op ?** » otp$_h$	– (x,y) » ⊞ » otp$_h$ – opid$_i$ » 📱 » **op ?** » otp$_i$
Sparkasse	DE	🖩 ▣ 📱🗝	🏛 🏛 🌐💬	opid$_o$ » 🖩 💳 » **op ?** » otp$_h$ otp$_m$ » ▣ » otp$_h$ opid$_n$ » 📱🗝 » **op ?** » otp$_h$	opid$_o$ » 🖩 💳 » **op ?** » otp$_h$ – opid$_i$ » 📱🗝 » **op ?** » otp$_i$
Commerzbank	DE	🖩 ⊞ ▣ 📱🗝	🌐✉ 🌐 🌐✉ 🌐💬	opid$_o$ » 🖩 » **op ?** » otp$_h$ (x,y) » ⊞ » otp$_h$ otp$_m$ » ▣ » otp$_h$ opid$_n$ » 📱🗝 » **op ?** » otp$_h$	opid$_o$ » 🖩 » **op ?** » otp$_h$ – – opid$_i$ » 📱🗝 » **op ?** » otp$_i$
Barclays	UK	🖩 📱🗝 📱👆	🏛 🌐🖩/🏧 🌐🖩/🏧	🖩 💳🗝 » otp$_h$ 📱🗝 » otp$_h$ 📱👆 » otp$_h$	– opid$_i$ » 📱🗝 💳 » otp$_i$ opid$_i$ » 📱👆 💳 » otp$_i$
RBS	UK	🔑 🖩 📱🗝	🌐 🌐✉ 🌐💬	🔑 » opid$_h$ » 🖩 💳🗝 » otp$_h$ –	– – opid$_i$ » 📱🗝 » otp$_i$
LLoyds Bank	UK	🔑 ▣	🏛 🏛	🔑 » opid$_h$ » ▣	🔑 –
HSBC	UK	🖩🗝 📱🗝	✉🌐 🌐	🖩🗝 » otp$_h$ 📱🗝 » otp$_h$	– opid$_i$ » 📱🗝 » **op ?** » otp$_i$
Banca Intesa	IT	🖩 📱🗝 📱👆	🏛 🌐🖩 🌐🖩	🖩 » otp$_h$ opid$_n$ » 📱🗝 » **op ?** » otp$_n$ opid$_n$ » 📱👆 » **op ?** » otp$_n$	🖩 » otp$_h$ opid$_i$ » 📱🗝 » **op ?** » otp$_i$ opid$_i$ » 📱👆 » **op ?** » otp$_i$
CheBanca	IT	▣ 🔑 📱🗝	📞 🌐 🌐💬	🔑 » otp$_m$ » ▣ » otp$_h$ 📱🗝 » otp$_h$	– – opid$_i$ » 📱🗝 » **op ?** » otp$_i$
Unicredit	IT	🖩 ⊞ 📱🗝 📱👆	🏛 🏛 🌐💬@ 🌐💬@	🖩 » otp$_h$ (x,y) » ⊞ » otp$_h$ opid$_h$ » 📱🗝 » **op ?** » otp$_h$ opid$_h$ » 📱👆 » **op ?** » otp$_h$	– – opid$_i$ » 📱🗝 » **op ?** » otp$_i$ opid$_i$ » 📱👆 » **op ?** » otp$_i$
BNP Paribas	FR	▣ 📱🗝	🌐 🌐	otp$_m$ » ▣ » otp$_h$ opid$_n$ » 📱🗝 » **op ?** » otp$_n$	otp$_m$ » ▣ » otp$_i$ opid$_i$ » 📱🗝 » otp$_i$
Credit Agricole	FR	▣	🏛/🌐	otp$_m$ » ▣ » otp$_h$	–
Societe Generale	FR	▣ 📱🗝	🏛/🌐 🌐💬	otp$_m$ » ▣ » otp$_h$ opid$_n$ » 📱🗝 » **op ?** » otp$_n$	– opid$_i$ » 📱🗝 » **op ?** » otp$_i$
B. Populaire	FR	🖩 ▣	🏛 🏛	🖩 💳🗝 » otp$_h$ otp$_m$ » ▣ » otp$_h$	– –
B. Santander	ES	🔑 ▣	🏛 🏛	🔑 » otp$_m$ » ▣ » otp$_h$	🔑 » otp$_m$ » ▣ » otp$_i$
BBVA	ES	▣	🏛/🏧	otp$_m$ » ▣ » otp$_h$	otp$_m$ » ▣ » otp$_i$
CaixaBanca	ES	⊞ ▣	🏛 🏛	(x,y) » ⊞ » otp$_h$	otp$_m$ » ▣ » otp$_i$

📱 **SW OTP Generator (O).** An OTP can also be software-generated. For instance, some banks distribute a mobile app. The apps are dedicated to the OTP generation or include it as one of their functionalities. SW OTP generation is the counterpart of HW OTP generation and works analogously.

