International Cybersecurity Law Review (2024) 5:79–120
https://doi.org/10.1365/s43439-023-00108-8

ORIGINAL PAPER

Harmonizing open banking in the European Union: an analysis of PSD2 compliance and interrelation with cybersecurity frameworks and standards

Marianna Gounari · George Stergiopoulos · Kosmas Pipyros · Dimitris Gritzalis

Received: 13 November 2023 / Accepted: 29 November 2023 / Published online: 25 January 2024

Abstract This paper focuses on the security protocols enacted in banking transactions across the European Economic Area (EEA), as stipulated by the Second or Revised Payment Service Directive (commonly referred to as 'PSD2' or simply 'the Directive'). The study aims to comprehensively analyse the implementation and efficacy of these security measures within the specified jurisdiction. The Directive incorporates fundamental rights and obligations that all stakeholders are compelled to adhere to and delineates specific security measures and standards that both traditional banking institutions and third-party providers (TPP) are mandated to implement. In particular, one of the cardinal mandates for banking and financial institutions under PSD2 is the obligation to facilitate third-party access to customer data via open application programming interfaces (API). While this open banking paradigm and the consequent proliferation of data sharing unquestionably bring about various advantages, such as enhanced consumer choice and market competition, they concurrently expose the financial ecosystem to a slew of potential security vulnerabilities and privacy risks. Upon conducting a comprehensive review of the

Marianna Gounari · George Stergiopoulos
Dept. of Information & Communication Systems Engineering, University of the Aegean, Samos, Greece

Marianna Gounari
E-Mail: marianna.gounari96@gmail.com

George Stergiopoulos
E-Mail: g.stergiopoulos@aegean.gr

Kosmas Pipyros
Dept. of Computer Science, Philips University, Nicosia, Cyprus
E-Mail: pipyros.k@philipsuni.ac.cy

✉ Dimitris Gritzalis
Dept. of Informatics, Athens University of Economics & Business, Athens, Greece
E-Mail: dgrit@aueb.gr

security requirements and measures stipulated under PSD2 and a comparative analysis with essential cybersecurity frameworks and standards (NIS2, Cybersecurity Act, GDPR, ISO 27001:22 and PCI DSS), we have ascertained a discernible lack of harmonisation and clarity concerning the technical security specifications for its effective implementation. This lacuna substantiates the challenges banks face in fully grasping the extensive spectrum of compliance obligations mandated by PSD2. The aim of this research is to offer a valuable contribution to both the comprehension and the pragmatic deployment of security standards in the context of banking transactions, as regulated by the PSD2. The paper serves as a valuable resource for traditional banking institutions and relevant stakeholders by guiding them through the complexities of PSD2 implementation while also evaluating the effects of the security measures on transactional safeguards, data security, and the provision of payment services.

Keywords Security protocols · Payment service directive · Third-Party access · Security vulnerability · Enhanced consumer choice

1 Introduction

Over the last few decades, technological advancements have introduced remarkable transformations across multiple aspects of our daily lives. Innovations such as smartphones and digital technologies have particularly revolutionized the payment services sector. The latest technological developments in the payment sector have compelled both established and emerging stakeholders to rapidly adapt to novel paradigms. In the context of an escalating trend in e-commerce, payment service providers (PSP) are under increasing pressure to deliver their services in a more efficient, effective, and user-centric manner, offering a diversified array of options to cater to consumer preferences [1]. In light of these trends, many users, notably millennials, demonstrate a propensity for seamless transactions facilitated by mobile devices and wearables without wasting time or effort. This consumer behaviour inherently necessitates that PSP access pertinent personal data to provide a more user-friendly payment experience [2]. Consequently, the criticality of ensuring robust security protocols for payment transactions and stringent data privacy measures has been elevated.

In recognition of the burgeoning trends in the payment sector, particularly driven by the proliferation of data-centric technologies, the European Union (EU) adopted the Second or Revised Payment Service Directive (PSD2) [3] on October 8, 2015, which provides the legal foundation for further development and improvement of multiple fields of the electronic payments within the EU. The Directive was officially implemented on January 13, 2018, serving as an augmentation and modernization of its precursor, the original Payment Services Directive (commonly known as PSD), which was promulgated in 2007 [4]. PSD2 constitutes a pivotal regulatory framework, enacted with the explicit aims of fortifying the security apparatus governing electronic payments, stimulating innovation, and enhancing competition within the payment services sector. It is a policy instrument designed with the overarching objective of optimizing the European payment ecosystem. It aims to make payment systems more interconnected and efficient, thereby simplifying payment processes and bolstering their security, while simultaneously nurturing an environment conducive to innovation and competitive parity within the industry. Thus, PSD2, not only extends the foundational regulatory principles set forth by its predecessor, PSD, but also adapts and refines them to meet the challenges and opportunities presented by a rapidly evolving digital payments landscape.

In a significant departure from its predecessor, PSD2 expanded the regulatory framework for Internet payment services to encompass new and unconventional market participants. More specifically, PSD2 introduced two novel categories of services: account information services (AIS) and payment initiation services (PIS). Payment initiation service providers (PISP), such as PayPal, Sofort, IDeal, and Tikkie, are now authorized to initiate payment orders directly from a user's bank account at the user's behest. Similarly, account information service providers (AISP), including firms like Moneybox, Spiir, Trustly, and Fintonic, are empowered to aggregate and display consolidated financial data gathered from one or more of a user's bank accounts. It is noteworthy that both PISP and AISP were operational prior to the advent of PSD2. However, the seminal change precipitated by PSD2 lies in the formal regulation of these entities—PISP and AISP—thereby establishing a legal foundation for their continued and expanded operation in the online payment marketplace. To offer innovative services, these third-party providers (TPP) are mandated to secure access to pertinent payment account information and personal data of their users. This legislative shift thus legitimizes the role of TPPs, albeit with requisite regulatory oversight, facilitating a more competitive and diversified online payment environment while attempting to ensure transactional security and data privacy [5].

PSD2 offered numerous benefits, particularly in the facets of information security and data protection. Furthermore, the European Banking Authority's (EBA) regulatory technical standards (RTS) [6] have served as a key component in the regulatory framework surrounding PSD2. These RTS provided a more detailed set of guidelines that facilitate the implementation of the high-level principles established in PSD2 aiming to create a secure and interoperate environment for electronic payment in the EU. Yet, they are not without their complexities and ambiguities, necessitating a robust understanding and continual vigilance from all stakeholders to ensure full and sustained compliance. Many stakeholders find themselves grappling with the technical specifications that would render them fully compliant with PSD2. Indeed, the EU Member States (MSs) have observed a lack of consistency and clarity in terms of the defined security standards and measures delineated by the Directive and the EBA's RTS. In this context, taking into consideration the rapid pace of technological advancements and the escalating threats to information security and data protection in the financial services sector, a comprehensive analysis of the security measures covered by PSD2 and RTS is critical to equip stakeholders with the requisite knowledge and guidance needed to ensure robust compliance with the Directive.

2 A general overview of PSD2

Based on the aforementioned, the objective of this section is to provide an overview of the rights and protections and to analyze the security measures mandated by the PSD2 in order to provide a better understanding and guidance to traditional banks and stakeholders during implementation. Furthermore, by focusing particularly on the RTS and guidelines (GL) propagated by the EBA, we aim to furnish the respective stakeholders with an in-depth understanding required for seamless PSD2 implementation and to emerge the impact in terms of protecting transactions, data, and payment services.

PSD2 represents a fundamental shift in the regulatory landscape governing financial transactions within the EU, with a clear emphasis on enhancing consumer rights and protections. In early 2018, the European Commission (EC) produced a "user-friendly" electronic leaflet listing consumers' rights under the Directive and related EU law [7]. More specifically, the Revised Payment Services Directive aims to:

- Reduce and manage industry fraud rates without negatively impacting customer experience while increasing consumer trust.
- Develop two-factor authentication to improve the process. PSD2 requires SCA for all European e-commerce transactions beginning on December 31, 2020.
- Provide more online banking and payment options for e-commerce customers as EU payment markets open to new entrants.
- The emergence of TPPs will drive payment innovation and competition.
- Demand greater clarity and transparency in the fine print of e-commerce application licensing agreements.
- Reduce consumers' liability for unauthorized payments and institute an 8-week unconditional ("no questions asked") refund right for direct debits in euros.
- Ensure that when a transaction is completed, card issuers make all banking funds available.
- Prohibit surcharging, which is the practice of charging additional fees for payments made with consumer credit or debit cards in stores or online.
- Improve the complaints procedure because it requires organizations to accept and resolve complaints in a timely manner using predefined methods.

Furthermore, PSD2 establishes a conducive regulatory environment that not only modernizes the existing payment ecosystem but also actively encourages market competition by paving the way for emerging FinTech companies. For the facilitation of the new entrants in the payment industry, banks have to provide their Application Programming Interfaces (APIs) to those that request it, where consumers are expected to be able to consolidate their account information and payment options on a single device having, subsequently, better control and convenience. This is a fairly radical change, known as "Open Banking", that reinforces the EU's desire to promote increased competition and Fintech innovation [8]. The Open Banking EU Directory Service provides banks with a single, standardized reference point for accurately identifying which TPPs are authorized to access their interfaces and which roles and services they are authorized to perform on behalf of their customers. In addition, a Transparency Directory has been created to assist TPP in understanding developer portals and account servicing payment services Providers (ASPSP) in understanding TPP brands. In essence, the Directory serves as a trust mechanism, underpinning the secure and regulated exchange of financial information between banks and third-party entities [9].

Another significant key objective of PSD2 is to ensure customer protection by increasing the level of security of electronic payments. The PSP must comply with specific security requirements related to strong customer authentication (SCA) when they process payments or provide payment-related services on behalf of consumers [10]. PSD2 specifically requires multi-factor authentication (MFA) via specific identification requirements. This is primarily accomplished through APIs with identity authentication via PSD2 compliance certificates. For trusted commerce transactions on websites, these secure sockets layer (SSL)/transport layer security (TLS) certificates encrypt sensitive data and authenticate banking entities and TPP. This method of improving transaction security on both corporate and host-to-host communication systems is based on SCA, the new requirement that introduces specific technical standards such as PSD2-compliant certificates. The applicable requirement standards also specify when PSP are exempt from such authentication [10]. Additionally, all PSPs, including banks, PI, and TPP, must demonstrate that they have in place certain security measures to ensure safe and secure payments. Moreover, on a yearly basis, the PSP must assess the operational and security risks at stake, as well as the measures implemented [11].

As far as it concerns third-party access, PSD2 introduced a significant change in the accessibility of consumer bank account data, aggregate data, and payment data as prompted by the consumer to authorize TPP when the customer has provided explicit consent for the granting [12]. In general, the Directive does not significantly alter the conditions for granting authorization to PI in comparison to PSD1 (see also Appendix, Table 1). Payment initiation services (PIS) and account information services (AIS) will be required to have professional indemnity insurance or a comparable guarantee as a condition of authorization or registration [7]. When a payment is made, this allows larger organizations and merchants to retrieve banking industry data directly from the source, eliminating the intermediate. Many online retailers benefit from this process because it allows them to obtain additional verification of their customers' financial identities as well as instant debit resolution [11]. Consumers can manage their personal finances more efficiently by using applications that, for example, aggregate information from multiple bank accounts. Banks must establish secure communication channels to transmit data and initiate payments in order for this to be possible. As a result, from the most sophisticated corporations to those who are financially excluded, new services enable customers to take greater control of their finances [12]. Below are the newly regulated PSP:

a. Payment initiation services providers (PISP): This allows third-party companies to initiate payments on a consumer's behalf without requiring the consumer to visit their online bank's portal. PISP give consumers payment flexibility while also assuring retailers that the money is on its way. A practical use case would be the automatic transfer of funds to a customer's savings account ([13]; Fig. 1).

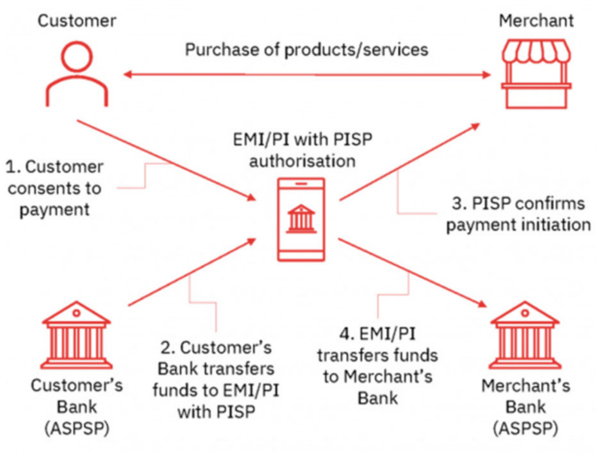

Customer
Merchant
Purchase of products/services
EMI/PI with PISP authorisation
1. Customer consents to payment
3. PISP confirms payment initiation
2. Customer's Bank transfers funds to EMI/PI with PISP
4. EMI/PI transfers funds to Merchant's Bank
Customer's Bank (ASPSP)
Merchant's Bank (ASPSP)

Fig. 1 Role of a payment initiation service provider (*PISP*)

b. Aggregators and account information service providers (AISP): These are third-party companies that have access to a consumer's bank and can display account information. They can request permission to connect to the bank account via an API and then provide their service using the bank account information. Having such access to such data, however, implies that you can "read-only", i.e., these providers cannot move funds from the account. An AISP, for example, allows a consumer to aggregate information from multiple accounts in a single application, providing them with a snapshot of available accounts, balances, and financial situation ([13]; Fig. 2).

c. Card-based payment instrument issuing providers (CBPIIP/CISP/PIISP): Any provider who performs payment instrument issuing and/or payment transaction acquisition—CBPII services.

d. Account servicing PSP (ASPSP): To provide the new services, the aforementioned TPP will need to rely on other PSP to gain access to customer accounts or data.

