UNIVERSITY OF TWENTE.

**Faculty of Electrical Engineering,
Mathematics & Computer Science**

Balanced, as all things should be: PSD2 and cybersecurity risks

Dragoș-Marian Chivulescu

M.Sc. Thesis
July 2021

Senior Examiner:
prof. dr. A. Peter
Supervisors:
dr. ing. F.W. Hahn
dr. A. Abhishta
S. Fransen

Computer Science Group
Faculty of Electrical Engineering,
Mathematics and Computer Science
University of Twente
P.O. Box 217
7500 AE Enschede
The Netherlands

Summary

The revised Payment Services Directive (PSD2, Directive (EU) 2015/2366 is now in full use in the EU. PSD2 mandates how the payment user information can be transferred to and used by third parties, a measure aimed at welcoming new participants to the market. PSD2 makes use of Regulatory Technical Standards (RTS) for guidance on the new market processes. While many studies focused on the RTS on Strong Customer Authentication (SCA) aspect of PSD2, the Common and Secure Communication (CSC) dimension has been mostly overlooked. This exploratory research investigated whether the RTS on CSC increased the overall cybersecurity risk level, given the new payments ecosystem, and if PSD2 does not, in fact, make e-payments less secure (opposite of the objective of the directive).

The research used a qualitative approach to understand better the effects of a principle-based regulation on the cybersecurity of the regulation's subjects. After placing PSD2 in the overall trend of Open Banking and analyzing the background information on the topic, an understanding of CSC is created based on the RTS official guidelines. Then, a risk assessment on the cybersecurity aspects of CSC was performed, using a methodology developed from the industry standards, ISO 27005 and NIST 800-30. After the risks have been identified, the relevant market participants subject to these risks in the Dutch e-payment market have been discovered. A subset of these participants has been interviewed using a semi-structured approach to verify the previously found risks. Ultimately, CSC was deemed not to increase the overall cybersecurity risk for Dutch e-payment market participants and PSD2 to make e-payments safer and more secure, as planned by the European regulators.

Acknowledgments

The present work represents the final project of my master's studies, studies that have taken me to two foreign countries, France and the Netherlands. While more than half of my studies were online and were affected by the start of the COVID-19 pandemic, I managed to adapt, overcome challenges and, most importantly, learn in the new reality. This journey introduced me to the world of payments and showed me, once again, how important is cybersecurity for our daily lives. I am happy with the outcome of this research and grateful for everything I have learned.

Completing this work would not have been possible without the help and guidance of some extraordinary people. Firstly, I would like to thank my family, in Romania and abroad, for their unconditional love and support. Secondly, my team of super-supervisors, Abhishta, Florian and Sanne, challenged me and made me ask more of myself. Consequently, the supportive colleagues of EY Netherlands gave me the opportunity to do this thesis in an engaging work environment full of bright minds and ideas. While a large number of colleagues contributed, directly and indirectly, special thanks go to Rudrani Djwalapersad and Vanessa Simões de Azevedo. The thesis couldn't have been completed without the interview participants who dedicated their time and expertise to aid understanding on the topic of PSD2. Last but not least, all my friends, inspiring and optimistic, deserve mentioning for supporting me throughout this period.

Dragoș-Marian Chivulescu

July 2021

Contents

Appendices

Chapter 1

Introduction

The revised Payment Services Directive (PSD2, Directive (EU) 2015/2366) came into full effect in the EU after the extended deadline for implementing Strong Customer Authentication (SCA) has passed on 31st December 2020 [1]. The directive replaces the original Payment Services Directive (PSD, or PSD1; from 2007), providing a legal framework for the new market realities. PSD2, which was initially passed by The Council of the European Union in 2015 [2], underwent many changes, revisions and a substantial amount of lobbying from the parties involved [3]. The revised directive can be seen as a step towards Open Banking in the EU, a new paradigm of digital banking. PSD2 proposes three main objectives. The first objective is to strengthen the European market for e-payments. The second objective concerns the development of innovative payment services enabled by opening the market to new entrants. Lastly, it aims to make e-payments safer and more secure.

To achieve these objectives, the European Banking Authority (EBA) released Regulatory Technical Standards (RTS), a legal document that offers guidance on the technical implementation of the new systems needed to comply with the PSD2 legislation [2]. The main standard comprises Strong Customer Authentication (SCA) and Common and Secure Communication (CSC).

SCA is authentication that uses “two or more elements categorized as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something only the user is)” [2]. This is the same approach used in multi-factor authentication schemes but presents a few exceptions when less strong authentication can be used.

CSC represents the way Account Servicing Payment Service Providers (ASPSPs) are required to open communication channels that: allow Account Information Service Providers (AISPs) and Payment Initiation Service Providers (PISPs) to identify themselves ahead of transferring payment service users (PSUs)' data; send, request and receive information on one or more payment accounts and associated transactions; initiate a payment order from the payer's payment account. This communication is done through APIs; if an API is not provided, the ASPSPs have to allow the use of a "customer-facing interface". The customer-facing interface is usually the standard web page of the ASPSP, used by customers in Internet banking. This interface must use an identification process between the ASPSP and the third party (essentially screen-scraping[1], with extra steps.). The identification process, which must be present in the API access, must use qualified certificates. These qualified certificates are special certificates used to secure the communication and digital signatures (proving an entity's identity), and their specifications come from a European regulation called eIDAS [4].

If we focus on the PSD2 objective to make e-payments safer and more secure, we observe an apparent asymmetry. On the one hand, traditionally, financial institutions such as banks presented advanced security measures due to them being highly regulated and complying with different industry standards [5]. This was the status quo in an environment where banks had complete control over the systems the users interacted with and the data the clients used. On the other hand, new companies such as FinTechs usually lack cybersecurity maturity [6] as they focus primarily on user-centricity. The e-payment chain is now longer under PSD2, and the attack surface seems to be more prominent [7]. As cybercrime continues to be on the rise[2], the cybersecurity implications of this asymmetry become important.

A question arises: Has PSD2 had a negative effect on the cybersecurity of e-payment organizations, despite its goal of making e-payments more secure?

1.1 Research Questions

In order to state the research question, a working definition for the key variable must be provided, not being possible without defining the crucial concepts. Cybersecurity[3] can be defined as protecting different assets from "unauthorized access or criminal use and the practice of ensuring confidentiality, integrity and availability of information" (commonly abbreviated CIA). The first step in improving cybersecurity is to recognize the risks. The more risks are identified, and the more critical they

[1] Process of collecting data displayed on the screen from one application and translating it so that another application can display it

[2] https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

[3] https://us-cert.cisa.gov/ncas/tips/ST04-001

are, the less secure organizations are [4].

After defining the key variable, the main research question can be formulated:
Research question:

What was the effect on the cybersecurity risks of e-payment market participants following the implementation of PSD2?

1.1.1 Scope

This subsection outlines the research scope.

Firstly, as we have seen, PSD2 proposes a number of RTS that have technological implications. Many pieces of work have been dedicated to SCA, an element of RTS, sometimes by leveraging the multi-factor authentication technical problem (as can be observed in the Background chapter). CSC has received less attention, a research gap being identified. Thus, studying the details of the common and secure communication aspect of PSD2 comes naturally.

Additionally, the RTS present many articles and paragraphs that concern the governance of the processes around the technical changes mandated by the revised directive. In this paper, the focus lies on technical cybersecurity risks and not on factors such as processes, policies, resilience, reporting or crisis management. A future expansion of the present work might include these aspects.

Lastly, this paper focuses on the e-payment market, the country where the author studies and works. There are multiple reasons for choosing this scope. Firstly, the EU comprises multiple e-payment markets with distinctive traits (such as size, growth [8]), making the overall European market non-uniform. In this reality, contextualization is important for observing trends, and one way of achieving this is by focusing on one national market. Secondly, the Netherlands has a highly digital national payment market since before PSD2 came into effect [9]. This factor can have significance when considering the new digital systems needed for the legislation, as the payment providers already use advanced technology systems. Lastly, a good collaboration can be observed in the Dutch payment market, proved by several joint initiatives (e.g., iDeal, iDin, Dutch Payments Association). These initiatives show the desire of market participants to continuously improve their offerings.

In order to answer the research question in the defined scope, a number of subquestions have been elected.

[4] Please note that there might be other definitions.

1.1.2 Sub-questions

Using the background information, the first sub-question is:

(I) *What are the main technical implications of CSC?*

This sub-question aims to compare and contrast the technical details that stem from CSC's changes to organizations in the e-payment sector in the Netherlands. Understanding these provisions is essential for assessing the risks, which is the aim of the next sub-question:

(II) *What are the cybersecurity risks related to CSC?*

The second sub-question builds upon the first one by using the identified technical details and knowledge from the literature as a first step in performing a risk analysis of CSC. Next, it is essential to identify the organizations for which these risks are applicable, as not managing risks effectively can have negative consequences (financial, reputational and legal, to name a few).

(III) *Who are the relevant stakeholders for CSC in the Dutch e-payment market?*

This sub-question presents the different entities that are subject to CSC. After the relevant stakeholders have been identified, their general experience with CSC-related risks can be discovered:

(IV) *What cybersecurity risks have been encountered by the relevant stakeholders in the Dutch e-payment market with regards to CSC?*

The fourth sub-question's objective is to validate the risks identified previously and possibly extend the risk model. This is relevant for understanding the difficulties that the relevant stakeholders face, in their quest to serve their clients, comply with regulators and avoid security incidents.

(V) *Do relevant stakeholders in the Dutch e-payment market think CSC increased their overall cybersecurity risks?*

Finally, the perception of the relevant stakeholders helps probe the cybersecurity effect of the common and secure communication technical standard and allows to answer the main research question.

1.2 Methodology

This section describes the methodology used for conducting the research. Exploratory in nature, due to the gaps identified in the research, the approach is one of a qualitative, exploratory case study with a holistic design - single unit of analysis at different cases [10]. Yin provides five constructing components, being addressed as the following:

- research question - defined in the Research Questions subsection;
- propositions - stemming from the descriptive analysis, detailed below;
- unit of analysis - the risks (description and severity) identified at e-payment market participants in the Netherlands, related to the systems mandated by the CSC standard;
- logic linking of the data to the propositions - a supposition is proposed after the first stage of the research, which is verified for accuracy in the second stage, allowing the possibility of extension;
- criteria for interpreting the findings - comparing the initial set of risks with the ones produced following semi-structural interviews.

For ease, two main stages of the research have been devised:

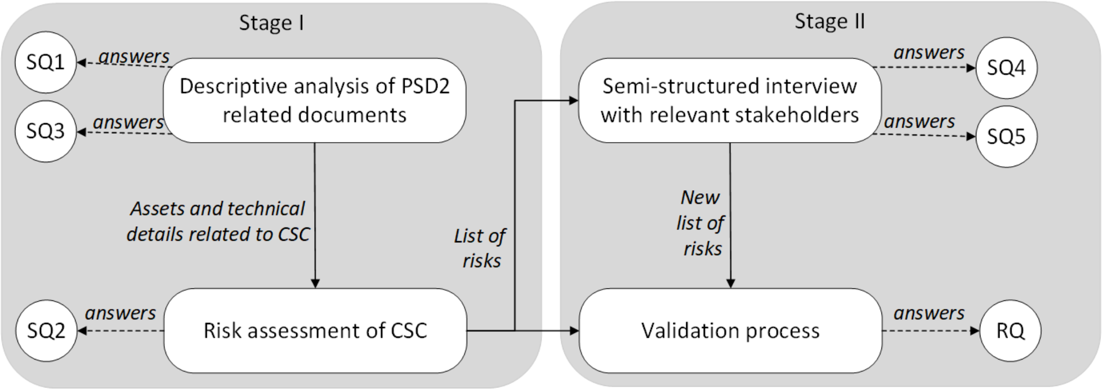

Figure 1.1: Research stages. SQ - Sub-question; RQ - (main) research question

1.2.1 Stage I

The first stage of the research has two parts. Firstly, the research uses the descriptive analysis [11] of the legislation surrounding PSD2 (such as [2], [4], [12], [13]). A descriptive analysis identifies “the characteristics of the population or situation being studied”. This approach provides a solid understanding of the cybersecurity-related aspects of CSC (zooming in on APIs and qualified certificates). In this part, the answer to the first and third sub-questions can be formulated. The answer to the first sub-question is provided through the study of CSC in the RTS and relevant literature. The third sub-question can be answered from the study of the PSD2 legislation, which identifies the roles in the new e-payment ecosystem, and the background information, which discusses the relationships between actors in the market.

Secondly, relevant cybersecurity risk assessment frameworks and guidelines ([14], [15]) used in practice by financial organizations and recommended by regulators are used to perform the risk assessment for the technical aspects of CSC. More precisely, Clause 7 and 8 of ISO 27005 (“Information security risk assessment”) and Chapter Three of NIST 800-30 (“The process”) provide the approach and steps for performing a risk assessment. Using the technical details and (organizational) assets related to CSC (the outcome of the last part) as a starting point for the risk assessment, the answer to the second sub-question can be formulated.

The outcome of this stage is a list of cybersecurity technical risks (description and severity) regarding the CSC requirements of PSD2.

1.2.2 Stage II

The second stage has two parts as well.

Firstly, using the previous stage’s output, a verification process is established through conducting semi-structured interviews with relevant stakeholders from the e-payment market in the Netherlands. This qualitative research approach is useful to provide new insights and to explain phenomena [16].

The semi-structured interviews are used to gather empirical data and build a theoretical model. They provide flexibility which facilitates the expression of ideas from the respondents. This approach enables the respondents to use their own words and base their statements on their own relevant personal experience [16]. The interviews are conducted in English, recorded, and then transcribed to enable a thorough analysis. A pilot interview is conducted before the official interviews to help refine the data collection plans. Access to the respondents is offered by EY Netherlands and its business network, thanks to the author’s thesis internship at EY Netherlands. This aspect aids the process by leveraging the expertise and connections accumulated in the company through their FSO Cybersecurity consultancy business. An emphasis is put on the respondents’ role and the relation to the cybersecurity aspect of PSD2. Furthermore, a diverse group of respondents from different organizations is desired. This part aims to answer the last two research sub-questions.

For the second and final part of the research, the output of the interviews, a new list of verified cybersecurity risks related to CSC, is compared to the initial list, highlighting any significant differences and arguing for the underlying causes. The validation process answers the main research question of this work.

1.3 Ethical considerations

A critical aspect of each research endeavor is its morality. True advancement of science should be undergone in an ethical manner.

Firstly, this research aims to be an open and truthful academic work. The prerequisites, scope, limitations and findings are explicitly presented, giving any reader the possibility to verify their veridicality.

Secondly, the present paper requires the participation of human subjects; thus, their rights and liberties must be protected. In order to do so, the description of the research, aims, and objectives, are presented to the interview participants from the initial touchpoint, allowing them to be involved in the research or decline. The interviewees answer anonymously, the employee's names and the employer are removed, the latter being replaced by a generic description (e.g. ASPSP).

The interview recordings have a private character, not being shared with the public, being available only to the respondent giving the interview, the author of this work and the committee supervising this research. The storing of the interview recordings is done securely and redundantly, the copies being destroyed after enough time has passed after the defense of this work or on participant request.

1.4 Contribution

In this subsection, the relevance of the research and its contribution is presented. This research is useful for several reasons:

- Provides insights for a current theme that is PSD2, after the legislation has been finalized;
- Discusses concepts that the literature has mostly omitted in this context;
- Acts as a starting point for a discussion on the effects of the revised Payments Directive;
- Provides insights that might be valuable in future research needed for the subsequent directives and legislation;
- Identifies risks and challenges that might arise for a new organization that joins the e-payment ecosystem;
- Helps companies in the e-payment market with their risk assessment process by providing a starting point for the determination of residual risk.

The resulting artifact of the research is the present academic paper, which is comprised of different sections.

1.5 Document outline

The research findings are organized in chapters. An overview of the chapters can be seen in Figure 1.2. The arrows represent how one chapter relies on the information presented in the previous one. The last two chapters rely on the information presented throughout the whole paper.

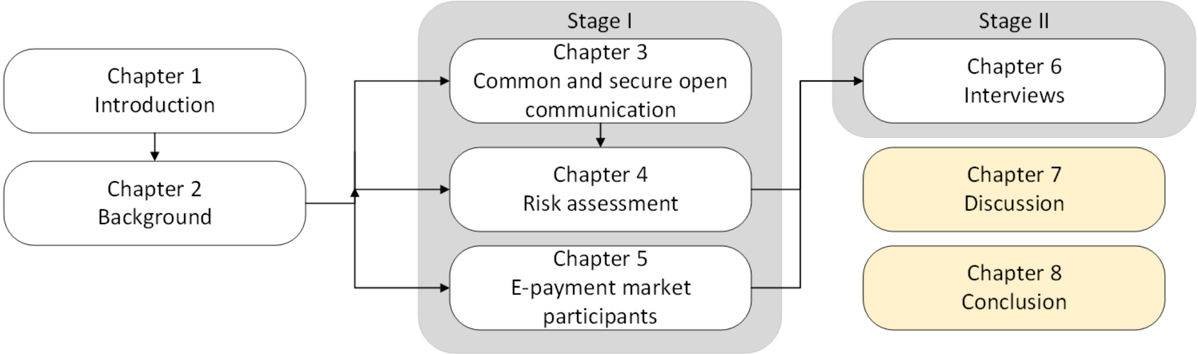

Figure 1.2: Document outline

The first chapter introduces the reader to the research theme using a high-level overview of the PSD2 legislation. Then, a research gap is identified, which prompts the creation of the research question. Having set a scope, five sub-questions are formulated for guiding the research. The rest of the chapter concerns the chosen methodology, the research contribution and the paper outline.

The second chapter, entitled "Background", provides the necessary background information of the concepts closely related to the research: Open Banking, PSD2, RTS, API and qualified certificates, using official documents and literature work as sources.

Chapter 3 describes the articles from the RTS that make up the "Common and secure open communication" technical standard and answers the first research sub-question.

The Risk Assessment chapter presents the application of the risk assessment methodology to the case of CSC for e-payment organizations, following the ISO and NIST standards. This chapter answer the second sub-question.

Chapter 5, which answers the third sub-question, uses information from the background study to identify the relevant stakeholders of the second Payments Directive in the Netherlands.

The interviews chapter explains the method and the output of the interviews performed with relevant e-payment market participants from the Netherlands. The chapter is organized according to the main discussion topics.

In the Discussion chapter the answer to the last two sub-questions are provided. Additionally, a critique of the research and future improvements are discussed.

Finally, the last chapter provides a conclusion of the research, highlighting the main findings.

Chapter 2

Background

In this chapter, relevant background information is presented. The methodology used for discovering the relevant scientific work is the snowball strategy or “citation pearl growing” [17]. This strategy complements the use of a large selection of official documents and standards, the vast majority of the relevant concepts being described from legal and regulatory texts. The snowball strategy entails starting from a few relevant documents for the topic and adding works that are related, have been referenced or cited, in the initial selection. The analysis of literature ends when convergence to the previously discovered items is observed.

The repositories used for finding scientific work are Scopus, Web of Science and Google Scholar. The papers which were not offered under open access or provided access using the University of Twente’s institutional login were discarded. Since PSD2 was passed as legislation in 2015, the literature older than 2015 was discarded as well. The author does not expect to miss many relevant documents through this elimination.

The keywords used for searches (by themselves or in combinations) are, in no particular order: *PSD2, PSD II, payment services directive, Open Banking, API, payments security, qualified certificates, qualified signature, API, RTS, CSC, SCA, cybersecurity risks, ISO 27005, NIST 800-30*.

The chapter is structured according to the main concepts related to the present work. Some overlaps can be observed between closely related concepts. Definitions and references to official documents are provided, where these have not been supplied previously.

2.1 Open Banking

We begin the state-of-the-art with Open Banking, as the general current of which PSD2 is part of. Open Banking is defined as "an initiative which facilitates the secure sharing of account data with licensed third parties through APIs" [18]. [19] traces the origin of Open Banking to the Competence Center Electronic Markets in Switzerland and the attempt to create an electronic market for the leading Swiss banks in the mid-1990s. This initiative failed mainly due to discussions of market influence and ownership. Today, we witness regulatory-driven initiatives like PSD2 in Australia and Hong Kong and market-driven initiatives in the US, Singapore, India, and South Korea [20]. One can already observe a certain level of fragmentation and diversity in approaches. O'Leary et al. note a lack of maturity and global standards, which act as inhibitors for developing digital systems in Open Banking. One can speculate that this lack of maturity and standards can affect the cybersecurity risks in the market. However, it is worth noting that some standards emerged in Europe, the most prominent ones being The Berlin Group NextGenPSD2, a pan-European initiative [21] and Open Banking Standard from the United Kingdom [22].

[19] and [23] suggest that currently, we are moving more towards "platform banking" than Open Banking. Platform banking entails accessing a specific "banking-mix" as named by Dratva, which are services offered by a provider's ecosystem and not a truly open marketplace, as Dratva defines Open Banking. Zachariadis in [24] also notices the emergence of platform banking. He also mentions the problems incumbents in the financial sector have with legacy IT systems. Solutions start to emerge in this sphere, for example, [25] proposing a technique for identifying scalability threats as a form of tech debt used at a Nordic FinTech company.

[26] highlight the API as the enabler of Open Banking but draw attention to how APIs represent a new attack vector for cybercriminals. [7] calls this new attack vector "man in the middle", as PSPs become an extra step in the interaction between users and traditional financial institutions, hinting at the popular class of attacks well known in the cybersecurity world. The risk of API as a new attack vector can be identified. Mansfield-Devine is optimistic that multi-factor authentication (SCA) can increase the security of payments. [27] successfully predicted, before PSD2 being in full effect, that the need for APIs might drive the market towards the emergence of "gateway service providers"[1]. As the specifications of the "off-the-shelf" gateways are not usually publicly disclosed, their security is hard to assess. Assessing the risk of such external systems and partners falls under Third-Party Risk Management and

[1] Examples of these are https://www.axway.com/en/solutions/financial-services, https://connect.finleap.com/ and https://www.sibsapimarket.com/

is outside of the scope of this paper. However, UK's Open Banking standard, just like the Berlin Group's standard, is public. [28] present a formal security correctness proof of the Open Banking standard.

Lastly, Open Banking might not bring innovation only in the financial sector. [29], for example, proposes a way of calculating one's carbon footprint by analyzing one's transactions, leveraging the Swedish digital identity scheme and Open Banking.

We can draw a few conclusions regarding Open Banking initiatives. They are present in different geographies, usually materialize in "platform banking", and help create innovation in terms of business models (gateway providers) or applications (carbon footprint). However, Open Banking poses cybersecurity challenges through new attack vectors and risks emerging from additional parties like gateway providers.