⊞ **Access Matrix (O).** It consists of a matrix where every cell contains a number. To generate an OTP, the user is requested to provide the sequence of numbers appearing in the given cells.

▣ **SIM Card (O).** Using a SIM card, the remote service sends the OTP directly to the phone number associated to the user, e.g., via SMS or voice call.

🔑 **Extra Knowledge (K).** A piece of information shared between the user and the bank. Commonly a PIN number, pass-phrase or a secret question that the user has to recall (sometimes referred to as memorable information). The extra knowledge can be decided by either the user or the bank.

[1] The full table and data are available at the companion website.

[2] Banque Populaire and Credit Agricole allow to execute MPs without SA (only basic authentication is required).

🫆 **User Fingerprint (I).** The mobile device of the user embeds a reader that recognizes her fingerprint.

It is worth noticing that some ownership AEs are combined with a dedicated knowledge or inherence AE, e.g., a credit card may have a PIN or an app may request the user fingerprint. To denote these AEs, we add an extra annotation like in 💳🔑 and 📱🫆.

3.2 AE Provisioning (P)

The provisioning is the process used to issue and activate an AE to the user (see D4). We distinguish among the following actions.

- 🏛 The user goes to a local branch. For instance, a user can retrieve an object (e.g., an HW OTP generator 🖩), establish a shared extra knowledge (🔑) or register her SIM card phone number (▣).
- 🌍 The user interacts with the web portal of the bank. For instance, the user can download/activate a SW OTP generator (📱), an access matrix (▦) or exchange an extra knowledge (🔑) with the bank.
- 📞 The user has a phone call with a remote service. Often it is used to activate an AE such as a credit card (💳) or a SIM card (▣).
- @ The user sends/receives an email. For instance, the user can receive instructions or secret codes necessary to unlock/activate/register an AE.
- ✉ The bank and the user communicate via snail mail or courier. This channel can be used for the same purposes of @. Also, is often used to deliver an AE, e.g., an HW OTP generator (🖩).
- 🏧 The user operates via an automated teller machine (ATM). For instance, ATM can be used to activate a SIM card (💬) or an SW OTP generator (📱).
- 💬 Similar to @, but carried out through the SMS service of the user's mobile telco provider.

To denote a provisioning procedure we use a sequence of the symbols given above. The meaning is that the user has to perform the corresponding operations in sequence, e.g., 🌍💬 means that the user interacts with a web portal and then sends/receives one or more SMS. Notice that we also use AE symbols when the provisioning procedure requests them. Finally, when the flow admits two independent alternatives we use /. For instance 🌍🖩/🏛 denotes that the provisioning can be carried out either online (🌍) or in a local branch (🏛). In the first case, the AE 🖩 is also necessary.

Table 3: List of data objects.

	Description	R/W agent
$\texttt{opid}_h$	human-readable opid	human
$\texttt{opid}_o$	scannable opid	camera
$\texttt{opid}_n$	network notified opid	app
$\texttt{opid}_i$	interprocess notified opid	app
$\texttt{otp}_h$	human-readable otp	human
$\texttt{otp}_i$	interprocess notified otp	app
$\texttt{otp}_n$	network notified opt	app
$\texttt{otp}_m$	otp on sms	gsm
$\texttt{(x,y)}$	coordinates	human

3.3 Remote Payment Transactions (IP, MP)

We characterize a payment procedure through the sequence of AE (see above) that it involves and their input/output data. In particular, we use the following notation.

- A plain text denotes a data object. Also, each data object is transmitted through a specific channel. Table 3 shows the list of the data objects appearing in the online payment procedures.
- Icons denote the AEs, e.g., ▦ for an access matrix. When two or more AEs are combined we put them in sequence, e.g., 🖩💳 for a smart card used with an HW OTP generator (card reader).
- » is used for input/output and concatenation. For example, we write $\texttt{(x,y)}$ » ▦ » $\texttt{otp}_h$ to represent that some coordinates are given as the input of an access matrix (▦) to obtain an OTP that the user reads ($\texttt{otp}_h$). Notice that the interpretation of the » symbol may vary in accordance with the payment context (see at the end of this Section).
- **op ?** indicates that the user is prompted with the details of the ongoing operation and she must authorize the continuation of the procedure.