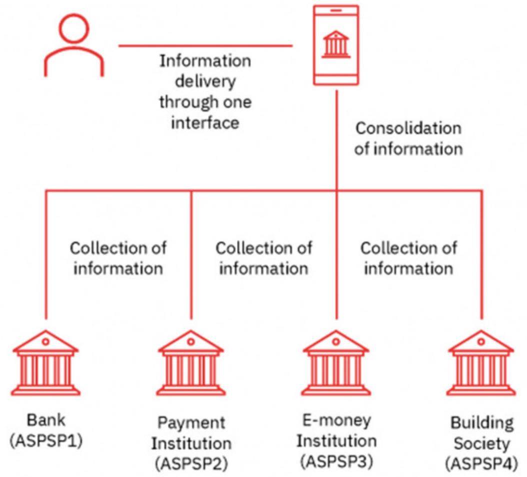

Information delivery through one interface
Consolidation of information
Collection of information
Collection of information
Collection of information
Bank (ASPSP1)
Payment Institution (ASPSP2)
E-money Institution (ASPSP3)
Building Society (ASPSP4)

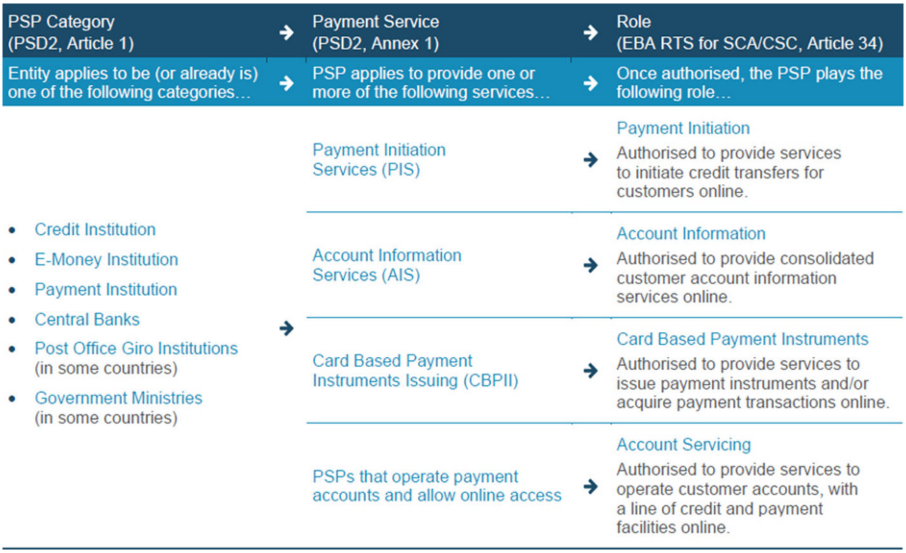
Fig. 2 Role of an account information service provider (*AISP*)

ASPSP, which provide and operate payment accounts for payment service users (PSU), will be the primary PSP responsible for enabling this access. ASPSP are typically banks and other similar financial institutions, such as building societies and payment companies, that offer and maintain financial accounts with online access for their customers [14]. ASPSP are critical components of open banking. They usually publish APIs so that customers can share their account data with TPP so that they can initiate payments on their behalf.

e. Payment service users (PSU): Customers who use any of the services mentioned above.

According to Article 34 of the EBA's "Regulatory Technical Standards for Strong Customer Authentication and Common Secure Communications Under PSD2" (EBA/RTS/2017/02), the new types of XS2A payment services are associated with payment service roles that can only be held by the aforementioned PSP categories, depending on the XS2A services that PSPs are authorized to provide. Entities that want to provide a new XS2A service must first apply to a national competent authority (NCA) to be categorized as a PSP and to be authorized to provide the desired payment service. If the application is approved, the PSP will be able to provide PSD2 payment services by taking on a specific role. Exempted PSPs cannot be granted authorization for PIS or AIS roles unless they first apply to become one of the permitted PSP categories [9]. Figure 3 summarizes the payment categories, services, and roles under PSD2.

Within the realm of payment transactions, the stipulations of PSD2 concerning transparency and informational disclosures, as with its predecessor, the PSD, are pertinent to transactions conducted in a Member State's currency when both PSP involved are situated within the EU. As depicted in Fig. 4, PSD2 broadens these



PSP Category (PSD2, Article 1)	Payment Service (PSD2, Annex 1)	Role (EBA RTS for SCA/CSC, Article 34)
Entity applies to be (or already is) one of the following categories…	PSP applies to provide one or more of the following services…	Once authorised, the PSP plays the following role…
• Credit Institution • E-Money Institution • Payment Institution • Central Banks • Post Office Giro Institutions (in some countries) • Government Ministries (in some countries)	Payment Initiation Services (PIS)	Payment Initiation Authorised to provide services to initiate credit transfers for customers online.
	Account Information Services (AIS)	Account Information Authorised to provide consolidated customer account information services online.
	Card Based Payment Instruments Issuing (CBPII)	Card Based Payment Instruments Authorised to provide services to issue payment instruments and/or acquire payment transactions online.
	PSPs that operate payment accounts and allow online access	Account Servicing Authorised to provide services to operate customer accounts, with a line of credit and payment facilities online.

Fig. 3 Payment categories, services, and Roles under PSD2

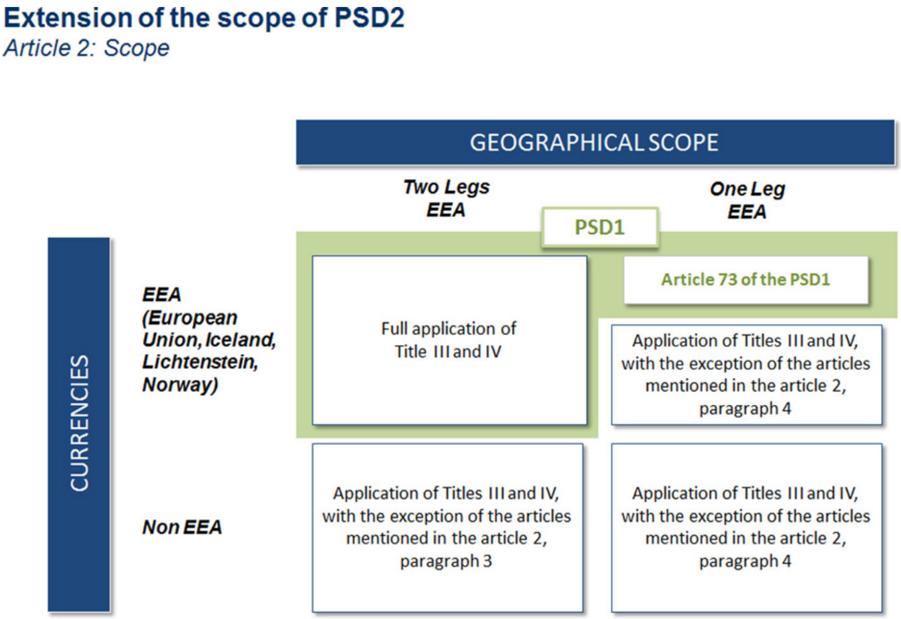
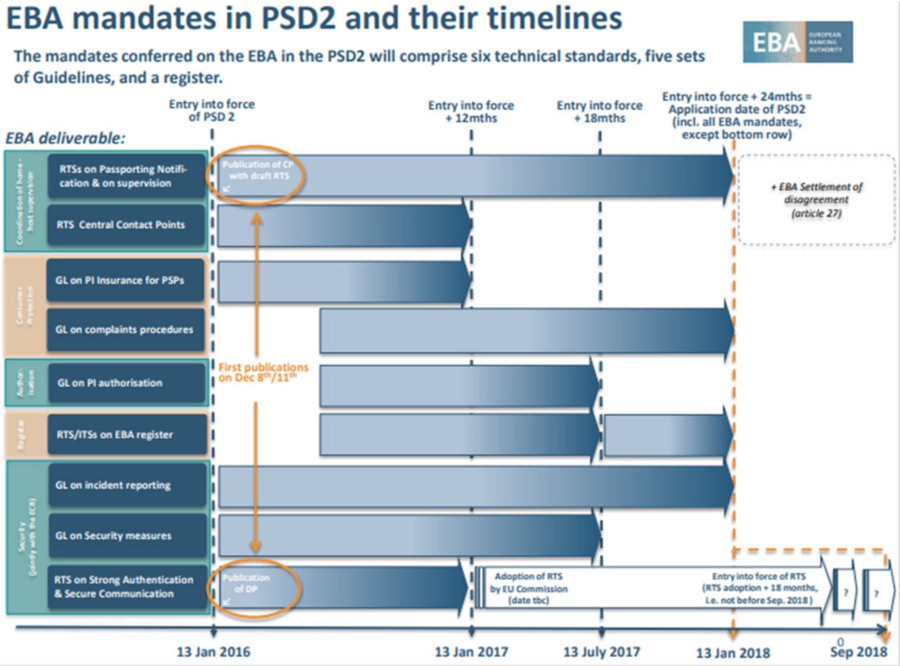

Extension of the scope of PSD2
Article 2: Scope
GEOGRAPHICAL SCOPE
Two Legs EEA
One Leg EEA
PSD1
CURRENCIES
EEA (European Union, Iceland, Lichtenstein, Norway)
Non EEA
Full application of Title III and IV
Article 73 of the PSD1
Application of Titles III and IV, with the exception of the articles mentioned in the article 2, paragraph 4
Application of Titles III and IV, with the exception of the articles mentioned in the article 2, paragraph 3
Application of Titles III and IV, with the exception of the articles mentioned in the article 2, paragraph 4

Fig. 4 Expansion of payments transactions scope of PSD2

transparency and informational mandates beyond the scope of the original Directive. It now encompasses transactions conducted in any currency where only one PSP resides within the EU, often referred to as the “one-leg-out transaction”. It is noteworthy that such regulations are binding on those segments of the payment process that transpire within the EU’s jurisdiction. Furthermore, despite the emphasis primarily being on EU-based banks and payment processors, entities headquartered outside the EU are not exempt. They may fall under the ambit of these rules if they serve customers or users within the EU. For instance, US-based corporations must ascertain that their EU divisions adhere to PSD2 regulations. Hence, enterprises contemplating entry into the EU market should brace themselves for inevitable PSD2 compliance [15].

In terms of ensuring security, safety and convenience for financial institutions’ consumers, market players must meet certain criteria to fulfil the new obligations set forth by PSD2. To that end, the EBA has formulated a series of RTS and Implementing Technical Standards (ITS) in close collaboration with the European Central Bank (ECB). Since the implementation of PSD2 on January 13, 2016, the EBA has published a consultation paper (CP) with a first draft of the RTS and ITS, a set of minimum requirements which all firms, including banks acting as ASPSP, building societies, PIs, e-money institutions, and their customers, must comply with [16]. PSD2 empowered the EC to adopt the RTS draft submitted by the EBA after 1 year (13 January 2017), and the EC made some limited substantive amendments to this. Consequently, the mandatory incorporation of various technical specifications was contingent upon the approval of the RTS crafted by the EBA and sanctioned by the Commission. Nevertheless, there have been multiple delays in both adoption


EBA mandates in PSD2 and their timelines

The mandates conferred on the EBA in the PSD2 will comprise six technical standards, five sets of Guidelines, and a register.

Fig. 5 Technical standards and guidelines scope and timelines

and development, stemming from tardiness in integrating the Directive into Spanish legislation and the EBA's deferment in establishing technical standards for regulating third-party access and strong authentication [10]. Having said that, and in light of the potential negative impact that PSD2 implementation could have on e-commerce, PSD2 requirements began gradually entering into force in January 2018 by not all having to be implemented at the same time [13]. The following Gantt chart highlights the EBA mandates and their scope, as well as the timelines for their implementation from EU MS (Fig. 5).

Another important requirement imposed by PSD2 on PI is registration in their home MS. According to Article 14 of PSD2, each NCA must manage and maintain a national register that is publicly accessible, known as the "NCA Public Register". Every PSP in the MS country of the EU and the EEA, including any agents and branches, will have their registration, payment services authorizations, passporting, and other status details recorded in each NCA Public Register.

It should be noted that branches of PIs must be registered in their home MS if they provide services in an MS other than their home MS. This public register shall identify the payment services authorized by the PI or registered by the natural or legal person. Authorized PIs must be listed in the register separately from natural and legal persons who are exempt under Articles 32–33. Furthermore, the register must be open to the public, accessible online, and updated on a regular basis. Any withdrawal of authorization and any withdrawal of an exemption pursuant to Articles 32–33 must be recorded in the public register, and the NCA must notify the EBA

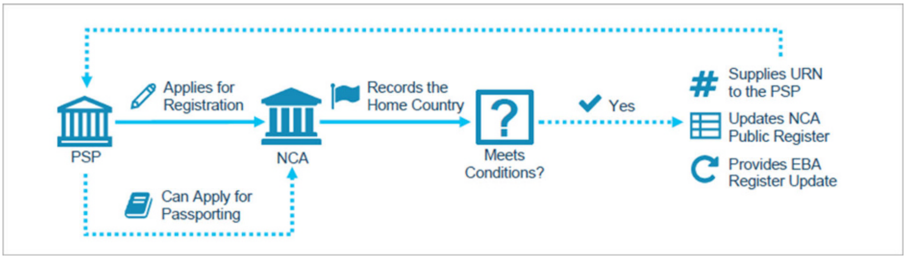


Fig. 6 Registration in the home Member State (NCA Public Register)

of the reasons for the withdrawal of any authorization and any exemption pursuant to Articles 32–33.

The stages of the home MS registration process applied to PI and EMI are depicted in the below graphical representation. It also may apply to credit institutions, but it may differ depending on the country (Fig. 6).

As set out in Article 28 of PSD2, passporting is the exercise by a business of its right to carry out activities and provide services regulated by EU legislation in another EEA state based on authorization or registration in its home EEA state. The activities can be carried out through a host-state establishment (establishment passport) or on a cross-border services basis without using a host-state establishment (cross-border service passport). PI, PISP, and AISP may use PSD2 passporting rights to provide payment services in another EEA country. The definition of PIS includes services to initiate a payment order at the payer's request in relation to a payment account held at another PSP in one of the EEA states. More precisely, the payer *"has the right to make use of a PISP to obtain the service referred to in point (7) of Annex I of PSD2"* if the payment service is provided within the EEA according to article 2 of PSD2 (Fig. 7).