2.2 Payment Services Directive 2

In this section, PSD2, a regulatory-driven Open Banking initiative, is presented through the lens of recent literature. The selection presented here focused on work that emerged after the legislation has been finalized to eliminate the speculations regarding the final form of the directive and its associated documents.

In terms of the need for the regulation, [30] believes that PSD2 did not emerge from customers wishing for a more open e-payment market. [31] highlights that a more important goal from European political leaders was to challenge the US credit card scheme duopoly, Visa and Mastercard.

Observing the effects of PSD2, [32] studied the distribution of PSP licenses up to January 2020. As much as 75% of licenses were obtained by companies already operating before the regulation has been introduced. This might show that PSD2 is not yet driving innovation by creating new companies but gives new directions for existing enterprises to diversify their offering. Polasik et al. also notice that one factor determining an increase in licenses in a country is offering "regulatory sandboxes", which provides potential entrants with an environment to test ideas before launching. This oferring might be a result of good national market collaboration. Collaboration can be useful in other ways, too: [33] mentions that in the Netherlands, through the Dutch Payments Association, organizations actively look for ways to reduce fraud, money laundering and other financial crimes. This collaboration will continue to be helpful in the context of PSD2.

[34] look at the rationale of accessing data under PSD2 (XS2A) and advocate for a "reciprocity clause" that would enable the ASPSPs to use the insights and analytics

obtained by TPPs from the data they provide. In this article, BigTech is frequently mentioned and how the current state of affairs might exacerbate their monopolistic practices with XS2A. [35] and [36] also mention the negative effect BigTech might have on the competitiveness of the e-payment industry in the future, however specifying it is too early to confirm such effect. [31] presents a similarly pessimistic angle, reminding of how Apple (one organization included in the BigTech group) exclusively decided the terms of access to their current (non-financial) APIs. Platforms, in this respect, might create more barriers for developers and, ultimately, users.

To conclude, PSD2 might not have emerged from a customer market push. Despite trying to disrupt dominant market participants such as credit card schemes, it might introduce, in the future, players that will erode the market's competitiveness, such as BigTechs. Ultimately, a collaboration between organizations is essential for PSD2 licensing and for continuing to tackle financial crimes.

2.3 Regulatory Technical Standards

The Regulatory Technical Standards, accompanying the directive, present significant changes for the e-payment market participants. The security of these changes has come under scrutiny.

[37] highlight that privacy and security are capital for the competitiveness on the market following PSD2. A study in South Korea shows that the reliability (which is one aspect of security) of mobile payment services is capital for user adoption [38], further adding to the argument that security is essential in an e-payment context.

[6] agrees that PSD2 (and RTS through extension) will pose security challenges for companies, mentioning different causes. Firstly, the author mentions how the "mindset" of TPPs might not prioritize security to the same level banks do. [39] illustrate Noctor's point with a security assessment of N26, a growing FinTech digital bank, which lacked many security controls. Secondly, APIs fragmentation and the need to integrate with multiple architectures might create complexity difficult to manage. A cybersecurity risk can be identified here.

[40] zoom in on the access to accounts (XS2A) component, mentioning the screen scraping debate and how ultimately the advancement of the market is a more important goal of the directive compared to security and privacy. This idea is reinforced by [41], who present five different attacks for a proposed PSD2 architecture. While most of these security vulnerabilities are being addressed by companies, it shows that the new status quo is vulnerable if proper due care is not ensured.

[3] discuss how the RTS were debated and lobbied by companies in the financial sector who pushed for screen scraping not to be totally forbidden. The EBA currently accepts screen scraping as a fallback mechanism and demands authentication between the scraper (TPP) and the information source (ASPSP). The fallback mechanism can be omitted if specific reasons to exempt are met. One can observe that the existence of the fallback mechanism increases the fragmentation in the data transfer sphere, which is already affected by the fragmentation created by the different API architectures.

[42] analyze PSD2 (SCA) and other similar regulations and standards through the lens of multi-factor authentication compliance. Their work is valuable as market participants must pay attention to more than one set of regulatory requirements. [43] mention transaction manipulation attacks when the 2 factors of authentication rely on a single device. This is an important implication that developers of SCA systems must be aware of. [44] gives a warning sign regarding companies using SMS one-time passwords (OTPs) as a means of complying with SCA, as these have proved to be easy to abuse by hackers[2].

In summary, the RTS have important cybersecurity implications, and organizations must prepare for challenges such as lack of maturity at TPPs, data transfer fragmentation leading to complexity, screen scraping and different inherent vulnerabilities of systems.

2.4 Application Programming Interface

In this section, APIs, one of the crucial aspects of the CSC regulatory technical standard, is presented from the literature.

At a basic level, an API is “a way for two computer applications to talk to each other over a network using a common language that they both can understand” [45]. Despite being around for some time, APIs present themselves as a novelty to many existing players in the e-payment industry. [36] state that banks should see the APIs and the emerging digital platform as opportunities, warning at the same time that the benefits will be observed in the long term. Zachariadis et al. compare this to Amazon, which needed several years to build excellent IT systems to become a global giant that offers user-centric services. [46] come to aid with an agile reference model for large barks to adopt APIs. [47] provide an overview of translating business needs of interoperability and data transfer to a FinTech API gateway. Their study

[2] https://www.europol.europa.eu/newsroom/news/sim-highjackers-how-criminals-are-stealing-millions-highjacking-phone-numbers

features a real-world implementation from a Turkish bank. On the other end of the process, [48] show an integration on an example technology stack and assess its security using OWASP's Top 10 Web Application Security risks [49]. Their work highlights TLS and the communication channel's security, an aspect explored later in this paper. [50] offers a systematic approach for PSD2 API testing and validation, with a focus on XS2A. An automated approach in the same context is presented by [51], which draws knowledge from [52] and OWASP's Top 10 API Security issues [53].

Issues that were identified by [54] regarding APIs in a PSD2 context are functionality and availability. Functionality is a challenge as integrations might be done in a "watered down" fashion just to comply with the requirements or only with specific, large-enough partners, thus not achieving an ideal data exchange. This goes back to the idea of platforms and "banking-mix" of services, contrasting a truly open marketplace. Availability is an inherent technical challenge that requires participants to build robust, scalable services, including the APIs and the fallback screen scraping mechanism, if present.

To conclude, much research has been done in the area of APIs for financial organizations and in a PSD2 context, highlighting security risks and implementation advice, making use of reputable vulnerability sources such as OWASP.

2.5 Qualified certificates

In this section, qualified certificates for PSD2 will be discussed, from the legal grounds to what advancements the literature proposes.

[4] provides the framework for the legality of electronic transactions in the EU. Following this regulation (eIDAS), different eID (digital identity) schemes have been developed or adapted to the standard. [55] analyzes the security of such schemes, finding 7 out of 15 of them being vulnerable. TLS is a common theme in these vulnerabilities, a relevant aspect as TLS is used across the Internet for secure communication. As the authors described it, "the insecurity of one component can bypass the security of the entire system, even if all the other components are secure".

According to [4], a qualified digital certificate is a PKI certificate that ensures the data integrity and authenticity of an electronic signature and its related data (such as a message). It is issued by a qualified trust service provider (QTSP). The qualified certificate must present the following information:

- Details of the qualified trust service provider that produced the certificate, such as: (EU) member state, name and registration number;

- Validation data, to be used electronically to validate the certificate;
- Validity of the certificate (starting and ending date).

The qualified certificates have different applications in e-governance: [56] show an integration of qualified electronic signatures with blockchain transactions for verifying academic diplomas; [57] employs homomorphic encryption for preserving privacy in the context of the Dutch eID scheme.

In a PSD2 context, the specifications for the qualified certificates are defined by [13]; [12] specifies their specific use cases for the different parties involved in the data transfers:

- QWAC - qualified certificate for website authentication - used for confidential communication and identification of PSPs to ASPSPs (without being able to verify the origin of the data present in the communication on its own);
- QSealC - qualified certificate for electronic seal - used for identifying PSPs to ASPSs (without ensuring the confidentiality of the transfer on its own).

In terms of literature focusing on PSD2 qualified certificates, [51] provide an example of how QWAC uses TLS to ensure the security of the communication and incorporate TLS as a step in their testing framework. In general, one can observe a lack of focus of works discussing QWAC and QSealC in the current literature, this gap being explored in the present paper.

In summary, the specifications, technical details and use cases of qualified certificates for digital signature stem from a legal basis from entities such as the European Parliament and EBA. The research around the subject mainly concerns applications in e-governance such as eID and less on PSD2 and the e-payment market.

2.6 Conclusion

In this chapter, an overview of the necessary background information has been presented in a structured way: starting from the top-level concept of Open Banking towards the regulatory framework of PSD2, its technical aspects represented by RTS and the systemic components APIs and qualified certificates.

Chapter 3

Common and secure open communication

The term CSC was coined and originated in the RTS. The first section of this chapter is dedicated to a descriptive analysis of the CSC articles from the Regulatory Technical Standards. The second section summarizes the main technical aspects extracted from the articles and identifies cybersecurity requirements through their connection with CIA. The final section uses the previous two for observing the technological assets that are needed or must undergo changes for CSC.

3.1 Articles

[2] discusses CSC in Chapter 5, “Common and secure open standards of communication”, covering articles 25 to 31. This section is structured according to the articles, providing a commentary for each of them.

3.1.1 Article 25 - Requirements for identification

The first CSC article stipulates that the PSPs must ensure secure communication between a payer’s device and a payee’s acceptance devices when making electronic payments. The article does not express how “secure” must be interpreted here.

3.1.2 Article 26 - Traceability

The Traceability article explains what traceability should be in the present context: “ensuring knowledge ex-post of all events relevant to the electronic transaction in the various stages". Additionally, the article mandates a unique session identifier, timestamps based on "a unified time-reference system", and detailed logging of transactions data, including the transaction number.

3.1.3 Article 27 - Communication interface

Article 27 is the most extensive article concerning CSC from the RTS.

In paragraph 1, the reader is presented with requirements such as identification and secure communication between ASPSPs and TPPs. These detail entail that identification must also happen in the case of screen scraping.

In paragraph 3, the article requires that the "integrity and confidentiality of the personalized security credentials" must be ensured, a more concrete explanation of secure communication than the previous parts.

Also, in this article, a distinction is made between a "dedicated" interface (API) and the interface users typically use for direct interaction with the ASPSP (which can be screen scraped). Both have to follow "standards of communication which are issued by international or European standardization organizations". This detail is essential, as it shows how CSC relies on unnamed supporting standards, which can create confusion.

Lastly, testing facilities and support must be provided by ASPSPs for the interface(s) they make available.

3.1.4 Article 28 - Obligations for dedicated interface

This article provides additional rules for the dedicated interface. Firstly, it must have "the same level of availability and performance" as the standard interface used by the users. Its availability and performance must be monitored. Lastly, the dedicated interface must use "ISO 20022 elements, components or approved message definitions, for financial messaging". A high-level explanation of the ISO 20022 elements is given below.

ISO 20022 elements ISO 20022 [58] is a standard for message exchange between financial institutions. It aims to provide a common understanding of interpreting the data used in financial operations. The main provision of the standard is the use of XML as the common syntax for messages. As XML is more verbose than other syntaxes and the volume of data increases as technology becomes more used, ISO 20022 mandates ASN.1 for encoding the data in XML for compactness and improved encoding/decoding speed. These two elements, XML and ASN.1, are used for the definition of data structures. A “dictionary” which provides semantic descriptions for business components and types of messages is managed by ISO 20022 Registration Authority[1]. It is worth noting that in [59], a translation model is offered as an effort to adapt ISO 20022 concepts to the use of JSON syntax and RESTful APIs, which provides more freedom in adopting the standard.

3.1.5 Article 29 - Certificates

This article gives guidance on the use of digital certificates. The certificates that are to be used for CSC are qualified certificates for electronic seals (QSealC) and qualified certificates for website authentication (QWAC) as defined by eIDAS. Some changes to the eIDAS specifications are in place:

- The registration number specified by the certificate must be the authorization number given by a home member state to the PSP following the licensing process;
- An extra data entry in the certificate must be the role of the PSP, for example, PISP or AISP;
- An extra data entry in the certificate must be the “name of the competent authorities” where the PSP is registered, for example, the Dutch National Bank.

3.1.6 Article 30 - Security of communication session

In the first paragraph, Article 30 stipulates that secure encryption (“strong and widely recognized encryption techniques”) must be used during the communication between all the PSD2 parties to safeguard the confidentiality and integrity of the data.

The subsequent paragraphs discuss how the communication access sessions must be “securely linked to the relevant sessions” of the PSUs to prevent “misrouting” (other users or actors seeing details not belonging to their sessions). Furthermore, the sessions must be kept as short as possible and be terminated after the “requested action has been completed”.

The last paragraph of this article presents a restriction to the transferred data. The security credentials of users or authentication codes cannot be readable, directly or indirectly, by any staff.

[1] https://www.pwc.dk/da/publikationer/2017/strong-customer-authentication-common-secure-communication-psd2-nutshell-4.pdf

3.1.7 Article 31 - Data exchanges

The last article for “Common and secure open standards of communication” specifies mostly functional requirements for the communication participants. One detail related to security is that if an interface does not function properly, the other exchange participants must be notified; if there are problems with the API, this must give notification messages about the issues.

3.2 Technical details

After describing the CSC articles, a summary can be created from the essential points. The findings are presented in Table 3.1:

Technical details	Article(s)
Secure communication (integrity and confidentiality)	25, 27, 30
Traceability	26
Unique, short-lived session which is linked to the right user	26, 30
Use of APIs	27
Testing facilities and support	27
Using ISO 20022 messaging concepts	28
Identification through (extended) QWAC & WSealC certificates	29
Strong and widely recognized encryption techniques	30
Participants notification in case of failure	31

Table 3.1: CSC technical details

The list can be refined in order to identify concrete cybersecurity requirements. The approach used for this is to tie a technical detail identified before to a direct way of preserving CIA (Confidentiality, Integrity or Availability) in information systems. For example, “Participants notification in case of failure” does not have a direct impact on CIA, the notification happening after the loss of CIA, not helping to prevent the loss. On the other hand, “strong and widely recognized encryption techniques” help preserve the confidentiality of communication, being selected as a concrete cybersecurity requirement.

The results are listed in Table 3.2.

Cybersecurity requirements	Article(s)
Secure communication (integrity and confidentiality)	25, 27
Unique, short-lived session which is linked to the right user	26, 30
Identification through (extended) QWAC & WSealC certificates	29
Strong and widely recognized encryption techniques	30

Table 3.2: CSC cybersecurity requirements

3.3 Impacted assets

As shown in the previous sections, the RTS on CSC mandates changes to sustain the function of communicating PSU data. The assets affected by these changes are found in this section, completing the descriptive analysis of CSC. For identifying the organizational assets related to CSC, a working definition of "asset" must be provided. An asset is "anything that has value to the organization and which therefore requires protection" [14]. CSC essentially requires a (business and technical) process of transferring data between ASPSPs and TPPs. Using the ISO 27005 exemplification of assets from the standard's Annex B.1.1, we can classify this as follows:

- PSU data sharing process (between ASPSPs and PSPs; used for both AISPs and PISPs) - business process/activity ("necessary for the organization to comply with contractual, legal or regulatory information")
- PSU data (customer details and transactions) - information ("vital information for the exercise of the organization's mission or business")

The supporting assets that enable the primary assets have been identified using Annex B.1.2 of [14] for a more granular view. The selection process involved checking if a supporting asset mentioned in the standard supports the CSC primary assets. An example of inclusion is hardware, which is comprised of devices such as routers that enable connectivity between parties in the PSD2 architecture. An example of exclusion is the organization, as, within the scope of the research, organizational aspects are not analyzed. An outlier is the support asset "Qualified certificates". Despite certificates not being mentioned in the ISO 27005 standard, the qualified certificates are valuable and a strict requirement of the RTS on CSC. The selected assets are listed in Table 3.3.

Supporting asset	Supports PSU data sharing process	Supports PSU data
Hardware (servers, data storage)	Yes	Yes
Databases	Yes	Yes
APIs	Yes	Yes
Communication network	Yes	No
Qualified certificates	Yes	No
Personnel	Yes	Yes
Website (normal interface)	Yes	Yes

Table 3.3: Selected supporting assets

While all supporting assets contribute to the existence of risks, PSD2 or CSC did not introduce assets such as hardware, databases or personnel to organizations. These assets were already present and assessed in terms of risk using standards such as [60], or [61]. Furthermore, they were regulated under NIS Directive [62] or GDPR [63]. Because of these considerations, the current work will not use all the supporting assets for the next steps of the research. Only the specific assets introduced by CSC are taken into consideration. APIs and qualified certificates are novelties mandated by PSD2. Also, all the CSC articles mention conditions and rules for communication, prompting the introduction of “Communication network” as an asset. The assumption here is that the PSD2 communication network is separated from the already existing communication networks present in an organization. In reality, they can also be the same. In summary, the assets to be studied are:

Supporting asset	Supports PSU data sharing process	Supports PSU data
APIs	Yes	Yes
Communication network	Yes	No
Qualified certificates	Yes	No

Table 3.4: Identified CSC-specific supporting assets

Chapter 4

Risk assessment

In this chapter, a cybersecurity risk assessment is performed on the CSC aspects of PSD2. The output is a prioritized list of risk scenarios and their level of risk, representing the answer to the second sub-question. The methodology used is adapted from Clause 7 and 8 of ISO 27005 (“Information security risk assessment”) and Chapter Three of NIST 800-30 (“The process”), which are parts of industry-recognized standards for cybersecurity risk assessment. The two approaches are combined in a similar fashion to [64] and [65] (which exemplified the technique proposed by Setiawan et al.). In essence, ISO 27005 is used as the main framework, providing the steps and approach for conducting the assessment. The output of one step serves as an input for the next one. The chapter is structured according to these steps. NIST 800-30 (Revision 1) provides proper concrete directions and tools for performing the assessment, such as assessment scales (for likelihood and impact). Throughout the chapter, the origin of concepts or examples is provided. The value in using such a methodology is ensuring that “repeated information security risk assessments produce consistent, valid and comparable results” [60].

For a top-level understanding of the method, together with the corresponding sections, a schema is provided in Figure 4.1.

4.1 Context establishment

The first step in performing cybersecurity risk assessment (the standards use the term “information security”[1]) is establishing the context. The context establishment is an important step because the decisions taken here influence the final result of

[1] While some differences exist, in practice, there is a large overlap between cybersecurity and information security (https://cloudacademy.com/blog/cybersecurity-vs-information-security-is-there-a-difference/)

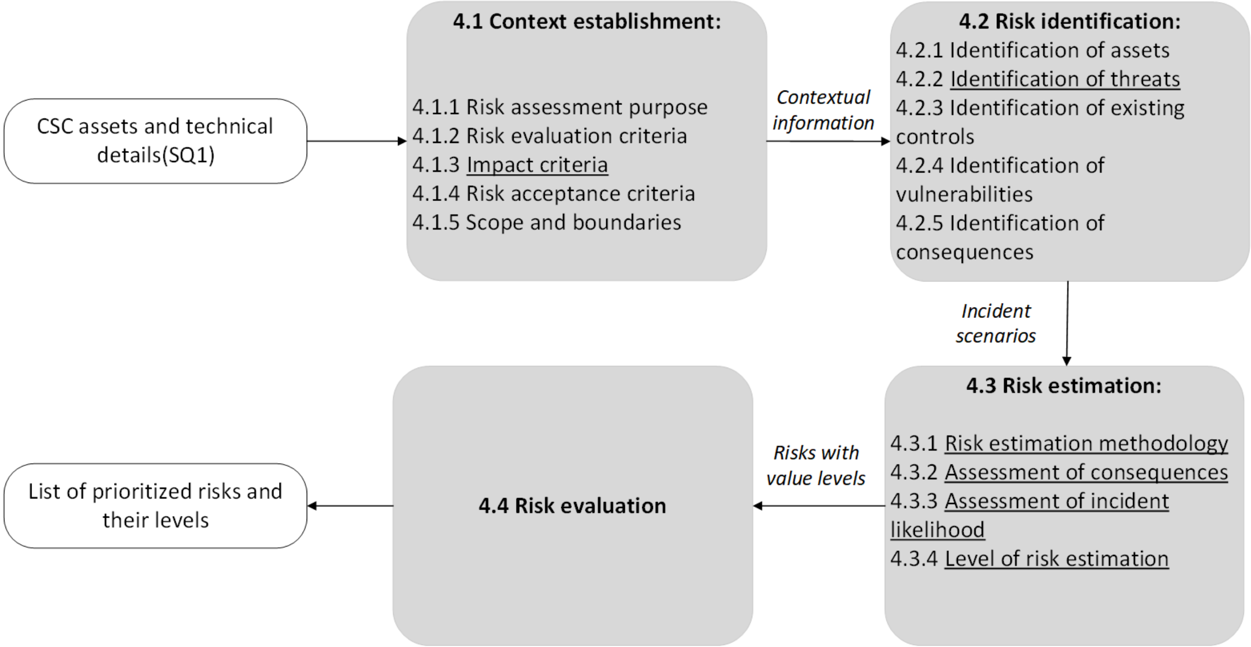
4.1 Context establishment:
4.1.1 Risk assessment purpose
4.1.2 Risk evaluation criteria
4.1.3 Impact criteria
4.1.4 Risk acceptance criteria
4.1.5 Scope and boundaries
4.2 Risk identification:
4.2.1 Identification of assets
4.2.2 Identification of threats
4.2.3 Identification of existing controls
4.2.4 Identification of vulnerabilities
4.2.5 Identification of consequences
CSC assets and technical details(SQ1)
Contextual information
Incident scenarios
4.3 Risk estimation:
4.3.1 Risk estimation methodology
4.3.2 Assessment of consequences
4.3.3 Assessment of incident likelihood
4.3.4 Level of risk estimation
Risks with value levels
4.4 Risk evaluation
List of prioritized risks and their levels

Figure 4.1: A combined methodology based on ISO 27005 and NIST 800-30. Underlined steps have input from NIST 800-30.

the process. At this stage, the purpose, risk evaluation criteria and impact criteria of the assessment are decided.

4.1.1 Risk assessment purpose

[14] gives examples of potential purposes. The applicability of each of them is discussed. “Supporting an ISMS” (information security management system) represents a purpose tied to an organization’s internal strategy. “Preparation of an incident response plan” and “Preparation of a business continuity plan” focus mainly on the processes needed for dealing with a cybersecurity incident and how to maintain the business processes available. “Legal compliance and evidence of due diligence” makes the assessment more focused on the applicable regulations and how the organization complies with them. For this research, the purpose loosely falls under “description of the information security requirements for a product, a service or a mechanism”. The purpose of the risk assessment for this research is to describe the information security requirements for a generic CSC system where an ASPSP shares PSU data with a licensed TPP.

