



DIGITAL IDENTITIES IN SOFTWARE PRODUCTS AND SERVICES

Lappeenranta–Lahti University of Technology LUT

Master's programme in Software Product Management and Business

2024

Eerika Peltonen

Examiners: Professor Kari Smolander

Post-doctoral Researcher Andrey Saltan

ABSTRACT

Lappeenranta–Lahti University of Technology LUT

LUT School of Engineering Sciences

Software Engineering

Eerika Peltonen

Digital identities in software products and services

Master's thesis

2024

58 pages and 3 figures

Examiners: Professor Kari Smolander and Post-doctoral researcher Andrey Saltan

Keywords: digital identity, software product, software service, software product management

The global adoption of digital identities in digital products and services require companies, especially software product managers, to manage growing number of laws, regulations and emerging technology trends when developing, managing or maintaining their solutions. Despite the growing attention, there is no prior research done on the relationship between digital identity and software product management.

The aim of this thesis is to explore the key research gaps related to the topic and propose ways to address them. This was achieved by understanding the current state of research and practice, company challenges when implementing digital identities in software products and services, and future research opportunities. The information to address these aspects was collected using explorative literature review and analysed based on the ISPMA framework for software product management.

The findings highlight the key research gaps, including issues of digital identity interoperability, company innovation practices, trust relationships in digital identity ecosystems, digital identity strategy, and the involvement of end users and their requirements. Ways to address these findings include further research on e.g. regulatory compliance, organizational structure and the use of digital identity strategy in companies.

TIIVISTELMÄ

Lappeenrannan–Lahden teknillinen yliopisto LUT

LUTin insinööritieteiden tiedekunta

Tietotekniikka

Eerika Peltonen

Digitaaliset identiteetit ohjelmistotuotteissa ja -palveluissa

Tietotekniikan diplomityö

2024

58 sivua ja 3 kuvaa

Tarkastajat: Professori Kari Smolander ja Tutkijatohtori Andrey Saltan

Avainsanat: digitaalinen identiteetti, ohjelmistotuote, ohjelmistopalvelu, ohjelmistotuotehallinta

Digitaalisten identiteettien globaali käyttöönotto digitaalisissa tuotteissa ja palveluissa vaatii yrityksiä, erityisesti ohjelmistotuotepäälliköitä, navigoimaan kasvavaa määrää lakeja, määräyksiä sekä teknologiaan liittyviä trendejä, kun näitä ratkaisuja kehitetään, hallitaan tai ylläpidetään. Kasvavasta huomiosta huolimatta, digitaalisen identiteetin ja ohjelmistotuotehallinnan välisestä suhteesta ei ole tehty aiempaa tutkimusta.

Tämän diplomityön tavoitteena on selvittää aiheeseen liittyviä keskeisiä tutkimusaukkoja ja ehdottaa tapoja niiden käsittelemiseksi. Tämä saavutettiin selvittämällä tutkimuksen ja käytännön nykytilanne, tunnistamalla yritysten haasteita digitaalisten identiteettien käyttöönotossa sekä kartoittamalla tulevaisuuden tutkimusmahdollisuuksia. Tiedot kerättiin tutkivan kirjallisuuskatsauksen avulla ja analysoitiin käyttäen apuna ohjelmistotuotteiden hallinnan ISPMA-kehystä.

Tulokset osoittavat, että keskeisiä tutkimusaukkoja ovat haasteet liittyen digitaalisen identiteetin yhteentoimivuuteen, yritysten innovaatiokäytänteisiin, luottamussuhteisiin digitaalisen identiteetin ekosysteemeissä, digitaalisen identiteetin strategiaan sekä loppukäyttäjien osallistumiseen ja heidän vaatimuksiinsa. Näitä löytöjä voisi käsitellä tekemällä lisätutkimuksia liittyen mm. erilaisten säännösten noudattamiseen, organisaatorakenteeseen sekä digitaalisen identiteetin strategian käyttämiseen yrityksessä.

ACKNOWLEDGEMENTS

First and foremost, I would like to express my deepest gratitude to my thesis supervisors, Professor Kari Smolander and Post-doctoral researcher Andrey Saltan, for your invaluable guidance and support throughout the entire process of writing this thesis. Your insight and expertise on the subject matter have enabled me to produce a thesis that not only am I profoundly proud of but will be highly useful in the future. I am excited to continue the research in my doctoral dissertation under your supervision.

I would also like to extend my sincere appreciation to the entire software department at LUT University. To Fateme, Katja and Nan, your positive energy, constant support, and assistance, even with the smallest things, have been immensely valuable and deeply appreciated. I am excited to embark on the doctoral journey with you. Additionally, I wish to thank Stepan for important insights into the subject and for offering helpful advice whenever I needed it.

Finally, to my family and friends, thank you for your constant encouragement and support throughout my academic journey thus far, particularly during the writing of this thesis. I will forever be grateful for always being there for me.

ABBREVIATIONS

CEO	Chief Executive Officer
CFO	Chief Financial Officer
CMO	Chief Marketing Officer
COO	Chief Operating Officer
eIDAS	Electronica Identification, Authentication and Trust Services
EU	European Union
EUDI	European Digital Identity
FTC	Federal Trade Commission
GDPR	General Data Protection Regulation
ID4D	Identification for Development Initiative
IdM	Identity Management
IdP	Identity Provider
IPR	Intellectual Property Rights
ISPMA	International Software Product Management Association
KPI	Key Performance Indicator
PaaS	Platform as a Service
PDM	Product Data Management
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SSI	Self-Sovereign Identity
SSO	Single-Sign On
SCM	Software Configuration Management

SPM Software Product Management

UX User Experience

Table of contents

Abstract

Acknowledgements

Abbreviations

1	Introduction	9
2	Background.....	12
2.1	Digital Identity	12
2.2	Software Product Management.....	15
3	Methodology.....	20
3.1	Research Questions and Motivation	20
3.2	Research Process.....	22
3.2.1	Explorative Literature Study.....	22
3.2.2	Information Collection.....	24
3.2.3	Information Analysis	26
4	Results	31
4.1	Current State of Research and Practice.....	31
4.1.1	Strategic Management	32
4.1.2	Product Strategy.....	34
4.1.3	Product Planning.....	35
4.2	Company Challenges in Implementing Digital Identities.....	36
4.2.1	Strategic Management	36
4.2.2	Product Strategy.....	38
4.3	Future Research Directions.....	38
4.3.1	Strategic Management	39
4.3.2	Product Strategy.....	41
4.3.3	Product Planning.....	41
4.4	Key Research Gaps and Future Research Recommendations	42
5	Discussion.....	45
5.1	Future of digital identities in software products and services	45

5.2	Common themes and future research opportunities	46
5.3	Limitations and validity	48
6	Conclusions	50
	References.....	51

1 Introduction

A century ago, oil was considered the most valuable resource in the world, governed by numerous laws and regulations to ensure responsible extraction. In case of mismanagement, there were severe consequences. In modern world, however, data has surpassed oil as the world's most valuable resource, as argued by *The Economist* (2017). Among the vast quantities of personal data, digital identities stand out as repositories of significant and sensitive information. Digital identities extensively employed in daily activities, such as e-government, financial services, healthcare and travel. According to a report by Liminal (2022), the global market size for reusable or shareable digital identities is expected to grow from \$32.8 billion in 2022 to \$266.5 billion in 2027. Companies that are responsible for developing, managing or maintaining software products and services involving digital identities must navigate a range of important considerations, much like oil companies, due to the fundamental role of digital identity in society and the necessity to comply both with regulations and security and privacy standards. In addition to this responsibility, various technological trends are shaping the landscape of digital identity. These trends include digital twin, identity-based signcryption, blockchain and distributed networks (Ante, Fischer and Strehle, 2022).

To ensure the legitimate use of digital identities, several regulations around the world have been implemented, including European Union's (EU) regulation on electronic identification and trust services (eIDAS) and US Federal Trade Commission's (FTC) identity protection laws. Recently, the European Commission reviewed the original eIDAS regulation and addressed its shortcomings by proposing a new framework for European Digital Identity, also known as EUDI regulation (European Commission, 2024a). The new regulation introduces European digital identity wallet, which allows citizens to manage their data and access public and private online services across the EU (European Commission, 2024b).