On December 13, 2017, the EBA published the final Report on the RTS and the ITS on the EBA register for adoption by the EC: "Draft Regulatory Technical Standards setting technical requirements on development, operation and maintenance of the electronic central register and on access to the information contained therein, under Article 15(4) of Directive (EU) 2015/2366 (PSD2)" [17] and "Draft Imple-

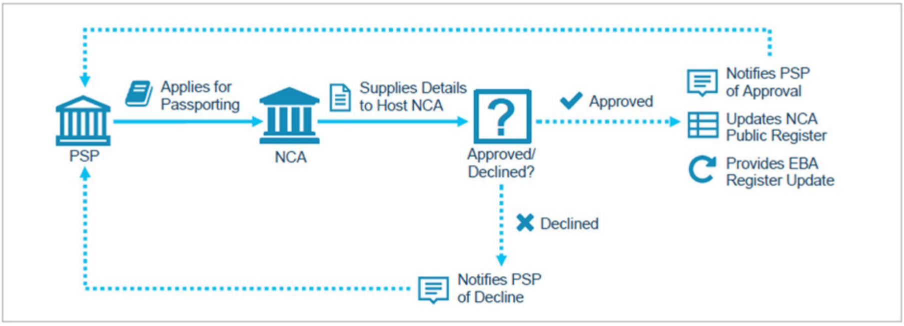


Fig. 7 Passporting application process

menting Technical Standards on the details and structure of the information entered by NCAs in their public registers and notified to the EBA under Article 15(5) of Directive (EU) 2015/2366" [18]. In the following section, regulatory and technical standards under PSD2 will be examined.

3 The regulatory and technical standards under PSD2

The implementation of the PSD2 has paved the way for numerous advantages and possibilities, particularly by stimulating innovation and enhancing competition in the payments sector. The most significant alterations include the broadening of the market landscape for PSP and the integration of advanced technological solutions and authentication protocols for accessing payment accounts, commonly referred to as XS2A. Nevertheless, the increasingly prevalent utilization of personal and financial data by TPP, coupled with a growing dependency on information technology infrastructures, has escalated security vulnerabilities. These vulnerabilities can manifest in multiple ways: unauthorized data sharing with TPP, fraudulent activities perpetrated by conscienceless TPP or compromised customers, susceptibilities to malware or social engineering attacks in transactions initiated via TPP, and the exploitation of TPP by malevolent actors to confound the fraud detection mechanisms of banks.

To that end, the EBA responded on December 12, 2017, based on the mandate in Article 95 of PSD2, by introducing a set of GL (EBA-GL-2017-17) [17] where PSD2 requires PSP to establish a framework with appropriate mitigation measures and control mechanisms to manage those operational and security risks raised by the payment services they provide (hereafter "risk management framework"). These measures must be proportionate to the security risks involved. PSP must establish and maintain effective incident management procedures, including those for detecting and classifying major operational and security incidents, as part of that risk management framework [18]. In addition, a regular reporting mechanism should be established to ensure that PSP provide the NCA with an up-to-date assessment of their security risks and the measures they have taken in response to those risks on a regular basis [19].

However, these GL are aimed at PSP and only apply to their payment services, despite the fact that they are applicable to a broader range of institutions. As a result, they have been drafted to address a broader range of financial institutions under the EBA's jurisdiction, namely, credit institutions that previously fell under the scope of the GL on security measures for their payment services but now fall under the scope of these GL for all activities, as well as investment firms. The "Guidelines on ICT and security risk management" (EBA/GL/2019/04) [20] outline how financial institutions should manage the ICT and security risks to which they are exposed, as well as providing them with a better understanding of supervisory expectations for ICT and security risk management.

These GL are one of three security-related mandates granted to the EBA by PSD2, and they were developed in close collaboration with the ECB. Access to accounts, as well as the initiation and execution of internet payments, are subject to additional control and security measures through the use of SCA and CSC channels

[18]. Certain PSD2 RTS on SCA and CSC (EBA/RTS/2017/02) were published in the Official Journal of the EU on March 13, 2018, and took effect on September 14, 2019 [21]. During the transition period, PSP could already provide their services under PSD2, but they were not legally required to implement the necessary security measures. In addition to the RTS, the EBA issued an Opinion on June 13, 2018, to seek clarification in a number of areas related to the implementation of the RTS on SCA and CSC (EBA-Op-2018-04) [22]. The RTS, in particular, contains rules on SCA and CSC, as well as a number of exemptions/exceptions that PSP (i.e., the payer's and payee's PSP) may invoke in order to avoid performing SCA on a given action [23].

On the one hand, these SCA and CSC security measures include the issuance and use of SCA solutions, which enable authorization to be dynamically linked to the specific amount and payee [19]. SCA, in essence, allows payments to be made more securely by requiring higher levels of authentication when completing a transaction. PSP must implement SCA processes for customers who access their accounts online, initiate electronic payments, or conduct transactions via remote channels. Because these activities carry a high level of risk, PSD2 requires PSPs to implement appropriate security processes to reduce the risk of potential threats. Adopting appropriate SCA processes promotes user confidentiality and ensures the integrity of PSUs' PSC and communication between participants regarding transactions taking place on any particular platform [24]. PSPs must also use adequate transaction and device monitoring mechanisms to detect potentially unusual payment patterns. On the other hand, PSD2 requires the use of open and CSC standards in the context of security measures. Specifically, a standardized and dependable access interface to payment accounts (i.e., an application programming interface, API) should be provided so that, as secure identification of TPPs is permitted, so is related communication between all parties involved [25].

Banks can reduce the risk of security attacks on payment transactions by following an API architectural approach, with more layers of fraud protection and authentication, because they can integrate security features like access control and threat detection directly into data-sharing offerings, allowing them to be proactive rather than reactive [24]. With market agreement on a single technical specification, all systems in the EU can eventually be based on one or a few technical API standards.

The PSD2 security mandates, conferred on the EBA, are finally supplemented by the PSD2 major incident reporting GL (EBA-GL-2017-10) [26], which were published on July 27, 2017. To minimize the impact on users, PSPs are required to report major security incidents to the appropriate authorities as soon as possible. When a PSP becomes aware of a major operational or security incident, it should first notify its supervising authority, and then notify its customers, if the event affects their financial interests [19].

Consequently, the subsequent section will elucidate and offer a comprehensive assessment of the requisite IT security measures and controls that should be established for both PSP and users. This is aimed at achieving an acceptable level of risk tolerance, especially in relation to operational and security risk management, secure authentication processes, safeguarded communications, and protocols for reporting incidents [24].

4 An overview of the security measures under PSD2

PSD2 lays down the foundational principles (articles 65–67, 97–98) for the provision of third-party access to account (XS2A) services. To complement these general principles, the EBA's RTS for strong customer authentication (SCA) and common and secure communication (CSC) delve into the granularities of the implementation aspects. More precisely, these RTSs mandate that ASPSP, offering online payment accounts, must adhere to a set of predefined interface requirements. The following paragraphs will dissect each of these security requirements, while also highlighting their relevance as mandated by the specific articles and GL of PSD2 legislation [27].

4.1 Communication interface

When a bank provides its customers with online access to their payment accounts, is required by the EBA's SCA and CSC RTS to have at least one interface in place that allows PSP to access the accounts. Pursuant to article 30(1) of the RTS, the interface must enable secure communication with AISP, PISP, and PSP that issue card-based payment instruments. The aforementioned providers should also be able to identify themselves to the ASPSP via the interface. The dedicated user interface shall allow AISP and PISP to rely on the authentication procedures provided by the AISP to the PSU for PSU authentication. The interface must specifically allow a PISP or an AISP to instruct the ASPSP to begin authentication. Throughout the authentication, communication sessions between the ASPSP, PISP, AISP, and PSU must be established and maintained. Furthermore, the PISP or AISP must ensure the integrity and confidentiality of PSC and that authentication codes are transmitted by or through them.

Banks or ASPSP must ensure that their interface(s) adhere to communication standards issued by international or European standardization organizations. To that end, it should be ensured that the technical specification of the interface is documented and, at the very least, freely available upon request by authorized PISP, AISP, and PSP issuing card-based payment instruments or having applied for the relevant authorization with their NCA. This documentation shall specify a set of routines, protocols, and tools required by PISP, AISP, and PSP issuing card-based payment instruments in order for their software and applications to interact with the ASPSP' systems.

Finally, a documentation summary should be publicly available on their website. ASPSP must ensure that, except in emergency situations, any change to the technical specification of their interface is made available in advance to authorized PISP, AISP, and PSP issuing card-based payment instruments (or PSP that have applied with their NCA for the relevant authorization) as soon as possible and no less than 3 months before the change is implemented. PSP should also document emergency situations in which changes were made and make the documentation available to NCA upon request. Last but not least, ASPSP must provide a testing facility, including support, for authorized PISP, AISP, and PSP issuing card-based payment instruments, or PSP that have applied for the relevant authorization, to test their software and applications used to provide a payment service to users. The testing facility shall not be used to share sensitive information [21].

4.2 Dedicated interface

According to article 27(2) of the EBA's SCA and CSC RTS, ASPSP have implemented a dedicated interface. To ensure PSUs' right to use PISP and the respective services enabling access to account information, as referred to in Articles 66–67 of PSD2, it is necessary to require that the dedicated interface have the same service level as the interface available to the PSU, including the same level of contingency measures. To that end, ASPSP must monitor the availability and performance of the dedicated interface and provide the resulting statistics to the appropriate authorities upon request. In addition, if the dedicated interface does not operate at the same level of availability and performance as the interface made available to the ASPSP's user when accessing its payment account online, the ASPSP must report it to the CA, restore the level of service for this interface case without undue delay, and take any action necessary to prevent its recurrence. The report must include the reasons for the deficiency as well as the steps taken to restore the required level of service. Furthermore, after reporting to the ASPSP, PSP that use the dedicated interface offered by the latter may also report to the NCA any deficiencies in the level of availability and performance required of the interface [28].

Finally, ASPSP have to include a strategy and plans for contingency measures in the design of the dedicated interface in the event of an unplanned outage of the interface and system breakdown. The strategy must include communication plans to notify PSP who use the dedicated interface in the event of a breakdown, measures to restore the system to normal operation, and a description of alternative options for PSPs that can be used during unplanned downtime [21].

4.3 TTP user management, access control, and identification

ASPSP must allow legitimate TPP to access their accounts without any contracts or barriers. To protect their customer resources and infrastructure, ASPSP must treat all unknown entities as potential malicious actors until they can verify the entity's identity and validate their regulatory access. To avoid potential threats such as denial of service (DoS), data loss, or privilege elevation, solutions that keep the ASPSP secure while granting XS2A API access to authorized third parties are required. Given the seriousness of these threats and their consequences for ASPSP and customer resources, ASPSP should be able to identify a TPP each time they attempt to connect, as well as block unknown entities, or provide access to known and trusted TPPs with valid access credentials. The process of verifying a TPP's identity and access rights is described in the EBA's RTS for SCA and CSC under PSD2 [29].

4.4 Secure communication session

The establishment of secure communication among the relevant entity providers allows AISPs to securely request and receive information on one or more designated payment accounts and associated payment transactions, and PISPs to safely initiate a payment order from the payer's payment account and receive information on the initiation and execution of payment transactions. According to Article 30 of the EBA's SCA and CSC RTS, ASPSP, PSP issuing card-based payment instruments, AISP, and PISP must ensure that, when exchanging data via the Internet, secure encryption is used between the communicating parties throughout the respective communication session to safeguard the confidentiality and integrity of the data, using strong and widely recognized encryption techniques [30]. By establishing transmission control protocols (TCP) and open systems interconnection (OSI) protocols, which can be used in combination at various network layers of the XS2A Communications Infrastructure, internet communication sessions over the XS2A and Internet banking can also maximize their security and maintain their stability and interoperability [31].

In addition, PSP issuing card-based payment instruments, AISP, and PISP must keep ASPSP access sessions as short as possible and actively terminate the session with the relevant ASPSP as soon as the requested action is completed. AISP and PISP must ensure that when maintaining parallel network sessions with the ASPSP, those sessions are securely linked to relevant sessions established with the PSU, to avoid the possibility of any message or information communicated between them being misrouted.

Furthermore, it is critical that the providers of AIS, PIS, and CBPII, as well as the ASPSP, include unambiguous references to each of the following items:

- The PSU or users, as well as the corresponding communication session, to distinguish multiple requests from the same PSU or users
- The uniquely identified payment transaction initiated for PISs
- For confirmation of fund availability, the uniquely identified request related to the amount required for the card-based payment transaction

Last but not least, AISP, PISP, and PSP that issue card-based payment instruments must ensure that PSC and authentication codes are not readable by any staff at any time. AISP, PISP issuing card-based payment instruments, and PISP shall promptly notify the payment services user associated with them and the issuer of the PSC if the confidentiality of PSC within their sphere of competence is breached.

4.5 Data exchanges

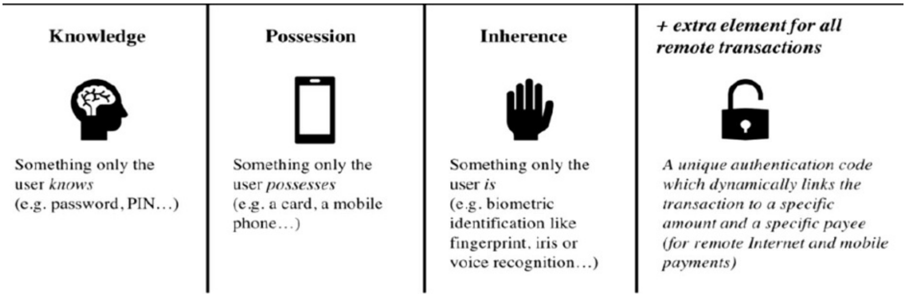
To access payment accounts and statement details, as well as other account information held by banks and ASPSP, traditional PSP typically need to share and exchange certain data with those TPP under PSD2. To that end, EBA has dedicated a section of the SCA and CSC RTS to addressing the issue of data exchanges, so that ASPSP are aware of the specific requirements with which they must comply. Firstly, they must provide AISP with the same information from designated payment accounts and associated payment transactions that the PSU makes available when directly requesting account information, provided that this information does not include sensitive payment data. Similarly, the same information should be provided to PISP as soon as the payment order is received. When the transaction is initiated directly by the PSU, this information refers to the initiation and execution of the payment transaction provided or made available to it. PISP must now provide ASPSP with the same information that the PSU requests when initiating the payment transaction directly. This case applies unless the PISP, the payer, and ASPSP agree otherwise regarding the collection of additional information for the purposes of providing the PIS.