4.1.2 Risk evaluation criteria

The risk evaluation criteria must be set at this stage of the context establishment. This step is valuable as the criteria can be used to "specify priorities for risk treatment". In our case, the criteria are selected from the list provided in [14] Section 7.2. The selection is based on how applicable are the criteria to the defined purpose. As an example, "legal and regulatory requirements" are applicable, as the ASPSPs and PSPs have to comply with regulations such as PSD2, NIS Directive [66] and GDPR [63]. Also, they all have reputations to maintain, and the public can have negative attitudes towards the brand following a cybersecurity incident[2].

As the current research provides a general, top-level view, some criteria have been omitted as an accurate estimation is not viable at this analysis level. While all criteria involve some organizational knowledge, the study omitted criteria that involve in-depth knowledge about the organization, such as the stakeholders' expectations, strategy or structure. The implication can be a loss of precision in performing the assessment (the introduction of "uncertainty", as expressed by [15]). However, considering the study is exploratory in nature, value is still captured despite the omissions. The research can act as a starting point from which organizations can include internal information to refine the criteria and perform a more accurate assessment.

The criteria that have been selected are listed below.

- The criticality of the information assets involved
- Legal and regulatory requirements
- Operational and business importance of confidentiality, availability and integrity (CIA)
- Negative consequences for the reputation

4.1.3 Impact criteria

Another aspect that must be developed is the impact criteria. The impact criteria are essential as they are used to evaluate the damage or costs to an organization for a cybersecurity event. In Chapter 7.2 from [14], a list of considerations is provided. Like before, some criteria have been discarded based on granularity and insights into specific companies. "Level of classification of the impacted information asset" cannot be known without having inside knowledge from organizations. The same reasons apply to the discard of "Disruption of plans and deadlines". "Impaired operations" is applicable, as the payment user data cannot be transferred anymore in

[2] https://tdwi.org/articles/2018/10/29/biz-all-impact-of-equifax-data-breach.aspx

case of disruptions (for example, availability), and some services might become unavailable (e.g. paying a merchant from a TPP's application). The applicable criteria to the CSC risk assessment are:

- Breaches of information security (e.g. loss of CIA)
- Impaired operations
- Damage of reputation
- Breaches of legal, regulatory or contractual requirements

Despite providing ideas about the crucial factors for considering impact, the ISO 27005 guidelines are not enough in practice. [15] aids at this step by providing an assessment scale for quantifying the impact of threat events. Table A.3 in the Appendix shows the concrete categories of impact.

4.1.4 Risk acceptance criteria

The next part of context establishment is defining the risk acceptance criteria. [14] stipulates that risk acceptance criteria "depend on the organization's policies, objectives and the interests of stakeholders". In this study, such information is not available as the research focuses on the generic risks. In contrast, the risk acceptance criteria are determined by each organization individually, considering their internal situation and risk appetite. In conclusion, no criteria can be set for what risk treatment action should be undertaken (for example, what constitutes an acceptable risk or what risks require immediate remediation).

4.1.5 Scope and boundaries

Setting the scope and boundaries is crucial to understanding what is and what is not included in the risk assessment. The scope of the present risk assessment is comprised of the information assets specific to CSC: the APIs used for customer data sharing under PSD2; the communication network used for this data sharing; the qualified digital certificates used for secure communication and identification of licensed parties, together with the process around securing the communication and identifying parties. This risk assessment focuses on particular areas, while a comprehensive risk assessment would incorporate much more assets, processes or functions.

Additionally, situations where multiple parties are involved are outside the scope due to the added granularity, making the analysis infeasible. Examples here include a

PSP using a gateway provider in charge of the data transfer and the co-existence of APIs and standard interface (website).

Lastly, depending on the internal organizational infrastructure, some inter-dependencies might exist. The PSU data might originate from the same database or data storage used by other business functions. A successful threat event at this level would have increased significance and damage. Due to the increasing complexity in accommodating edge cases and scenarios, the assumption is that the PSD2 systems are stand-alone.

4.2 Risk identification

After the context has been established, the next stage, according to [14], is risk identification. Per [14], a risk is “a combination of the consequences that would follow from the occurrence of an unwanted event and the likelihood of the occurrence of the event”. More concisely:

$$Risk = Likelihood * Impact$$

This section describes the identification of assets, threats, existing controls, vulnerabilities and consequences.

4.2.1 Identification of assets

The assets to be used in the risk assessment have been identified in the previous chapter in Table 3.4. The supporting assets are APIs, Communication network, Qualified certificates. [14] specifies the need to identify, for each asset, an asset owner. This person helps determine the asset’s value and is responsible for its “production, development, maintenance, use and security as appropriate”. At a high level of analysis, identifying these stakeholders is not possible, as it requires knowing the internal organization of companies.

The final part of asset identification is assigning each asset a value to rank and establish priorities. Considering the small set of assets (3) and the fact that PSD2 regulates their use through the RTS and stipulates fines in case of non-compliance[3], their value can be judged as equal.

[3] `https://zoek.officielebekendmakingen.nl/kst-34813-3.html` *(Dutch)*

4.2.2 Identification of threats

The next step is the identification of threats. A threat is, per [15], “any circumstance or event with the potential to adversely impact organizational operations and assets, individuals, other organizations, through an information system”. It can be both internal and external. Important attention must be given to human threat sources. Due to their importance in handling money and personal information, credit institutions and payment service providers are a prime target for an extensive list of human threats. A comprehensive list is provided in the Annex in Table A.8. The list is supplied by [14] (Annex C - Examples of typical threats).

[14] also provides a list of generic threats in Annex C of the standard (also called a “threat catalog”). [15] provides a threat catalog in Table E-2. The two lists are used as the basis of identifying threats and their relation to the supporting assets identified previously, matching according to type.

This matching process can be explained with examples. The APIs are instances of software, thus can be subject to threats affecting software (like “software malfunction”). The communication network is matched to threats related to networking. For qualified certificates, threats associated with the process of validating certificates are identified from the catalog. One must notice how the guarding of a company’s own certificates is not included, as this falls under certificate/secrets management and is outside of the scope of this research. Other threat types outside the scope are environmental or natural threats such as hurricanes, flooding or fires, etc.

Some threats have been deemed not applicable for the scenario at hand. For example, “Fraudulent copying of software” refers to piracy and intellectual property theft. In the case of systems built for CSC, the implementation is aided by the standards proposed by entities such as the Berlin Group and the Open Banking Standard. Thus, the systems cannot be judged as unique, attackers being more interested in perturbing the service or stealing data. In the future, it is expected to see new systems that provide unique value [36], for example, by leveraging Artificial Intelligence or other novel techniques, which make use of proprietary algorithms. This example shows the importance of frequent assessment: what might not be a risk today can become one in the future. Per NIST 800-30, “risk assessments are not simply one-time activities that provide permanent and definitive information”.

The selected threats can be found in Table 4.1.

Type of threat	**Threat**	**Origin**	**Affected supporting assets**
Compromise of functions	Abuse of rights	A, D	APIs
	Denial of actions	D	Communication network, Qualified certificates
	Error in use	A	APIs, Qualified certificates
	Forging of rights	D	APIs, Communication network, Qualified certificates
Compromise of information	Eavesdropping	D	Communication network
	Tampering with software	A, D	APIs
Technical failures	Saturation of the information system	A, D	APIs, Communication network
	Software malfunction	A	APIs
Unauthorized actions	Corruption of data	D	APIs
	Illegal processing of data	D	APIs
	Remote spying	D	Communication network
	Unauthorized use of equipment	D	Communication network

Table 4.1: Identified threats related to CSC. A - accidental; D - deliberate.

4.2.3 Identification of existing controls

The subsequent step in the ISO methodology is the identification of existing controls. This step avoids "unnecessary work or cost" in both the risk assessment and the actions taken by organizations following the assessment results. The output of the risk assessment thus becomes residual risk (the risk left after some security controls are implemented).

Applying the methodology strictly, one would review internal organizational documents or audits or consulting the information security team regarding what controls exist and if they work correctly. Since this study looks at generic risks that might apply to a class of organizations, selecting controls that may or may not exist in the organizations is challenging. Furthermore, assuming the controls are working efficiently would deem incorrect results. The decision is not to assume any existing controls are deployed for the threats identified previously. This decision results in identifying inherent risk (risk in the absence of any implemented controls).

4.2.4 Identification of vulnerabilities

The next step is the identification of vulnerabilities. Again, [14] provides an extensive catalog that is adapted to the output of the threat identification step. The matching is done through the threats - a vulnerability can be used by a threat to create damage. For example, if in the previous step, "abuse of rights" was selected for one or more assets, one listing from [14] such as "well-known flaws in the software" can be chosen since APIs have some standards flaws if not implemented correctly [53]. On the other hand, "lack of audit trail" concerns the cybersecurity governance and is outside of the scope. Table 4.2 shows the identified vulnerabilities and provides examples.

Asset	Threat	Vulnerability	Example
APIs	Abuse of rights	Well-known flaws in software	[4]
	Abuse of rights	Wrong allocation of access rights	[5]
	Corruption of data	Wrong parsing of data	[6]
	Error in use	Incorrect parameter set up	[7]
	Illegal processing of data	Lack of malware protection	[8]

	Forging of rights	Lack of identification and authentication mechanisms like user authentication	9
	Forging of rights	Unnecessary services enabled	10
	Saturation of the information system	Lack of rate-limiting	11
	Software malfunction	Unclear or incomplete specifications for developers	12
	Tampering with software	Uncontrolled use of software	13
Communication network	Denial of actions	Lack of proof of sending or receiving a message	14
	Eavesdropping	Unprotected sensitive traffic	15
	Forging of rights	Lack of identification and authentication of sender and receiver	16
	Remote spying	Insecure network architecture	17
	Remote spying	Transfer of passwords in clear	18
	Saturation of the information system	Inadequate network management (resilience of routing)	19
	Unauthorized use of equipment	Unprotected public network connections	20
Qualified certificates	Error in use	Wrong certificate validation	21
	Forging of rights	Theft of certificates or keys	22

	Denial of actions	Lack of proof of sending or receiving a message	[23]

Table 4.2: Identified vulnerabilities related to CSC

4.2.5 Identification of consequences

The last step of risk identification is the identification of consequences. A consequence can be "loss of effectiveness, adverse operating conditions, loss of business, reputation, damage, etc.". An essential part of the risk assessment framework, being aware of the consequences allows one to understand the harmful effect threats can have in different areas and on the organization as a whole.

The scenarios in Table 4.3 are developed based on the threats, vulnerabilities and examples provided, using knowledge sources for adversary tactics and techniques, MITRE ATT&CK[24] and [53] being the most famous ones. The consequences are identified from a CIA perspective. It is worth noting the consequences can unfold in other areas too. For example, a scenario where PSU data is leaked can result in

[4] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3025

[5] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1973

[6] Rounding error such as https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7619

[7] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0269

[8] Malware used to steal data: https://enterprise.verizon.com/resources/reports/dbir/

[9] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28148

[10] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3242

[11] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-20252

[12] Lack of clarity derived from the RTS [67]

[13] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1443

[14] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3025

[15] Not using encryption to make the traffic confidential.

[16] Communication protocols such as IP are inherently insecure; not using additional protocols means the communicating parties are not authenticated https://www.cloudflare.com/learning/network-layer/what-is-ipsec/

[17] https://www.redscan.com/news/ten-top-threats-to-vlan-security/

[18] https://heartbleed.com/

[19] https://www.zdnet.com/article/ddos-attacks-big-rise-in-threats-to-overload-business-networks/

[20] https://www.dw.com/en/access-all-areas-why-public-wifi-networks-are-as-insecure-as-they-were-15-years-ago/a-17966256

[21] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3449

[22] https://securelist.com/stuxnet-and-stolen-certificates/29724/

[23] Signature service, not specific to qualified certificates: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13101

[24] https://attack.mitre.org/

reputational damage[25] and regulatory fines[26].

[25] https://www.csoonline.com/article/3019283/

[26] https://www.theguardian.com/business/2019/jul/09/marriott-fined-over-gdpr-breach-ico

Asset	Threat	Vulnerability	Scenario	Consequence (Loss of C, I or A)
APIs	Abuse of rights	Well-known flaws in software	An attacker exploits an injection vulnerability to access more data than allowed[27]	C, I, A
APIs	Abuse of rights	Wrong allocation of access rights	An attacker elevates their API rights to access confidential data or perform privileged actions[28]	C, I
APIs	Corruption of data	Wrong parsing of data	A programming error leads to payment amounts to be erroneously rounded, leading to data inconsistency[29]	I
APIs	Error in use	Incorrect parameter set up	A permissive Cross-Origin Resource Sharing (CORS) policy allows an attacker to connect to an API[30]	C, I

APIs	Illegal processing of data	Lack of malware protection	A host system with access to payment information gets infected with malware, which exfiltrates data[31]	C
APIs	Forging of rights	Lack of identification and authentication mechanisms like user authentication	An attacker communicates with the API without being authorized[32]	C, I
APIs	Forging of rights	Unnecessary services enabled	The API response contains more information than needed for the provision of the service[33]	C
APIs	Saturation of the information system	Lack of rate limiting	An attacker overloads the system with a large number of requests, making it unavailable[34]	A
APIs	Software malfunction	Unclear or incomplete specifications for developers	The lack of clarity introduces flaws in the APIs[35]	C, I or A

APIs	Tampering with software	Uncontrolled use of software	An attacker modifies settings or the environment the API runs in, resulting in abnormal behavior[36]	C, I or A
Communication network	Denial of actions	Lack of proof of sending or receiving a message	An attacker spoofs a payment confirmation, allowing themselves to keep/gain funds[37]	I
Communication network	Eavesdropping	Unprotected sensitive traffic	An attacker eavesdrop on the network, analyzing the traffic and stealing private data[38]	C
Communication network	Forging of rights	Lack of identification and authentication of sender and receiver	An attacker spoofs their IP address to access the communication network, pretending to be a trusted party[39]	C
Communication network	Remote spying	Insecure network architecture	An attacker joins a private network[40]	C

Communication network	Remote spying	Transfer of passwords in clear	An attacker is able to read passwords, codes and secrets that are transmitted[41]	C
Communication network	Saturation of the information system	Inadequate network management (resilience of routing)	An attacker floods the network with requests, leaving benign requests without answer[42]	A
Communication network	Unauthorized use of equipment	Unprotected public network connections	An attacker leverages a data transfer or process happening on a network they have control over, disrupting the communication[43]	A
Qualified certificates	Error in use	Wrong certificate validation	An attacker sends a maliciously crafted message to be validated as a qualified certificate and is authorized by the system[44]	C, I

Qualified certificates	Forging of rights	Theft of certificates or keys	An attacker uses a stolen certificate or key to identify itself as a licensed party[45]	C, I
Qualified certificates	Denial of actions	Lack of proof of sending or receiving a message	An attacker interacts with the CSC infrastructure without being traced by the system[46]	C, I

Table 4.3: Incident scenarios and consequences

[27] https://attack.mitre.org/techniques/T1190/

[28] https://attack.mitre.org/techniques/T1548/

[29] https://support.microsoft.com/en-us/topic/the-rounding-is-incorrect-and-the-final-amount-is-incorrect-when-you-use-the-payment-method-with-the-invoice-rounding-precision-parameter-set-in-the-hungarian-version-of-microsoft-dynamics-nav-2009-r2-fd8e967f-65b9-77f3-4515-ea0fcedc35d4

[30] API7:2019 Security Misconfiguration [53]

[31] https://attack.mitre.org/techniques/T1587/001/

[32] API2:2019 Broken User Authentication [53]

[33] API3:2019 Excessive Data Exposure [53]

[34] https://attack.mitre.org/techniques/T1499/

[35] An idea developed by [67]

[36] https://attack.mitre.org/techniques/T1584/004/

[37] https://owasp.org/www-community/attacks/Repudiation_Attack

[38] https://attack.mitre.org/techniques/T1040/

[39] Spoofing as part of threat modeling: https://owasp.org/www-pdf-archive//OWASP-BeNeLux_2010_ThreatModeling.pdf

[40] https://attack.mitre.org/techniques/T1133/

[41] https://attack.mitre.org/techniques/T1040/

[42] https://attack.mitre.org/techniques/T1498/

[43] https://www.ieee-icnp.org/2000/papers/2000-24.pdf

[44] https://attack.mitre.org/techniques/T1190/

[45] https://attack.mitre.org/techniques/T1588/004/

[46] API10:2019 Insufficient Logging & Monitoring [53]

4.3 Risk estimation

Risk estimation is a collection of steps that involves attributing values to the components identified previously.

4.3.1 Risk estimation methodology

[14] explains different methodologies for risk estimation, in general being one of qualitative, quantitative or a combination of the two. The qualitative estimation is often "used first to obtain a general indication of the level of risk and to reveal the major risks". An advantage of a qualitative estimation is "the ease of understanding by all relevant personnel". Since the risk assessment findings are to be shared and validated with the Dutch e-payment market participants, this ease of understanding prompted the use of a qualitative estimation methodology. A scale (Very Low, Low, Medium, High and Very High) is used to rank the magnitude of potential consequences and the likelihood of these consequences. The scale is larger than the example given in [14](Low, Medium and High) to provide a finer-grained classification. It also matches the scales used by [15]. Making these methodology decisions explicit can be helpful for organizations that want to use this research as a starting point for their own assessment.

4.3.2 Assessment of consequences

In the assessment of consequences, the "business consequences of loss or compromise of the asset", given an incident scenario, is analyzed. There are different types of impact that are relevant. Their categorization [14] is presented below.

Direct impact:

- The cost of suspended operations due to the incident until the service is restored
- The scenario results in an information security breach

Indirect impact:

- The cost of interrupted operations
- Potential misuse of information obtained through a security breach
- Violation of statutory or regulatory obligations

Considering the two categories of impact and [15]'s assessment scale of impact of threat events (available in Table A.3, the following impact assessment is created from the incident scenarios and consequences by applying the scale to each scenario. A commentary is provided for explaining the thought process and aiding replicability. The results of this step can be found in Table 4.4.

Asset	Scenario	Impact	Commentary
APIs	An attacker exploits an injection vulnerability to access more data than allowed	Moderate	Results in significant damage to the customer data; results in significant harm to individuals as their data is leaked; however, no serious or life-threatening harm is inflicted; the organization is still able to perform its functions.
APIs	An attacker elevates their API rights to access confidential data or perform privileged actions	Moderate	Results in significant damage to the customer data; results in significant harm to individuals as their data is leaked; however, no serious or life-threatening harm is inflicted; the organization is still able to perform its functions.
APIs	A programming error leads to payment amounts to be erroneously rounded, leading to data inconsistency	Low	Causes a degradation in mission capability. Results in minor damage to organizational assets and minor financial loss.
APIs	A permissive Cross-Origin Resource Sharing (CORS) policy allows an attacker to connect to an API	Very Low	Negligible adverse effect on organizational operations; connecting to an API does not necessarily mean data can be queried.

APIs	A host system with access to payment information gets infected with malware, which exfiltrates data	High	Results in major damage to the organization assets, as a large volume of data can be leaked; the malware can also steal more company secrets or private data than just PSU data; can result in major financial loss, as GDPR and other regulations require companies to guard customer data [63].
APIs	An attacker communicates with the API without being authorized	High	Results in major damage to the customer data; results in significant harm to individuals as their data is leaked; however, no serious or life-threatening harm is inflicted; the organization is still able to perform its functions. The reputation is damaged, and fines can be inflicted.
APIs	The API response contains more information than needed for the provision of the service	Very Low	Results in a negligible adverse effect, as only licensed parties can see the excess information.

APIs	An attacker overloads the system with a large number of requests, making it unavailable	High	Results in major damage to the APIs; The organization cannot perform its PSU data sharing function mandated by PSD2.
APIs	The lack of clarity introduces flaws in the APIs	Moderate	Depending on the flaw, it can result in significant degradation in mission capability or significant financial loss.
APIs	An attacker modifies settings or the environment the API runs in, resulting in abnormal behavior	Low	Results in minor damage, the organization is still able to perform its functions.
Communication network	An attacker spoofs a payment confirmation, allowing themselves to keep/gain funds	Moderate	Results in significant financial loss and significant financial harm to individuals (PSUs) affected.
Communication network	An attacker eavesdrop on the network, analyzing the traffic and stealing private data	Moderate	Results in significant damage to the PSU data; results in significant reputation damage, financial loss and potential fines.
Communication network	An attacker spoofs their IP address to access the communication network, pretending to be a trusted party	Low	Results in minor damage to organizational assets, as using a different IP is not enough to participate in the communication, which makes use of qualified certificates.

Communication network	An attacker joins a private network	Low	Results in minor damage to organizational assets, as being part of the network is not enough to intercept confidential communication.
Communication network	An attacker is able to read passwords, codes and secrets that are transmitted	High	Results in major damage to organization assets as APIs, communication network and other assets owned by an organization; the PSD2 data sharing must be temporarily stopped to avoid more secrets leakage that can cascade in other systems being breached.
Communication network	An attacker floods the network with requests, leaving benign requests without answer	Moderate	Results in significant damage to the communication network; the PSD2 data sharing function is significantly reduced.
Communication network	An attacker leverages a data transfer or process happening on a network they have control over, disrupting the communication	Low	Limited adverse effect, as data can be usually routed through other networks; causes a degradation as the transfer might take longer than before.

Qualified certificates	An attacker sends a maliciously crafted message to be validated as a qualified certificate and is authorized by the system	Moderate	Results in significant damage to the PSU data, as this can be now exfiltrated through the APIs.
Qualified certificates	An attacker uses a stolen certificate or key to identify itself as a licensed party	Moderate	Results in significant damage to the PSU data, as this can be now exfiltrated through the APIs.
Qualified certificates	An attacker interacts with the CSC infrastructure without being traced by the system	Low	Results in minor damage to the PSU data, as a relatively small number of actions cannot be traced (non-repudiation); can result in payment fraud.