Digital identity has been researched from various perspectives, including user requirements for user-centric digital systems (Maler, 2009; Bakhaev *et al.*, 2023), research streams and future research directions for digital identity (Ante, Fischer and Strehle, 2022), and emerging trends such as blockchain and digital twins (Uhlemann, Lehmann and Steinhilper, 2017; Zwitter, Gstrein and Yap, 2020; Sedlmeir *et al.*, 2021). Additionally, numerous reports

regarding digital identities, their application, and technical details have been published. For instance, the European Commission (2023) released a report on the current status and future of Digital Decade in EU, discussing the digital transformation of Europe along with international measures. The report outlines policies, objectives and targets for EU member states, as well as for their citizens and businesses (European Commission: Directorate-General for Communications Networks, Content and Technology, 2023). Similarly, World Economic Forum, an international organization that provides information to stakeholders in business, academia and civil society (World Economic Forum, 2024b), has published several reports over the years regarding digital identities, digital identity ecosystems, and the digital future (World Economic Forum, 2018b, 2018a, 2021, 2023). However, the software product management aspect of digital identities has received limited attention in research. As the integration of digital identities in various products and services expands across the globe, it is important to consider them from the point of view of software product managers or individuals in similar positions, who are responsible for orchestrating and strategically managing these products and services.

Given the rapidly evolving field of digital identity and the lack of previous research to understand its use within software products and services, this presents new research opportunities. Therefore, the goal of this thesis is to investigate the current state, company challenges and research gaps related to digital identities in software products and services. To achieve this, one primary research question and three sub-questions were formulated. The primary research question for the thesis is as follows:

- What are the key research gaps in the use of digital identity within software product management, and how can they be effectively addressed?

To further address the primary question, three sub-questions are answered:

- What is the current state of research and practice in digital identity within software product management?
- What specific challenges do companies face when implementing digital identity in software product management?
- What future research directions can help overcome the challenges associated with digital identity in software product management?

To answer these questions, this thesis employs explorative literature study, specifically a scoping review framework by Arksey and O'Malley (2005), to collect academic, white and grey literature. The methods for collecting information included search string (Kitchenham and Brereton, 2013) and reference list snowballing (Wohlin, 2014) to find relevant sources. After evaluating the suitability and relevance of the sources, the information was extracted using mind mapping and then organized according to the ISMPA framework by Kittlaus (2022), for software product management related activities. This research will be continued onto a doctoral dissertation and the thesis will act as a plan for future research.

The thesis is structured into six chapters. Following this introduction, in second chapter presents the background, essential concepts related to digital identities and software product management as well as previous research. Third chapter outlines the methodology, including the explorative literature study and the processes for information collection and analysis. Fourth chapter presents the results for current state of research and industry, company challenges and research gaps. Following the results is discussion chapter, where common themes and implications from results are analysed and discussed. Finally, the last chapter concludes the thesis including a short description of the work summary of the results and the future research.

2 Background

This chapter offers essential background information on topics relevant to the research. To enhance reader's understanding of the concepts mentioned throughout the thesis, this chapter provides a detailed introduction to digital identity, including its definition, different perspectives to identity, digital identity management systems, related activities, the digital identity ecosystem, technologies, and existing research. Additionally, the chapter presents the Software Product Management (SPM) framework by the International Software Product Management Association (ISPMA), outlining both the participation and core responsibility, and explaining their respective activities for software product manager.

2.1 Digital Identity

Before exploring the definition and various aspects of digital identity, it is important to consider different approaches to understanding the concept of identity. Identity can be defined as “set of information that is used to define an entity” (Utesheva, 2020). Research done by Zwitter et al. (2020) presents two philosophical perspectives on identity: naturalist world view and constructivist world view. The naturalist perspective views identity as a set of unique properties tied to a person or object, making people and objects distinguishable from each other. In contrast, the constructivist perspective views identity as a combination external factors, such as relationships with others, norms and rules of the environment and society, and the institutional recognition of identity. Zwitter et al. (2020) propose a “median threshold”, a balance between the naturalist and the constructive perspectives, suggesting that neither of the extreme perspectives are sustainable, whether identity theory or in the practice of digital identity. It can be concluded that identity is always expressed as combination of different factors in every individual, there emphasizing the idea of wholeness of identity (Zwitter, Gstrein and Yap, 2020). As technology in the heart of the transformation, the concept of identity was further developed into something more complex (Utesheva, 2020), and therefore, the concept of digital identity was born.

There are many concepts to understand regarding digital identities. To start off with definition, digital identity can be defined as “a set of electronically captured and stored

attributes and/or credentials that uniquely identify a person.” (Natarajan, Appaya and Balasubramanian, 2018). Diving more into the definition, the personal identity attributes in this context can include name, age, sex, place of birth, an identity number or fingerprints while common types of identity credentials include ID cards, certificates, numbers or passwords (Natarajan, Appaya and Balasubramanian, 2018). In addition to attributes and credentials, identifiers can be used to identify a person. Identifiers are series of digits, characters, symbols, or some other form of data that can be used to identify a subject, such as user account names, mobile phone numbers, employee numbers or passport numbers (Bertino and Takahashi, 2010).

To further understand how digital identity is utilized in software products and services, concepts such as authentication, authorization, and identification must be understood. According to Mueller et al. (2006, p. 406), authentication refers to the process of determining if user is who they have identified themselves as. Different entities performing the authentication require different attributes from the individual, some needing only a name, some requiring more information such as date of birth or an identity number. On the other hand, authorization is the mapping of different user identities to organizational policies so that user’s access to different resources is regulated (Mueller *et al.*, 2006, p. 406). Lastly, identification refers to the process of establishing information about certain individual, which can include examining passports or birth certificates, collecting biometric information or consulting different sources for confirming the identity that is being claimed (Landrigan, Wilson and Fraser, 2024). For example, in universities people identify themselves as students or staff with either student card or HR system, get physical keycard for their respective role. Then they can authenticate themselves with these keycards to different rooms of the university, according to the authorization settings of certain roles. Both university staff and students can access classrooms, but university staff can also access staff rooms, which students cannot access based on how they have been authenticated, authorized and identified with their keycard.

To combine all four concepts of digital identity, authentication, authorization and identification, the identity management (IdM) systems are needed. These systems keep track of the “life cycle” of the identifier to either set up, maintain or terminate it (Mueller *et al.*, 2006, pp. 406–407). The identity life cycle consists of four steps: the first step being registration, where identity data is collected and proofed, followed by issuance, where

credentials, such as fingerprints, ID cards or certificates are issued and bound to specific person, third step is called use, where the identity of the person is checked and authentication and authorization happens, and the last and fourth step of the identity lifecycle is management, where identities and credentials are maintained with actions such as updating or revoking them (World Economic Forum, 2023). In addition, governance can be seen in the middle of digital identity lifecycle, which affects other phases of the lifecycle by governing identity-related transactions with different policies and recording every transaction to account for liability (Bertino and Takahashi, 2010). Closely related to IdM systems, are the concepts of identity provider (IdP) and relying party (RP). IdP supply identities to subjects, and have four essential responsibilities: generating and assigning distinct identity attributes to a subject, binding one identity attribute to another identity attribute of the same subject, generating assertions of subject's identity attributes, and arranging credentials that record identity attributes and assertions (Bertino and Takahashi, 2010). On the other hand, RP refers to a party that require users, or agents acting behalf of them, to submit valid credentials to access services or resources (Bertino and Takahashi, 2010). A key responsibility for relying parties is to assess how much they can trust the credentials and the associated attributes or assertions related to them and relying parties may need to comply with laws and regulations related to prevent identity theft (Bertino and Takahashi, 2010).

Three archetypes of identity systems are described by the World Economic Forum (2018b), including centralized, federated and decentralized identity system. In centralized identity system, a single organization establishes and manages the identity, as can be seen with social media platforms, bank or government. Federated system entails different separate systems, who have established trust with each other and can offer multiple different services to users with single credentials. The trust between the system owners can be established with accepting each other's digital identity systems and their standards. Lastly, decentralized identity system, which is the newest of the three, entails the user being in charge of their own digital identity and choosing which attestation or attribute, stored in their identity data store, to share with which system entity, such as governments, banks or employers. (World Economic Forum, 2018b, pp. 13–15)

To further understand how companies are utilizing digital identity in their software products and services, there is a concept called digital identity ecosystem. Generally, the concept of

ecosystem refers to “any complicated system consisting of many different people, processes, activities, etc., especially relating to technology, and the way that they affect each other” (Cambridge Dictionary, 2024a). According to the book by Bertino and Takahashi (2010), identity ecosystem is based on four entities; business, individual, government and technology. Each of these entities have their own effect on rest of the ecosystem. As presented in the book, individuals have their needs, businesses offer solutions, public organizations have policies, and lastly various standards and technologies exist (Bertino and Takahashi, 2010).