However, a number of respondents have inquired about the specific type of information included in the data exchange. They needed to clarify if it included information for overdraft limits, waiting transactions (those with future execution dates), failed transactions, standing orders and their details, direct debit authorizations, a list of associated payment instruments, and so on. According to the authority's analysis, because ASPSP have different online platforms for their PSU, with potentially different information, and because PSD2 does not harmonize the information, the RTS can only require that if the ASPSP provides a dedicated interface, the information be "the same information" as what is available under the customer online interface.

Moreover, when a payment transaction is about to be executed, ASPSP must immediately confirm to PSP whether the amount required for this execution is available on the payer's payment account. This confirmation must be as simple as a 'yes' or 'no' response. In the event that unexpected events or errors occur during the process of identification, authentication, or data element exchange, the ASPSP shall send a notification message to the PISP or AISP, as well as the PSP issuing card-based payment instruments, explaining the reason for those unexpected events or errors. Where the ASPSP provides a dedicated interface for SCA and CSC, in accordance with Article 28 of the EBA RTS, the interface shall provide for notification messages concerning unexpected events or errors to be communicated to the other PSP participating in the communication session by any PSP that detects the event or error.

ASPSPs must also have appropriate and effective mechanisms in place to prevent access to information other than from designated payment accounts and associated payment transactions, with the user's explicit consent. It should be noted that explicit consent is required in three situations mentioned in three different PSD2 Articles (65–67). Finally, AISP must be able to access information from designated payment accounts and associated payment transactions held by ASPSP in order to perform the AIS in either of the following scenarios:

- Whenever the PSU actively seeks such information
- No more than four times in a 24-h period where the PSU is not actively requesting such information unless a higher frequency is agreed upon between the AISP and the ASPSP with the PSU's consent [32]



Knowledge

Something only the user *knows* (e.g. password, PIN…)

Possession

Something only the user *possesses* (e.g. a card, a mobile phone…)

Inherence

Something only the user *is* (e.g. biometric identification like fingerprint, iris or voice recognition…)

+ extra element for all remote transactions

A unique authentication code which dynamically links the transaction to a specific amount and a specific payee (for remote Internet and mobile payments)

Fig. 8 Factors for strong customer authentication [33]

4.6 Strong customer authentication (SCA)

PSD2 seeks to strengthen security in payments and of customers' personalized credentials by mandating SCA or, as it is sometimes referred to: "2 Factor Authentication", as an integral component of opening up the payments market to TPPs through CSC provided by the third-party interface. SCA undoubtedly played a significant role in the changes and innovative initiatives established by PSD2's new security obligations [35].

SCA, as defined in PSD2 Article 4(30), is a multi-factor authentication based on the use of two or more elements to validate the user or the transaction. The factors for strong customer authentication are analyzed in Fig. 8.

These elements are independent in the sense that a breach of one element does not compromise the reliability of the others, and they are designed to protect the confidentiality of the authenticated data [34]. In other words, the vulnerability of one authentication factor should not compromise the security of the second. Solutions that combine knowledge and possession factors with weak protection do not typically meet this requirement [35]. For remote transactions, such as online payments, the security requirements go even further, requiring a dynamic link between the amount of the transaction and the payee's account to further protect the user by minimizing risks in the event of errors or fraudulent attacks. Furthermore, in response to continuing market actors' inquiries about which authentication approaches the EBA considers to be SCA-compliant, and in order to facilitate proper and timely implementation, the EBA published an opinion on the elements of SCA under the PSD2 on 21 June 2019 [36].

SCA is a key requirement of the EBA GL because it protects customers from fraud, builds trust in the internet payment ecosystem, and protects sensitive data. Overall, the core principle of SCA is to reduce the risk of fraud and protect the confidentiality of the user's financial and personal data while having as minimal impact on the customer experience as possible, i.e., without introducing too much friction into the payment process. According to Article 97 PSD2 (Authentication), an SCA is required whenever PSU (individually or through an intermediary) access their payment account online, trigger/initiate an electronic payment process, or engage in an act involving the risk of fraud in payment transactions or other misuse via remote access. The elements "amount" and "payment recipient" must be dynamically incorporated into the data submitted for authentication in the case of a remote payment operation [37]. Authentication refers to procedures that enable a PSP to verify a PSU's identity or the validity of using a specific payment instrument, including the use of user-personalized security details.

4.7 Transaction monitoring

PSPs must put in place a transaction monitoring mechanism to detect unauthorized or fraudulent payment transactions in order to implement the security measures referred to in SCA. This transaction monitoring mechanism, in particular, should be based on an analysis of payment transactions that consider elements that are typical of the PSU in the context of normal use of the PSC by the PSU. The PSPs must ensure that the transaction monitoring mechanisms consider, at a minimum, the following risk-based factors:

- Lists of authentication elements that have been compromised or stolen
- The total value of each payment transaction
- Known fraud scenarios in payment service provision
- Signs of malware infection in any authentication procedure session

Furthermore, where PSP exempt the application of the SCA security requirements in accordance with Article 16 "Transaction risk analysis" of the EBA's RTS, they must ensure that the transaction monitoring mechanisms consider, at a minimum, and in real-time, each of the risk-based factors listed below:

- The individual PSU's previous spending patterns
- The payment transaction history of each PSU of the PSP
- The payer's and payee's location at the time of the payment transaction, if the PSP provides the access device or software
- The PSU's abnormal payment patterns in relation to the payment transaction history
- If the PSP provides the access device or software, a log of the PSU's use of the access device or software, as well as any abnormal use of the access device or software

Finally, electronic payment services must be carried out in a secure manner, using technologies capable of ensuring the safe authentication of the user and reducing the risk of fraud to the greatest extent possible. The authentication procedure must include, in general, transaction monitoring mechanisms to detect attempts to use a PSU's PSC that were lost, stolen, or misappropriated, as well as mechanisms to ensure that the PSU is the legitimate user and thus consenting to the transfer of funds and access to its account information through normal PSC use.

4.8 Security measures review

Because fraud methods are constantly evolving, the requirements for SCA should allow for innovation in technical solutions to address the emergence of new threats to electronic payment security. To ensure that the requirements of this regulation are effectively implemented on a continuous basis, it is also appropriate to require that the security measures for the application of SCA and its exemptions, the measures to protect the confidentiality and integrity of the PSC, and the measures establishing CSC be documented, tested, evaluated, and audited on a regular basis by internal or external independent and qualified auditors. Such a review can be carried out in accordance with the PSP's applicable audit framework.

Also, the interval between audit reviews must be determined in accordance with the relevant accounting and statutory audit framework applicable to the PSP. PSP that make use of Article 16 exemption should conduct an audit of the methodology, model, and reported fraud rates at least once a year. It should also be noted that the audit review will evaluate and report on the PSP's security measures' compliance with the requirements outlined in this regulation. NCA should have full access to this report upon request.

4.9 Dynamic linking

Because electronic remote payment transactions are more vulnerable to fraud, additional requirements for the SCA of such transactions are required, ensuring that the elements dynamically link the transaction to an amount and a payee specified by the payer when initiating the transaction. By imposing this requirement, Articles 97(2) of PSD2 and 5(1) of the RTS strengthen the required authentication. Dynamic linking is enabled by the generation of authentication codes, which are subject to stringent security requirements. This means that the generated authentication code must be associated with a specific amount and payee. Any modification should render it null and void. This establishes the payment order's "integrity". The RTS, on the other hand, does not appear to require that third parties, such as banks, be able to verify the authentication or integrity of the payment order. This obligation exists only in the user's relationship with the authenticating PSP. It does not, for example, require that the authentication code be secured by a digital signature or another specific technique that establishes "non-repudiation". The RTS most likely does not impose this requirement because digital signature technology is not widely used yet, or because it must remain technologically neutral. As a result, as long as the security requirements are met, authentication codes should be based on solutions such as generating and validating one-time passwords, digital signatures, or other cryptographically underpinned validity assertions using keys and/or cryptographic material stored in the authentication elements.

Furthermore, the PSP is required to inform the payer of the amount and the payee. The generated authentication code must be specific to the amount of the payment transaction and the payee specified by the payer when initiating the transaction. Finally, the authentication code accepted by the PSP corresponds to the original specific amount of the payment transaction as well as the payee specified by the payer. Any changes to the amount or payee will render the generated authentication code invalid. Pursuant to RTS Article 5(2), the PSP should implement security measures to ensure the confidentiality, authenticity, and integrity of the amount, payee, and displayed information during all phases of authentication, including the generation, transmission, and use of the authentication code [21]. For the purposes of these requirements, and where PSPs use SCA in accordance with Article 97(2) of PSD2 in relation to a card-based payment transaction for which the payer has given consent to the exact amount of funds to be blocked in accordance with Article 75(1) of that Directive, the authentication code must be specific to the amount that the payer has given consent to be blocked and agreed to by the payer when initiating the transaction. Similarly, when SCA is used in accordance with Article 97(2) of PSD2 for payment transactions in which the payer has given consent to execute a batch of remote electronic payment transactions to one or more payees, the authentication code must be specific to the total amount of the batch of payment transactions as well as to the payees specified [29].

Although Article 5 of the RTS only applies to electronic remote payment transactions, the underlying principles are applicable to AIS as well. In this case, a change in the privileged service provider or the scope of access would render the authentication code invalid. Furthermore, the user must be made aware of the privileged provider and the precise scope of the access throughout all phases of the authentication. Overall, dynamic linking is important for SCA implementation, not only because it provides additional security guarantees (non-repudiation), but also because signed statements can be passed on by the PSP and verified by the bank itself. Without this requirement, the RTS cannot eliminate the additional risks posed by allowing PSP to use their own authentication procedures [21].

4.10 SCA interface implementation

The bank's SCA interface should allow PSPs to rely on all of the authentication procedures that the bank provides to the user. This option makes it easier to provide payment services. It enables a PSP to provide services without developing and deploying its own SCA. PSP can instruct the bank to initiate the authentication procedure in conjunction with the payment order or request for information. Nonetheless, even after the release of the EBA's draft RTS, it remains unclear how this authentication should be resolved and what the authentication technologies should eventually look like. However, Figs. 9 and 10 highlight the most significant variations.

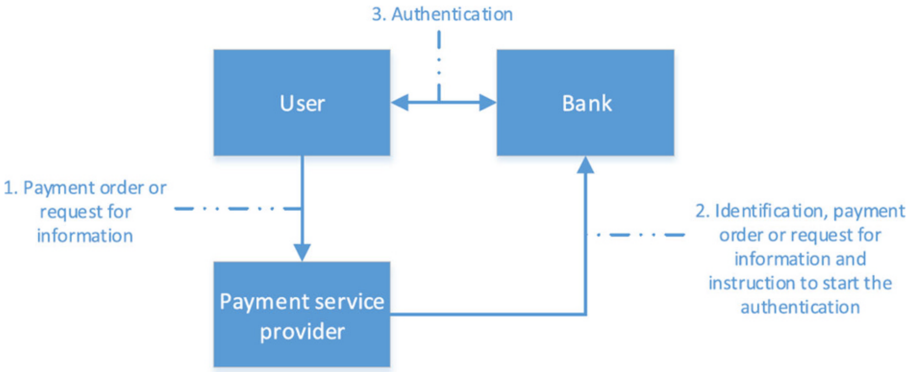

3. Authentication
User
Bank
1. Payment order or request for information
2. Identification, payment order or request for information and instruction to start the authentication
Payment service provider

Fig. 9 Strong customer authentication interface: redirection or decoupled approach [21]

According to RTS Article 30(2)(b), the interface should establish and maintain communication sessions between the bank, PSP, and the user. The existence of a communication session between the bank and the user implies that the authentication can be resolved without involving the PSP. Instead, the PSP redirects the user to the bank or uses a decoupled approach for authentication. The decoupled interface approach can be based on other technical interfaces in accordance with PSD2 Articles 66–67 by using a federation protocol, such as Security Assertion Markup Language (SAML) or OpenID Connect (OIDC), which is based on the OAuth 2.0 Authorization Framework. These standardized, simple, and user-driven authentication protocols and frameworks enable authentication and authorization without revealing the user's PSC to TPPs [40]. As a result, this is consistent with the PSD2 goals. An AISP may not request sensitive payment data, including PSC, and a PISP may not store it. Furthermore, at the time of the authorization application, Article 5(1)(g) of the PSD2 requires a PI to submit a description of the process used to restrict access to sensitive payment data [38].

The system of Fig. 9 keeps security risks to a minimum. Potential attackers cannot steal or intercept security credentials from the PSP because the PSP does not have access to them and cannot abuse them. These benefits are lost if the authentication, including the PSC issued by the bank, is handled entirely or partially by the PSP using an embedded approach. This system also makes it easier to commit fraud. Prior to PSD2, banks warned customers not to share their PIN or other security credentials with anyone. These warnings cannot be issued if the PSD2 allows the Fig. 10 system. This allows a criminal to impersonate a legitimate PSP in order to induce a user to share his PSC.