Table 4.4: Impact evaluation

4.3.3 Assessment of incident likelihood

Having assessed the impact of the incident scenarios, the next step is evaluating the likelihood of the scenarios. The likelihood is a factor that helps compute the risk, together with the impact. Factors that affect the likelihood are, according to [14]:

- experience and applicable statistics for threat likelihood
- for deliberate threat sources: the motivation and capabilities, which will change over time, and resources available to potential attackers, as well as the perception of attractiveness and vulnerability of assets for a possible attacker
- vulnerabilities, both individually and in aggregation

Once again, [15] comes to aid with a clear delimitation of likelihood. The standard discusses the likelihood of threat event initiation/occurrence (depending on if the threat originates from an adversary or is accidental) and the likelihood of the threat event resulting in adverse impacts. They can be consulted in the Annex in Tables A.4 and A.5, respectively. Combining the two, the overall likelihood is created (Table A.6). Applying the scales to the scenarios, we obtain the following:

Asset	**Scenario**	**Likelihood of initiation/occurrence**	**Commentary**
APIs	An attacker exploits an injection vulnerability to access more data than allowed	Very High	Automated injection tools[47] make the initiation very easy.
APIs	An attacker elevates their API rights to access confidential data or perform privileged actions	High	An adversary is highly likely to initiate the event due to the value of performing privileged actions (like discovering files on the system).
APIs	A programming error leads to payment amounts to be erroneously rounded, leading to data inconsistency	Low	The event is unlikely to occur or occurs less than once a year (e.g. during the initial implementation of payment calculations).
APIs	A permissive Cross-Origin Resource Sharing (CORS) policy allows an attacker to connect to an API	Very High	Attackers are almost certain to try to connect to an API by bypassing CORS due to the value[48] of the data accessible through the API.

APIs	A host system with access to payment information gets infected with malware, which exfiltrates data	Very High	An adversary is almost certain to initiate the threat event, as malware has been widely spread in recent years, including in the financial sector[49].
APIs	An attacker communicates with the API without being authorized	Very High	An adversary is almost certain to initiate the threat event due to the value of the data.
APIs	The API response contains more information than needed for the provision of the service	Low	Unlikely to occur, as extensive testing is required by API owners [50].
APIs	An attacker overloads the system with a large number of requests, making it unavailable	Moderate	An adversary is somewhat likely to initiate the threat event[51].
APIs	The lack of clarity introduces flaws in the APIs	Low	Error or accidents are unlikely to occur thanks to the numerous standards that help with PSD2 implementation.
APIs	An attacker modifies settings or the environment the API runs in, resulting in abnormal behavior	Moderate	An adversary is somewhat likely to initiate the event to disrupt the service or get data access.

Communication network	An attacker spoofs a payment confirmation, allowing themselves to keep/gain funds	High	An adversary is highly likely to initiate the event to gain money[52].
Communication network	An attacker eavesdrop on the network, analyzing the traffic and stealing private data	Very High	An adversary is almost certain to initiate the threat event to steal valuable data.
Communication network	An attacker spoofs their IP address to access the communication network, pretending to be a trusted party	Very High	An adversary is almost certain to initiate the threat event, as IP spoofing is an aged and established technique[53].
Communication network	An attacker joins a private network	Very High	An adversary is almost certain to initiate the threat event to see traffic and map out the communication network for further attacks.
Communication network	An attacker is able to read passwords, codes and secrets that are transmitted	Very High	An adversary is almost certain to initiate the threat event due to the value the secrets have.

Communication network	An attacker floods the network with requests, leaving benign requests without answer	High	An adversary is almost certain to initiate the threat event, as Denial-of-Service attacks are a popular attack[54].
Communication network	An attacker leverages a data transfer or process happening on a network they have control over, disrupting the communication	Moderate	An adversary is somewhat likely to initiate the threat event, depending on how much disruption it can cause or if they try to distract from another attack[55].
Qualified certificates	An attacker sends a maliciously crafted message to be validated as a qualified certificate and is authorized by the system	Very High	An adversary is almost certain to initiate the threat event, as having a validated qualified certificate can be a step in accessing valuable data from the APIs.
Qualified certificates	An attacker uses a stolen certificate or key to identify itself as a licensed party	Very High	An adversary is almost certain to initiate the threat event, as presenting valid keys can be a step in accessing valuable data from the APIs.

Qualified certificates	An attacker interacts with the CSC infrastructure without being traced by the system	Very High	An adversary is almost certain to initiate an interaction with the CSC infrastructure due to the importance of data transferred through it.

Table 4.5: Likelihood of initiation/occurrence

Asset	**Scenario**	**Likelihood of adverse impacts**	**Commentary**
APIs	An attacker exploits an injection vulnerability to access more data than allowed	High	The threat is highly likely to have adverse impacts, such as data exfiltration[56].
APIs	An attacker elevates their API rights to access confidential data or perform privileged actions	High	The threat is highly likely to have adverse impacts[57].

[47] https://owasp.org/www-community/Vulnerability_Scanning_Tools

[48] https://www.itproportal.com/features/what-is-the-value-of-stolen-digital-data/

[49] https://securelist.com/financial-cyberthreats-in-2020/101638/

[50] Article 27 of [2] on CSC specifies the requirement for testing facilities.

[51] https://www.computerweekly.com/news/450411443/Lloyds-Bank-hit-by-massive-DDoS-attack

[52] A similar scenario happened in relation with PIN confirmation: https://thehackernews.com/2021/02/new-hack-lets-attackers-bypass.html

[53] https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=9d18fc06-b229-4c4a-8ca5-7386d0870c01&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments

[54] https://www.itsecurityguru.org/2020/09/09/massive-rise-in-ddos-attacks-post-covid-19/

[55] https://www.infradata.nl/en/news-blog/ddos-attacks-growing-ever-more-sophisticated-and-efficient/

APIs	A programming error leads to payment amounts to be erroneously rounded, leading to data inconsistency	High	The threat is highly likely to have adverse impacts due to the importance of precision in calculations.
APIs	A permissive Cross-Origin Resource Sharing (CORS) policy allows an attacker to connect to an API	Moderate	The threat is somewhat likely to have adverse impacts, as other vulnerabilities might be exploited afterwards.
APIs	A host system with access to payment information gets infected with malware, which exfiltrates data	Very High	The threat is almost certain to have adverse impacts, such as data breaches.
APIs	An attacker communicates with the API without being authorized	Very High	The threat is almost certain to have adverse impacts, such as data breaches[58].
APIs	The API response contains more information than needed for the provision of the service	Low	The threat is unlikely to have adverse impacts, as only licensed partners should see the API responses in the first place.
APIs	An attacker overloads the system with a large number of requests, making it unavailable	Very High	The threat is almost certain to have adverse impacts, as the other parties cannot access the data.

APIs	The lack of clarity introduces flaws in the APIs	Moderate	The threat is somewhat likely to have adverse impacts, depending on the flaws introduced.
APIs	An attacker modifies settings or the environment the API runs in, resulting in abnormal behavior	Moderate	The threat is somewhat likely to have adverse impacts in terms of access control and availability.
Communication network	An attacker spoofs a payment confirmation, allowing themselves to keep/gain funds	Very High	The threat is almost certain to have adverse impacts such as loss of funds.
Communication network	An attacker eavesdrop on the network, analyzing the traffic and stealing private data	Very High	The threat is almost certain to have adverse impacts in terms of the loss of confidentiality of data.
Communication network	An attacker spoofs their IP address to access the communication network, pretending to be a trusted party	Low	The threat is unlikely to have adverse impacts, as additional origin checks (like certificates) should be in place[59].
Communication network	An attacker joins a private network	Moderate	The threat is somewhat likely to have adverse impacts[60].

Communication network	An attacker is able to read passwords, codes and secrets that are transmitted	Very High	The threat is almost certain to have adverse impacts as the secrets can be used to gain access to organizational resources [61].
Communication network	An attacker floods the network with requests, leaving benign requests without answer	Very High	The threat is almost certain to have adverse impacts as the data transfer would be temporarily stopped[62].
Communication network	An attacker leverages a data transfer or process happening on a network they have control over, disrupting the communication	Low	The threat is unlikely to have adverse impacts in terms of loss of availability.
Qualified certificates	An attacker sends a maliciously crafted message to be validated as a qualified certificate and is authorized by the system	High	The threat is highly likely to have adverse impacts as the attacker is identified as a trusted partner who can communicate with the APIs.

Qualified certificates	An attacker uses a stolen certificate or key to identify itself as a licensed party	High	The threat is highly likely to have adverse impacts as the attacker is identified as a trusted partner who can communicate with the APIs.
Qualified certificates	An attacker interacts with the CSC infrastructure without being traced by the system	Moderate	The threat is somewhat likely to have adverse impacts, as the attacker must be authorized first, but possible errors and abuses are not being detected.

Table 4.6: Likelihood of adverse impacts

Asset	**Scenario**	**Likelihood of initiation/occurrence**	**Likelihood of adverse impacts**	**Overall likelihood**

[56] https://www.bleepingcomputer.com/news/security/freepik-data-breach-hackers-stole-83m-records-via-sql-injection/

[57] https://attack.mitre.org/tactics/TA0004/

[58] https://nordicapis.com/5-major-modern-api-data-breaches-and-what-we-can-learn-from-them/

[59] Article 29 of [2] on CSC specifies the requirement for identification.

[60] If data is not encrypted, it can be leaked to the attacker; even if it is, discovering the networking topology is possible, and it is useful in starting other attacks: https://attack.mitre.org/techniques/T1590/004/

[61] https://threatpost.com/florida-water-plant-hack-credentials-breach/163919/

[62] Article 28 of [2] on CSC specifies the requirement for monitoring the availability and performance of the APIs; if these are not kept at a high level, this must be reported to the national competent authority.

APIs	An attacker exploits an injection vulnerability to access more data than allowed	Very High	High	Very High
APIs	An attacker elevates their API rights to access confidential data or perform privileged actions	High	High	High
APIs	A programming error leads to payment amounts to be erroneously rounded, leading to data inconsistency	Low	High	Moderate
APIs	A permissive Cross-Origin Resource Sharing (CORS) policy allows an attacker to connect to an API	Very High	Moderate	High.

APIs	A host system with access to payment information gets infected with malware, which exfiltrates data	Very High	Very High	Very High
APIs	An attacker communicates with the API without being authorized	Very High	Very High	Very High
APIs	The API response contains more information than needed for the provision of the service	Low	Low	Low
APIs	An attacker overloads the system with a large number of requests, making it unavailable	Moderate	Very High	High
APIs	The lack of clarity introduces flaws in the APIs	Low	Moderate	Low

APIs	An attacker modifies settings or the environment the API runs in, resulting in abnormal behavior	Moderate	Moderate	Moderate
Communication network	An attacker spoofs a payment confirmation, allowing themselves to keep/gain funds	High	Very High	Very High
Communication network	An attacker eavesdrop on the network, analyzing the traffic and stealing private data	Very High	Very High	Very High
Communication network	An attacker spoofs their IP address to access the communication network, pretending to be a trusted party	Very High	Low	Moderate
Communication network	An attacker joins a private network	Very High	Moderate	High

Communication network	An attacker is able to read passwords, codes and secrets that are transmitted	Very High	Very High	Very High
Communication network	An attacker floods the network with requests, leaving benign requests without answer	High	Very High	Very High
Communication network	An attacker leverages a data transfer or process happening on a network they have control over, disrupting the communication	Moderate	Low	Low
Qualified certificates	An attacker sends a maliciously crafted message to be validated as a qualified certificate and is authorized by the system	Very High	High	Very High

Qualified certificates	An attacker uses a stolen certificate or key to identify itself as a licensed party	Very High	High	Very High
Qualified certificates	An attacker interacts with the CSC infrastructure without being traced by the system	Very High	Moderate	High

Table 4.7: Likelihood evaluation

4.3.4 Level of risk estimation

Finally, the level of risk can be identified by using the previously computed impact and likelihood, using the scale for level of risk from [15](shown in the Annex in Table A.7). The overall risk is presented below. Where the scenario has a High or Very High level of risk, the level is shown in bold.

Asset	Scenario	Likelihood	Impact	Level of risk
APIs	An attacker exploits an injection vulnerability to access more data than allowed	Very High	Moderate	Moderate
APIs	An attacker elevates their API rights to access confidential data or perform privileged actions	High	Moderate	Moderate
APIs	A programming error leads to payment amounts to be erroneously rounded, leading to data inconsistency	Moderate	Low	Low

APIs	A permissive Cross-Origin Resource Sharing (CORS) policy allows an attacker to connect to an API	High	Very Low	Very Low
APIs	A host system with access to payment information gets infected with malware, which exfiltrates data	Very High	High	**High**
APIs	An attacker communicates with the API without being authorized	Very High	High	**High**
APIs	The API response contains more information than needed for the provision of the service	Low	Very Low	Very Low

APIs	An attacker overloads the system with a large number of requests, making it unavailable	High	High	**High**
APIs	The lack of clarity introduces flaws in the APIs	Low	Moderate	Low
APIs	An attacker modifies settings or the environment the API runs in, resulting in abnormal behavior	Moderate	Low	Low
Communication network	An attacker spoofs a payment confirmation, allowing themselves to keep/gain funds	Very High	Moderate	Moderate

Communication network	An attacker eavesdrop on the network, analyzing the traffic and stealing private data	Very High	Moderate	Moderate
Communication network	An attacker spoofs their IP address to access the communication network, pretending to be a trusted party	Moderate	Low	Low
Communication network	An attacker joins a private network	High	Low	Low
Communication network	An attacker is able to read passwords, codes and secrets that are transmitted	Very High	High	**High**

Communication network	An attacker floods the network with requests, leaving benign requests without answer	Very High	Moderate	Moderate
Communication network	An attacker leverages a data transfer or process happening on a network they have control over, being able to read the data transmitted	Low	Low	Low
Qualified certificates	An attacker sends a maliciously crafted message to be validated as a qualified certificate and is authorized by the system	Very High	Moderate	Moderate

Qualified certificates	An attacker uses a stolen certificate or key to identify itself as a licensed party	Very High	Moderate	Moderate
Qualified certificates	An attacker interacts with the CSC infrastructure without being traced by the system	High	Low	Low

Table 4.8: Level of risk

For convenience, the risk scenarios have been numbered (Table 4.9) and placed in a matrix that shows their distribution according to the likelihood and impact. In Table 4.10, the contents of a cell are the number (or IDs) of risk scenarios that have the likelihood corresponding to the y/vertical axis and the impact corresponding to the x/horizontal axis. The non-empty cells at the High/Very High intersections have been colored red.

#	**Scenario**
1	An attacker exploits an injection vulnerability to access more data than allowed
2	An attacker elevates their API rights to access confidential data or perform privileged actions
3	A programming error leads to payment amounts to be erroneously rounded, leading to data inconsistency
4	A permissive Cross-Origin Resource Sharing (CORS) policy allows an attacker to connect to an API
5	A host system with access to payment information gets infected with malware, which exfiltrates data
6	An attacker communicates with the API without being authorized

7	The API response contains more information than needed for the provision of the service
8	An attacker overloads the system with a large number of requests, making it unavailable
9	The lack of clarity introduces flaws in the APIs
10	An attacker modifies settings or the environment the API runs in, resulting in abnormal behavior
11	An attacker spoofs a payment confirmation, allowing themselves to keep/gain funds
12	An attacker eavesdrop on the network, analyzing the traffic and stealing private data
13	An attacker spoofs their IP address to access the communication network, pretending to be a trusted party
14	An attacker joins a private network
15	An attacker is able to read passwords, codes and secrets that are transmitted
16	An attacker floods the network with requests, leaving benign requests without answer
17	An attacker leverages a data transfer or process happening on a network they have control over, being able to read the data transmitted
18	An attacker sends a maliciously crafted message to be validated as a qualified certificate and is authorized by the system
19	An attacker uses a stolen certificate or key to identify itself as a licensed party
20	An attacker interacts with the CSC infrastructure without being traced by the system

Table 4.9: Numbered list of scenarios

Impact Likelihood	**Very Low**	**Low**	**Moderate**	**High**	**Very High**
Very Low					
Low	7	17	9		
Moderate		3, 10, 13			
High	4	14,20	2	8	
Very High			1, 11, 12, 16, 18, 19	5, 6, 15	

Table 4.10: Level of risk - Matrix

Out of the 20 identified risk scenarios, the distribution of risk level looks the following:

- Very Low: 2 scenarios
- Low: 7 scenarios
- Moderate: 7 scenarios
- High: 4 scenarios
- Very High: 0 scenarios

One can observe an absence of Very High risks. A possible explanation for this might be that the PSD2 sharing function is just one function the organizations perform, successful threat events in this area not perturbing the whole organizational activity. Critical disruption might happen provided systems are shared (e.g. customer database); however, such scenarios have not been taken into account due to the scope of the research. In the case of credit unions and banks, the PSD2 sharing function is secondary to the main banking activities for customers. For TPPs and Fintechs, this function likely has higher importance due to their reduced reach than with the banks. The interview research stage aims to uncover differences between the two groups of organizations in their perception of risk. The most prominent risks, having the level "High", are:

- A host system with access to payment information gets infected with malware, which exfiltrates data
- An attacker communicates with the API without being authorized
- An attacker overloads the (API) system with a large number of requests, making it unavailable
- An attacker is able to read passwords, codes and secrets that are transmitted

The first scenario, regarding the malware infection, shows how common and dangerous this attack vector is [68]. "Communicating with the API without being authorized to do so" has a Very High likelihood and High impact, as PSU data can be extracted, resulting in a data breach, an event that affects organizations in multiple ways: breaches [63]'s principle of data confidentiality, and can result in fines and reputational damage. The third scenario, essentially a denial-of-service attack, has great importance due to the commoditization of such attacks[63]. The last scenario concerns the security of communication and how the protection of sensitive information like passwords or codes is essential, as the use of stolen credentials continues

[63] https://www.forbes.com/sites/davelewis/2015/04/29/commoditization-of-ddos-attacks/

to be a leading action variety for data breaches [68].

4.4 Risk evaluation

Finally, the risk evaluation compares the risk estimation results with the risk evaluation criteria to identify priorities for risk treatment. The output of this step would be "a list of risks prioritized according to risk evaluation criteria" [14].

As seen in the previous steps, four risk scenarios present a High level. While some of the other risk scenarios have either the likelihood or impact classified as High or Very High (e.g. "An attacker eavesdrop on the network, analyzing the traffic and stealing private data"), a common approach is first to treat the scenarios which overall have a High or Very High risk (Per [15]: "the greatest attention going to high-risk events"). How these risks are compared to the risk criteria can be observed in 4.11.

Risk evaluation criteria	Applicability to High-risk scenarios
The criticality of the information assets involved	The information assets involved are critical for the PSD2 data sharing function.
Legal and regulatory requirements	If the incidents happen, regulators will demand explanations: competent national authorities can request reports and investigations might be launched to determine if organizations have employed the proper due diligence and due care, e.g. protecting personal data [63] or ensuring an appropriate level of performance and availability of systems [2]. Depending on these, fines might be issued.
Operational and business importance of confidentiality, availability and integrity (CIA)	As reputation is important, the CIA properties can be deemed important as well for the businesses.
Negative consequences for reputation	Data leakage or systems unavailability can be harmful to the reputation.

Table 4.11: Applicability of risk evaluation criteria to High-risk scenarios

Following the arguments in Table 4.11, the High risks should be prioritized in terms of risk treatment.

4.5 Conclusion

By applying a combined methodology of [14] and [15], a risk assessment has been performed on the assets created by the RTS on CSC. A number of risk scenarios are evaluated to have a High level, which should prompt action from the organizations implementing PSD2 systems as risk treatment. These risks can be observed below.

Risk scenario	Affected asset	Level of risk
A host system with access to payment information gets infected with malware, which exfiltrates data	APIs	High
An attacker communicates with the API without being authorized	APIs	High
An attacker overloads the system with a large number of requests, making it unavailable	APIs	High
An attacker is able to read passwords, codes and secrets that are transmitted	Communication network	High

Table 4.12: Prioritized risk scenarios

Chapter 5

E-payment market participants

After assessing the CSC cybersecurity risks, the PSD2 legislation and academic studies are analyzed to identify the relevant stakeholders for CSC. In this context, stakeholders represent entities such as companies or organizations that are subject to the changes mandated by PSD2, having to comply with the directive. Having discovered the general roles, an inquiry is made into the organizations which are subject to CSC in the Dutch e-payment market. The output of this chapter is two lists of stakeholders, which is also the answer for the third research sub-question.

5.1 General roles

[69], the official PSD2 law, distinguishes different roles in the new PSD2 ecosystem. A short description and their connection with CSC is provided below.

Payment Service Provider A generic institution that offers e-payment services to Payment Service Users (PSUs), which also existed before PSD2. They might share PSU data with other entities, under or outside of PSD2.

Account Servicing Payment Service Provider The ASPSP represents a traditional financial institution that provides payment accounts (such as current accounts, credit cards) to consumers. Examples of ASPSPs are banks and credit card companies. CSC mandates that any ASPSP must provide an interface (can be an existing one) for TPPs to identify themselves with and to communicate securely with when accessing customer financial information (for AISP) or initiating a payment (for PISP). The RTS on CSC then specifies details of the security of the interfaces and how aspects such as traceability, logging, encryption or identification must be implemented. When emergencies require technical changes, the ASPSP must document these changes and make them available to the competent national authority on request. Furthermore, if a dedicated interface is used, its availability and performance must be monitored, and the resulting statistics must be made available to the competent authorities, on request. If the dedicated interface operates at a lower level of availability than the normal interface, this must be reported to the competent authorities.

Account Information Service Provider AISPs act as a common link between different PSU's accounts from one or more ASPSPs. The primary purpose is to offer a unified view of one's accounts. Competent authorities grant them licenses.

Payment Initiation Service Provider The PISP provides a PSU with the possibility to initiate a payment from (one of) their account(s) to a payee. It eliminates the user's need to use a payment network that might incur interchange fees. The competent authorities must authorize a PISP through a license.

Electronic Money Institution Electronic Money institutions, or E-Money institutions, are authorized to issue e-money, offer money remittance services, process payment transactions and other services typical to a PSP. They do not necessarily share PSU data with other entities.

Payment Service User The end customer, which holds one or more accounts with one or more ASPSPs. The PSU authorizes a PSP by giving explicit consent to their financial data or to the action of making a payment. There is no requirement for a contract between the customer and a Payment Service Provider (PSP) [30].

Competent authorities PSD2, as a pan-European piece of legislation, is transposed into the local regulation of each member state [70]. Each country has different authorities that are tasked with aspects such as licensing and compliance.

After listing the roles described in the directive, a focused exploration of the Dutch participants can be made.

5.2 Dutch organizations

In order to discover the relevant Dutch actors of the e-payment ecosystem, one approach is to start with the regulators. In the Netherlands, the supervision of PSD2 is divided between a number of actors [1]:

- AFM (Autoriteit Financiële Markten) supervises the complaints procedures, the right of PSUs to use services from TPPs and the provision of information from PSPs in general;
- De Nederlandsche Bank (DNB) is in charge of issuing licenses to TPPs, the access to accounts (XS2A), risk management and authentication for PSPs;
- The Dutch Data Protection Authority (AP) supervises the protection of people's privacy (in relation to GDPR);
- The Dutch Authority for Consumers and Markets (ACM) is responsible for compliance with competition rules, access to payment systems and supervises the calculation of surcharges for payments.