The previous research related to digital identity emphasizes emerging technologies used with different identity system archetypes. Influential emerging technologies researched by Ante et al. (2022), include digital twin, signcryption, distributed network, encryption schemes, Internet of Things and lastly blockchain. Some fundamental technologies, principles and standards related to digital identity include digital credentials, Single-Sign On (SSO), Self-Sovereign Identity (SSI), Security Assertion Markup Language (SAML) and OpenID (Bertino and Takahashi, 2010). As this thesis focuses on the business and product management aspect of digital identity, these technologies are not thoroughly presented. Following the presentation of key concepts related to digital identity, it is essential to provide an overview of the other critical concept of this thesis: software product management.

2.2 Software Product Management

This chapter introduces the other key aspect of the thesis: fundamental concepts of software product management. Given the complexity of SPM, the ISPMA framework is employed throughout the thesis to simplify and systematically address its various aspects. The ISPMA framework and many related terms are explained in this chapter. Starting from the basics, according to the Cambridge Dictionary (2024b), software can be defined as “the instructions that control what a computer does”. Nowadays, software is used globally to handle or aid people to perform certain computer-related tasks. These tasks can be related to the fields of education, financial services, human resource management, traveling or media. For instance, the worldwide financial markets are entirely dependent on IT, since it can handle high number of transactions and is efficient in terms of speed of execution (Kittlaus, 2022, p. 9).

Another basic term is product, which can be defined as “a combination of material or intangible goods and services, which one party (called vendor) combines and evolves in support of their commercial interests, with the intention to transfer defined rights to one or more second parties (called customers)” (Kittlaus, 2022, p. 11). Combining the definitions of both software and product, software product can be defined as “product whose primary component is software” (Kittlaus, 2022, p. 11). Closely related to the concept of software product, a solution is usually used in marketing and can be defined either as “a product that is a combination of other products, human services, and possibly some glue code and customization.” or as “a combination of products and customer-specific code that is developed and implemented for a specific customer” (Kittlaus, 2022, p. 12). The software can be offered to customers through multiple ways such as SaaS, which comes from words Software as a Service, or PaaS as in Platform as a service. In SaaS, software infrastructure, middleware an application is offered over the internet, also known as cloud computing (Kittlaus, 2022, p. 15). According to the ISPMA compliant study guide by Kittlaus (2022, p. 15), PaaS offers an infrastructure and pre-installed enabling products through cloud computing.

In general, product management means planning and coordinating all the applicable aspects of a product both inside and outside the company with the goal of optimizing the success of a product as sustainably as possible, but it is important to note that the responsibilities of a product manager highly depends on the context of the product (Kittlaus, 2022, p. 1). Additionally, it is important to consider that software is increasingly used in multiple fields of services, such as healthcare, automobiles and financial services. Therefore, industries that have not always been using products with software embedded into them, can now benefit from understanding SPM and the framework. Therefore, software product management applies to different parties. These parties include vendors of software products and software-intensive technical services, such as SaaS and PaaS, or apps running on smart devices, vendors of software-intensive products in all industries, vendors of professional human services that increase productivity, and lastly, corporate IT industries of all industries (Kittlaus, 2022, p. 2). In this thesis, the focus is on the person responsible for performing SPM, the software product manager, who is the person responsible for all the aspects of their products (Kittlaus, 2022, p. 45).

To aid the software product manager in their duties, the framework for SPM was created by the International Software Product Management Association (ISPMA). ISPMA is a non-profit association consisting of experts, researchers and professionals helping in software product management related matters since 2009 (The International Software Product Management Association, 2024). According to the study guide by Kittlaus (2022, p. 37), the ISPMA framework (Figure 1) is divided into seven functional areas of software company; Strategic Management, Product Strategy, Product Planning, Development, Marketing, Sales and Fulfilment, and lastly, Delivery Services and Support. Out of these seven, Product Strategy and Product Planning are the core SPM responsibility areas of software product manager, having direct responsibility of the activities under these areas. Strategic Management is seen as participation responsibility for the product manager, but activities of market analysis and product analysis can be seen as product manager's direct responsibility, especially in smaller software companies (Kittlaus, 2022, p. 37). Lastly, in the remaining responsibility areas of Development, Marketing, Sales and Fulfilment, and Delivery Services and Support, the software product manager assumes orchestration role. While the specific activities within these areas are managed by the respective teams, such as the marketing team handling marketing-related tasks, it is the software product manager's responsibility to coordinate and oversee the integration of all these functions and their activities (Kittlaus, 2022, p. 38).

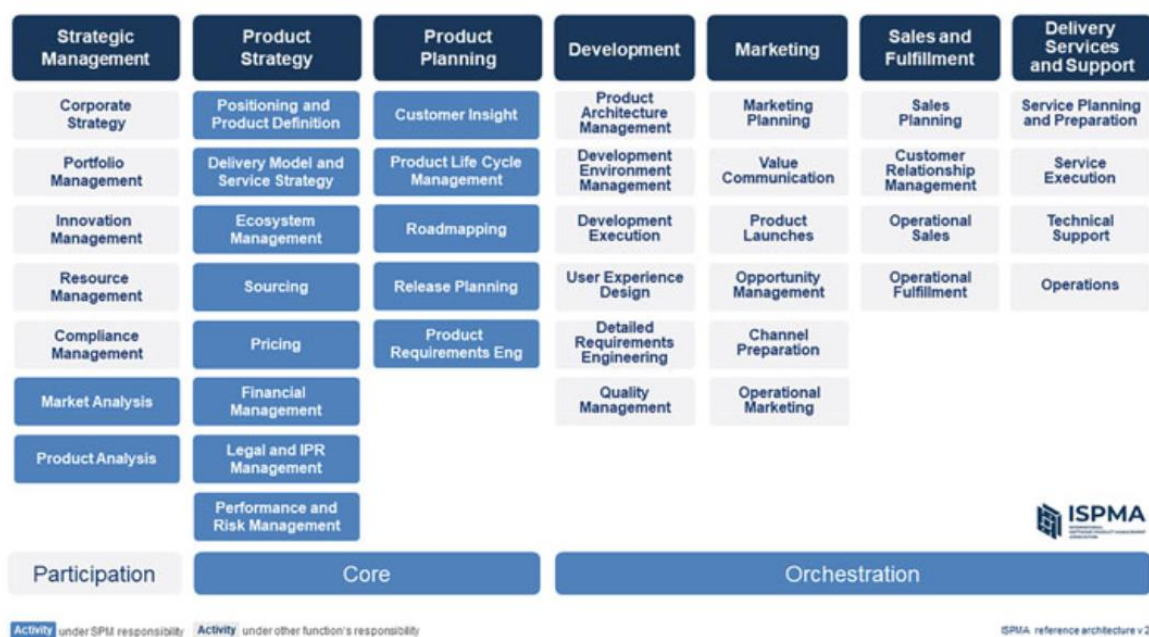


Figure 1. ISPMA SPM framework by Kittlaus (2022, p. 37)

The specific activities under the core SPM area of Product Strategy include positioning and product definition, delivery model and service strategy, ecosystem management, sourcing, pricing, financial management, legal and intellectual property rights (IPR) management, and performance and risk management. On the other hand, in Product Planning area, the software product manager is responsible for activities such as customer insight, product life cycle management, roadmapping, release planning, and product requirements engineering. To further understand the activities better, the market analysis, which can be seen as the first responsibility of the software product manager in the framework, can be defined as research for current and future aspects of customers, relevant technologies, competitors and economic developments (Kittlaus, 2022, p. 232). On the other hand, product analysis “defines the data relevant for the management of a product, locates or generates it, accesses it reliably and regularly, aggregates it based on agreed definitions, and makes it available in an appropriate way to everybody who has a need to know” (Kittlaus, 2022, p. 239). Closely related to product analysis is the concept of key performance indicators, or KPI for short. KPIs can include finance-related numbers such as cost of the product and current revenue, customer-related KPIs such as number of licenses ordered or installed for licenced product or number of active customers for SaaS product, and lastly, development-related KPIs such as productivity of the development team (Kittlaus, 2022, p. 240). Through different KPIs, software product manager can assess requirements and act accordingly.