Several norms indicate that this system is permissible. Articles 66(3)(b) and 67(2)(b) of the PSD2 state that PSP must ensure that PSC are not accessible to anyone other than the user and the issuer of the credentials. Furthermore, the articles require them to send security credentials via secure and efficient channels. Following that, Article 30(2) of the RTS states that the interface must ensure the integrity and confidentiality of credentials transmitted by or through PSP. Finally, in accordance with Article 35(5) of the RTS, PSP must ensure that transmitted PSC and authentication codes are not readable by any staff at any time. They are required to notify the user and the issuer if the confidentiality of credentials within their sphere

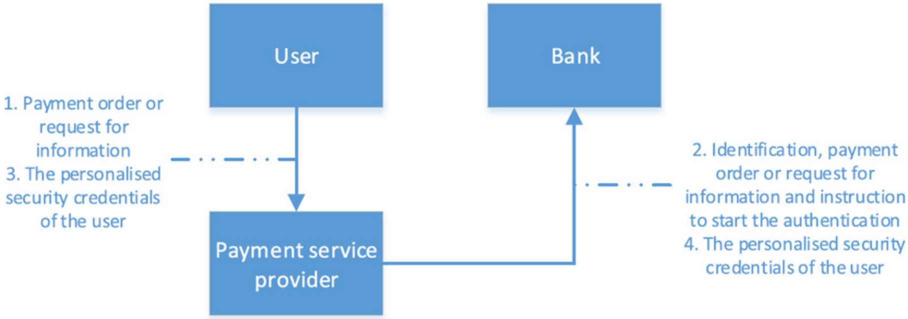

User
Bank
1. Payment order or request for information
3. The personalised security credentials of the user
Payment service provider
2. Identification, payment order or request for information and instruction to start the authentication
4. The personalised security credentials of the user

Fig. 10 Strong customer authentication interface: embedded approach [21]

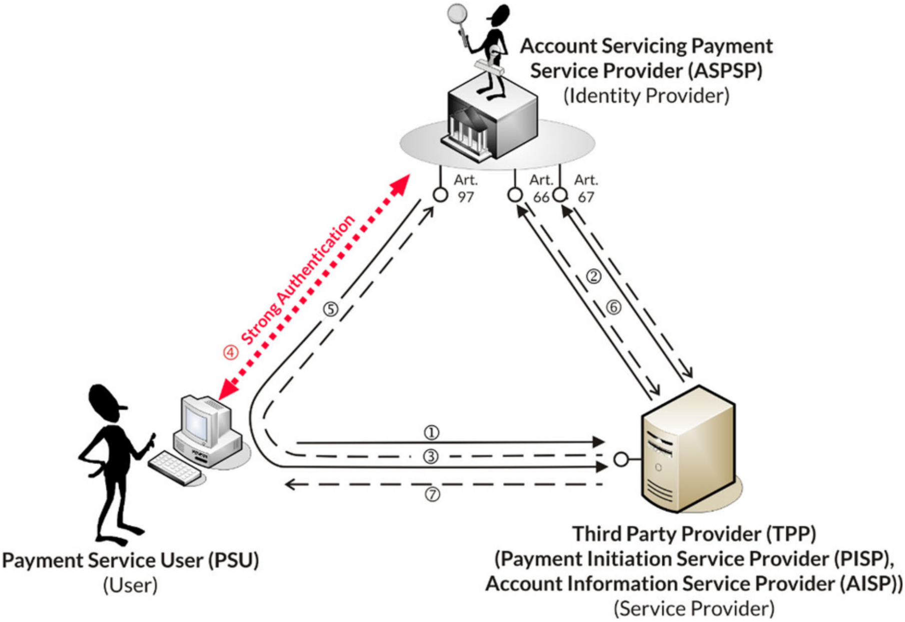

Account Servicing Payment Service Provider (ASPSP)
(Identity Provider)
Art. 97
Art. 66
Art. 67
④ Strong Authentication
⑤
②
⑥
①
③
⑦
Payment Service User (PSU)
(User)
Third Party Provider (TPP)
(Payment Initiation Service Provider (PISP), Account Information Service Provider (AISP))
(Service Provider)

Fig. 11 Co-operation between PSU, TPP and ASPSP (PSD2 [36])

of competence is compromised. These standards demonstrate that PSP can act as an intermediary in an authentication procedure provided by another party, such as a bank [21].

Figure 11 depicts the “triangular relationship” implied by Article 97(5) PSD2 and Article 27(3)(a) between the PSU (User), the TPP (service provider), and the ASPSP (identity provider). Among the currently relevant international standards that enable strong authentication, the “triangular” relationship depicted in Fig.11, the aforementioned SAML Version 2.0 and the OAuth 2.0-based OpenID Connect deserve special mention. While the two protocols differ in technical details, they both support the architecture depicted in the figure and thus could serve as the foundation for the implementation of PSD2-specific interfaces. Thus, it is theoretically possible to specify a corresponding PSD2 interface based on both SAML and OAuth 2.0/ OpenID Connect, with technical interfaces based on both SOAP and REST-based web services [36].

4.11 Security and operational risk management

While many regulated financial institutions (FI; including PSP) will have policies, systems, and controls in place to manage operational and security risks, PSD2 solidifies the requirements with EBA guidance. The main requirement of these provisions is the creation and maintenance of a risk management framework document. An updated version of the framework document must be submitted to the PSP NCA at least once a year. In doing so, the PSP must also comment on the sufficiency of the mitigation and control mechanisms put in place in response to those risks.

This will entail some kind of auditing function. In order to meet these requirements, the EBA issued the GL mandated by Article 95 of PSD2, subject to the principle of "proportionality". This means that all PSPs will have to comply with each GL. The level of detail should be proportionate to the size of the PSP as well as the nature, scope, complexity, and riskiness of the specific services that the PSP offers or intends to offer. The final GL cover a wide range of security topics, including governance, risk assessment, risk control and mitigation, incident monitoring and reporting, sensitive payment data protection, security measure testing, outsourcing, and customer awareness, education, and communication. Other recent requirements include business continuity management, scenario-based continuity plans, situational awareness, and continuous learning for a PSP's own personnel, partners, and external stakeholders. The openness promoted by PSD2 is not without risks.

5 PSD2 compliance and further interrelation with cybersecurity frameworks and standards

Over the past few years, we have witnessed transformative legislative efforts in the EU to promote open banking, enhance cybersecurity and protect personal data. PSD2 is at the heart of this movement, with its objective of fostering competition and innovation in the payment services sector. Yet, alongside PSD2's vision for a more integrated and efficient payment market, there's a broader narrative unfolding—one that considers the imperative to secure digital transactions and protect sensitive personal data. In this regulatory landscape, instruments such as the Network and Information Security (NIS) 2 Directive [37], the EU Cybersecurity Act [38], and the General Data Protection Regulation (GDPR) [39] have emerged as foundational pillars.

5.1 PSD2 and NIS2: synergies and challenges in financial services and network security

The EU has persistently been at the forefront of legislating innovative and holistic regulations that address the evolving challenges of the digital era. The NIS2 Directive is a vital evolution in the EU's approach to network and information security, building upon its predecessor, the Directive on Security of Networks and Information Systems (NIS) Directive. The NIS Directive was the first legislative initiative focused on cybersecurity with the aim to enhance the security of network and information systems across the EU. Recognizing the evolving challenges in the digital landscape, the European Commission proposed a revised version of the Directive.

NIS2 expands upon the entities that fall under its purview. While the original NIS Directive focused on operators of essential services (OES) and digital service providers (DSP), NIS2 broadens this to encapsulate other vital entities, like medium and large-side entities, public administrators and more [40]. NIS2 mandates stricter security requirements, necessitating entities to implement measures that address both cyber and physical resilience [41]. It advocates for a risk management approach tailored to the specific threat landscape of each sector. NIS2 also introduces stricter incident reporting requirements. Entities must report any significant incident to competent authorities, ensuring that a comprehensive picture of the cybersecurity landscape within the EU is maintained [42]. The authorities are granted increased powers under NIS2. They can not only issue binding instructions but also impose sanctions for non-compliance [43]. The Directive emphasizes enhanced cooperation among MS. This includes the sharing of best practices, threat intelligence, and coordinated responses to significant cross-border incidents [44]. The NIS2 Directive underscores the EU's commitment to ensuring a high common level of cybersecurity across member states. By recognizing the changing threat landscape and expanding its scope, the directive aims to create a more resilient and unified digital space within the EU.

PSD2 and NIS2 stand as testimonies to the EU's commitment towards promoting both financial innovation and cyber resilience. Unravelling the interconnections between these two Directives elucidates a comprehensive approach to secure digital finance. PSD2, building upon its predecessor, fosters a harmonized and integrated European payments market, aiming to increase competition and encourage payment innovations by integrating TPP into the ecosystem [45]. Simultaneously, NIS2, an evolution of the NIS Directive, accentuates the enhancement of cybersecurity and the fortification of essential and digital service providers against network and information system incidents. While PSD2 primarily targets payment service providers, including banks and TPP, NIS2's spectrum encompasses a broader range of entities, namely essential and digital service providers, which include cloud computing services, online marketplaces, and search engines. However, given the interwoven nature of the digital ecosystem, a breach in one sector (e.g., cloud services) could have repercussions for entities governed by PSD2, underlining the interconnected risk landscape.

Both Directives enforce rigorous standards for security and mandate timely incident reporting [46]. PSD2 requires payment service providers to establish robust security measures to manage operational and security risks. Similarly, NIS2 necessitates entities to implement adequate and proportionate security measures and notify competent authorities of any significant incidents [47]. While PSD2 places an emphasis on the integrity and confidentiality of payment service users' data, NIS2 accentuates the security of network and information systems, ensuring data availability. Both Directives, in essence, work conjointly to guarantee that financial transactions remain confidential and are perpetually available and resilient to disruptions [48].

NIS2 introduced a reinforced framework for cooperation among EU MSs, aiming to establish a culture of shared cyber threat intelligence. Given the cross-border nature of financial services, this collaborative approach significantly benefits entities under PSD2, enhancing their ability to anticipate, defend against, and respond to cyber threats. The confluence of PSD2 and NIS2 underscores the EU's comprehensive vision of a digital single market that is both innovative and secure. By understanding the intricate mesh of financial services and cyber security articulated by these directives, stakeholders can harmonize their strategies to thrive and safeguard their operations in the increasingly interconnected digital landscape [49].

5.2 PSD2 and the EU cybersecurity act: converging pathways in the modernization of financial cybersecurity

The EU Cybersecurity Act represents a milestone in strengthening the EU's cybersecurity architecture, which encompasses the framework for establishing European cybersecurity certification schemes. Originally came into force in 2019, the Cybersecurity Act forms a part of the European Union's initiative to improve the digital single market's resilience against cyber threats. The Act bestows the European Union Agency for Cybersecurity (ENISA) with a permanent mandate and institutes a framework for European cybersecurity certification schemes for ICT products, services, and processes. The aim of the Act is to strengthen ENISA's cybersecurity instrumental role in setting up and maintaining the European cybersecurity certification framework. Additionally, the Agency engages in raising cybersecurity awareness and helping organize annual EU-wide cybersecurity exercises.

The Act's cornerstone is the European cybersecurity certification framework, aiming to harmonize the cybersecurity certification landscape across EU MSs. It promotes mutual recognition of certifications among MSs, reducing barriers to trade and fostering a high level of cybersecurity in the EU. The framework is inherently voluntary, meaning that businesses can choose whether or not to certify their ICT products, services, or processes. The Act introduces three distinct assurance levels: basic, substantial, and high. These levels are dependent on the risk associated with the intended use of the ICT product, service or process. A publicly accessible registry maintained by ENISA lists all the certification schemes, ensuring clarity and transparency for all stakeholders. The EU Cybersecurity Act signifies a pivotal moment in the evolution of the EU's cybersecurity paradigm. By bolstering ENISA's position and introducing a comprehensive certification framework, the Act seeks to instill a consistent level of cybersecurity assurance, promote trust, and facilitate a seamless digital single market.

While PSD2 focuses on creating a more integrated and efficient European payments market, the EU Cybersecurity Act seeks to fortify the overall cybersecurity landscape of the EU digital single market. Together, they represent the EU's commitment to advancing digital innovation securely. PSD2, besides its financial integration objectives, is particularly prescriptive about security. With the rise of open banking, where TPPs can access bank customer's data, the security implications are profound [50]. PSD2 mandates the application of SCA for electronic payment transactions, ensuring enhanced security for users [18]. In addition, payment service providers under PSD2 are required to report major operational and security incidents to their national competent authorities [51]. The EU Cybersecurity Act's aim is to establish a common cybersecurity certification framework for products, services, and processes [52]. While its scope is broader and not limited to financial services, its provisions do apply to entities governed by PSD2. The framework is designed to harmonize cybersecurity certification procedures across the EU, promoting consistent security standards [53]. The strengthened position of ENISA as an advisory body means that sectors, including finance, can benefit from its expertise [54]. While both regulations converge on the goal of enhancing cybersecurity, they cater to different needs. PSD2 is sector-specific, addressing unique risks inherent to the financial sector. In contrast, the Cybersecurity Act provides a broader framework applicable to a diverse range of digital products and services. However, entities under PSD2 can leverage the certification framework established by the Cybersecurity Act to demonstrate compliance with cybersecurity standards [55]. Conclusively, the synergy between PSD2 and the EU Cybersecurity Act underscores the European Union's holistic approach to digital transformation. While PSD2 addresses the financial sector's specific needs, the Cybersecurity Act lays the foundation for a secure and resilient digital single market.

5.3 PSD2 and GDPR: collisions between financial innovation and data privacy

PSD2 and the EU's GDPR 2016/679 [39] emerged in close succession and have notably reshaped the financial and data privacy landscapes. However, their simultaneous implementation has unveiled various intersections, challenges and synergies. Fundamentally, both regulations aim to fortify consumer rights. While PSD2 aspires to establish a unified EU payments market, ensuring heightened competition and innovation, the GDPR primarily seeks to empower EU citizens regarding their data privacy rights [56]. The security of sensitive payment data and user personal information becomes critical necessitating the implementation of protective measures within the framework of PSD2 and GDPR. PSP, in particular, should ensure that the collection, routing, processing, storing and/or archiving, and display of sensitive payment data of the PSU is adequate, relevant, and limited to what is required for the provision of its payment services [52]. Article 94 of PSD2 sets the overarching standard for data protection within the applicable legal context, compelling PSP to access, manipulate, and preserve only the personal data that is necessary for the delivery of payment services and only with the explicit authorization of the PSU. Additionally, all activities involving the processing of personal data under PSD2 must comply with the EU's GDPR 2016/679 [39]. Both regulatory frameworks—PSD2 and GDPR—are designed to bolster data protection by placing data subjects at the core and requiring their consent to capture, store, or process any data.