For finding entities supervised under PSD2 in the Netherlands, one must either turn to DNB or EBA. The data for Dutch organizations is provided to EBA by DNB and AFM[2].

Firstly, for discovering "credit institutions" as defined by PSD2 for the role of ASPSPs, which have the country of residence The Netherlands, the banks register of the DNB is queried [3]. The selected entities have the following type ("Registratietype"): Provision of bank services to EEA, Carrying on the business of a bank. They are all based in the Netherlands. Branches of international banks active in the Netherlands are excluded, as they are more likely to implement PSD2 systems on a global level or in their home markets. The complete list can be consulted from Table A.1 in the Appendices.

Secondly, the same approach used by [32] is deployed for finding licensed payment service providers. EBA's Payment Institutions Register [4] is queried to find licensed institutions which are of the following types: (1) Payment Institutions (PI; includes organizations with AISP or PISP license) and (2) Electronic Money Institutions (EMI). Institutions licensed outside the full scope of PSD2 and not allowed to provide payment services outside of the country they gained licenses in were excluded. Annex A.2 offers the reader the complete list.

In the Netherlands, other actors emerge, which are not mentioned in the official PSD2 documents, as they are specific market collaborative initiatives.

[1] https://www.afm.nl/nl-nl/professionals/onderwerpen/psd2 (*Dutch*)

[2] https://www.eba.europa.eu/risk-analysis-and-data/register-payment-electronic-money-institutions-under-PSD2

[3] https://www.dnb.nl/en/public-register/register-of-banks/

[4] https://euclid.eba.europa.eu/register/pir/search

Dutch Banking Association The *Nederlandse Vereniging voor Banken (NVB)* is the association of banks in the Netherlands. It is a group of interest that acts as “the link between the banking sector, the government and the public”[5]. As they engage in consultations with legislators and supervisors, they represent banks collectively.

Dutch Payments Association The *Betaalvereniging* has as members providers of payment services: banks, electronic money institutions and payment institutions. The association manages “the collective aspects of cybersecurity policy in relation to the payment system”, aiming to contain cybercrime [33]. Many of the credit institutions or payment providers previously identified are part of this association[6]. One notable mention of the association is the establishment of an IBAN-Name check that helps prevent fraud and incorrect transfers[7].

United Payment Institutions Netherlands The *Verenigde Betaalinstellingen Nederland* (VBIN) is the Dutch interest group for payment institutions registered or exempted as a Payment Institution or Electronic Money Institution. They represent the interests of such organizations in legislation and regulation, PSD2 being a major focus[8]

In conclusion, relevant participants for this research count over 100 entities, grouped in four categories: credit institutions, payment institutions, regulators and different associations for banking or payments.

[5] https://www.nvb.nl/english/dutch-banking-association-nederlandse-vereniging-van-banken/

[6] https://www.betaalvereniging.nl/over-ons/leden/

[7] https://www.betaalvereniging.nl/en/actueel/nieuws/dutch-banks-introduce-innovative-iban-name-check/

[8] https://www.vbin.nl/over-ons/ *(Dutch)*

Chapter 6

Interviews

This chapter provides the approach, methodology and answers from the interview phase of the research (Stage II of the methodology).

6.1 Interview approach

In order to validate the findings of prioritized cybersecurity risk scenarios related to CSC, obtained through a risk assessment detailed in Chapter 4, semi-structured interviews are used. They offer a flexible way [71] to understand the cybersecurity effect market participants experienced. The first section explains the interviewing approach, while the second part presents the output from the interviews.

6.1.1 Interview methodology

The chosen structure for the interviews is semi-standardized (or semi-structured). This structure allows for the discovery of unanticipated directions to explore [72]. Specifically for this study, the unanticipated directions might be represented by risks not found by the risk assessment or other factors that affect the cybersecurity consequences of CSC. This type of interviewing is also useful when one attempts "to delve deeply into a topic and to understand thoroughly the answers provided" [73].

The development of the interview approach has been structured according to principles outlined by [72]. The first step is the setting of objectives. The objectives of the interviews are:

- To understand the risks organizations face concerning CSC, starting from a pre-determined list (obtained through the risk assessment of a generic PSD2 CSC system). By doing so, the fourth research sub-question can be answered;

- To probe if the relevant Dutch stakeholders believe CSC increased their overall cybersecurity risks (last sub-question).

The next step is the identification of the kinds of data needed for the stated objectives. The data required has the form of (validated and ranked) risk scenarios and their risk levels (resulting from likelihood and impact), and the expert opinions/impressions from the interviewees. Thanks to the flexibility of the approach, the interviews allow the discovery of different trends or factors that might not be expected initially (a hypothetical example can be very different risk levels due to specific organizational features).

Based on the types of data to be obtained that support achieving the objectives of the interviews, the interview protocol (parts and questions) is explained in the next paragraph, following a theoretical basis.

Firstly, the interview participants are presented with the question topics before the interview (as part of the information brochure that is made available) and how long the discussion is expected to last; this allows for a more informed decision of the interviewees to be involved in the research or not [72]. Since the interviews are semi-structured, the questions are not fixed, the interviewer having the freedom to insist more on some while skipping others. Also, the tone of the questions is more informal, and highly technical words and jargon are avoided. This allows for a "more flowing and conversational interview interaction" [72]. On the same note, the interviewer's attitude is one of an "interested listener", who listens attentively.

The interview protocol has been structured using two main components. The first component is a "funnel protocol" [73]. [72] encourages that, after the formalities, the interview starts with easy questions (e.g. "What is your position at Company X?") for building rapport between the interviewer and the participant and fostering "a degree of commitment" on the participant's side. Then, the funnel protocol employs broad questions (also called grand tour) where the interviewee discusses their work, the relation with PSD2 and if they came across risks stemming from the directive. The questions become increasingly directed, reaching specifics about the risk scenarios found by the author through the risk analysis and how critical these scenarios are. Then, the second component of the protocol is an "inverted funnel". Here, the interviewee is placed in the context of the topic. Having asked about the specifics of CSC cybersecurity risks, the high-level goals and implications of PSD2 are discussed, ending in questions about a desired future state (e.g. hypothetical PSD3). The second stage is used to lead to a broader discussion about PSD2.

Overall, the interview protocol, presented in Section A.9 in the Annexes, contains different types of questions: throwaway questions [72] (initial questions, greetings, mood checks), essential questions (about CSC risks and opinion on PSD2's cybersecurity implications), probing questions (e.g. "Could you tell me more about that?") and ranking questions [73](e.g. "Can you rank these?"). The protocol avoids "problem" questions: double-barreled, leading, with double negatives, vague, using emotional language or unfamiliar jargon [73].

Lastly, for better transparency towards the interviewees, the transcript created following the interviews is sent back to the interview participants. They are given the option to amend answers or retract their consent to participate in the research.

6.1.2 Interview participants

The interview participants can be found in Table A.10 in the Annexes. Based on the author's advertising of the study, they have been selected based on the lists comprised in Chapter 5, based on voluntary participation following the advertising of the study, via email and LinkedIn. This is a "cluster sampling" approach [73] that helps reach a certain population (working individuals in organizations that are influenced by PSD2 either through compliance or through regulatory powers) from one geographic area (the Netherlands). In total, 92 organizations were contacted (36 banks, 49 payment providers, 4 regulators and 3 associations), some requiring multiple points of contact (e.g. initial message, explanation of the research, introduction by work colleagues or supervisors). Eleven respondents from these organizations participated in the interviews, some with overlapping roles (e.g. a consultant who provided guidance to both ASPSPs and TPPs). One participant, working for one of the four regulators mentioned in the study, participates in the study with a personal opinion that does not represent a policy stance. The resulting participation rate (interviewed/contacted) is 11,95%. It is worth noting that some participants have been referred by earlier participants in a snowball sampling fashion [73]. Snowball sampling is sampling that "occurs when the research benefits from one participant suggesting or introducing another participant to the researcher". Another important aspect to note that the author's thesis internship with a global consultancy facilitated finding interview participants through the company's business network.

6.2 Interview answers

In this section, the interview answers are presented and analyzed. The outputs are split between the discussion about CSC cyber risks (the first stage of the interview, which collects data for the fourth research sub-question) and the opinion on the CSC effect on overall cybersecurity risk (the second stage of the interview and the last sub-question). Each subsection is structured according to the main topics discussed in the interviews, generally outlining the participants' position regarding the subject, making use of quotes given by them.

6.2.1 Common and Secure Communication cybersecurity risks

This discussion theme encompassed showing the participants the four prioritized risks identified in the study (Table A.9) and questions around cybersecurity risks for their organization or the market. In terms of process and risk assessment awareness, most participants mentioned the initial risk analysis performed in the license application process coupled with the yearly risk assessment (both supplied to the DNB). In contrast, others respondents mentioned their internal risk assessments, also needed for other standards (like PCI-DSS [74]).

Applicability of the prioritized cybersecurity risks The interview participants were asked whether or not they found each of the prioritized risks to be applicable to their organization/to organizations in the payments ecosystem. Most of the participants confirmed the four risks as relevant, some of them (respondents #1, #6 and #7) even stating these risks are present in their own risk assessments. One participant deemed one scenario to be inapplicable to them (respondent #2, scenario B). The reason is the AISP and PISP licenses not being used by their organization, and for a party to communicate with their APIs "you need the website key that we give to the merchant to communicate with us, and then you have a secret key, also. There's a lot of responsibility at the merchant also to protect the data, so to speak. We provide the guidelines for them and then they have to keep their stuff secure and then we can safely communicate". This process differs from the authentication and authorization one used by PSD2, which relies on a trust provider and qualified certificates. Thus, scenario B was deemed not applicable for this organization at this moment. The percentage of validated scenarios (the number of validated scenarios divided by the total number of scenarios, considering all participants, multiplied by 100) is 97.72%.

Extending the list of cybersecurity risks The respondents did not add any additional cybersecurity risk scenarios in the scope of the research to the provided list; this further validates the risk assessment findings (the second part of Stage I of the study). However, they mentioned some risk insights in other areas which can be of relevance to organizations. Respondent #5 stated that "even if the risk per company stays the same, it will be multiplied by the number of extra TPPs". This view matches the one of [6]. Furthermore, "next to that, a big risk if you ask me from PSD2 is that you actually you only need one aggregator, as I call them, with a license, and they can send all the account information to other service providers that don't have a license. You will need GDPR consent for that, but it's not as regulated as the financial institutions are". This risk can be viewed as a governance one (since it involves the oversight, or lack of it, for some organizations in this market). Participant #10 also suggested an additional scenario where data might fall into the wrong hands: a rogue TPP being introduced in the ecosystem. This case falls primarily under governance, as agreed by the participant. It can also be seen as an instance of scenario B ("An attacker communicates with the API without being authorized") if authorization is understood as the right to participate in the PSD2 PSU data exchanges following a rigorous compliance and oversight process. Participant #11 indicated a scenario where payments are initiated in an unauthorized way ("I think that the financial damage of unauthorized payments could be quite large for a firm"). Two risk scenarios in the study's analysis can include this attack: "An attacker spoofs a payment confirmation, allowing themselves to keep/gain funds" and the unauthorized communication with the API (scenario B, which is used to initiate transactions). Only the second scenario is present in the final list. The payment spoofing scenario was classified with a Moderate impact and Very High likelihood (overall risk being Moderate), not being included in the prioritized list.

Classifying the likelihood, impact and overall risk of the scenarios For the next interview topic, the interviewees were asked to either confirm or reclassify the likelihood, impact and overall (inherent) risk of the scenarios, using a 5-level scale (Very Low - Low - Moderate - High - Very High). In their answers, the participants gave classifications motivated by different factors, which can increase or decrease the severity of risks without being controls (as the presence of controls implies the analysis of residual risks).

Firstly, factors reducing the risk levels are presented. The internal system architecture reduced both the likelihood and impact for respondent #8 for most scenarios by rendering data extraction difficult for an attacker, even in the absence of controls. One potential explanation for the presence of this factor is that the respondent is part of an organization that can be judged technologically advanced (their primary activity being a digital one, outside of the sphere of payments). Respondent #3, also from a tech-savvy organization, believes that using scalable infrastructure can lower the likelihood of scenario C "If I put a system on AWS or Azure or GCP, the chance that you can out-buy GCP is not really high, but the impact would of course still be high, because if you use a lot of my servers, I get a high bill, [...] not really something I want"); this resulted in a Moderate likelihood for scenario C). Another factor that lowers the likelihood is, according to the same interview participant, good practice coding, code reviews and hiring competent developers who “will do better than putting an API into production without at least somewhat decent authorization scheme”. Interviewees #1 and #7 stated that the likelihood of scenarios D and C, respectively, are also lower than the author’s classification: attackers might prefer attacking companies that are not licensed or supervised and have higher financial capabilities, as an attacker might deem this to be more cost-benefit viable. Participant #9, from a Payment Institution (PI), does not use PSU data from banks nor shares the payment data they use internally. They stated that “the data as such is not that valuable for them (the attackers) because it’s not containing any passwords or secrets that they could use, but the inherent likelihood, I would say is High (for scenario D)”. Using the same consideration, this respondent lowered the impact of scenario A. For scenario C, according to participant #10, “the impact is only on the availability. Maybe the impact could be a bit lower [...] Availability is lower on the radar than integrity so, if your data is being altered or changed, that is much worse than that you cannot access your data, based on the debate in the society, based on the debate within the government”. Thus, they classified this impact as Moderate, which, together with the High likelihood, brings the overall risk to Moderate. Respondents #4, #6 and #11 also saw unavailability as less impactful compared to data leakage or modification, with the fourth one mentioning how the current low adoption of AISP and PISP services makes availability not critical to most companies that provide these services.

The factors that elevate the risk dimensions of the scenarios (likelihood, impact, overall risk) are diverse across the participants’ answers. For scenario A, the impact is Very High according to interviewees #1, #2, #4 and #7. These respondents provided the following justifications: firstly, cards schemes (MasterCard and Visa) need to be notified (respondent #1: “and if you don’t have a really good reputation with your cards schemes and not a solid response, then they can even revoke your cards scheme license, and then you cannot do business anymore”); then, “companies might even lose their (PSD2) license” (respondent #7); finally, the consequences of having malware on the system are severe (“If it actually starts exfiltrating data right away, a company like ours that really relies on 100% availability all the time, I think to stop it we have to take drastic measures, maybe take some systems down. So, I think the impact would be Very High for us. Also, in terms of reputation, I think it could be catastrophic for us”). For any scenario where customer data is leaked, respondents #5, #6, and #11 see the impact as at least High (respondent #5: “doesn’t matter what type of scenario it is, then we will have reputational damage, not just financial damage”). Scenario D, which discussed insecure communication capturing secrets by attackers, prompted a Very High impact classification by participants #1 and #4 as attackers can effectively enter and see what is happening in a company.

Contrasting to other participants that view availability loss as less severe, this respondent saw the impact of scenario C, concerning a Denial-of-Service attack, as Very High, “because the law requires us to have, let’s say, 99.98% of (up)time. We also have agreements with our customers which also specify something like that. So, basically, there is almost zero tolerance for downtime”.

One respondent did not classify the scenarios (respondent #5, which has a role in IT Risk Management for an ASPSP). The complexity of their internal infrastructure, data and steps in the attack chain made it infeasible for them to classify the likelihood and impact and subsequently, the overall risk: “what we do in risk management is to give a rating based on very specific cases so we know what data is going through, what processes involves and what can be the potential damage, and if everything goes wrong, how much we’re losing, money-wise, reputation-wise and then we can give a rating”. The respondent’s answers can show that the risk scenarios found in the study, albeit relevant, are too broad and high-level for some organizations. Other participants confirmed this situation (e.g. respondent #7, about scenario D: “very relevant, but also a bit high level; we split passwords, codes and secrets in two different scenarios”). Respondent #11 classified the likelihood and overall impact of all risk scenarios. In contrast, they found it challenging to choose a value for the impact and decided instead to give a range, between High and Very High, for the four risks.

6.2.2 Common and Secure Communication and PSD2 opinion

In the second part of the interviews, participants were asked about the effect CSC had on their overall cybersecurity risk level, whether or not PSD2 achieved its objective of making payments safer and more secure and the shortcomings and potential improvements for the directive.

The PSD2 licensing/compliance journey A subset of the respondents described in detail their organization’s journey to implementing the changes mandated by PSD2 for acquiring a license or becoming compliant with the directive. One respondent from an E-Money organization which can be viewed as technologically advanced described this process as “long and hard”. The reasons are their organization not originally being a “financial institution” and, considering this environment, “it is harder to build the controlled processes and enforce specific controls”. Respondent #2 described their PSD2 compliance journey as “a lot of the rules; although they try to make it easy for small companies, also to be applied to them, I think a lot of them were still made with banks and such in mind. Some things are a little heavy for us so and they wouldn’t solve a lot of problems because we maybe had other measures in place to address the risks involved. Overall, it's a very bureaucratic thing, especially for a company like us, we like to be a little Fintech-type company". This view was confirmed by interviewee #4, as they believe many new entrants were not used to this amount of requirements, from PSD2 and the associated guidelines. On the other side of Open Banking, participant #6, from an ASPSP, also mentioned the great number of requirements and how their organization had to go back and forth with a regulator on some implementation aspects.

Effect of CSC on the overall cybersecurity risk level of organizations When asked about their opinion on this matter, the general answer from the participants was not clear. Respondents #8 and #11 believe CSC decreased these risks; respondents #6 and #10 think these were increased. At the same time, the other participants are unsure: some stating no tangible effect (participants #2, #3, #5 and #9), one mentioning the additional effort being needed for complying with another piece of legislation which cancels some benefits (the first respondent) and two stating that the cybersecurity levels were elevated, but also the sensitivity of data has increased (respondents #4 and #7).

PSD2's objective of increasing the safety and security of payments When asked about whether or not e-payments were made safer and more secure by PSD2, 6 out of the 11 participants agreed this was the case, five of them mentioning SCA as a leading factor in this, with additional participants highlighting the benefits of SCA (confirming the view of [7]). Three remaining participants did not clearly state that the directive increased or decreased the safety and security of e-payments. One of them (respondent #3) saying that PSD2 just acted as "an inspiration" to improve their security, the main improvements laying outside the PSD2 requirements, in their ISO 27001 certification journey. Two participants, working for an ASPSP and consulting TPPs, respectively, believe the payments are not safer and more secure following the directive, stating as cause the lack of control over the data in partner organizations or the lack of security maturity for some market participants. Overall, these results show a positive trend in the interviewed population. Correlating these findings with the ones regarding CSC and overall cybersecurity risks, a supposition can be made. It seems that SCA, mentioned by the majority of respondents in their answers to this question, contributed more than CSC at decreasing risks for PSD2 compliant organizations. SCA emerges as the essential novelty and area that organizations had to work on, while CSC resembles concepts and practices known by organizations, as they consistently worked on establishing secure communication channels.

Shortcomings of PSD2 and the future of the directive The final part of the interview contained questions about the shortcomings of the directive in the cybersecurity sphere, according to the interview participants. The respondents were also asked what they would like to see in the future (e.g. in a hypothetical PSD3) regarding cybersecurity. The respondents provided the author with extensive answers.

Some participants felt that the directive and its guidelines were at times hard to implement considering their specific organizational reality. Respondent #6 found as a shortcoming “the requirements which are related to the change management; they are very much hard to implement in the Agile companies”. Moving forward, they would like the EBA guidelines to be updated to “become more suitable for the technological companies, Agile companies”. The only missing aspect, which should be improved in the future, for respondent #9, is SCA. “The only thing, that we sometimes are struggling with, is the Strong Customer Authentication. It would be nice if more practical examples could be given about how the PSD2 legislation should be interpreted in different situations, because sometimes it’s assumed to be applicable to just a couple of examples[...] (The PSD2 landscape) is more an ecosystem with a lot of different organizations working together to provide a service where you have a certain payment facility. And I think it’s sometimes difficult to understand what is meant with PSD2 legislation from our perspective”. Respondent #6 also felt like the requirements were not entirely clear and had difficulties with SCA. Another participant believes that some rules should be proportionate to the organization’s risks (“The regulation places a lot of demands on firms; not all firms are in the same risks, I think the regulation could have permitted a little bit of flexibility there, for instance, there’s a lot of emphasis on business continuity. Now, business continuity is of course important, but it means something different for a very big bank and for a very small firm. I think there could have been a little bit more differentiation there so that firms can really put the effort in where the biggest risks are”). On the other hand, participant #2 states about potential shortcomings: “That is not how we look at them. We really look at them if we have any shortcomings regarding the guidelines they provide, because they have to write it for a very broad public so if it’s not really for us, then that is understandable”. This view contrasts the answers of the previously mentioned respondents that felt that, for their organizations, the guidelines and examples provided were not always applicable.

Participant #3 found shortcomings in the area of enforcing the directive at a national level. Firstly, the DNB guidelines for becoming licensed included verifying the company’s directors to prevent malicious actors from having leading positions in PSD2 companies. Still, this process was not an easy one for this participant. “What I found strange is that the risks for information security are in many PSD2 license companies much higher than the risks for a bad director because the director has a direct financial incentive to treat his own company in the right way, and the amount of hassle it takes to get your director verified is really, it much is quite enormous”. Secondly, a policy-focused approach of the regulator was observed by this interviewee. “Information security should be treated as a living thing, and I find it strange that DNB does not do that; they just want your policies, but the policies are just a bunch of papers, and there’s no guarantee for the papers being accurate in practice. If I were to design a PSD2 regulation, I would say, ‘OK, you should at least have an information security management system’. I believe it’s legally complicated to mandate an ISO 27001 certification, but you could just say, ‘OK, I want proof of a working ISMS[1]’ and then DNB can verify themselves, whether they find proof of a ‘plan, do, check, act’ cycle[2] in working, or they could say ‘OK, you can also let yourself be certified and then if you send us yearly your renewed certification, you get less visits from us because we can basically outsource trust’”. Lastly, this respondent disagrees that the Know Your Customer (KYC) and Anti Money Laundering (AML) checks must also be done by the TPPs sharing the PSU data from the banks. They believe it adds an extra barrier to entry. “I am 100% sure that the solution we designed (for KYC and AML) is not better than the solution the bank has because I have basically a development team of three people. I have to also create my app and have to create what actually adds value for my customers. All these PSD2 apps, all these Fintech companies basically have their own small Anti Money Laundering pipelines. These small pipelines will never be as sophisticated as you want at the bank. It’s the wrong amount of decentralization, rather, on the wrong level”.