The activities under responsibility area of Product Strategy, according to the study guide by Kittlaus (2022), the first activity, positioning and product definition includes defining scope, customer value, target market segments and channels of the product. The second activity combines delivery model and service strategy. Through delivery model it is explained how the software product is made available to customers and what options customers have to tailor the product according to their specific needs. On the other hand, service strategy includes explaining what professional services will be offered by which provider as part of the whole offering of a product. The third activity, sourcing, includes determining where the resources, especially human resources and software, are originating from. Pricing, on the other hand determines how prices of the products or services are defined and maintained with time. The next activity, financial management plans and tracks different financial aspects, such as benefits and costs and forecast, from both short- and long-term perspective. Ecosystem management includes defining the roles of different entities in relevant ecosystems and managing relationships with external stakeholders. The next activity, legal

and IPR management, takes care of all the legal aspects of the product. Lastly, performance and risk management, defines and takes action based on continuous risk and business performance assessment. (Kittlaus, 2022)

According to Kittlaus (2022), the first activity under Product Planning responsibility area, customer insight refer to deep and up-to-date information on customer problems, context and dynamics and it heavily defined the other activities under the responsibility area. The next activity, product life cycle management, refers to different responsibilities according to the different phases in the product's life cycle. On the other hand, roadmapping refers to long-term strategical planning of the evolution of the product. The next activity, release planning refers to management of different contents and schedule of future product releases. Lastly, product requirements engineering includes eliciting stakeholder's needs and expectations and identifying different concepts to meet these needs while also validating the identified concepts actually satisfy the needs. (Kittlaus, 2022)

This concludes describing activities under the responsibility areas of Strategic Management, Product Strategy, and Product. These three responsibility areas are the focal point of this thesis, according to the information analysis results. There are more activities under other responsibility areas, but as the focus of this thesis is on SPM and responsibilities of software product manager, those activities will not be covered on this background section. Activities under orchestration part of SPM are explained in more detail in the book by Kittlaus (2022). The focus of this thesis is on the type of software products and services that use digital identities to identify, authenticate and authorize the user before using the software. Prior research has not been conducted towards combining both software product management and digital identities. Therefore, this thesis aims to identity future research opportunities by examining the current state of research and practice of digital identities, exploring the company challenges faced in managing digital identities within software products and services, and highlighting gaps for future research.

3 Methodology

This chapter introduces the research motivation, methodology and relevant processes of the thesis. The first subchapter will introduce and justify the research motivation and goal in more detail through discussing the reasons for choosing this specific topic and presenting the research question and its sub-questions. The second subchapter introduces the research methodology and the processes of information collection and information analysis. Through introducing methodology in detail, the reader can understand how the results were achieved.

3.1 Research Questions and Motivation

The goal of this thesis is to understand the current state and research gaps of digital identities within software product management based on the collected academic, white and grey literature. To formulate the research goal into questions, one primary research question and three sub-questions were created. The sub-questions address the primary question and narrows it down into smaller parts. The research questions were formulated together with thesis supervisors as well as brainstorming and reformulating them with ChatGPT, similar to what was done when creating the search string for the information collection. The primary research question of this thesis is:

- What are the key research gaps in the use of digital identity within software product management, and how can they be effectively addressed?

To further understand primary research question, three sub-questions are addressed:

- What is the current state of research and practice in digital identity within software product management?
- What specific challenges do companies face when implementing digital identity in software product management?
- What future research directions can help overcome the challenges associated with digital identity in software product management?

The thesis goal will be fulfilled by successfully answering the research questions. As mentioned, the research done in this thesis will be continued to doctoral dissertation. The dissertation plan will be constructed according to the answers to the research questions in this thesis. Therefore, this thesis will subsequently act as a plan for future research, in this case, the dissertation. Additionally, the thesis will offer future research gaps and opportunities to other researchers as well.

The research done in this thesis is motivated by many reasons. First, the author of the thesis has studied in master's programme focused on SPM and business as well as has some experience from software engineering industry. The industry-related responsibilities include working as a software developer but few times lightly covering duties of a Product Owner in addition to having inspiring conversations with people working under responsibilities related to software product management. These factors heavily influenced the topic to be related to SPM. Second distinctive motivator for the thesis is the lack of previous research done on the topic of the thesis. This was discovered through initial background reading on the topic and doing lightweight mapping of existing research before properly starting the research process. Even though digital identities have been researched and reported from many different points of view throughout the years, no research has been done from the SPM point of view.

Third motivator for this thesis is the security concern of the software solutions that utilize digital identities. Security has been one of the concerns of multiple researchers of digital identity (Mueller *et al.*, 2006; Cullen, 2009; Alpár, Hoepman and Siljee, 2013; Bakhaev *et al.*, 2023) and for a reason; when you share your personal information and different credentials and attributes in digital form, there is always a chance that someone will try to maliciously access and use them. SpyCloud, a company that offers automated identity threat protection for more than 4 billion accounts of employees and consumers (SpyCloud, 2024b), reported in their annual report in 2023, that there is one in a fifth chance of being a victim of an infection attack by an infostealer and there is a prediction that global cost of cybercriminal activities will nearly triple from \$8.44 in 2022 to \$23.84 billion in 2027 (SpyCloud, 2024a).

This thesis explores the critical relationship between business and product management within the context of digital identities. The findings of the thesis, along with future research, will provide valuable insights for professionals in both software product management and

business management, guiding the development of more responsible and secure software products and services. Furthermore, as management people are more knowledgeable, these insights will indirectly assist software engineers in understanding and integrating digital identities into their work, offering not only new perspectives but also practical support in their development tasks.

3.2 Research Process

This chapter introduced the research process in more detail, including the research methodology as well as the information collection and analysis processes. First subchapter will go through explorative literature study, more specifically scoping review, which was utilized as means of gathering information. Information collection process is further explained in the second subchapter. Lastly, the research process subchapter will end with detailed description of the information analysis done on the collected information.

3.2.1 Explorative Literature Study

To understand the current state of the research and practice, company challenges and future research gaps, a literature review is often needed to understand what has been already researched or generally written in literature before conducting any future research. The considerations for choosing the method for the literature review were time, future research benefit and the width of the information gathered. The chosen type of literature study for this thesis is scoping review, following the framework by Arksey and O'Malley (2005). Scoping reviews attempt to understand the initial nature and potential size of available literature regarding certain topic by comprehensively and, if necessary, iteratively engaging with existing literature (Arksey and O'Malley, 2005). As further mentioned by Arksey and O'Malley (2005) one of the four reasons for choosing scoping study, the need for identifying research gaps of existing literature, matches this thesis. With the structure of scoping review, more sources of different literature types could be found, and the data could be relatively quickly analysed compared to systematic literature reviews. Some influence from systematic literature review was considered as option in the beginning of the thesis, and it was additionally investigated for suitability as process of analysing the collected information.

However, as scoping review allows more flexibility and is more time efficient, it was chosen instead of a systematic literature review. The scoping review methodology framework adopted by Arksey and O'Malley (2005) includes five stages:

1. Identifying the research question
2. Identifying relevant studies
3. Study selection
4. Charting the data
5. Collating, summarizing and reporting the results

These five stages were adopted in this thesis as well, even though there were slight differences in some stages. The first stage of the thesis was to come up with a research question to further study the relationship between SPM and digital identities. The primary question was the guiding research question during most of the thesis, which was then divided into three sub-questions that were individually addressed through the collected and analysed information. The next stage included identifying relevant studies, in this thesis also grey and white literature, which was collected through creating a search string related to both SPM and digital identities, and going through reference lists of first the background reading and later more suitable sources as they were found, to identify any additional sources with relevant information. Similarly highlighted by Arksey and O'Malley (2005) in their respective research, this thesis also picked up large number of irrelevant sources, especially through using the search string. Therefore, some exclusion criteria had to be created. The exclusion criteria of this thesis are further presented in the following subchapter dedicated for information analysis. Next stage of the scoping methodology framework included charting the data, in the case of this thesis, information, based on the selected sources. Instead of the Excel used by Arksey and O'Malley (2005), this thesis utilized Zotero to collect related information about the sources and some notes about what information the source includes were added as well. Creating an Excel sheet of the sources was considered multiple times during the thesis but those had to be discarded due to the pressing schedule of the thesis.

The fifth and last stage includes collating, summarizing and reporting the results. As mentioned by Arksey and O'Malley (2005), scoping studies aims to present an overview of

all the collected data, compared to systematic literature reviews, where some of the sources will remain hidden from the final publication. In this thesis, the last steps included extracting relevant information from each included source into a mind map and then organizing the information according to the ISPMA framework for different responsibility areas for software product management. As last step, the individual pieces of information were categorized into three categories according to the sub-questions of the thesis: current state, company challenges and future research gaps. The primary question then synthesizes the results to the sub-questions. These stages can be iteratively revisited as needed (Arksey and O'Malley, 2005). Indeed, in this thesis there was some iteration between the second and third stages of identifying and selecting relevant studies even after the fourth stage of charting the data had begun. For example, there were some relevant sources that came to the knowledge quite late on the process, such as the master's thesis by Rahman (2024), which was released in the beginning of September and was included in this thesis since it included some useful information. More information on how information was collected and analysed are presented in the following two subchapters. The limitations of scoping review as a method are presented in the discussion chapter.