More specifically, both regulations underscore the significance of explicit and informed consent [57]. With PSD2 ushering TPPs into the payment realm, these TPP (PISP and AISP) can access consumers' bank account data for services such as account aggregation or initiating payments, but only with the customer's explicit consent [58]. According to Article 33(2) PSD2, AISPs are not bound by Article 94 PSD2. However, Article 67 PSD2 explains AISPs' obligation to obtain explicit consent from their users before providing AISs. Despite the fact that it is widely accepted that Article 94 PSD2 will not be applied to AISPs, particularly Article 94(2) PSD2, *"PSPs shall only access, process and retain personal data necessary for the provision of their payment services, with the explicit consent of the payment service user"*, AISP (as well as PISP and banks) must still follow the GDPR data processing principles. To comply with GDPR, PISP, AISP, and banks must also fully implement data protection '*by design and by default*', as well as recent data protection-oriented technology. In other words, even if PSD2 did not include a data protection provision, TPP and banks would still be required to access, process, and retain personal data required for the provision of payment services in accordance with GDPR requirements. Furthermore, when AISP are exempted from Article 94 PSD2, there is no meaningful explanation or benefit to be gained. To clarify the situation, the European Data Protection Board (EDPB) acknowledged that obtaining explicit consent is required for AISP to provide AIS under PSD2, *"Pursuant to Article 33 (2) of the PSD2, this requirement of the explicit consent of the payment service user does not apply to AISP. However, Article 67 (2)(a) of the PSD2 still provides for explicit consent for AISP for the provision of the service"*. Thus, it is accepted, similarly to the approach of the EDPB and the GL, that explicit consent is directly about providing a contractual service rather than processing users' personal data. As a result, it is preferable for TPP to use the GDPR's "necessary for the performance of a contract" legal basis for data processing operations [60].

Furthermore, according to PSD2 Article 94(2), PSPs may only access a user's personal information with that user's express consent to provide their services. The PSD2 is more stringent than the GDPR in this regard. Processing is permitted in accordance with Article 6(1)(a) and (b) of the GDPR if the data subject (customer/user/PSU) has consented to it or if it is required for the performance of a contract to which the data subject is a party. Both requirements must be satisfied, according to Article 94(2) of the PSD2. Additionally, it calls for explicit consent (in some circumstances that have previously been discussed in earlier sections). The EDPB claims that this is a contractual condition that differs from the GDPR's definition of (explicit) permission. The GDPR consent is just one of the grounds available and applies to the processing of personal data generally. PSD2's reference to consent relates to payment services. The data subjects must be fully informed of the purposes for which their personal data will be collected, used, processed, and disclosed prior to signing a contract with a PSP. Their personal data will also be utilized in this regard for marketing and sales opportunities. To make it simple for individuals to understand the implications of open banking and to give informed, meaningful consent, notifications and consent requests must be kept to a single screen or page [61]. This notification must be fulfilled by stipulations that are clearly identifiable from the rest of the contract's provisions, and consent may be withdrawn at any moment. Article 7 of the GDPR requires ASPSPs, who are data controllers, to be able to establish that permission was freely provided. These provisions must be explicitly agreed upon by the data subjects. According to Article 94(1), consent is not required for the processing of personal data necessary for the prevention, investigation, and detection of payment fraud. TPPs must align their consent mechanisms with the mandates of both PSD2 and GDPR, ensuring provisions for easy withdrawal of consent as stipulated by the GDPR [46]. Balancing this PSD2's requirements, especially when TPPs seek extensive data for innovative services, is a challenge that calls for careful data management strategies [59].

Moreover, it is important to understand what constitutes "sensitive payment data" under PSD2. The Directive includes a definition of "sensitive payment data", however, this only applies to PSC that could be used to commit fraud and is distinct from the concept of "special categories of personal data" as defined in GDPR Article 9(1). As a result, it makes no difference what types of data will be exchanged with TPP. However, some data types are more privacy sensitive than others and may cause more risks for data subjects. In this instance, data subjects should be able to select the specifics of the shared data while providing explicit consent under PSD2 [39].

From the ASPSPs' perspective, there is a legal requirement to share the data with the TPP under the rules of PSD2. Other than consent, this gives a valid basis for the processing. Indeed, PSD2 (Articles 66(1) and (4), as well as Article 67(1)) requires ASPSPs to send all necessary data to the AISP or PISP. The legal obligation to allow access to payment data and send payment data to TPP also serves as a legitimate basis for processing personal data under the GDPR (see GDPR Articles 6(1)(c) and 6(3)(a)). Once a TPP obtains access to a PSU's personal data, the TPP assumes its own duties as a controller in the processing of these data. At that point, it must be understood that, under PSD2, both the ASPSP and the TPP are controllers in their own right, and each is responsible for its own processing (but not the processing of the other party). Furthermore, the TPP is a licensed (or registered, in the case of AISP) company, its actions are overseen by the national supervisory authority, it is not chosen by the ASPSP, and it is a compulsory interlocutor for the ASPSP. As a result, while ASPSPs are responsible for ensuring that the interfaces they provide work, they are not required by PSD2 to verify a TPP's GDPR compliance.

The GDPR requires ASPSP to ensure the security of data flows. PSD2 and the RTS for SC and CSC establish particular standards for ensuring the security of data transfers from ASPSP to TPP (PISPs and AISP are also required to ensure secure data transfers). As a result, compliance with the RTS requirements, particularly the CSC must be regarded as sufficient for the ASPSP to meet GDPR requirements relating to the security of the transfer, especially given the ASPSP's legal obligation to allow access to the data under PSD2. However, because the RTS refers to both TPPs and ASPSPs as payment entities, both institutions are required to follow the set-out standards. Compliance with PSD2 and the RTS provides a legal foundation for data transfer from ASPSP to PISP or AIS. Furthermore, PSD2 and GDPR both mandate the minimization of personal data processing. GDPR's core principle of data minimization suggests that only essential data should be processed [60]. TPP are only permitted to access personal data for the purpose(s) expressly requested by users. PSD2 states that data should not be used for any reason other than providing the service requested by the PSU, and hence additional uses are incompatible. This signifies that "further processing" is subject to limitations. In this case, the user must either consent under Article 6(1) of the GDPR or the processing must be mandated by EU or MS law to which the controller is subject, such as anti-money laundering or terrorist financing laws. When a payment firm depends on consent, it must meet the consent standards and, in particular, demonstrate that the PSU has a genuine option.

In addition, because each PI should have access to varied types and amounts of data based on the services they provide, they must closely adhere to all GDPR principles and standards while providing their services including data minimization and purpose limitation principles. If TPP can access all bank account data without restriction, this practice will violate GDPR principles and rules, particularly sensitive personal data processing and obtaining explicit consent in cases of automated decision-making, including profiling, which may have legal consequences for users and have a significant impact on them. Furthermore, no provision in PSD2 offers legal justification or exclusions for banks and TPP to share sensitive personal data and make automated decisions, including profiling. As a result, banks should take technical steps to isolate accounts that may contain sensitive personal data or data used to develop more accurate user profiles from conventional accounts. Banks and TPP shall also take the necessary precautions to avoid any access that may reveal sensitive personal data about users that is not required for contract fulfilment. Thus, technical solutions that may aid in the separation of data required for contract execution from unneeded and sensitive personal data should be implemented [39].

Moreover, for PI, the GDPR's data minimization criteria are consistent with PSD2's: only data required to initiate a payment transaction may be requested and accessed. This regulation must be followed, particularly when seeking access as indicated in the RTS on SCA (articles 33(4) and 33(5)) and the EBA's Opinion of 13 June 2018 (paragraph 26). For AIS, PSD2 states that the provider shall *"not use, access or store any data for purposes other than for performing the account information service explicitly requested by the payment service user, in accordance with data protection rules"*. Data minimization criteria will be supported by dedicated interfaces designed to allow TPP to request certain data sets in accordance with PSD2 rules. It should also be noted that other legal responsibilities than those provided by the PSD2 may apply. This is an example of a duty regarding data content in payment orders. Furthermore, in the context of AIS and PIS, the TPP offering these services bears the main responsibility for information provision to users. PSD2 creates standardized GL to ensure that TPP furnish PSU with required, adequate, and understandable information. Articles 44–45 state that, in the interest of efficiency, the required information shall be reasonably proportionate to the needs of the user and delivered in a standard format. The transfer of data from the ASPSP to the TPP could be termed "further processing" by the ASPSP. However, when expressing its approval to the TPP, the PSU should have received information on the data transfer. As a result, the ASPSP would be excused from explaining this a second time under GDPR Article 13(4). However, ASPSPs may mention in their privacy notices that a possible transfer to an AIS or PISP may occur (because of a legal obligation) [62].

The GDPR requires that data be securely stored and that after any legal, contractual, or regulatory retention limit has elapsed, the data be erased or de-identified. The security safeguards used must be proportionate to the sensitivity of the data. Finally, the GDPR grants an individual the right to be forgotten and, in certain circumstances, the right to be erased. However, due to the legal complexities involved, these rights are beyond the reach of an open banking framework. PSD2 open banking broadens traditional banking data flows by putting the clients at the centre and giving them control over their financial data [45]. Finally, both PSD2 and GDPR have breach notification provisions [63]. Establishing robust incident detection and reporting mechanisms that fulfill the requirements of both regulations is thus of paramount importance for entities in the payments arena.

Conclusively, despite potential conflicts, the regulations also offer synergies. A sound GDPR compliance program naturally reinforces compliance with PSD2's security provisions [64]. The GDPR's focus on data encryption and regular security assessments can enhance the measures stipulated by PSD2. Both PSD2 and GDPR underscore EU's dedication to promoting innovation while safeguarding citizen's data rights [65]. By addressing the intertwined challenges and capitalizing on the synergies between PSD2 and GDPR, organizations can effectively navigate this dual regulatory landscape.

5.4 A comparative analysis of PSD2 with ISO/IEC 27001:2022 and PCI DSS

To facilitate comprehensive and effective compliance with PSD2 among various FI, a high-level correlation and comparison between the security components addressed by the Directive and those highlighted in globally acknowledged and directly relevant Standards—specifically, payment card industry data security standard (PCI DSS) and ISO/IEC 27001:2022—is considered essential. A detailed analysis of all related standards, documents and guidelines is provided at the end in the Appendix, Table 1. This section delves into more critical thinking and analysis following a critical view on potential shortcomings and collisions, as a result of trying to implement PSD2 and/or PCI DSS over GDPR and current privacy laws, as transferred to each MS.

On the one hand, the PCI DSS is a security standard developed by the Payment Card Industry Security Standards Council (PCI SSC) tailored for entities and intermediaries processing credit or debit card transactions. This standard is a culmination of a collaborative effort among five leading global payment entities—American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and security procedures [47]. PCI DSS is designed to address the particular security threats and risks that exist in the payments industry. It sets forth guidelines for safeguarding payment card information and sensitive authentication data during its processing, storage, or transmission, coupled with verification techniques and guidelines to aid organizations in being informed of current payment data security threats [66].

ISO/IEC 27001, on the other hand, is the world's most well-known standard for information security management systems (ISMS). It has been designed to offer requirements for the establishment, implementation, maintenance, and continuous improvement of an ISMS. The adoption of an ISMS is a strategic decision for an organization, and its development and implementation are influenced by the organization's needs and objectives, security requirements, organizational procedures used, and the organization's size and structure. The ISMS protects the confidentiality, integrity, and availability of information through the use of a risk management process, giving interested parties confidence that risks are adequately managed. Because the ISO/IEC 27001 Standard is broadly focused on ISMS implementation, fulfilling the specified aims implicitly involves assurance that payment data is likewise protected [67].

A structured table which encapsulates the analysis of the security provisions of PSD2 and a high-level mapping and comparison between the security areas covered by the Directive and those covered by the two internationally recognized security standards is provided in the Appendix, Table 1. This mapping is based on the latest version v4.0 of PCI DSS, and the ISO/IEC 27001, using the new version of the Standard published on October 25, 2022 [68]. The mapping table compares each control of the two Standards to the PSD2 standards, as well as identifies and maps the applicable PSD2 requirements for each control by indicating which security controls contribute to PSD2 compliance and which contribute to PCI DSS compliance. The high-level correlation and comparison between the security components covers eight domains and can be used by stakeholders to demonstrate compliance and mitigate security risks. For example, the mapping can assist in determining where the installation of a specific security control from PCI DSS or ISO/IEC 27001 can satisfy a PSD2 need. Furthermore, these Standards may assist an entity in being better prepared for internal assessments performed in its organization to determine the effectiveness of PSD2 security measures employed. However, PCI DSS and ISO/IEC 27001 may not guarantee that the standards' implementation will cover all areas of PSD2 security requirements [68].

As a result, banks and organizations will have a better understanding of the solutions available to them for information security, risk management, and data protection. Banks could also be informed about the extent of their effective PSD2 compliance by implementing the two examined standards, allowing them to achieve efficiencies in their existing processes and controls. Finally, the research will produce results indicating (i) which PSD2 requirements are covered by the implementation of ISO/IEC 27001:2022 and PCI DSS, (ii) which are not covered, and/or (iii) which could potentially need further enhancement and improvement. Consequently, stakeholders will be equipped with a valuable reference tool, aiding them in harmonizing their security initiatives to meet the objectives laid out by PSD2 through the incorporation of these two standards [69].