One recurrent theme that appeared in multiple interviews was the scope of PSD2 and how it can be enlarged. Interviewee #5 mentioned some areas of extension for the type of data under scrutiny (“There are controls that are really required, for instance, customer related stuff that needs to be protected. It still does not solve the problem completely because there is much information, and we work sometimes in silos, so, the fact that some combination of information can really make it more sensitive, but we don’t really always have the view. PSD2 does really emphasize very strongly in the customer data, payment data specifically, but there are loads of other data within the bank that has the same issue. Of course, we’re always working towards this direction, but it’s not perfect”). Another area of improvement can be accounting for new technologies: “it will be great to have some guidance, not the requirements, about how we should deal with new technologies, such as AI and robotics, because these topics are happening right now. We also use these

[1] Information Security Management System

[2] iterative design and management method used for the control and continuous improvement of processes and products (https://asq.org/quality-resources/pdca-cycle)

technologies to support payment processes. Eventually, if for instance, a machine or a robot executes a payment based on some human users, what are the security requirements there? That is something that is really unclear at the moment, so hard for us to write policy too. That is a future direction that I'm looking at". Related to data, respondent #7 sees as a shortcoming the problem of aggregators not falling under supervision ("You need only one aggregator with a license to provide the whole Europe at least with account information. So, via one aggregator you can access all the EU banks and, well, that is a loophole because it is out of the financial supervision then"). This respondent believes that, moving forward, this aggregator problem must be addressed. One way to do this is not to have a further iteration of the directive, but move towards a new regulation: "what you probably need is Payment Service Regulation or Data Services Regulation; well, it is PII data, but Data Services Regulation is broader than GDPR, so that is my outcome, to opt for Data Services Regulation". It is important to note that a regulation must be implemented in the same way in the national legislation of EU countries. At the same time, a directive can be modified by the national legislators. Thus, a regulation would imply a common ground in Europe, as GDPR did for data protection. The view that the GDPR and PSD2 must either be merged or complement each other is also shared by respondent #4. Another participant (respondent #10) believes the directive's scope must be enlarged through the inclusion of more parts of the payments ecosystem. "To do a payment, you are part of an ecosystem, and this ecosystem also holds your mobile phone, the telecom sector, social media and the BigTechs. For me, the purely focused on the payments institution is still a very traditional one. Now, also with the DORA initiative[3], oversight is also in place for the cloud parties. For me, every part in the chain should do everything to decrease the fraud and increase security. And that is also the ISP, the social media platform, your Apple or Google Android or iOS platform; all the new fraud is also using those parts and you cannot say 'well, we know all this, but the banks or the financial institutions are the only ones who must stop the fraud'. So, from my point of view, the ecosystem is much more broader. If I would set up PSD3, I would also include those parties".

Finally, the fact that the eIDAS regulation was not included as a way to verify a payment user's identity is a major shortcoming, according to respondent #3. "DNB wants me to verify my client's identity and the people that created the PSD2 regulation should have known about the eIDAS regulation. So, there is a European scheme for identity verification and there's a European scheme for Open Banking. And they do not seem know much about each other. The large problem with the

[3] Digital Operational Resilience Act, proposed legislation for financial serviceshttps://www.ey.com/en_lu/consulting/the-dora--strengthening-the-operational-resilience-of-the-financ

eIDAS scheme is that nobody uses it unless they are forced to. We have invested an enormous amount of money as Europe in digital infrastructure for signature at a very high security level and they are not used, they are not widely adopted and PSD2 could have been the key to make that happen, to create wide adoption for eIDAS [...] If they're making two independent schemes they are not cooperating together; because there is a really good scheme for identity, there is a good scheme for Open Banking, but that Open Banking has requirements for identification and they are not looking into their European library of schemes certifications/regulation because there would have been a group: 'Oh yes, this is a nice book with ideas about identity. We could just use it', but they don't". The eIDAS standard is used as a basis for qualified certificates, but the digital identity scheme, one of the main areas of eIDAS, is indeed not used in PSD2.

In summary, the shortcomings and potential improvements for PSD2 range from incremental changes that involve more clarity on how the directive applies to certain cases to concerns about new technologies, scope extensions and integrating other European initiatives like digital identity.

Chapter 7

Discussion

The outputs and outcomes of the interviews are analyzed in this chapter, using the results for answering the remaining research sub-questions. Furthermore, it provides a critique of the research and future directions of expansion.

7.1 Interview outputs

The outputs of the interviews are structured according to the two main parts of the interview protocol, each answering one research question.

Common and Secure Communication cybersecurity risks Based on the data collected from the first part of the interview, various statistics can be computed.

The percentage of validated scenarios (the number of validated scenarios divided by the total number of scenarios, considering all participants, multiplied by 100) is 97.72%. The list of risk scenarios has not been extended with items in the scope of the research.

The values adjusted (or not) by the participants for each scenario according to likelihood, impact and overall risk have been assigned values from 1 (representing Very Low) to 5 (Very High). If a risk was deemed not applicable by a participant, all three values (likelihood, impact and overall risk) were assigned 0. There were no values assigned from participant #4 because they stated the difficulty of estimating risks at a high level of analysis. Participant #11 argued that the impact of the four scenarios could be between High and Very High, with scenario C having a significantly lower impact than the other three. Thus, their classifications have been encoded using two data entries, one set with a High impact for all scenarios and one with a Very High impact for scenarios A, B and D, and High for C, with the likelihood remaining the same across the two classifications. The overall risk was computed using the two. The following paragraphs describe each scenario and its classifications.

For scenario A ("A host system with access to payment information gets infected with malware, which exfiltrates data"), Figure 7.1 shows the distribution of classifications. The majority of respondents saw the classifications for impact and likelihood swapped compared to the initial values, with Very High for the former and High for the latter. The median High overall risk matches the author's classification. The respondents' median impact was Very High due to the catastrophic implications: reputation loss and potential license(s) suspension (different standards, from the national authority or the cards scheme). There are outliers in all three categories (likelihood, impact and overall risk), from one respondent who labeled all of them as Low.

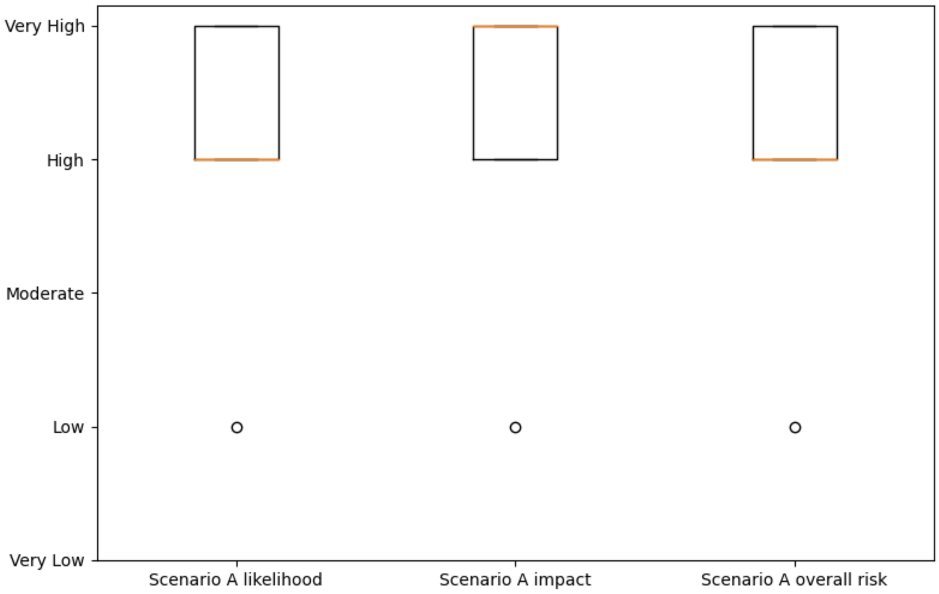

Figure 7.1: Distribution of scenario A's classifications

Scenario B, concerning unauthorized communication with an API, has its distribution represented in Figure 7.2. Outliers on the minimum end of the distribution are present in all risk components, stemming from the fact that this scenario was deemed not applicable by one respondent. The median likelihood of High is one level lower than the author's classification. For impact, disregarding the outliers, most estimations were High. The overall risk, without the outliers outside the scale and at Very High, all the classifications are High.

One can observe a variety of classifications in Figure 7.3 for scenario C ("An attacker

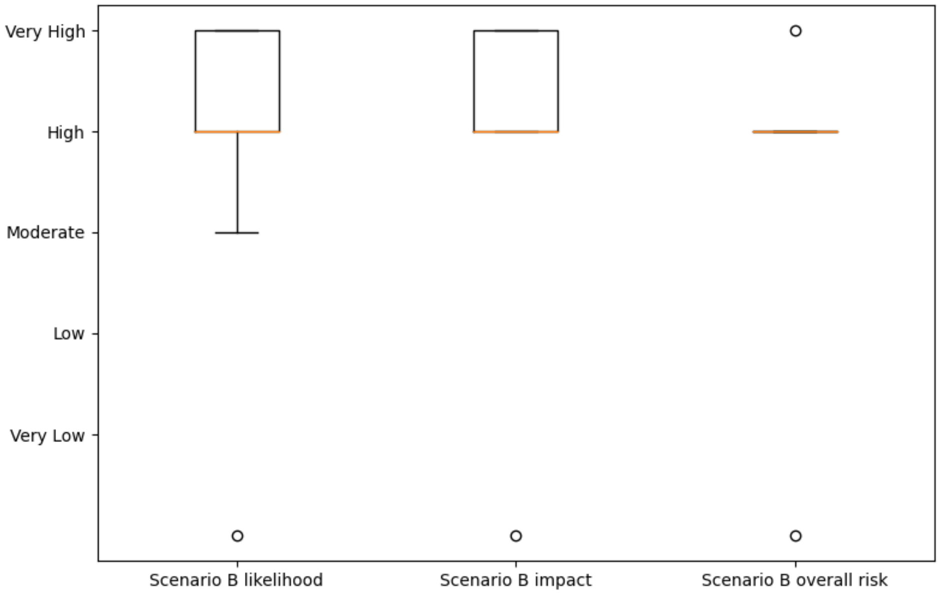

Figure 7.2: Distribution of scenario B's classifications

overloads the (API) system with a larger number of requests, making it unavailable". The median values of High for likelihood, impact and overall risk confirm the original estimation. Outliers are present for the likelihood in the vicinity of the High classification. Minimum values can be observed for the likelihood (Low), while the values for impact contain a minimum and maximum (Low and Very High). In general, participants saw the loss of availability as less critical than the loss of confidentiality or integrity (considering the higher number of Moderate and Low classifications compared to other scenarios). Losing confidentiality or integrity is usually seen as catastrophic due to the potential consequences (respondent #3: "I get all your bank transactions. I know how much liquor you buy. I know where you live because that is where you go to the ATM, and I know which supermarket you visit. I know how much you spend on the gym. I know so many things about you; the stakes for storing that securely are so high").

Finally, for scenario D, Figure 7.4 also shows varied distributions. Here, the likelihood is not the expected one, the median laying at a High level, lower than the original Very High. The impact for this scenario lies in the [High, Very High] interval, with a median of High and an outlier at Low. Scenario D's overall risk has most of the classifications in the top part of the scale, with a median of High, also presenting a minimum value outlier.

Overall, the median values match the original estimation in 8 out of 12 cases (66.67%),

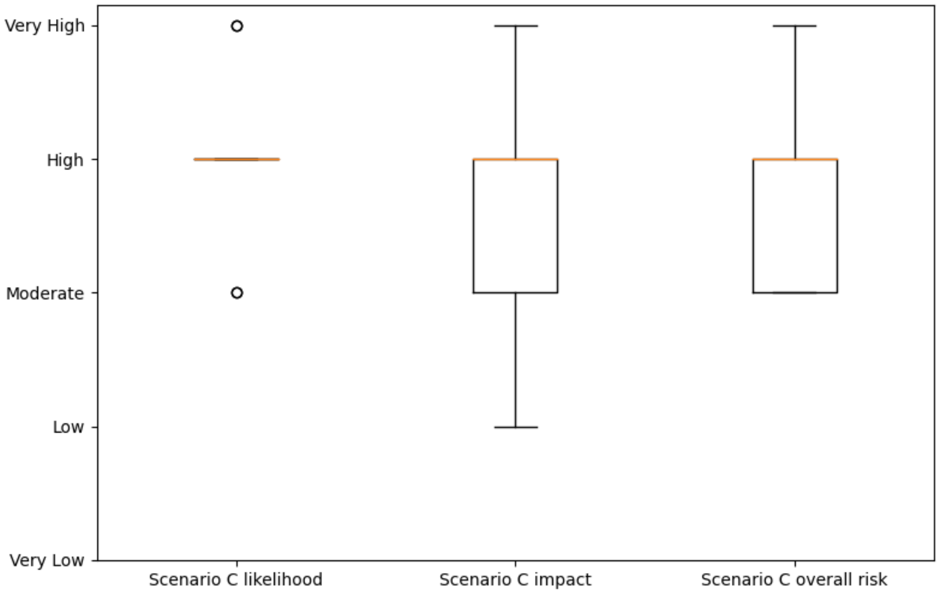

Figure 7.3: Distribution of scenario C's classifications

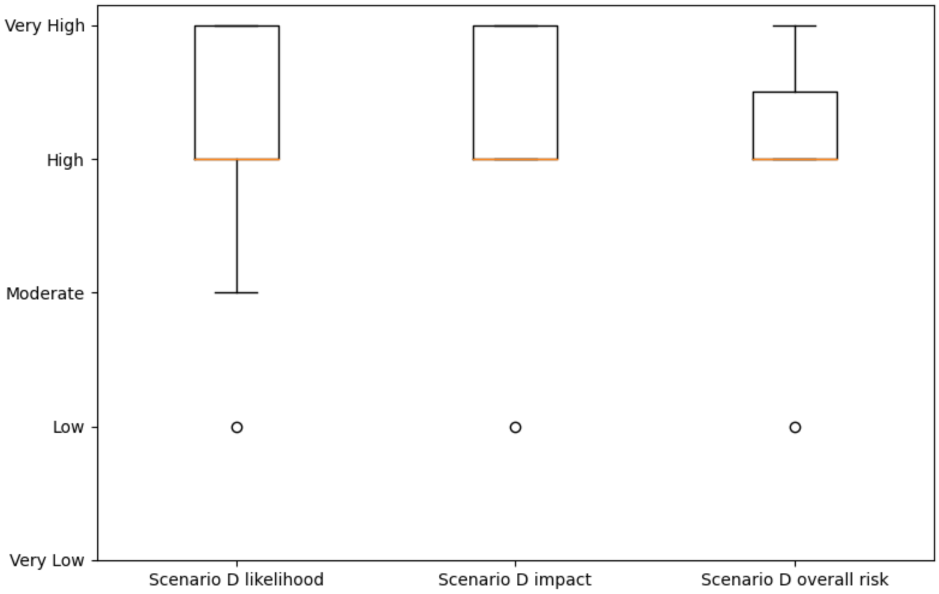

Figure 7.4: Distribution of scenario D's classifications

with the following deviations:

- scenario A: the likelihood is one level lower, and the impact is one level higher than predicted

- scenario B: the likelihood is one level lower than predicted
- scenario D: the likelihood is one level lower than predicted

One initial area to explore for this study was the difference between ASPSPs and TPPs (AISP and PISP) regarding risk perception. The following respondents have been grouped in two categories corresponding to their organizations:

- Participants #1, #3 and #4 were included in the **TPPs group**. Despite being part of an organization with AISP and PISP licenses, Respondent #2 was excluded as these licenses are not currently use;
- Respondent #6 was included in the **ASPSP group**. Respondent #5, working for a bank, did not rate the risks and was therefore excluded;
- Participant #7 was not included in any group on the basis of working with both of them in their consultancy activities. The other respondents from E-Money, PI, association and regulatory organization types were not included in any group either.

The classifications provided by the members of each group have been combined, and median classifications analyzed. The TPP respondents had 6 median classifications (50%) that were higher than the median classification of the sole respondent from the ASPSP group. This result might show that TPPs judge risks as being severe than ASPSP, one potential explanation being their cybersecurity maturity [18]. [6] states that TPPs might not prioritize security as much as incumbents; the higher classifications from this group might aid organizations in deciding to make these severe risks a priority.

In Table 7.1, the standard deviation of all the classification values can be observed. The lowest standard deviation is for the likelihood of scenario C (0.60), where 6 out of 11 classifications were High. The highest standard deviation is for the likelihood of scenario B (1.41), where no majority prevailed. One respondent found this scenario not relevant and applicable, which increased the deviation for the likelihood and the impact and overall risk. The deviations can be explained by various organizations' attributes (such as security maturity, whether or not PSD2 enables the main business function, technological affinity).

Classification	**Standard deviation**
Scenario A likelihood	0.86
Scenario A impact	0.89

Scenario A overall risk	0.83
Scenario B likelihood	1.41
Scenario B impact	1.34
Scenario B overall risk	1.21
Scenario C likelihood	0.60
Scenario C impact	0.86
Scenario C overall risk	0.64
Scenario D likelihood	0.93
Scenario D impact	0.86
Scenario D overall risk	0.79

Table 7.1: Standard deviation of classification of risk scenarios' likelihood, impact and overall risk

Table 7.2 presents the mean value of the classifications given by the respondents. The mean values, which, once approximated to the nearest integer (greater or less, for whichever the difference is smaller), are different from the base value (the author's classification), are presented in italic font. The outliers are the likelihoods of scenarios A, B and D. These have judged less likely to occur by the participants, some mentioning causes like better architecture choices or processes around the development of software and systems.

Classification	**Mean**	**Base value**
Scenario A likelihood	*4.27*	*5*
Scenario A impact	4.45	4
Scenario A overall risk	4.18	4
Scenario B likelihood	*4*	*5*
Scenario B impact	4	4
Scenario B overall risk	3.72	4
Scenario C likelihood	4	4
Scenario C impact	3.72	4
Scenario C overall risk	3.63	4
Scenario D likelihood	*4.18*	*5*
Scenario D impact	4.27	4
Scenario D overall risk	4.09	4

Table 7.2: Mean values for likelihood, impact and overall risk

In terms of the ranking of the four risks, the results can be observed in Figure 7.5. In the figure, "1st" signifies the most severe of the four risks, with "4th" representing the least severe scenario. The median values show B and C on the last two positions of the ranking, while A and D are on the same level. This might show the severity of malware attacks and the loss of secrets and passwords, and how highly severe they are regarded by organizations. On the other end of the ranking, scenario C, concerning availability, has been placed on the last position by most interview participants. Scenario B presents a minimum value outside the scale of four positions due to respondent #2 not finding this risk scenario applicable.

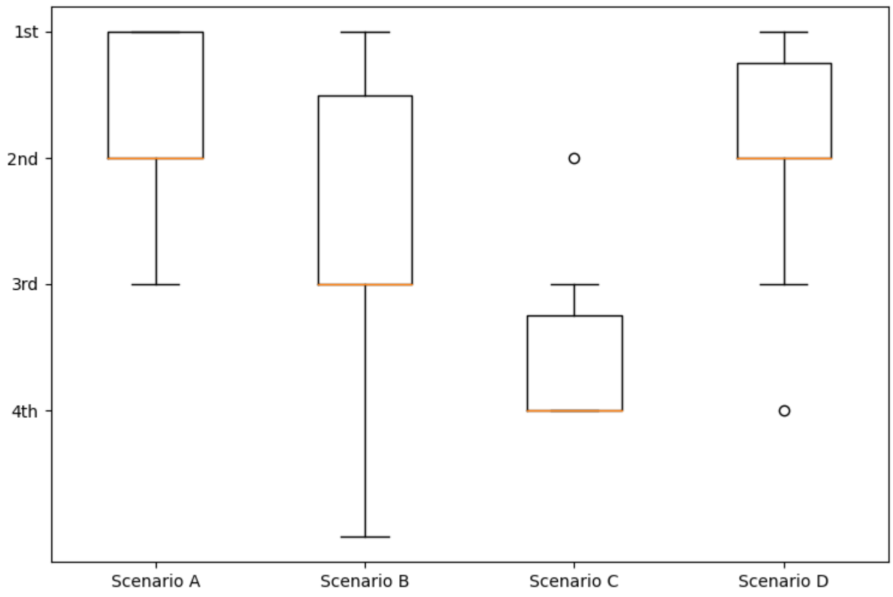

Figure 7.5: Distribution of scenario D's classifications

The fourth sub-question ("*What cybersecurity risks have been encountered by the relevant stakeholders in the Dutch e-payment market with regards to CSC?*") can be answered following the validation process of the risk scenarios with the interview participants. With an applicability score of 97.72% and the median classification match score of 66.67 % match, corroborated with the absence of new scenarios added to the list, this result shows the four prioritized risks to have been encountered by the Dutch e-payment market participants. [26] described the API as a new attack vector for PSD2 organizations, this result agreeing to their view.

Common and Secure Communication and PSD2 opinion As seen before, there was no consensus on the effect of CSC on the overall cybersecurity posture of organizations. One explanation of this result might that CSC contains elements known by organizations and did not provide complex. Firstly, different forms of secure communications were in place before PSD2, for example, as required by PCI-DSS, mentioned by three respondents[1]. Secondly, many organizations in the e-payment market, especially PSPs, used APIs before PSD2 for transferring data (respondent #2: "We prefer [an API] because it's the easiest way to set up, more secure way and less work for us because if they [other organizations] send files, I think that there's a larger margin of error, so APIs are the way to go". A completely new aspect of CSC, qualified certificates, did not emerge explicitly as a source of severe risks following the risk assessment. All these factors considered, it looks like CSC did not have a significant effect on the overall cybersecurity risks of organizations. The answer to the research sub-question V ("*Do relevant stakeholders in the Dutch e-payment market think CSC increased their overall cybersecurity risks?*") is negative.

7.2 Research limitations

After the answers to the research sub-questions have been provided in this and previous chapters, the critique of the research is presented to the reader.

The current study focuses on one part of PSD2, the Common and Secure Communication component of the Regulatory Technical Standards proposed by EBA. While being an essential component of the PSD2 requirements, CSC seems to be less of a concern for the market participants than another RTS component, SCA. Many studies had SCA as their core research focus in the state-of-the-art, the same not applying to CSC. In the second part of the research, SCA has been mentioned by the majority of interview participants as a critical aspect that produced changes for organizations in terms of security. At the same time, CSC was not deemed to be a notable factor. One limitation of the study is, therefore, the narrow focus on CSC. This limitation was partially addressed in the semi-structured interviews, where the author sought to understand the general context and allowed flexibility in terms of interview questions.