3.2.2 Information Collection

The information to understand the current research status and gaps as well as future research opportunities was collected using two methods: search string and snowballing. This allowed wider scope for information collection and minimized the possibility of not finding all relevant sources. Before proper data collection, some sources were already provided for preliminary reading to understand the topic of digital identity before starting the research, which then helped in formulating and applying the information collection methods.

To collect the information, first, search string was utilized and then references were scanned with snowball effect to find relevant sources. The search string was built upon the initial reading of background material as well as discussing different synonyms and words with the widely popular AI tool by OpenAI called ChatGPT. With the help of the tool, the following search string, including the primary concepts of both digital identity and software product management as well as multiple synonyms for both, was constructed: ("*digital identity*" OR "*electronic identity*" OR "*user identity*" OR "*virtual identity*") AND ("*software product*

management" OR "software project management" OR "product lifecycle management" OR "product development management" OR "agile project management"). The search string was ejected to Google Scholar and 497 results were found. As the sources were further examined, many of the results found by Google Scholar were outside the scope of the thesis. Therefore, snowballing through reference lists of related work turned out to be more useful method for collecting information. In reference list snowballing, the reference lists of the most suitable articles are scanned with ambition of finding more relevant sources for further analysis by moving forward and backwards in list of references of the defined start set and including or excluding sources as necessary (Wohlin, 2014). In this case, the start set included the papers that were given in the beginning of the project as background reading. These papers included the conference paper by Bakhaev et al. (2023), doctoral dissertation by Bazarhanova (2020) and lastly a conference paper by Bazarhanova and Smolander (2020). New sources were included in the start set of the snowballing process as they were found and deemed suitable. Every time there was a source that could possibly contain useful information on the topic, it was saved to Zotero. Zotero is a tool to collect, organize, cite and share sources of research (Zotero, 2024).

As mentioned, many of the sources found by Google Scholar through the search string were outside the scope of the thesis when examined more thoroughly. These sources included more technical sources that focused more on the relationship between software development and digital identity without including software product management in any form but merely mentioned SPM in the text. Additionally, some sources were aimed towards different fields, such as manufacturing, which included relevant information on the field or digital identity but not regarding the software product management. There are two possible reasons for these sources to be included in the search results. First reason being the nature of using a search string, which often casts a wide search based on the strings defined without considering the relationship between the two keywords beyond the Boolean operator “AND” which only instructs the search engine to include both strings. The second possible reason is that when the search string was inserted, there was an option in Google Scholar to only include the keywords in titles, which could have limited the number of results and emphasized the relationship between the keywords. This option was not however utilized to allow the widest possible search on sources to be found on the topic, which then required more thorough examination to further deem sources either included or excluded from the research.

The type of sources that were collected through both information collection methods consisted of journal articles, conference proceedings and white scientific literature such as research reports done by businesses and organizations. In addition to academic and white literature, grey literature such as books, regulatory publications, and theses was included. Grey literature can be defined as any document that has “not gone through formal peer review for publication” (Institute for Work & Health, 2008). To have the deepest possible understanding of the topic and find the most valuable information from multiple sources, the search string and snowballing were both utilized, and literature such as published peer-reviewed literature as well as grey and white literature was included.

3.2.3 Information Analysis

To find the suitable sources for further information analysis, each source saved to Zotero was read thoroughly and the sources were either included or excluded from further information extraction according to certain criteria. The requirement for a source to not be included in information analysis is that the source fulfils at least one of the three following exclusion criteria. The source either:

- a) do not fit inside either the participation or core SPM activities of the ISPMA framework
- b) is technically focused on the concept of digital identity or
- c) do not create any relationship between software product management and digital identity but rather discussed these topics separately.

In this context, technically focused sources included, for example, discussing the technical aspects of some digital identity technology or identity management system in detail. Even though those sources could mention SPM, and would therefore be found by the search engine, the sources would not be able to provide information relevant to the research questions. After a sufficient number of sources were collected, saved to Zotero, and deemed suitable, the information was analysed. Several approaches to information analysis were considered, including methods like systematic data collection and synthesizing in Excel. After evaluating these options, mind mapping was selected as the primary method for analysis.

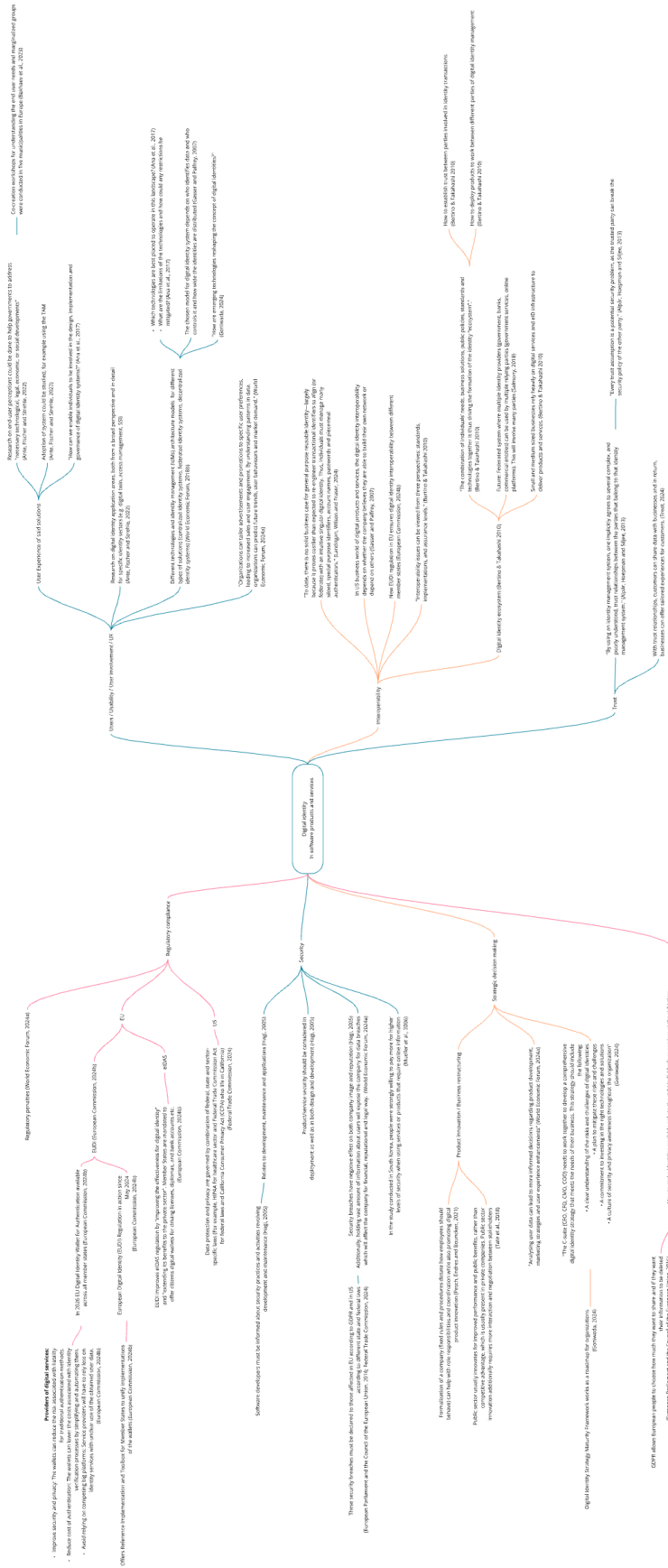


Figure 2. Mind map of the extracted information

Although systematic data collection methods were briefly considered, they were ultimately found unsuitable due to the inherently flexible and exploratory nature of this research, which differs from the structured approach typical of systematic literature reviews. Consequently, mind mapping was used to extract key information (Figure 2), which was then categorized to a structure (Figure 3) highlighting the participation and core activities of the framework created by ISPMA. The tool for both mind mapping and organizing the information into the framework was Miro, which is a digital collaboration tool for visual planning of strategies, product development workflows and workshops (Miro, 2024).

In mind mapping, the sources were individually and thoroughly read through, and any key insight related to the topic was placed into a mind map. The outline of the mind map is presented in Figure 2. As more information was gathered, individual pieces of information were categorized under common themes. These themes included regulatory compliance, security, privacy, trust, interoperability and strategic decision making. There was also one collective category for any user related information including usability, user experience (UX) or user involvement. As information was added to the mind map, the corresponding source was added to a list of references for information categorization.