6 Conclusion

The implementation of PSD2 aimed to revitalize the payments sector by fostering innovation and widening the competitive landscape for payment service providers (PSP). Given that third-party providers (TPP) operate by utilizing sensitive personal and financial data, the market is not only more accessible to an increased number of competitors but also inherently dependent on the IT frameworks of multiple entities, thereby raising several risk factors [28]. Prior to the advent of PSD2, banks monopolized the financial arena and controlled exclusive access to consumer accounts, while other PSP had no authorized access to such data. However, PSD2 has been a double-edged sword, offering significant advancements in information security and data protection, yet also generating uncertainty due to a lack of clarity and consistency in its regulations. While the EBA's regulatory technical standards (RTS) have attempted to clarify these ambiguities, they have not fully resolved questions regarding the technical security specifications required for full compliance.

The RTS mandate that ASPSP must provide TPP with access to their technical interfaces and a testing facility. However, the RTS only require compliance with communication standards, not a common API standard, opening the door for innovative solutions like API aggregation. This approach allows Fintech companies to serve as connectors between banks and other licensed startups, fostering a competitive and functional market in both API aggregation and consumer services. Considering a centralized authority to coordinate API implementation and performance could be a viable alternative. Instead of focusing on a single API standard, the EU may establish a central independent organization or empower existing entities to focus on API implementation and performance across banks. This would be analogous to the Open Banking Implementation Entity in the United Kingdom, which has enforcement powers from the Competition and Markets Authority and aided in the advancement of open banking at a faster rate than other comparable markets. A central independent entity might serve as a single reliable source of open banking data [68]. Following the work of the SPAA (SEPA Payment Account Access) MSG (Multi-Stakeholder Group), the EU should additionally define how existing standards organizations bodies should interact with norms set by the European Payments Council. The interrelationship among PSD2, ISO/IEC 27001:2022, and PCI DSS serves as a pertinent illustration of this necessity. Pursuing additional mapping of standards is imperative to discern areas within PSD2 that require refinement (such as the establishment of API standards) as well as to recognize which PSD2 security domains are already robustly fortified through established security controls (like ISO/IEC 27001 and PCI DSS).

An additional complexity presented by PSD2 pertains to the ambiguity surrounding what the final form of authentication technologies will be, even after the release of EBA's RTS. Article 97 of PSD2 outlines strong authentication, which is anticipated to be distinct from the technological interfaces mentioned in Articles 66–67, likely through the employment of federation protocols like SAML or OAuth 2.0 along with its extension OIDC. Both protocols, despite their technical differences and divergent standard approaches, could potentially fulfil this requirement and act as the backbone for specialized PSD2 interfaces. Consequently, it is conceivable to develop PSD2-specific interfaces using both SAML and OAuth 2.0/OpenID Connect, accommodating technical interfaces grounded in either SOAP or REST-based web services. Future research in PSD2 implementation architecture should delve into secure channel bindings featuring Holder-of-Key or the emerging Token-Binding. Another pivotal element in a decentralized PSD2 ecosystem is the trust relationship between ASPSPs and TPPs, which is expected to leverage qualified certificates for website authentication or electronic seals. Although this study only briefly addresses the topic, a more exhaustive examination involving data exchange and dynamic discovery via electronic seals and a unified European repository or trusted lists remains to be explored.

7 Appendix

Table 1 Comparison among PSD2, PCI DSS (v4.0), and ISO/IEC 27001:2022

PSD2		PCI DSS v4.0	ISO/IEC 27001:2022
Strong customer authentication and secure open standards of communication	Strong customer authentication (SCA)	Requirement 8 (8.2, 8.3): Identify and authenticate access to system components	A.5.14 Information transfer A.5.15 Access control A.5.16 Identity Management A.5.17 Authentication information A.8.5 Secure authentication
	Personalized security credentials protection	Requirement 2 (2.3, 2.6): Do not use vendor-supplied defaults for system passwords and other security parameters Requirement 3 (all): Protect stored cardholder data Requirement 4 (all): Encrypt transmission of cardholder data across open, public networks Requirement 8 (8.1, 8.2, 8.3, 8.5, 8.6, 8.7): Identify and authenticate access to system components	A.5.14 Information transfer A.5.15 Access control A.5.16 Identity management A.5.17 Authentication information A.5.18 Access rights A.5.34 Privacy and protection of PII A.8.2 Privileged access rights A.8.3 Information access restriction A.8.5 Secure authentication A.8.26 Application security requirements A.8.24 Use of Cryptography ISO 27701:2019—Clause 6.15.1.4 Privacy and protection of personally identifiable information ISO 27701:2019—Clause 7.2 Conditions for collection and processing ISO 27701:2019—Clause 7.3 Obligations to PII principals ISO 27701:2019—Clause 7.5 PII sharing, transfer and disclosure ISO 27701:2019—Clause 8.2 Conditions for collection and processing
	Open banking API standardization	Requirement 2 (2.2, 2.3): Do not use vendor-supplied defaults for system passwords and other security parameters Requirement 4: Encrypt transmission of cardholder data across open, public networks Requirement 6: Develop and maintain secure systems and applications	A.5.1 Policies for information security A.5.14 Information transfer A.5.16 Identity Management A.5.17 Authentication information A.5.37 Documented operating procedures A.8 Technological Controls
	TPP user management	Requirement 7 (7.2): Restrict access to cardholder data by business need-to-know Requirement 8 (8.1, 8.2, 8.6): Identify and authenticate access to system components	A.5.15 Access Control A.5.16 Identity Management A.5.17 Authentication information A.8.3 Information access restriction A.8.24 Use of Cryptography
	Secure communication session	Requirement 2 (2.3, 2.6): Do not use vendor-supplied defaults for system passwords and other security parameters Requirement 4 (all): Encrypt transmission of cardholder data across open, public networks Requirement 6 (all): Develop and maintain secure systems and applications	A.5.14 Information transfer A.8.24 Use of Cryptography A.8.26 Application Security Requirements

Table 1 (Continued)

PSD2		PCI DSS v4.0	ISO/IEC 27001:2022
	Data exchanges	Requirement 3 (3.1, 3.2): Protect stored cardholder data Requirement 7 (all): Restrict access to cardholder data by business need-to-know Requirement 8 (8.7): Identify and authenticate access to system components Requirement 10 (all): Track and monitor all access to network resources and cardholder data Requirement 11 (11.5): Regularly test security systems and processes Requirement 12 (12.8, 12.9): Maintain a policy that addresses information security for all personnel	A.5.14 Information transfer A.5.31 Legal, statutory, regulatory and contractual requirements A.6.8 Information security event reporting A.8.3 Information access restriction A.8.12 Data leakage prevention A.8.15 Logging A.8.16 Monitoring activities
Governance	Governance	Requirement 1 (1.5): Install and maintain a firewall configuration to protect cardholder data Requirement 2 (2.2, 2.5): Do not use vendor-supplied defaults for system passwords and other security parameters Requirement 3 (3.7): Protect stored cardholder data Requirement 4 (4.3): Encrypt transmission of cardholder data across open, public networks Requirement 5 (5.4): Protect all systems against malware and regularly update anti-virus software or programs Requirement 6 (6.7): Develop and maintain secure systems and applications Requirement 7 (7.3): Restrict access to cardholder data by business need-to-know Requirement 8 (8.1, 8.8): Identify and authenticate access to system components Requirement 9 (9.10): Restrict physical access to cardholder data Requirement 10 (10.8, 10.9): Track and monitor all access to network resources and cardholder data Requirement 11 (11.6): Regularly test security systems and processes Requirement 12 (all): Maintain a policy that addresses information security for all personnel	ISO 27701:2019—Clause 5.3 Leadership Clause 4 Structure of this standard A.5.1 Policies for information security A.5.2 Information security roles and responsibilities A.5.3 Segregation of duties A.5.4 Management responsibilities A.5.24 Information security incident management planning and preparation A.5.25 Assessment and decision on information security events A.5.26 Response to information security incidents A.5.27 Learning from information security incidents A.5.35 Independent review of information security A.5.36 Compliance with policies, rules and standards for information security A.5.37 Documented operating procedures A.8.25 Secure development life cycle A.8.27 Secure system architecture and engineering principles A.8.30 Outsourced development A.8.32 Change management

Table 1 (Continued)

PSD2		PCI DSS v4.0	ISO/IEC 27001:2022
Risk assessment	Identification and classification of functions, processes, and assets	Requirement 2 (2.4): Do not use vendor-supplied defaults for system passwords and other security parameters Requirement 9 (9.6): Restrict physical access to cardholder data Requirement 12 (12.4, 12.5, 12.8, 12.9): Maintain a policy that addresses information security for all personnel	ISO 27005:2022—A.2.2 Assets Clause 6.1.2 Information security risk assessment A.5.2 Information security roles and responsibilities A.5.9 Inventory of information and other associated assets A.5.10 Acceptable use of information and other associated assets A.5.11 Return of assets A.5.12 Classification of information A.5.13 Labelling of information A.8.32 Change Management
	Risk assessment of functions, processes, and assets	Requirement 6 (6.1, 6.6): Develop and maintain secure systems and applications Requirement 10 (10.6): Track and monitor all access to network resources and cardholder data Requirement 11 (11.2, 11.3, 11.5): Regularly test security systems and processes Requirement 12 (12.2, 12.10): Maintain a policy that addresses information security for all personnel	ISO 27005:2022—A.1.1 Criteria related to risk assessment ISO 27005:2022—A.1.2 Risk acceptance criteria ISO 27005:2022—A.2.1 Information security risk components ISO 27005:2022—A.2.3 Risk sources and desired end state ISO 27005:2022—A.2.4 Event-based approach ISO 27005:2022—A.2.5 Asset-based approach ISO 27005:2022—A.2.6 Examples of scenarios applicable in both approaches ISO 27005:2022—A.2.7 Monitoring risk-related events ISO 27005:2022—Clause 8.6.3 Acceptance of the residual information security risk Clause 6.1.2 Information security risk assessment A.6.8 Information security event reporting ISO 27701:2022—A.5.7 Threat Intelligence A.5.25 Assessment and decision on information security events A.5.26 Response to information security incidents A.5.27 Learning from information security incidents A.5.28 Collection of evidence A.5.29 Information security during disruption A.8.8 Management of technical vulnerabilities A.8.16 Monitoring Activities A.8.32 Change Management

Table 1 (Continued)

PSD2		PCI DSS v4.0	ISO/IEC 27001:2022
Protection	Data and systems integrity and confidentiality	Requirement 2 (2.3): Do not use vendor-supplied defaults for system passwords and other security parameters Requirement 3 (all): Protect stored cardholder data Requirement 4 (all): Encrypt transmission of cardholder data across open, public networks Requirement 7 (all): Restrict access to cardholder data by business need-to-know Requirement 12 (12.8, 12.9): Maintain a policy that addresses information security for all personnel	A.5.3 Segregation of duties A.5.14 Information transfer A.5.18 Access rights A.5.31 Legal, statutory, regulatory and contractual requirements A.5.32 Intellectual property rights A.5.33 Protection of records A.5.34 Privacy and protection of PII A.5.35 Independent review of information security A.8.2 Privileged access rights A.8.3 Information access restriction A.8.7 Protection against malware A.8.10 Information deletion A.8.11 Data masking A.8.12 Data leakage prevention A.8.19 Installation of software on operational systems A.8.20 Networks security A.8.21 Security of network services A.8.22 Segregation of network A.8.27 Secure system architecture and engineering principles A.8.29 Security testing in development and acceptance A.8.32 Change Management A.8.34 Protection of information systems during audit testing ISO 27701:2019—Clause 6.15.1.4 Privacy and protection of personally identifiable information ISO 27701:2019—Clause 7.2 Conditions for collection and processing ISO 27701:2019—Clause 7.3 Obligations to PII principals ISO 27701:2019—Clause 7.4 Privacy by design and privacy by default ISO 27701:2019—Clause 7.5 PII sharing, transfer and disclosure ISO 27701:2019—Clause 8.2 Conditions for collection and processing
	Access control	Requirement 6 (6.2): Develop and maintain secure systems and applications Requirement 7 (all): Restrict access to cardholder data by business need-to-know Requirement 8 (all): Identify and authenticate access to system components Requirement 10 (10.2): Track and monitor all access to network resources and cardholder data Requirement 11 (11.5): Regularly test security systems and processes	A.5.3 Segregation of duties A.5.15 Access Control A.5.18 Access rights A.5.17 Authentication information A.8.2 Privileged access rights A.8.3 Information access restriction A.8.5 Secure authentication A.8.15 Logging A.8.16 Monitoring activities A.8.32 Change Management

Table 1 (Continued)

PSD2		PCI DSS v4.0	ISO/IEC 27001:2022
	Physical security	Requirement 9 (all): Restrict physical access to cardholder data	A.7 Physical controls
Detection	Incident monitoring and reporting	Requirement 10: Track and monitor all access to network resources and cardholder data Requirement 12 (12.10): Maintain a policy that addresses information security for all personnel	ISO 27701:2022—A.5.7 Threat Intelligence ISO 27701:2022—A.5.24 Information security incident management planning and preparation ISO 27701:2022—A.5.25 Assessment and decision on information security events ISO 27701:2022—A.5.26 Response to information security incidents ISO 27701:2022—A.5.27 Learning from information security incidents ISO 27701:2022—A.5.28 Collection of evidence ISO 27701:2022—A.8.15 Logging ISO 27701:2022—A.8.16 Monitoring activities ISO 27701:2022—A.8.17 Clock synchronization
	Fraud detection	Requirement 5 (all): Protect all systems against malware and regularly update anti-virus software or programs Requirement 6 (6.1, 6.2, 6.5, 6.6): Develop and maintain secure systems and applications Requirement 9 (9.9): Restrict physical access to cardholder data Requirement 10 (all): Track and monitor all access to network resources and cardholder data Requirement 11 (11.1, 11.4, 11.5): Regularly test security systems and processes	ISO 27701:2022—Clause 9.1 Monitoring, measurement, analysis and evaluation ISO 27701:2022—A.5.7 Threat Intelligence ISO 27701:2022—A.7.4 Physical security monitoring ISO 27701:2022—A.7.5 Protecting against physical and environmental threats ISO 27701:2022—A.8.15 Logging ISO 27701:2022—A.8.16 Monitoring activities ISO 27701:2022—A.8.7 Protection against malware A.8.8 Management of technical vulnerabilities A.8.12 Data leakage prevention A.8.30 Outsourced development
Business continuity	Business continuity	Requirement 12 (12.10): Maintain a policy that addresses information security for all personnel	A.5.30 ICT readiness for business continuity
Testing of security measures	Testing of security measures	Requirement 5 (all): Protect all systems against malware and regularly update anti-virus software or programs Requirement 6 (6.1, 6.2): Develop and maintain secure systems and applications Requirement 10 (10.6): Track and monitor all access to network resources and cardholder data Requirement 11 (all): Regularly test security systems and processes Requirement 12 (12.1, 12.11): Maintain a policy that addresses information security for all personnel	Clause 9 Performance evaluation A.5.36 Compliance with policies, rules and standards for information security A.8.8 Management of technical vulnerabilities A.8.29 Security testing in development and acceptance A.8.33 Test information A.8.34 Protection of information systems during audit testing