A second limitation is represented by the scope of the research, which does not account for regulatory aspects such as governance, operations, policies, processes or resilience. This is a limitation because these aspects all have consequences for organizations and were mentioned by a subset of the interview participants during the discussions about risk (respondent #5: "we looked more at operational risks that might occur [with the PSD2 licenses]"). Cybersecurity is seen today as a business issue, not a technical issue; thus, the mentioned aspects have evident importance.

[1] Due to the fact that the PCI-DSS standard compliance is a requirement for any business that accepts card payments (https://storekit.com/payments/pci-dss/), it is likely to be present at many of the respondents.

The number of participants, representing less than 10% of the market, can also be seen as a limitation. Despite the author's efforts, many potential participants declined to express their views. Understanding the effect of a piece of legislation requires the ones affected to speak out and express their views. While the author attempted to make participation facile, employing flexible scheduling and anonymity, some reluctance in answering the interview was observed. To address this limitation and further research in the PSD2 area, collaboration must be established, and the parties subject to PSD2 must be willing to present "their side of the story".

Finally, different aspects can be viewed as limiting for the risk assessment. The exclusion of non-CSC specific supporting assets (such as hardware, databases, personnel) limits the coverage of the risk assessment. Additionally, the fact that the study looks at inherent risks (in the absence of controls) made the research "theoretical" for some participants. Furthermore, they stated that their risk assessment is performed in their organizations at a granular level, where the actual systems and the data types involved in risk scenarios are explicitly stated. Some scenarios, for example, B and D, were deemed high level and vague by some participants. Some respondents also recommended the use of scenarios that include different steps and actions from attackers. About inherent risks, one participant mentioned that even when a new company is created and systems are launched for the first time, some level of assurance is required, and even the design of that system might already include some controls. They hint at the fact that rarely, in practice, systems exist without any guard measures, and ultimately the value lies in identifying residual risks and protecting assets.

7.3 Future directions

In this subsection, future directions and extensions of the research are presented, acting as a starting point for interested researchers in this field.

The research can be expanded by increasing the focus and evaluating the effect on cybersecurity risk of organizations following PSD2 on a broader scale, considering all components of the RTS and other pieces of legislation in multiple areas (cybersecurity, governance, operations, etc.). A larger number of participants would offer a more general understanding of the effect of the second Payments Directive in the Netherlands. Following this, correlating the participant's answers with data about their organizations might help further the understanding of cybersecurity for Dutch organizations in the e-payment market. When they obtained the license, size, and capital, a security maturity score can provide more context and identify factors that influence organizational cybersecurity.

Another potential extension of the study can be the inclusion of controls in the risk assessment. For this to be practical, a certain baseline of controls must be established to be present at the market participants. One possible way of doing this is to follow a cybersecurity standard (like [60]) or analyze the controls needed for existing regulations such as [74] or [62], which are already implemented in most organizations.

Ultimately, presenting a risk scenario as a chain of actions would make the scenario clearer to understand for different stakeholders and can also contribute to a better identification of weak points and where to place controls.

Chapter 8

Conclusion

Finally, the last chapter summarizes study results by presenting the answers to the research sub-questions, which provide the building blocks for answering the main research question.

8.1 Sub-questions

(I) What are the main technical implications of CSC?

The answer to the first sub-question is discovered in the third chapter. Here, the Common and Secure Communication is detailed through a descriptive analysis which primarily used the official documents introducing the concept. The main technical implications of CSC are presented below. They require companies to implement significant changes in areas such as cryptography (qualified certificates, secure communication, encryption techniques), system engineering (APIs, testing facilities) and operations (notifications for participants, support), among others.

- Secure communication (integrity and confidentiality);
- Traceability;
- Unique, short-lived session which is linked to the right user;
- Use of APIs;
- Testing facilities and support;
- Using ISO 20022 messaging concepts;
- Identification through (extended) QWAC & WSealC certificates;
- Strong and widely recognized encryption techniques;

- Participants notification in case of failure.

(II) What are the cybersecurity risks related to CSC?

The Risk assessment chapter provided a cybersecurity risk assessment on the organizational assets specific to CSC, using a combined methodology that used two industry standards, ISO 27005 and NIST 800-30. Four high overall risk scenarios have been identified and prioritized after going through the stages of context establishment, risk identification, risk estimation, and risk evaluation. They concern threats and vulnerabilities affecting the supporting assets of APIs and communication channel:

- A host system with access to payment information gets infected with malware, which exfiltrates data - Very High likelihood - High impact - High overall risk;
- An attacker communicates with the API without being authorized- Very High likelihood - High impact - High overall risk;
- An attacker overloads the (API) system with a large number of requests, making it unavailable - High likelihood - High impact - High overall risk;
- An attacker is able to read passwords, codes and secrets that are transmitted - Very High likelihood - High impact - High overall risk.

(III) Who are the relevant stakeholders for CSC in the Dutch e-payment market?

Chapter 5 identified the relevant players or actors for CSC in the Netherlands. The first part investigated the roles at a general level, stemming from the official directive's documents. The second part identified the licensed parties in the Dutch market, using data from the Dutch National Bank and the European Banking Authority, together with the regulators enforcing PSD2 and the market initiatives that represent collective interests in the Dutch payments ecosystem. The list of licensed credit institutions (ASPSPs) and licensed payment institutions are provided in the Annexes in Table A.1 and Table A.2, respectively. The regulators overseeing PSD2 in the Netherlands are the Autoriteit Financiële Markten, De Nederlandsche Bank, the Dutch Data Protection Authority and the Dutch Authority for Consumers and Markets. The payments associations are the Dutch Banking Association, Dutch Payments Association and United Payment Institutions Netherlands. In total, the ecosystem is comprised of more than 100 organizations.

(IV) What cybersecurity risks have been encountered by the relevant stakeholders in the Dutch e-payment market with regards to CSC?

The fourth sub-question used as a basis the risks identified in Chapter 4 and validated these in semi-structured interviews (Chapter 6) with a subset of the actors identified for the previous sub-question. In total, 11 interviews were conducted. The applicability score of the four risk scenarios was 97.72%. The median classification of the risk components (likelihood, impact, overall risk) by the participants, against the initial estimation of the author, yielded a 66.67% match score. These results confirm the four risk scenarios as applicable and accurate for the majority of respondents, showing that the cybersecurity risks Dutch e-payments market participants are facing in this area are related to malware, unauthorized API access, API Denial-of-Service and insecure communication. TPPs likely see these risks as more severe than APSPS, which might be a consequence of their cybersecurity maturity.

(V) Do relevant stakeholders in the Dutch e-payment market think CSC increased their overall cybersecurity risks? The last sub-question was also answered using semi-structured interviews. The majority of the eleven interviewees were unsure CSC affected their cybersecurity risks, two stating they actually decreased and other two believing that these risks increased because the data they (PSPs) can access through PSD2 became more valuable. Overall, there is no correlation between CSC and an increase in the overall cybersecurity risks, so the answer to this sub-question is negative.

8.2 Main question

What was the effect on the cybersecurity risks of e-payment market participants following the implementation of PSD2?

Finally, using the answers to the five research sub-questions, the answer to the main question can be formulated. As seen before, there are different technical implications in various areas for the over 100 Dutch e-payment market participants. Some of these organizations grouped in associations to facilitate collaboration and better represent themselves to the four regulators. The study found that these organizations do not see CSC as a factor of increase for their overall cybersecurity risks, on the contrary, seeing PSD2 as making payments safer and more secure (which was one of the directive's objectives). Overall, organizations in the Dutch e-payment market face different risks related to PSD2 in areas like cybersecurity, governance, and fraud. Thanks to the Directive and its associated guidelines, the experience accumulated and controls deployed for other, sometimes overlapping regulations, these organizations are able to face these risks and offer payment services to users more safely and securely than they did before; critical negative consequences stemming from the Common and Secure Communication angle of the Regulatory Technical Standards have not been observed. Finally, the Dutch e-payment actors balance the benefits of PSD2 and the cybersecurity risks.

Glossary

AISP Account Information Service Provider; aggregates data from PSU accounts from one or more ASPSPs, after being granted the customer's consent. An example of such a service is a dashboard with all accounts balance and transactions for a customer across different banks. 1, 101

API Application Programming Interface; the technical communication means between organizations in PSD2; See more in the API literature review. 2, 101

ASN.1 Abstract Syntax Notation One; standard language for defining data together with encoding rules. 18

ASPSP Account Servicing Payment Service Provider; 'Traditional' payment service provider, for example, a bank or credit card company. PSUs have accounts with them and can use these accounts to initiate payments. 1, 99, 100

CIA Confidentiality, Availability, Integrity; concept model for cybersecurity. 2, 17

CSC Common and Secure Communication; See more in the Background section. 1

Currence Initiative that facilitates the workings of the payments market in the Netherlands; Collaborative effort between the largest Dutch banks. Brand owner of iDeal and iDin. 100

Dutch Payments Association *Betaalvereniging*, in Dutch; Association that facilitates cooperation in the Dutch payments market. 3

EBA European Banking Authority; regulatory agency of the European Union. 1

eIDAS electronic Identification, Authentication and trust Services; EU regulation from 2014. See more in the Qualified certificates literature review. 2

FinTech New company active in the financial sector, which makes use of recent technological advancements such as Big Data and AI. 2

GDPR General Data Protection Regulation; EU law on data protection and privacy in the European Union and the European Economic Area. 22

iDeal E-commerce payment system used in the Netherlands, supported by all major banks in the country. Owned by Currence. 3, 99

iDin Authentication service offered by Dutch banks; permits customers to identify, login and confirm age on other websites or platforms. Owned by Currence. 3, 99

ISO International Organization for Standardization; promotes worldwide standards and works in 165 countries. 6

JSON JavaScript Object Notation - open standard of rules for presenting data in both human- and machine-readable format; Used in favour of XML in many systems. 19

NIST National Institute of Standards and Technology; a US Department of Commerce agency. 6

OWASP Open Web Application Security Project; online community that provides cybersecurity advice, mainly for web and API application security. 15

PISP Payment Initiation Service provider; starts a payment to an entity (such as a merchant) from the PSU's account after being granted the customer's consent. 1, 101

PKI Public Key Infrastructure; a system of binding digital keys to identities in the digital sphere; used for secure electronic transfer of information; Involves the use of a "public" key, available to anybody, and a "private" key, kept secret. 15

PSP Payment Service Provider; offers e-payment service(s) to PSUs. 100

PSU Payment Service User; end-user (consumer or a business) that has an account with an ASPSP. Uses services from a PSP. 2, 99, 100

QSealC Qualified certificate for electronic seal; See more in the Qualified certificates literature review. 16

QTSP Qualified Trust Service Provider; authority that guarantees through its status and reputation the electronic signing process. 15

QWAC Qualified certificate for website authentication; See more in the Qualified certificates literature review. 16

REST REpresentational State Transfer; a software architectural style that uses a stateless approach: for example, each API request is independent of the previous; A system that follows the REST principles is called RESTful. 19

RTS Regulatory Technical Standards; See more in the Background section. 1

SCA Strong Customer Authentication; See more in the Background section. 1

TPP Trusted Third Party; Generic term for AISP or PISP. 13, 101

XML eXtensible Markup Language - open standard of rules for presenting data in both human- and machine-readable format. 18, 100

XS2A (third party) Access to Accounts; concept introduced by PSD2, a requirement for banks to allow TPPs access to one or more customers accounts through APIs. 12

Bibliography

[1] EBA, "Opinion on the deadline and process for completing the migration to strong customer authentication (SCA) for e-commerce card-based payment transactions," Oct. 2019. [Online]. Available: https://www.eba.europa.eu/eba-publishes-opinion-on-the-deadline-and-process-for-completing-the-migration-to-strong-customer-authentication-sca-for-e-commerce-card-based-payment

[2] ——, "Final draft RTS on SCA and CSC under PSD2 (EBA-RTS-2017-02)," Feb. 2017. [Online]. Available: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/1761863/314bd4d5-ccad-47f8-bb11-84933e863944/Final%20draft%20RTS%20on%20SCA%20and%20CSC%20under%20PSD2%20%8EBA-RTS-2017-02%29.pdf

[3] G. Colangelo and O. Borgogno, "Data, Innovation and Transatlantic Competition in Finance: The Case of the Access to Account Rule," Social Science Research Network, Rochester, NY, SSRN Scholarly Paper ID 3251584, Apr. 2019. [Online]. Available: https://papers.ssrn.com/abstract=3251584

[4] European Parliament, "Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC," Aug. 2014, legislative Body: EP, CONSIL. [Online]. Available: http://data.europa.eu/eli/reg/2014/910/oj/eng

[5] European Commission, "EU banking and financial services law," 2021. [Online]. Available: https://ec.europa.eu/info/law/law-topic/eu-banking-and-financial-services-law_en

[6] M. Noctor, "PSD2: Is the banking industry prepared?" *Computer Fraud & Security*, vol. 2018, no. 6, pp. 9–11, Jun. 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1361372318300538

[7] S. Mansfield-Devine, "Open banking: opportunity and danger," *Computer Fraud & Security*, vol. 2016, no. 10, pp. 8–13, Oct. 2016. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S136137231630080X

[8] S. Jhamb, "Payments in the five largest EU e-commerce markets," Sep. 2020. [Online]. Available: https://paymentsnext.com/payments-in-the-five-largest-eu-e-commerce-markets/

[9] J.P. Morgan, "2019 Global payments trends report – Netherlands Country Insights," 2019. [Online]. Available: https://www.jpmorgan.com/merchant-services/insights/reports/netherlands

[10] R. K. Yin, *Case Study Research and Applications: Design and Methods*. SAGE Publications, Sep. 2017.

[11] P. Shields and N. Rangarajan, *A Playbook for Research Methods: Integrating Conceptual Frameworks and Project Management*. New Forums Press, Jul. 2013.

[12] EBA, "EBA Opinion on the use of eIDAS certificates under the RTS on SCACSC | European Banking Authority," Dec. 2018. [Online]. Available: https://www.eba.europa.eu/file/58802/

[13] ETSI, "Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366," ETSI, Tech. Rep., Jul. 2018. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/119400_119499/119495/01.01.02_60/ts_119495v010102p.pdf

[14] ISO, "ISO/IEC 27005:2018," 2018. [Online]. Available: https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/52/75281.html

[15] National Institute of Standards and Technology, "NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments," *Special Publication*, p. 95, 2012.

[16] M. Saunders, P. Lewis, and A. Thornhill, *Research Methods for Business Students*, 8th ed. New York: Pearson, Sep. 2018.

[17] J. Rowley and F. Slack, "Conducting a literature review," *Management Research News*, vol. 27, Jun. 2004.

[18] K. O'Leary, P. O'Reilly, T. Nagle, C. Filelis-Papadopoulos, and M. Dehghani, *The Sustainable Value of Open Banking: Insights from an Open Data Lens*. University of Hawai'i at Manoa, Jan. 2021, accepted: 2020-12-24T20:13:44Z

Pages: 5891. [Online]. Available: http://scholarspace.manoa.hawaii.edu/handle/10125/71333

[19] R. Dratva, “Is open banking driving the financial industry towards a true electronic market?” *Electronic Markets*, vol. 30, no. 1, pp. 65–67, Mar. 2020. [Online]. Available: https://doi.org/10.1007/s12525-020-00403-w

[20] Deloitte, “Open Banking around the world | Deloitte | FSI.” [Online]. Available: https://www2.deloitte.com/global/en/pages/financial-services/articles/open-banking-around-the-world.html

[21] The Berlin Group, “PSD2 Access to Bank Accounts | The Berlin Group,” 2021. [Online]. Available: https://www.berlin-group.org/psd2-access-to-bank-accounts

[22] Open Banking Implementation Entity, “Open Banking Documentation | API Specifications, Guidelines and Documentation,” 2021. [Online]. Available: https://standards.openbanking.org.uk/

[23] C. Bourne, “Fintech’s Transparency–Publicity Nexus: Value Cocreation Through Transparency Discourses in Business-to-Business Digital Marketing,” *American Behavioral Scientist*, vol. 64, no. 11, pp. 1607–1626, Oct. 2020, publisher: SAGE Publications Inc. [Online]. Available: https://doi.org/10.1177/0002764220959385

[24] M. R. King and R. W. Nesbitt, *The Technological Revolution in Financial Services: How Banks, FinTechs, and Customers Win Together*. University of Toronto Press, Aug. 2020, google-Books-ID: AA_8DwAAQBAJ.

[25] G. K. Hanssen, G. Brataas, and A. Martini, “Identifying Scalability Debt in Open Systems,” in *2019 IEEE/ACM International Conference on Technical Debt (TechDebt)*, May 2019, pp. 48–52.

[26] A. Premchand and A. Choudhry, “Open Banking APIs for Transformation in Banking,” in *2018 International Conference on Communication, Computing and Internet of Things (IC3IoT)*, Feb. 2018, pp. 25–29.

[27] Laura Brodsky and L. Oakes, “Data sharing and open banking | McKinsey,” 2017. [Online]. Available: https://www.mckinsey.com/industries/financial-services/our-insights/data-sharing-and-open-banking#

[28] A. Almehrej, L. Freitas, and P. Modesti, “Account and Transaction Protocol of the Open Banking Standard,” in *Rigorous State-Based Methods*, ser. Lecture Notes in Computer Science, A. Raschke, D. Méry, and F. Houdek, Eds. Cham: Springer International Publishing, 2020, pp. 230–236.

[29] D. Andersson, "A novel approach to calculate individuals' carbon footprints using financial transaction data – App development and design," *Journal of Cleaner Production*, vol. 256, p. 120396, May 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0959652620304431

[30] A. Brener, "Payment Service Directive II and Its Implications," in *Disrupting Finance: FinTech and Strategy in the 21st Century*, ser. Palgrave Studies in Digital Business & Enabling Technologies, T. Lynn, J. G. Mooney, P. Rosati, and M. Cummins, Eds. Cham: Springer International Publishing, 2019, pp. 103–119. [Online]. Available: https://doi.org/10.1007/978-3-030-02330-0_7

[31] C. Westermeier, "Money is data – the platformization of financial transactions," *Information, Communication & Society*, vol. 23, no. 14, pp. 2047–2063, Dec. 2020, publisher: Routledge _eprint: https://doi.org/10.1080/1369118X.2020.1770833. [Online]. Available: https://doi.org/10.1080/1369118X.2020.1770833

[32] M. Polasik, A. Huterska, R. Iftikhar, and S. Mikula, "The impact of Payment Services Directive 2 on the PayTech sector development in Europe," *Journal of Economic Behavior & Organization*, vol. 178, pp. 385–401, Oct. 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167268120302328

[33] M. Doeland, "How to keep payments safe and secure in a changing world," *Journal of payments strategy & systems*, vol. 13, no. 2, 2019.

[34] F. Di Porto and G. Ghidini, ""I Access Your Data, You Access Mine": Requiring Data Reciprocity in Payment Services," *IIC - International Review of Intellectual Property and Competition Law*, vol. 51, no. 3, pp. 307–329, Mar. 2020. [Online]. Available: https://doi.org/10.1007/s40319-020-00914-1

[35] O. Borgogno and G. Colangelo, "The data sharing paradox: BigTechs in finance," *European Competition Journal*, vol. 16, no. 2-3, pp. 492–511, Sep. 2020, publisher: Routledge _eprint: https://doi.org/10.1080/17441056.2020.1812285. [Online]. Available: https://doi.org/10.1080/17441056.2020.1812285

[36] M. Zachariadis and P. Ozcan, "The API Economy and Digital Transformation in Financial Services: The Case of Open Banking," Social Science Research Network, Rochester, NY, SSRN Scholarly Paper ID 2975199, Jun. 2017. [Online]. Available: https://papers.ssrn.com/abstract=2975199

[37] I. Romanova, S. Grima, J. Spiteri, and M. Kudinska, "The Payment Services Directive II and Competitiveness: The Perspective of European Fintech

Companies," *EUROPEAN RESEARCH STUDIES JOURNAL*, vol. XXI, no. Issue 2, pp. 3–22, Nov. 2018. [Online]. Available: http://ersj.eu/journal/981

[38] H. Choi, J. Park, J. Kim, and Y. Jung, "Consumer preferences of attributes of mobile payment services in South Korea," *Telematics and Informatics*, vol. 51, p. 101397, Aug. 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0736585320300563

[39] V. Haupert, D. Maier, and T. Müller, "Paying the Price for Disruption: How a FinTech Allowed Account Takeover," in *Proceedings of the 1st Reversing and Offensive-oriented Trends Symposium on - ROOTS*. Vienna, Austria: ACM Press, 2017, pp. 1–10. [Online]. Available: http://dl.acm.org/citation.cfm?doid=3150376.3150383

[40] P. T. J. Wolters and B. P. F. Jacobs, "The security of access to accounts under the PSD2," *Computer Law & Security Review*, vol. 35, no. 1, pp. 29–41, Feb. 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0267364918302620

[41] V. Haupert and S. Gabert, "Short Paper: How to Attack PSD2 Internet Banking," in *Financial Cryptography and Data Security*, ser. Lecture Notes in Computer Science, I. Goldberg and T. Moore, Eds. Cham: Springer International Publishing, 2019, pp. 234–242.

[42] F. Sinigaglia, R. Carbone, G. Costa, and N. Zannone, "A survey on multi-factor authentication for online banking in the wild," *Computers & Security*, vol. 95, p. 101745, Aug. 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404820300316

[43] V. Haupert and T. Müller, "On App-based Matrix Code Authentication in Online Banking:," in *Proceedings of the 4th International Conference on Information Systems Security and Privacy*. Funchal, Madeira, Portugal: SCITEPRESS - Science and Technology Publications, 2018, pp. 149–160. [Online]. Available: http://www.scitepress.org/DigitalLibrary/Link.aspx?doi=10.5220/0006650501490160

[44] C. Stephens, "Why are SMS codes still the global ID solution?" *Biometric Technology Today*, vol. 2020, no. 8, pp. 8–10, Sep. 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0969476520301107

[45] D. Jacobson, G. Brail, and D. Woods, *APIs: A Strategy Guide: Creating Channels with Application Programming Interfaces*, 1st ed. Sebastopol, CA: O'Reilly Media, Jan. 2012.

[46] M. S. Tabares and E. Suescun, "Towards an APIs Adoption Agile Model in Large Banks," in *Trends and Innovations in Information Systems and Technologies*, ser. Advances in Intelligent Systems and Computing, Á. Rocha, H. Adeli, L. P. Reis, S. Costanzo, I. Orovic, and F. Moreira, Eds. Cham: Springer International Publishing, 2020, pp. 302–311.