After the information was placed on the mind map, the different information points were categorized into a structure of the ISPMA framework by Kittlaus (2022) presented more in the detail in the background chapter of the thesis. This structure of the categorized information can be seen in Figure 3. In the structure, the core SPM activities were incorporated into the analysis, which are highlighted by the blue rectangular box in the bottom of the structure. Due to the substantial amount of information related to the activities under the participation responsibility area, the decision was made to include the participation responsibility area of Strategic Management of the ISPMA framework to the information categorization as well. As can be observed from the structure, the responsibility area of participation received the most amount of information. Overall, the information was categorized under the first appropriate match of various SPM related activities, even though there was some overlapping with other activities as well.



Figure 3. Categorization of information to ISPMA framework by Kittlaus (2022, p. 37)

Where appropriate, arrows were drawn either between singular pieces of information or whole activities to emphasize similar information in both. For example, a relationship was identified between the market and product analysis activities under the strategic management as both contain overlapping information from multiple sources. Similarly, a connection was drawn between compliance management under strategic management and legal and IPR management under product strategy to emphasize the similarities. As illustrated in Figure 3, the orchestration responsibilities of SPM received relatively little information, likely due to their distinct nature compared to the core and participation responsibilities of the framework. After categorizing the information under respective areas of responsibility, different colours, green, orange and pink, were used to distinguish the current state (green), company challenges (pink), and future research opportunities (orange), as addressed by the research questions. This color-coding aided in formulating the answers to each individual research question. The information, first extracted and categorized in the mind map and then organized and color-coded using the ISPMA framework, was systematically applied to address the primary research question and its sub-questions. The results are presented according to each color-coded information under each responsibility area.

4 Results

This chapter presents the results by addressing the current state, company challenges, and future research gaps of digital identities in software products and services. The results chapter is structured into four sections, addressing three research sub-questions and one primary research question. The findings for each sub-question are first addressed individually, followed by the synthesis of these results in the last section dedicated to the primary research question. The beginning of each sub-question chapter also includes brief summaries of the results.

The first sub-question examines the current state of research and practice regarding the use of digital identities in software products and services. The second sub-question explores the challenges companies face when implementing digital identities to software products and services. The third sub-question addresses the future research directions to address these challenges. Finally, the primary research question integrates these findings, identifying key research gaps and proposing methods to effectively address them. The sub-question sections are further divided into subsections based on the core and participation responsibility areas as outlined in the ISPMA framework. These areas, which were central part of the data analysis, include Strategic Management, Product Strategy and Product Planning. The results are presented in relation to different activities inside these responsibility areas. In contrast, the primary research question is presented without these subsections to allow greater flexibility in presenting the synthesis of the sub-questions.

4.1 Current State of Research and Practice

The first research question addresses the current state of research and practice related to the use of digital identities within software products and services, to further lay foundation on what research have already been done and how things are done in the industry. As mentioned already in the chapter description, this chapter is divided into subsections of each responsibility area of the ISPMA framework. Each subsection addresses to the information in different areas of the data analysis structure in Figure 3. To briefly summarize, the current state of research and practice include the EU and US regulations, and the EU regulation is

currently changing the landscape. The results also highlight the important role of private companies on digital identity space, while no interoperability exists among digital identities. Users can share their data with companies, which can be analysed to predict future trends and make strategic decisions. End users have also been involved in many research projects investigating the requirements, pricing and privacy of digital solutions.

4.1.1 Strategic Management

Under the Strategic Management responsibilities in the data analysis structure based on the framework by the ISPMA, the first piece of information is related to current state of research in under the activity of innovation management. According to the report by Ana et al. (2017), private companies play important role in providing identities through activities such as innovation, development and supply. Currently private companies usually act as an IdP for identity solutions (Ana *et al.*, 2017). For example in Finland, people authenticate themselves to different services through banks and telecommunication companies acting as IdPs, using either banking identifiers, known as BankID, or through mobile identifiers, known as MobileID (Bazarhanova, 2020). This concept of private companies providing identities is closely related to identity ecosystem. The current trends of identity ecosystem was highlighted in the book by Bertino and Takahashi (2010) mentioning that these trends include service orientation, business restructuring, security and privacy, and compliance. Very few companies are building their own identity management systems (Caribou Digital, 2016), despite the fact that different technologies for digital identification, such as blockchain and biometrics, have been emerging in the digital identity field (Bertino and Takahashi, 2010). The current state of digital identity for users is highlighted in a journal article by Landrigan, Wilson and Fraser (2024), as they mention that currently users have to manage many siloed special purpose identifiers, account names or passwords, instead of having general purpose reusable identities, which would be very costly to re-engineer.

Many of the largest companies such as Google, Facebook and Apple are using the opportunity of knowing their individual customers to predict different things, such as customer attitudes and needs (Ana *et al.*, 2017). This phenomenon of taking of advantage of available user data was emphasized in other areas of SPM responsibilities as well. In market analysis activity, one current opportunity for organizations is predictive analytics which

helps companies predict future trends, market demand and user behaviour based on the patterns in data (World Economic Forum, 2024a). Similarly, the user information can be utilized in decision-making related to the products and services, such as creating marketing strategies, product development directions and enhancing user experience (World Economic Forum, 2024a). Even though personal data cannot be confused with identity attributes, personal data can be considered an identity attribute if it is combined with other elements (Domingo and Enríquez, 2018). Regarding personal data, it was revealed in a report, that consumers who are able to manage and protect their privacy, are up to 52% more willing to share information compared to those who are not able to manage these aspects themselves (Rose, Rehse and Röber, 2012).

Related to the compliance management activity, there are many current regulatory aspects of digital identity in action. As mentioned in the introduction, there has been significant number of regulatory changes in EU. The original eIDAS regulation which was put into action in 2014, was revised during 2020 and in 2021 European Commission proposed a new regulation called EUDI regulation to address the shortcomings of the original eIDAS regulation (European Commission, 2024a). The new regulation, that came into action April 2024, proposes European digital identity wallet which allows citizen to control their own data and have their driver's license, diplomas and bank accounts as well as other personal attributes linked to their digital wallet, which will be recognized across EU (European Commission, 2024b). This new regulation will tackle many of the issues present in research and documentation related to digital identities, such as interoperability and data privacy. Interoperability refers to interconnection of among identity system users, providers, and consumers, and permits transmission of digital identity among them in secure and private manner (Gasser and Palfrey, 2007). The EUDI regulation will also give multiple benefits for companies targeting their digital products and services towards European Union citizens, such as improved security and privacy, reducing the cost of authentication and having to rely less on identity services with unclear intentions towards user data (European Commission, 2024b). Regarding EU, another important regulation in action since 2016 is the General Data Protection Regulation, also known as GDPR, which heavily affects the processing of personal data, free data movement and individual's right to the protection of personal data (European Parliament and the Council of the European Union, 2016).

In US, different laws of digital identity, such as consumer privacy, credit reporting, identity theft and information security, are overseen and enforced by FTC's Division of Privacy and Identity Protection (2024). Currently, the division enforces laws such as Section 5 of the FTC Act towards fair and honest acts and practices involving the use or protection of personal information of the customer. Another law of FTC is the Fair Credit Reporting Act which makes sure that credit bureaus and other consumer reporting agencies are accurately and privately keeping information of the customers, as well as allowing customers to know what information is distributed to other entities. Related to financial services, another law enforced and overseen by FTC is the Gramm-Leach-Bliley Act, which requires financial institutions to ensure that the customer information is secure and confidential, that customers are notified of the institution's information practices, and allow customers to decide that their information should not be shared with specific third-party entities. Another field-specific laws of FTC are Children's Online Privacy Protection Act, which allows parents to control the information collected of their children by companies and how said information can be used, and Health Breach Notification Rule, which affects companies that are not covered by the Health Insurance Portability and Accountability Act, also known as HIPAA, to notify customers and other entities of data breach of electronic health information that is unsecured and can be identified to an individual. (Federal Trade Commission, 2024)

Regarding the general compliance management inside companies, it was mentioned by World Economic Forum (2024a) that not complying with different data protection regulations can lead to significant fines and different sanctions. Additionally, it was mentioned by Hagi (2005), that the legislative landscape and the regulatory requirements place growing emphasis on corporate governance towards application and software assurance. One recent example of issuing a fine for violating regulations was when Irish Data Protection Authority issued a fine of 1.2 billion euros for Facebook, owned by Meta, for transferring personal data of European users to US without compliance with GDPR, being the largest GDPR fine to date (European Data Protection Board, 2023).