Table 1 (Continued)

PSD2		PCI DSS v4.0	ISO/IEC 27001:2022
Security awareness	Situational awareness and continuous learning	Requirement 6 (6.5): Develop and maintain secure systems and applications Requirement 10 (10.8): Track and monitor all access to network resources and cardholder data Requirement 11 (all): Regularly test security systems and processes Requirement 12 (12.4, 12.5, 12.6, 12.9, 12.10): Maintain a policy that addresses information security for all personnel	ISO 27701:2022—Clause 7.3 Awareness ISO 27701:2022—A.5.2 Information security roles and responsibilities ISO 27701:2022—A.5.7 Threat Intelligence ISO 27701:2022—A.5.25 Assessment and decision on information security events A.5.27 Learning from information security incidents A.6.3 Information security awareness, education and training A.8.16 Monitoring Activities
	Payment service user relationship management	Requirement 12 (all): Maintain a policy that addresses information security for all personnel	Clause 7.3 Awareness A.5.5 Contact with authorities A.5.6 Contact with special interest groups A.5.7 Threat Intelligence A.5.27 Learning from information security incidents A.6.2 Terms and conditions of employment A.6.3 Information security awareness, education and training A.6.5 Responsibilities after termination or change of employment A.8.8 Management of technical vulnerabilities A.8.16 Monitoring Activities A.8.32 Change management

Funding Open access funding provided by HEAL-Link Greece.

Conflict of interest M. Gounari, G. Stergiopoulos, K. Pipyros and D. Gritzalis declare that they have no competing interests.

References

1. Chishti S, Barberis J (2016) The FINTECH Book: The Financial. Technology (Handbook for Investors, Entrepreneurs and Visionaries. John Wiley & Sons)
2. Goldfarb A, Tucker C (2019) Digital Economics. J Econ Lit 57(1):3–43. https://doi.org/10.1257/jel.20171452
3. Directive (EU) 2015/2366of the European Parliament and of the Council of 25 November 2015on 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.
4. Directive (EU) 2007/64 of the European Parliament and of the Council of 13 November 2007on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC and 2006/48/EC and repealing Directive 97/5/EC.
5. Khakan N, Mostafiz Najaf MIR (2021) Fintech firms and banks sustainability: Why cybersecurity risk matters? Int J Financial Eng. https://doi.org/10.1142/S2424786321500195
6. (2022) Regulatory Technical Standards on strong customer authentication and secure communication under PSD2, European Banking Authority. RTS 03(05):22
7. Directive 2015/2366—Payment services in the internal market—EU monitor, Available at: https://www.eumonitor.eu/9353000/1/j4nvk6yhcbpeywk_j9vvik7m1c3gyxp/vk0vn25mntsj
8. Payment Services Directive 2—all you need to know. https://www.jpmorgan.com/europe/merchant-services/insights/PSD2-all-you-need-to-know
9. "Open Banking Europe: Registration & Passporting Open Banking Europe—providing collaborative services to support PSD2 Access to Account (XS2A), in partnership with the financial industry", Open Banking Europe, Jan. 18, 2021. https://www.openbankingeurope.eu/media/1935/obe-psd2-xs2a-registration-passporting-guide.pdf
10. Payment Services Directive (PSD2): Regulatory Technical Standards (RTS) enabling consumers to benefit from safer and more innovative electro, European Commission. https://ec.europa.eu/commission/presscorner/detail/pl/MEMO_17_4961
11. What Is the PSD2 Regulation? Purpose & Compliance | Sectigo® Official. https://sectigo.com/resource-library/the-revised-payment-services-directive-psd2-explained
12. "Three ways PSD2 will benefit consumers," UK Finance. https://www.ukfinance.org.uk/blogs/three-ways-psd2-will-benefit-consumers
13. Payment Services Directive 2—all you need to know. https://www.jpmorgan.com/europe/merchant-services/insights/PSD2-all-you-need-to-know
14. "Open Banking: AISP, PISP & ASPSP Explained—Macro Global," May 18, 2022. https://www.macroglobal.co.uk/blog/regulatory-technology/open-banking-psd2/aisp-pisp-aspsp-explained/
15. "PSD2—Payment Services Directive 2 What is new?", Deloitte, 2016. https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/financial-services/Banking/lu_psd2-payment-services-directive2.pdf
16. "FCA finalises revised Payment Services Directive (PSD2) requirements," FCA, Sep. 18, 2017. https://www.fca.org.uk/news/press-releases/fca-finalises-revised-psd2-requirements

17. Guidelines on Draft Regulatory Technical Standards setting technical requirements on development, operation and maintenance of the electronic central register and on access to the information contained therein, under Article 15(4) of Directive (EU) 2015/2366, European Banking Authority, Dec 13, 2017.
18. Guidelines on security measures for operational and security risks under the PSD2, European Banking Authority, Jan. 12, 2018. https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-security-measures-for-operational-and-security-risks-under-the-psd2
19. "PSD2—Security Obligations," EmoneyAdvice, Jul. 08, 2017. http://emoneyadvice.com/psd2-security/
20. Guidelines on ICT and security risk management, European Banking Authority, Dec. 13, 2018. https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-ict-and-security-risk-management
21. Regulatory Technical Standards on strong customer authentication and secure communication under PSD2, European Banking Authority, Apr. 12, 2019. https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2
22. (2018) Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC, European Banking Authority. Jun 13:
23. EBF PSD2 Guidance Final December 2019 | PDF | Payments | European Union," European Banking Authority. https://www.scribd.com/document/534126697/EBF-PSD2-guidance-Final-December-2019
24. "PSD2 risks and IT controls to mitigate," Compact. https://www.compact.nl/en/articles/psd2-risks-and-it-controls-to-mitigate/
25. E. C. Bank, "The revised Payment Services Directive (PSD2)," European Central Bank, Oct. 05, 2018. https://www.ecb.europa.eu/paym/intro/mip-online/2018/html/1803_revisedpsd.en.html
26. (2021) Revised Guidelines on Major Incident Reporting. Eur Bank Auth 10:
27. P. Wolters and B. Jacobs, "The security of access to accounts under the PSD2," Computer Law & Security Review, vol. 35, no. 1, pp. 29–41, Feb. 2019, https://doi.org/10.1016/j.clsr.2018.10.005.
28. Communication Delegated Regulation (EU) 2018/389 of 27 Nov 2017, supplementing Directive (EU) 2015/2366of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication.
29. V. Bhatt, "TPP User Management for PSD2 Access to Account (XS2A)," Open Banking Exchange, Jul. 19, 2022. https://www.openbanking.exchange/europe/resources/publications/tpp-user-management-for-psd2-xs2a/
30. Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication, Available: http://data.europa.eu/eli/reg_del/2018/389/oj/eng
31. V. Bhatt, "eIDAS Qualified Certificates Under PSD2 Frequently Asked Questions," Open Banking Exchange, Jan. 18, 2021. https://www.openbanking.exchange/europe/resources/publications/eidas-qualified-certificates-under-psd2-frequently-asked-questions/
32. Are you PSD2-Ready? A guide to the latest information and sources of support—Corporates and Institutions. https://corporates.db.com/publications/White-papers-guides/are-you-psd2-ready-a-guide-to-the-latest-information-and-sources-of-support?language_id=1
33. M. Petrović, "PSD2 influence on digital banking transformation: Banks' perspective," J Process Man, New Technol, vol. 8, no. 4, pp. 1–14, 2020, https://doi.org/10.5937/jouproman8-28153.
34. "Additional Time Period for the Implementation of the Requirements for Strong Customer Authentication Standards of Delegated Regulation (EU) 2018/389—Kyriakides Georgopoulos Law Firm." https://kglawfirm.gr/additional-time-period-for-the-implementation-of-the-requirements-for-strong-customer-authentication-standards-of-delegated-regulation-eu-2018-389/
35. O. Maas, "How to handle EBA Guidelines on Internet payment security to prepare PSD2".
36. "EBA publishes an Opinion on the elements of strong customer authentication under PSD2," European Banking Authority, Jun. 21, 2019. https://www.eba.europa.eu/eba-publishes-an-opinion-on-the-elements-of-strong-customer-authentication-under-psd2
37. Directive (EU) 2022/2555of the European Parliament and of the Council of 14 December 2022on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)".
38. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

39. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016on 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)
40. Sittig F, Von dem Bussche A (2021) Analyzing the scope and evolution of the NIS2 Directive. Comput Law Secur Rev 40:105544
41. European Union Agency for Network and Information Security (ENISA). (2020). Recommendations on the EU's next-generation cybersecurity certification framework.
42. Gritzalis D, Tountas Y (2019) The EU NIS Directive: Suggestions for implementing its security-related requirements. Comput Secur 84:42–56
43. Eichensehr KE (2018) Public-private cybersecurity. Tex Law Rev 96(4):779–832
44. Tsouros C, Eichensehr KE (2021) A comparative analysis of cyber threat intelligence sharing in the EU and US. Int Data Priv Law 10(3):204–219
45. Zohdi A (2018) A review of the revised payment service directive (PSD2). Eu Int J Inf Manag 43:44–52
46. Kääriäinen J (2017) PSD2: Building a secure open banking ecosystem. J Digit Bank 1(4):311–321
47. Irion K, Luchetta G (2019) Revisiting the EU electronic communications regulatory framework. Comput Law Secur Rev 35(2):105341
48. Valero A, Rodrigues B (2020) PSD2 and cyber security: Risks and challenges in the digital era. J Financial Regul Compliance 28(3):241–255
49. Bucking H, Rodrigues D (2021) Toward a unified digital single market: The interplay of PSD2 and NIS2. Eur J Inf Syst 30(4):403–421
50. Centeno, V., & et al. (2018). Open banking and the PSD2 directive: Challenges and opportunities for the European banking industry. Computer Law & Security Review, 34(6), 1219–1228.
51. European Central Bank. (2017). Guidelines on major incident reporting under the PSD2
52. ENISA. (2019). The EU Cybersecurity Act—Boosting the EU's cybersecurity.
53. Santis GD, Sicari S (2019) An overview of the European Union's Cybersecurity Act. Comput Networks 160:107–115
54. ENISA. (2020). European cybersecurity certification: The road ahead.
55. Peacock T (2020) The EU. Cybersecurity (Act and its implications for the digital single market)
56. Voigt P, Von dem Bussche A (2017) The EU General Data Protection Regulation (GDPR). Springer
57. De Hert P, Papakonstantinou V (2016) The new General Data Protection Regulation: Still a sound system for the protection of individuals? Comput Law Secur Rev 32(2):179–194
58. Buckley RP, Arner DW, Barberis JN (2016) The emergence of regtech 2.0: From know your customer to know your data. J Financial Transform 44:79
59. Van Alsenoy, B. (2016). Liability under EU data protection law: From directive 95/46 to the General Data Protection Regulation. Journal of IP, Information Technology and E-Commerce Law, 7, 271.
60. Master Thesis HÖ (2021) "Personal Data Processing by Third Party Providers in Online Payment Transactions Under GDPR and PSD2: An in-depth Legal Analysis for GDPR and PSD2. Compliance
61. "Privacy at the epicentre", Deloitte, June 2018.
62. Albrecht JP (2016) How the GDPR will change the world. Eur Data Prot Law Rev 2(3):287–289
63. "EBF PSD2 Guidance Final December 2019 | PDF | Payments | European Union,"
64. Anghel ID, Cioaca SI (2017) GDPR and the new eIDAS based authentication services. Informatica Econ 21(3):20–29
65. Giannopoulou A, Dimitriou T (2017) Analyzing the coexistence of PSD2 and GDPR. Comput Law Secur Rev 36:105377
66. (2019) Mapping PCI DSS v3.2.1 to the NIST Cybersecurity Framework v1.1, Payment Card Industry Security Standards Council. https://listings.pcisecuritystandards.org/pdfs/Mapping-PCI-DSS-to-NIST-Framework.pdf(Created 06.2019)
67. Information technology—Security techniques—Information security management systems—Requirements, International Standard ISO/IEC 27001, Reference number ISO/IEC FDIS 27001:2022(E). http://www.itref.ir/uploads/editor/42890b.pdf
68. PCI DSS Compliance and Certification—7Security. https://www.7sec.com/compliance/pci-dss/?gclid=Cj0KCQjwyt-ZBhCNARIsAKH11740YKQHIJhpgaW30yK_gycT5KEFEQIFFe9yJ9iGayrwWZ6krW4r1ZsaAlW9EALw_wcB
69. TrueLayer Blog: PSD2: does Europe need a single API standard? https://truelayer.com/blog/product/psd2-does-europe-need-a-single-api/

Further reading

70. Eich D (2018) Payment services, third-party payment providers and data protection, with special regard to the PSD2. Era Forum 18(4):479–500
71. (2016) "Comparison of PCI DSS and ISO/IEC 27001 Standards," vol. 1. https://www.isaca.org/-/media/files/isacadp/project/isaca/articles/journal/2016/volume-1/comparison-of-pci-dss-and-iso-iec-27001-standards_joa_eng_0116