[47] E. Ünsal, B. Öztekin, M. Çavuş, and S. Özdemir, "Building a Fintech Ecosystem: Design and Development of a Fintech API Gateway," in *2020 International Symposium on Networks, Computers and Communications (ISNCC)*, Oct. 2020, pp. 1–5.

[48] D. Kellezi, C. Boegelund, and W. Meng, "Towards Secure Open Banking Architecture: An Evaluation with OWASP," in *Network and System Security*, ser. Lecture Notes in Computer Science, J. K. Liu and X. Huang, Eds. Cham: Springer International Publishing, 2019, pp. 185–198.

[49] OWASP, "OWASP Top Ten Web Application Security Risks | OWASP." [Online]. Available: https://owasp.org/www-project-top-ten/

[50] R. Coste and L. Miclea, "API Testing for Payment Service Directive2 and Open Banking," *International Journal of Modeling and Optimization*, vol. 9, no. 1, p. 5, 2019.

[51] A. Bisegna, R. Carbone, M. Ceccato, S. Manfredi, S. Ranise, G. Sciarretta, A. Tomasi, and E. Viglianisi, "Automated Assistance to the Security Assessment of API for Financial Services," in *Cyber-Physical Threat Intelligence for Critical Infrastructures Security: A Guide to Integrated Cyber-Physical Protection of Modern Critical Infrastructures*, J. Soldatos, J. Philpot, and G. Giunta, Eds. Now Publishers, 2020, pp. 978–1–68083–687–5.ch6. [Online]. Available: https://nowpublishers.com/article/Chapter/9781680836868?cId=978-1-68083-687-5.ch6

[52] Trendmicro, "Ready or Not for PSD2: The Risks of Open Banking," Trendmicro, Tech. Rep., 2019. [Online]. Available: https://documents.trendmicro.com/assets/white_papers/wp-PSD2-The-Risks-of-Open-Banking.pdf

[53] OWASP, "OWASP API Security - Top 10 | OWASP," 2019. [Online]. Available: https://owasp.org/www-project-api-security/

[54] J. Franklin, "PSD2: market struggles with APIs, SCA," 2020. [Online]. Available: https://www.iflr.com/article/b1lmx6bm8yp2pz/psd2-market-struggles-with-apis-sca

[55] N. Engelbertz, N. Erinola, D. Herring, J. Somorovsky, V. Mladenov, and J. Schwenk, “Security analysis of eidas – the cross-country authentication scheme in europe,” in *12th USENIX Workshop on Offensive Technologies (WOOT 18)*. Baltimore, MD: USENIX Association, Aug. 2018. [Online]. Available: https://www.usenix.org/conference/woot18/presentation/engelbertz

[56] M. Turkanović and B. Podgorelec, “Signing Blockchain Transactions Using Qualified Certificates,” *IEEE Internet Computing*, vol. 24, no. 6, pp. 37–43, Nov. 2020, conference Name: IEEE Internet Computing.

[57] E. R. Verheul, “The polymorphic eID scheme,” 2017. [Online]. Available: https://www.cs.ru.nl/B.Jacobs/PAPERS/naw5-2017-18-3-168.pdf

[58] ISO, “ISO 20022.” [Online]. Available: https://www.iso20022.org/iso-20022

[59] C. Wanner, “ISO 20022 and JSON: An Implementation Best Practices Whitepaper,” p. 50, 2018.

[60] ISO, “ISO/IEC 27001:2013,” 2019. [Online]. Available: https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/05/45/54534.html

[61] National Institute of Standards and Technology, “Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1,” National Institute of Standards and Technology, Gaithersburg, MD, Tech. Rep. NIST CSWP 04162018, Apr. 2018. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[62] European Commission, “The Directive on security of network and information systems (NIS Directive),” Jul. 2016. [Online]. Available: https://ec.europa.eu/digital-single-market/en/directive-security-network-and-information-systems-nis-directive

[63] European Parliament, “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance),” May 2016, legislative Body: EP, CONSIL. [Online]. Available: http://data.europa.eu/eli/reg/2016/679/oj/eng

[64] H. Setiawan, F. A. Putra, and A. R. Pradana, “Design of information security risk management using ISO/IEC 27005 and NIST SP 800-30 revision 1: A case study at communication data applications of XYZ institute,” in *2017 International Conference on Information Technology Systems and Innovation (ICITSI)*, Oct. 2017, pp. 251–256.

[65] M. A. Fikri, F. A. Putra, Y. Suryanto, and K. Ramli, "Risk Assessment Using NIST SP 800-30 Revision 1 and ISO 27005 Combination Technique in Profit-Based Organization: Case Study of ZZZ Information System Application in ABC Agency," *Procedia Computer Science*, vol. 161, pp. 1206–1215, 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050919319453

[66] European Commission, "Implementation of the NIS Directive in The Netherlands," May 2018. [Online]. Available: https://ec.europa.eu/digital-single-market/en/implementation-nis-directive-netherlands

[67] M. Cortet, N. Jung, H. Matzner, and C. Schaefer, "Payment Services Directive 2 - PSD2 sparks innovation in Open Banking ecosystems," Deutsche Bank, Tech. Rep., 2017. [Online]. Available: https://www.gtb.db.com/docs_new/PSD2_Open_Banking_Ecosystems_Innopay_DB_Article_June2017.pdf

[68] Verizon, "2020 Data Breach Investigations Report," 2020. [Online]. Available: https://enterprise.verizon.com/resources/reports/dbir/

[69] European Parliament, "Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance)," Dec. 2015, code Number: 337. [Online]. Available: http://data.europa.eu/eli/dir/2015/2366/oj/eng

[70] EUR-Lex, "National transposition measures communicated by the Member States concerning: Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance)," 2021. [Online]. Available: https://eur-lex-europa-eu.ezproxy2.utwente.nl/legal-content/EN/NIM/?uri=CELEX:32015L2366

[71] C. Wilson, *Interview Techniques for UX Practitioners*. Elsevier, 2014. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/C20120062096

[72] B. L. Berg and H. Lune, *Qualitative research methods for the social sciences*, 9th ed., ser. Books a la carte. Boston: Pearson, 2017.

[73] M. C. Harrell and M. A. Bradley, "Data Collection Methods: Semi-Structured Interviews and Focus Groups," RAND Corporation, Tech. Rep., Dec. 2009, publisher: RAND Corporation. [Online]. Available: https://www.rand.org/pubs/technical_reports/TR718.html

[74] PCI Security Standards Council, “The Prioritized Approach to Pursue PCI DSS Compliance,” PCI Security Standards Council, Tech. Rep., Jun. 2018. [Online]. Available: https://www.pcisecuritystandards.org/documents/Prioritized-Approach-for-PCI-DSS-v3_2_1.pdf?agreement=true&time=1613558960113

Appendix A

Appendices

A.1 Dutch licensed credit institutions subject to PSD2

Name	City	Type
ABN AMRO Bank N.V.	Amsterdam	Provision of bank services to EEA
ABN AMRO Clearing Bank N.V.	Amsterdam	Provision of bank services to EEA
ABN AMRO Groenbank B.V.	Amsterdam	Carrying on the business of a bank
ABN AMRO Hypotheken Groep B.V.	Amersfoort	Provision of bank services to EEA
Achmea Bank N.V.	's-gravenhage	Provision of bank services to EEA
Adyen N.V.	Amsterdam	Provision of bank services to EEA
Aegon Bank N.V.	Amsterdam	Provision of bank services to EEA

Amsterdam Trade Bank N.V.	Amsterdam	Provision of bank services to EEA
Anadolubank Nederland N.V.	Amsterdam	Provision of bank services to EEA
ASR Admin N.V.	Utrecht	Carrying on the business of a bank
Bank Mendes Gans N.V.	Amsterdam	Provision of bank services to EEA
Bank Ten Cate & Cie. N.V.	Amsterdam	Provision of bank services to EEA
BinckBank N.V.	Amsterdam	Provision of bank services to EEA
BNG Bank N.V.	Den Haag	Provision of bank services to EEA
Brand New Day Bank N.V.	Amsterdam	Carrying on the business of a bank
bunq B.V.	Amsterdam	Provision of bank services to EEA
Citco Bank Nederland N.V.	Amsterdam	Carrying on the business of a bank
Commonwealth Bank of Australia (Europe) N.V.	Amsterdam	Carrying on the business of a bank
Coöperatieve Rabobank U.A.	Amsterdam	Provision of bank services to EEA
Credit Europe Bank N.V.	Amsterdam	Provision of bank services to EEA

De Lage Landen International B.V.	Eindhoven	Carrying on the business of a bank
de Volksbank N.V.	Utrecht	Provision of bank services to EEA
Demir-Halk Bank (Nederland) N.V.	Rotterdam	Provision of bank services to EEA
GarantiBank International N.V.	Amsterdam	Carrying on the business of a bank
Hof Hoorneman Bankiers N.V.	Gouda	Provision of bank services to EEA
ING Bank N.V.	Amsterdam	Provision of bank services to EEA
ING Groenbank N.V.	Amsterdam	Carrying on the business of a bank
InsingerGilissen Bankiers N.V.	Amsterdam	Provision of bank services to EEA
International Card Services B.V.	Amsterdam	Provision of bank services to EEA
KAS BANK N.V.	Amsterdam	Provision of bank services to EEA
LeasePlan Corporation N.V.	Amsterdam	Provision of bank services to EEA
Mizuho Bank Europe N.V.	Amsterdam	Provision of bank services to EEA
MUFG Bank (Europe) N.V.	Amsterdam	Provision of bank services to EEA

Nationale-Nederlanden Bank N.V.	’s-gravenhage	Provision of bank services to EEA
NatWest Markets N.V.	Amsterdam	Provision of bank services to EEA
Nederlandse Financierings-Maatschappij voor Ontwikkelingslanden N.V.	’s-gravenhage	Carrying on the business of a bank
Nederlandse Waterschapsbank N.V.	’s-gravenhage	Provision of bank services to EEA
NIBC Bank N.V.	’s-gravenhage	Provision of bank services to EEA
Norinchukin Bank Europe N.V.	Amsterdam	Provision of bank services to EEA
Rabo Groen Bank B.V.	Utrecht	Carrying on the business of a bank
TD N.V.	Amsterdam	Provision of bank services to EEA
Triodos Bank N.V.	Zeist	Provision of bank services to EEA
Van Lanschot Kempen Wealth Management N.V.	’s hertogenbosch	Provision of bank services to EEA
Yapi Kredi Bank Nederland N.V.	Amsterdam	Provision of bank services to EEA

Table A.1: Dutch licensed credit institutions subject to PSD2

A.2 Dutch licensed payment institutions subject to PSD2

Name	City	Type
12Budget B.V.	Amsterdam	Payment Institution
Acapture B.V.	Amsterdam	Payment Institution
Avangate B.V.	Amsterdam	Payment Institution
Azimo B.V.	Amsterdam	Payment Institution
B.V. Suri-Change	Rotterdam	Payment Institution
Bizcuit Payments B.V.	Veenendaal	Payment Institution
Brainpoint Betaalsystemen B.V.	Rotterdam	Payment Institution
Buckaroo B.V.	Utrecht	Payment Institution
Buddy Payment B.V.	Rotterdam	Payment Institution
CCV Group B.V.	Arnhem	Payment Institution
CERON IT SOLUTIONS B.V.	Vught	Payment Institution
CM Payments B.V.	Breda	Payment Institution
CURO Payments B.V.	Oss	Payment Institution
Caleen Financial Services B.V.	Tilburg	Payment Institution
Cass Europe B.V.	Breda	Payment Institution
Currencycloud B.V.	Amsterdam	E-Money Institution
Cyber & Mason Exploitatie B.V.	Amersfoort	Payment Institution
Dyme B.V.	Amsterdam	Payment Institution
EU Lending B.V.	Almere	Payment Institution
European Merchant Services B.V.	Amsterdam	Payment Institution
Exact Payment Services B.V.	Delft	Payment Institution
Financial Transaction Services B.V.	Amsterdam	Payment Institution
Flow Money Automation B.V.	Tijnje	Payment Institution
Franx B.V.	Amsterdam	Payment Institution
GWK Travelex N.V.	Amsterdam	Payment Institution
Global Collect Services B.V.	Hoofddorp	Payment Institution
Global Reach FX B.V.	Amsterdam	Payment Institution
Icepay B.V.	Amsterdam	Payment Institution
Intersolve EGI B.V.	Woudenberg	E-Money Institution
Intertrust Escrow and Settlements B.V.	Amsterdam	Payment Institution
Invers B.V.	Voorburg	Payment Institution
InvoiceFinance B.V.	’s-hertogenbosch	Payment Institution
iban-XS B.V.	Voorschoten	Payment Institution
Jortt B.V.	Almere	Payment Institution

Lendex Nederland B.V.	Almere	Payment Institution
LaSer Nederland B.V.	’s-hertogenbosch	Payment Institution
MediaMedics B.V.	Delft	Payment Institution
Mollie B.V.	Amsterdam	Payment Institution
MoneyMonk B.V.	Utrecht	Payment Institution
MultiSafepay B.V.	Amsterdam	Payment Institution
Nederlandsche Betaal & Wissel Maatschappij N.V.	Amsterdam	Payment Institution
Ockto B.V.	Naarden	Payment Institution
PayCheckout B.V.	Venray	Payment Institution
PayPorter B.V.	Rhoon	Payment Institution
PayPro B.V.	Groningen	Payment Institution
PaySquare B.V.	Utrecht	Payment Institution
Payoneer Europe B.V.	Amsterdam	E-Money Institution
Payvision B.V.	Amsterdam	Payment Institution
Peaks B.V.	Amsterdam	Payment Institution
Rent a Pin B.V.	Amsterdam	Payment Institution
Rewire EU B.V.	Amsterdam	E-Money Institution
STP Groep B.V.	Dordrecht	Payment Institution
SafeNed B.V.	Amsterdam	Payment Institution
Santander Consumer Finance Benelux B.V.	Utrecht	Payment Institution
Sepay B.V.	’s-gravenhage	Payment Institution
Sisow B.V.	Helmond	Payment Institution
SkillSource B.V.	Aarle-rixtel	Payment Institution
Smart2Pay Global Services B.V.	Laren	Payment Institution
Stichting Nedsom Financial Services	Amersfoort	Payment Institution
Sunro Change B.V.	Amsterdam	Payment Institution
Takeaway.com Payments B.V.	Amsterdam	Payment Instit ution
TargetMedia B.V.	Huizen	Payment Institution
Tellow B.V.	Utrecht	Payment Institution
Tintel B.V.	Spijkenisse	Payment Institution
Twinfield International N.V.	Hoevelaken	Payment Institution
Uber Payments B.V.	Amsterdam	E-Money Institution
Unity Monetary Services B.V.	Amsterdam	Payment Institution
Verotel Merchant Services B.V.	Amsterdam	Payment Institution
Vitesse PSP B.V.	Rotterdam	Payment Institution
WEX Europe (Netherlands) B.V.	Amsterdam	E-Money Institution
World First Netherlands B.V.	Amsterdam	E-Money Institution
Worldpay B.V.	Amsterdam	Payment Institution

XE Europe B.V.	Amsterdam	Payment Institution

Table A.2: Dutch licensed payment institutions subject to PSD2

A.3 NIST 800-30 Assessment scale - Impact of Threat Events

Qualitative Values	Description
Very High	The threat event could be expected to have multiple severe or catastrophic adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
High	The threat event could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. A severe or catastrophic adverse effect means that, for example, the threat event might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.
Moderate	The threat event could be expected to have a serious adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A serious adverse effect means that, for example, the threat event might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.

Low	The threat event could be expected to have a limited adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A limited adverse effect means that, for example, the threat event might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
Very low	The threat event could be expected to have a negligible adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation.

Table A.3: Assessment Scale – Impact of Threat Events

A.4 NIST 800-30 Assessment scale - Likelihood of Threat Event Initiation/Occurence

Qualitative Values	**Description**
Very High	Error, accident, or act of nature is almost certain to occur; or occurs more than 100 times a year\Adversary is almost certain to initiate the threat event.
High	Error, accident, or act of nature is highly likely to occur; or occurs between 10-100 times a year\Adversary is highly likely to initiate the threat event.
Moderate	Error, accident, or act of nature is somewhat likely to occur; or occurs between 1-10 times a year\Adversary is somewhat likely to initiate the treat event.
Low	Error, accident, or act of nature is unlikely to occur; or occurs less than once a year, but more than once every 10 years\Adversary is unlikely to initiate the threat event.
Very low	Error, accident, or act of nature is highly unlikely to occur, or occur less than once every ten years\Adversary is highly unlikely to initiate the threat event.

Table A.4: Assessment Scale – Impact of Threat Events

A.5 NIST 800-30 Assessment scale - Likelihood of Threat Event Resulting In Adverse Impacts

Qualitative Values	Description
Very High	If the threat event is initiated or occurs, it is almost certain to have adverse impacts.
High	If the threat event is initiated or occurs, it is highly likely to have adverse impacts.
Moderate	If the threat event is initiated or occurs, it is somewhat likely to have adverse impacts.
Low	If the threat event is initiated or occurs, it is unlikely to have adverse impacts.
Very low	If the threat event is initiated or occurs, it is highly unlikely to have adverse impacts.

Table A.5: Assessment Scale – Likelihood of Threat Event Resulting In Adverse Impacts

A.6 NIST 800-30 Assessment scale - Overall likelihood

Likelihood of Threat Event Initiation or Occurence	Likelihood of Threat Event Results in Adverse Impacts				
	Very Low	**Low**	**Moderate**	**High**	**Very High**
Very High	Very Low	Moderate	High	Very High	Very High
High	Very Low	Moderate	Moderate	Very High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Moderate	Moderate
Very low	Very Low	Very Low	Very Low	Low	Low

Table A.6: Assessment Scale – Overall likelihood

A.7 NIST 800-30 Assessment scale - Level of risk

Likelihood(Threat Event Occurs and Results in Adverse Impact)	**Level of Impact**				
	Very Low	**Low**	**Moderate**	**High**	**Very High**
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very low	Very Low	Very Low	Very Low	Low	Low

Table A.7: Assessment Scale – Level of risk (combination of likelihood and impact)

A.8 Human threat sources

Threat source	Motivation	Threat Actions
Hacker, cracker	Challenge Ego Rebellion Status, Money	Hacking Social engineering System intrusion, break-ins Unauthorized system access
Computer criminal	Destruction of information Illegal information disclosure Monetary gain Unauthorized data alteration	Computer crime (e.g. cyber stalking) Fraudulent act (e.g. replay, impersonation, interception) Information bribery Spoofing System intrusion
Terrorist	Blackmail, Destruction Exploitation, Revenge Political Gain Media Coverage	Bomb/Terrorism Information warfare System attack (e.g. distributed denial of service) System penetration System tampering
Industrial espionage	Competitive advantage Economic espionage	Defence advantage Political advantage Economic exploitation Information theft Intrusion on personal privacy Social engineering System penetration Unauthorized system access (access to classified, proprietary,

		and/or technology related information)
Insiders	Curiosity Ego Intelligence Monetary gain Revenge Unintentional errors and omissions (e.g. data entry error, programming error)	Assault on an employee Blackmail Browsing of proprietary information Fraud and theft Information bribery Input of falsified, corrupted data Interception Malicious code (e.g. virus, logic bomb, Trojan horse) Sale of personal information System bugs System intrusion System sabotage Unauthorized system access

Table A.8: Human threat sources

A.9 Interview protocol

1. Formalities - 5 minutes

- Introduce the author.
- Introduce the research and the goals of the interview.
- Inform the interview participant of their rights and ask what data (name, employer) should not be shared.
- Ask the participant if they have any questions.
- Ask for permission to record the session.

2. Background - 10 minutes

- Shortly describe your work position and responsibilities.
- Is your organization subject to PSD2?
- What type of license does your organization hold (PISP/AISP)?
- What does PSD2 mean for your role?

3. PSD2 and cybersecurity risks - 35 minutes

- What can you tell me about your organization's journey to becoming PSD2 compliant?
- Did you follow a standard to aid in becoming compliant?
- Have you ever looked at/investigated the risks that might arise from PSD2? What do you think of them?
- Do you have knowledge about the Common and Secure Communication (CSC) Regulatory Technical Standard of PSD2?
- In this research, the cybersecurity risks for a generic PSD2 CSC architecture (APIs communicating over a network using qualified certificates) were identified by the author (these are inherent risks, not assuming any controls in place). Table A.9 shows the ones with the highest overall risk.
  - Do you think they are applicable to your organization/organizations in general?

  - How would you make this list more realistic (for an organization that tries to prevent these scenarios)? For example, think of changing impact/likelihood or suggesting new risk scenarios.
  - Do you think some risks are more important/critical than others? Can you order/rank them?
- CSC and PSD2 brought some changes to organizations (e.g. specific rules for APIs). What do you think was the effect of CSC on the overall cybersecurity risks for your organizations / for organizations subject to it?
- One objective of PSD2 is to make e-payments safer and more secure. Do you think this objective was achieved?
- Do you see any shortcomings in the PSD2 regulation in terms of security?
- What other elements would you have liked to see in PSD2 / What should have made it into the PSD2 but didn't (in terms of security) that could have helped your organization?
- What do you think should happen moving forward, to a hypothetical PSD3, in terms of security, for your organization?

4. Concluding - 5 minutes

- Ask if the interview participant has any more questions or points to mention.
- Tell the participant they will shortly receive a transcript and can amend their answers or retreat from the study.
- Ask the participant if they want to refer another eligible person as a potential interview participant.
- End the interview by thanking them for their time and cooperation.

ID	Prioritized risk scenario	Likelihood	Impact	Overall risk
A	A host system with access to payment information gets infected with malware, which exfiltrates data	Very High	High	High
B	An attacker communicates with the API without being authorized	Very High	High	High
C	An attacker overloads the (API) system with a large number of requests, making it unavailable	High	High	High
D	An attacker is able to read passwords, codes and secrets that are transmitted	Very High	High	High

Table A.9: Prioritized risk scenarios and their risk level

A.10 Interview respondents

#	Area of work	Organization type
1	Risk Management	AISP, PISP
2	Information Security	AISP, PI, PISP
3	Consultancy	AISP, PISP
4	Consultancy	AISP, PISP
5	IT Risk Management	ASPSP
6	Information Risk	ASPSP
7	Consultancy	ASPSP, AISP, PISP
8	IT Risk	E-Money
9	Information Security	PI
10	Risk Management	Association
11	Supervision	Regulatory

Table A.10: Interview respondents