4.1.2 Product Strategy

Under Product Strategy area of ISPMA framework, the first piece of information is related to the delivery model and service strategy activity. In an article by Treat (2024), trust-

relationships between customers and companies were introduced, meaning that customers can share discrete data in real time with businesses, who then can offer tailored experiences for customers. One example of this is the cookie policy of web browsers, where customer is looking for certain type of clothes in specific shop, the shop can then advertise similar clothes found in their collection to encourage the customer to buy something. The same method of customization can be applied in a larger scale to software products and services, where companies or individuals using a certain product or service can send real-time data, as they choose, which then can lead to tailored experience with the product or service. This kind of trust for users sharing information with a company must be earned through cybersecurity, safety, transparency, privacy, and interoperability, as highlighted by Treat (2024). Further related to delivery model and service strategy, the chosen model for digital identity, which is directly comparable to different IdM systems presented in the background section, depends on who holds the identifying information, who controls it and how widely the information should be distributed (Gasser and Palfrey, 2007). This way the IdM system for the current software products and services can be determined.

Regarding the next activity in Product Strategy responsibility area, ecosystem management, in US business world of different digital products and services, the interoperability of digital identity solutions depend on whether the company is confident on building their own network or they need to rely on others to create sufficient network for the solution to be useful for consumers (Gasser and Palfrey, 2007). Lastly, regarding the activity of pricing inside the Product Strategy responsibility area, a research conducted in South Korea found out that people are willing to pay more for the service in three different cases: if the identifier service allows them to refuse giving their sensitive private information to the service provider, if the service has wider coverage of identifiers, or if the service has high level of security (Mueller *et al.*, 2006).

4.1.3 Product Planning

For the last core SPM responsibility area, product planning, there were two mentions for current state of research and practice. Under the customer insight activity, currently research has been done to understand the current user requirements for emerging electronic identity management platforms of municipal services in five countries of European Union. In the

research by Bakhaev et al. (2023), the positive expectations included greater usability, time and resource efficiency and greater convenience of online services. On the contrary, perceptions such as accessibility, security, usability and support were recognized. This kind of insight can help with development and understanding customers of the current software products and services, especially if any of the emerging technologies are involved.

4.2 Company Challenges in Implementing Digital Identities

The second sub-question addresses the challenges that companies face when implementing software products or services with digital identity. Generally, through first acknowledging challenges, the solutions can be found. In this case, by acknowledging company challenges, the possible future directions for research can be found and those challenges can be effectively addressed, as the primary research question aims to achieve. To summarize the results, the company challenges include the regulatory requirements, security and the impacts of security or data breaches to the company. Interoperability of digital identities and security of trust relationships inside digital identity ecosystems are highlighted as challenges as well. Innovation-related differences and challenges exist between public sector and private companies. There is also integration challenges regarding tools that manage information of software products sent to market.

4.2.1 Strategic Management

The first mention of company challenge can be found under the corporate strategy activity in Strategic Management responsibility area. The report by Hagi (2005) discusses many of the challenges companies face, including regulatory requirements placing increasing emphasis on corporate governance, as mentioned in the current state as well. Additionally, Hagi (2005) discusses the negative effect of security breaches on company image and reputation. In 2005, there was not as extensive regulatory demand to declare security breaches publicly, but currently many laws and regulations, such as GDPR in EU and FTC's industry specific laws in US, force companies to declare security breaches to their customers. Even though this promotes transparency between companies and their customers, it still can heavily affect the reputation and company image of such unfortunate companies. This

challenge is additionally emphasized by World Economic Forum (2024a), as they discuss that holding large amounts of data can increase the risk of being a victim of data breach, and that the breaches can cause financial, reputational and legal harm to the attacked company. To mitigate the risk of being a victim of data breaches, security related aspects are further emphasized in the sources. For example, Hagi (2005) discusses the importance of considering the security of product or service in deployment as well as in design and development, and continues to point out that software developers should be informed about security practices and activities revolving about development and maintenance of products and services.

Further down the responsibility area, the next company challenges arise under innovation management, which apparently can be very different depending on whether discussing private companies or public sector. As briefly mentioned by Tate et al. (2018), based on highlights by both Cunningham and Kempling (2009) and Lee et al. (2012), public sector innovation is typically aimed at services rather than products, and public sector aims for public benefits and improved performance instead of competitive advantage, which is often present in private companies. Despite different goals, both entities have their challenges on innovation. In addition to increased need for interaction and negotiation with stakeholders, public sector struggles with innovation in silos, since there are no integrated approach across the government, engaging users and creating desired relationships with partners (Bertot, Jaeger and McClure, 2008). Both private companies and public sector struggle with the “fuzzy front end” of innovation (Smith and Reinertsen, 1992b), which refers to the phase of product development, where an innovation opportunity or problem has been identified but no one, a team or manager, has been assigned to progress on the matter (Smith and Reinertsen, 1992a).

Lastly, under product analysis activity, it was recognized by Dahlqvist (2005) that there are integration issues with tools for both Product Data Management (PDM) and Software Configuration Management (SCM), which manage information related to either hardware (PDM) or software products (SCM). This integration problem between PDM and SCM tools disrupt development efficiency, and to solve this challenge, companies have their own in-house tools for integration or use simpler PDM tools from the market to manage their products (Dahlqvist, 2005).

4.2.2 Product Strategy

Under Product Strategy responsibility area, the first activity that introduces company challenge is under delivery model and service strategy activity. As discussed already when addressing the first research sub-question, interoperability is common theme among the findings of this thesis. Report on case study of digital identity systems done by Gasser and Palfrey (2007) specifically addresses interoperability as a challenge in current as well as future digital identity systems. As highlighted in their report, interoperability requires widespread uptake for the interoperable identity to succeed and the possible pitfall include stakeholders splitting off or throwing support of said interoperable systems, therefore breaking down the collaboration between stakeholders. Interoperability-related challenges are further discussed by Bertino and Takahashi (2010) by asking a question of "How to make identities available only to the right individuals or services at the right time and place".

Under the next activity, ecosystem management, multiple company challenges can be found regarding the trust relationship that was introduced when addressing the first research question. It was addressed in journal article by Alpár et al. (2013) that using an identity management system implicitly involves agreeing to several complex and poorly understood trust relationships between different parties involved in that system. As seen in the background descriptions of three archetypes of different identity management systems, there are usually multiple parties involved in identity management systems, and for example user of these systems needs to trust every party of specific system. This trust on every party of the system can be further highlighted by Alpár et al. (2013) as a challenge in the ecosystem, since every assumption of trust inside the system is also a security issue, since one trusted party can break some security policy of another party. This trust between different parties in identity management ecosystems is further emphasized by Bertino and Takahashi (2010) by highlighting the challenge of establishing trust between parties involved in transactions of identities.

4.3 Future Research Directions

The last sub-question addresses future research directions related to digital identities in software products and services. The goal is to understand any references in the sources

regarding the future and what could be researched related to the topic. Through understanding future research, this can help formulate the plan for conducting future research. In this case, the research on the topic will continue in doctoral dissertation and therefore any knowledge on future research gaps will be highly valuable. To summarize the section, the future research directions emphasize end users and their requirements, involvement and perceptions when using digital identity in software solutions. Additionally, the impact of different digital identity technologies, either current or emerging, on the digital identity field could be researched. Innovation, digital identity strategy and returns of digital identity solutions could be researched to solve the related challenges. Regulations, especially in EU, require further research as well.

4.3.1 Strategic Management

The first relevant piece of information under Strategic Management, can be found under the first activity, corporate strategy. Goniwada (2024) introduces a concept of digital identity strategy that meets the need of the business and is created by the C-suite, referring to people working as Chief Executive Officer (CEO), Chief Financial Officer (CFO), Chief Marketing Officer (CMO) or Chief Operating Officer (COO). The digital identity strategy refers to the comprehensive steps to help companies with protection of their customer's data, complying with regulations, reducing fraud and identity theft and enabling new business models for the emerging technologies of digital identity. According to Goniwada (2024) the digital identity strategy should include the following information:

- Assessment of the risks and challenges associated with digital identities
- A plan to address and mitigate these risks and challenges
- A dedication to investing in appropriate technologies and solutions
- A strong organizational culture that emphasizes security and privacy awareness

To further support organizations to create such strategy for digital identity, Goniwada (2024) introduces the Digital Identity Strategy Maturity Framework, which can help organizations to realize their current capabilities and identify any gaps for the future path. The reason this digital identity strategy was included in the future research directions is that it helps companies to address some of the challenges presented in the previous sub-question. As the

book by Goniwada (2024) was just recently published, the digital identity strategy must not have received exhaustive attention and therefore it can be considered under further inspection in the future.