Although the most recent EU regulation (PSD2) does not distinguish between them, here we treat IP and MP separately (as in RSIP and RSMP). The main motivation is that we expect the collected data to support the security analysis of the SA implementations. For instance, IP and MP admit different attacker models, e.g., *man-in-the-browser* vs. *man-in-the-mobile* (see (Haupert and Müller, 2016)). These differences are discussed and motivated in Section 4. As a consequence of this distinction, the reader must take into account that IPs and MPs provide a context for the notation introduced above. For instance, the expression $\texttt{opid}_h$ » 🖩 » $\texttt{otp}_h$ has two interpretations: (IP) the user receives an $\texttt{opid}$ from the browser, uses it with an HW OTP generator and she submits the OTP to the browser; and, (MP) the user gets the `opid` from (and puts the OTP in) the mobile app.

4 LESSON LEARNED

Key Findings. We put forward some observations based on the results of the survey.

1. Ownership AEs are predominant and many banks use more than one of them. Also knowledge AEs are common, while inherence AEs are scarcely adopted.
2. Banks support multiple IP and MP procedures (on the average 2.3 IP and 1.6 MP) and AEs (average 2.5). This clearly enlarges the attack surface of the systems.
3. Among the considered SA implementations 21/26 leverage 📱 or ▣ for executing an IP. Among these, 7 do not provide alternatives, i.e. the user has to rely on her mobile device.
4. ▣ is adopted by 5 banks for both IP and MP. According to (Haupert and Müller, 2016), this could affect the independence of the AEs, as both 📱 and ▣ can reside on the same device.

Discussion. Beyond the previous observations, we put forward some general considerations.

Regulation is vague. As shown in Section 2, the lawmakers acknowledged the peculiarities of IP and MP in wavering manner. Moreover, at the current stage the features of the AEs have not been rigorously defined. Hence, a large variety of AEs exists and a comparison in terms of security features is extremely hard.

Mobile is a bottleneck. In case of MPs that only include operations on a mobile device, the AEs independence is at risk. As a matter of fact, the mobile device turns out to be a single point of failure and, thus, a privileged target for the attackers (Haupert and Müller, 2016).

Diversity of the implementations. Most banks implement their own SA mechanism. The reason is probably that they follow their specific interest toward legacy problems, usability, flavor of customers, etc. However, having many implementations increases the risk that some of them are flawed or incorrect.

Understanding of the user. Faced with many alternatives, often the user does not understand the importance of the operations and which SA mechanisms better fit with her necessities. Thus, the customers might tend to focus on the usability aspects, which they perceive as an added value. Clearly this could promote risky habits, e.g., storing knowledge AEs in an unsafe way.

5 CONCLUSION

We presented a survey taking into account both EU regulations and implementations of SA mechanisms for e-Banking services. We believe that the selected parameters and the results of our survey are a valuable starting point for a comparison and pave the way for an evaluation of the security of different SA mechanisms. As part of the future work, we plan to extend our survey by defining a classification method for categorizing the security risks affecting SA implementations. Such a mechanism should also be aware of the specific features of each AE and the relevant attacker models.

ACKNOWLEDGEMENTS

The present work has been partially supported by CINI Cybersecurity National Laboratory within the project FilieraSicura: Securing the Supply Chain of Domestic Critical Infrastructures from Cyber Attacks (www.filierasicura.it) funded by CISCO Systems Inc.

REFERENCES

Armando, A., Carbone, R., and Zanetti, L. (2013). Formal Modeling and Automatic Security Analysis of Two-Factor and Two-Channel Authentication Protocols. In *Network and System Security (NSS), Madrid, Spain.*

DeFigueiredo, D. (2011). The case for mobile two-factor authentication. *IEEE Security and Privacy*, 9:81–85.

EBA (2007). Directive 2007/64/EC of the European Parliament and of the Council on payment services in the internal market (PSD).

EBA (2015). Directive 2015/2366 of the European Parliament and of the Council on payment services in the internal market (PSD2).

EBA (2016). Draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of PSD2.

ECB (2013a). Recommendations for the Security of Internet Payments.

ECB (2013b). Recommendations for the Security of Mobile Payments - DRAFT.

FIDO (2017). The fido alliance. https://fidoalliance.org/about/overview/.

Hagalisletto, A. M. (2007). Analyzing two-factor authentication devices. Technical report, University of Oslo.

Haupert, V. and Müller, T. (2016). On app-based matrix code authentication in online banking. Technical report.

Relbanks (2016). Top 100 banks in the world by asset. http://www.relbanks.com/worlds-top-banks/assets.