Next future research directions refer to both portfolio management and innovation management activities. Discussed by Tate et al. (2018) and Pesch et al. (2021), the future efforts to allow innovation in companies and public sector. The research done by Pesch et al. (2021) highlights the relationship between organizational structure, especially formalization, and innovation. Their research results supports the hypothesis that formalization of a company, which refers to a structure where each role has distinctive responsibilities, can enhance digital product innovation radicalness and performance, especially in older firms (Pesch, Endres and Bouncken, 2021). The research done by Tate et al. (2018) also highlight that innovation requires nurturing environment, sponsorship from the high level of the company in addition to having appropriate authority to properly proceed in the innovation progress. To further introduce future research directions for innovation management activity, Ante et al. (2022), highlight the need for more knowledge or estimation on potential returns or margins of digital identity solutions, which can act as a driver for innovation as the monetary potential of said solutions can be understood more comprehensively.

Future digital identity solutions must be compliant with different regulations and laws. Under compliance management activity, one aspect to further study is the regulatory aspect of products and services that use digital identity. Especially, the effects of the new EUDI regulation, that mandates Member States of European Union to offer the EU Digital Identity Wallets to citizen by 2026 (European Commission, 2024b), would be insightful study from the point of view of companies and public sector entities that has to comply with the new regulation. It is also mentioned by European Commission (2024b), that the regulation offers new business opportunities and therefore new services and products. This could be one opportunity for future research as well. This need for further research on regulatory aspect is highlighted by Rahman (2024), as he proposes multiple future research directions, including mixed model of public sector and private sector identity systems to work together according to the EU regulations towards digital identity systems. Additionally, the European scheme for digital identity could be further studied to make it easier to use (Rahman, 2024).

Under market analysis activity, there are multiple future research directions. Related to emerging technologies of digital identities, Goniwada (2024) proposes multiple questions for future research. These questions include future directions related to the way emerging technologies, such as AI, blockchain and IoT, reshape the concept of digital identity or the way people interact online through these technologies. Additionally, technologies are under further consideration by Ana et al. (2017) as they question the future innovation pathways for digital identity systems from the point of view of behavioural attributes. The research also point out the limitations of technologies and how could the restrictions of technologies be mitigated (Ana *et al.*, 2017). Lastly, one future research direction includes studying digital identity application areas from broad perspective as well as in detail for specific sectors that utilize digital identity, as presented by Ante et al. (2022).

4.3.2 Product Strategy

The only future research direction that relate to the responsibility area of Product Strategy can be found under the activity of ecosystem management. Salmony (2018), aims his article towards rethinking the concept of current digital identity system towards the future. For the future, he proposes an interoperable federated system that would include having multiple identity providers, such as government, commercial parties, social media, mobile operators and banks. These providers could verify the rights to access, which then can be further used by multiple relying parties, including government services, online platforms, and internet of things. (Salmony, 2018)

4.3.3 Product Planning

Regarding the last responsibility area, Product Planning, many future research directions can be identified. First of all, under customer insight activity, one future direction includes researching user perceptions, such as motivations and needs of end users and stakeholders (Ante, Fischer and Strehle, 2022). This could help governments to address any technological, legal, economic or social developments and would act as a basis for regulations and policies that are innovation-friendly and sensible, as highlighted by Ante et al. (2022). Additionally, it is mentioned by Ante et al. (2022), that adoption rate of certain digital identity solutions

could be studied using surveys and expert interviews to test theories such as Technology Acceptance Model (TAM) to further understand the user needs and demand. Further research directions to understand end-users of digital identity solutions is provided by Ana et al. (2017), as they present the priority to research how individuals can be enabled to participate in the design, implementation and governance of digital identity system. Related to the last activity under the responsibility area, product requirements engineering, one future direction was found. Cabinakova et al. (2019) identified a need to replicate their research on user acceptance and user requirements of centralized and decentralized IdM systems under different circumstances, such as more heterogenous sample and including the effects of privacy concerns that were left out in the original research due to high amount of existing research on the topic.

4.4 Key Research Gaps and Future Research Recommendations

To summarize the findings of the three sub-questions, the key research gaps can be identified under common themes, including different influences, challenges and improvements. These key research gaps include interoperability, innovation, trust relationships, digital identity strategy, and involvement of end users and their requirements. Each research gap is individually presented and ways to address them are proposed. As mentioned, multiple times in the text, the research done on this thesis will act as a plan for doctoral dissertation and therefore through these research gaps, the future research can be planned accordingly. As can be seen from the names of the themes, not every future research gaps is directly related to software products and services or their management, but the discussed gaps still directly affect how SPM is performed.

Interoperability

It would be beneficial for both software companies and public sector to research interoperability. As highlighted in the results, there are multiple options for future research. Either interoperability could be researched with more US-focused approach, where interoperable digital identities, discussed multiple times in various sources (Gasser and Palfrey, 2007; Salmony, 2018; Landrigan, Wilson and Fraser, 2024), could be further investigated. This could help software companies, especially small or medium-sized companies, implement those in their products and services not only in the US but globally.

Another point of view would be focusing on EU area, and especially the new EUDI regulation active since April this year, which will promote interoperability across European Union. Through researching the new regulation as private companies and public sector being in the focus, any requirements on software products and services according to the regulation could be identified and addressed. Consequently, software products and services would comply with the regulation with better understanding of the requirements for interoperable solutions. Additionally, the new business opportunities created by the regulation, mentioned by European Commission (2024b), could be researched regarding new software products and services.

Trust relationships

Closely related to interoperability, the trust relationships inside digital identity ecosystems could be further researched to understand the current situation and the future opportunities for companies. These relationships are important on providing users with access to different digital services, including software products and services. As mentioned in the results by Alpár et al. (2013), every trust assumption is a potential security problem, as singular party can break the trust relationship by violating security policy of someone else within same trust relationship. Security was emphasized in the results and as these relationships are crucial for software product and service privacy and security, it would be beneficial for SPM of these solutions to further research the trust relationships and their possible problems inside digital identity ecosystems. Through better understanding of trust relationships, possible security issues can be identified and addressed.

Innovation

As innovation management was one of the most emphasized activities among the information analysis, the innovation processes and possible drivers related to software products and services with digital identities in them could be further researched. As highlighted by Pesch et al. (2021), more formalized structure of a company can enhance digital product innovation. This research could be replicated to take more industries into account to understand how company structure can affect the innovation practices. Additionally, as mentioned by Tate et al. (2018), and Smith and Reinertsen (1992a, 1992b), the phenomenon of “fuzzy-front end” of innovation could be studied. As discussed in the results in more detail, there seems to be general difficulties regarding innovation for both

private companies and public sector and these difficulties could be further researched, identified and addressed with appropriate methods.

Digital identity strategy

As presented by Goniwada (2024), the digital identity strategy and the related maturity framework could be further researched, for example, looking for real-world implementation of presented strategy in existing companies that offer software products and services. The digital identity strategy addresses many of the requirements for digital identity use, such as protecting customer's data, complying with regulations as well as enabling new business models (Goniwada, 2024). Therefore, further research could be beneficial to identify if companies have something similar to the digital identity strategy in use. The strategy could be further assessed to ensure it addresses all the necessary aspects. As the adoption of digital identities and emerging technologies progress, the strategy could help companies navigate the field and ensure secure products and services for customers along other benefits.

End user involvement and requirements

In various sources, there were mentions of end users of software products and services. Therefore, end users could be the attention for future research from multiple points of view, including further research on end user requirements (Bakhaev *et al.*, 2023), user acceptance or adoption rate of certain identity management systems (Cabinakova, Ostern and Krönung, 2019) or end-user involvement in the design, implementations and governance of said systems (Ana *et al.*, 2017) to further address any user-related issues of digital identities or their use in software products and services. Through research and better understanding of end-users of software products and services with digital identities in them, the products and services can better serve the users as they can be more involved, and their requirements would be better understood.

5 Discussion

The discussion chapter presents some thoughts on future of digital identities, common themes of the information analysis, short summary of key research gaps, and the limitations and validity of the thesis. The first section goes through the future landscape of digital identities that could affect software products and services. The second section introduces the common themes of the information analysis and summarizes the key research gaps regarding the topic, as addressed in the primary research question of the thesis. Lastly, the third section goes through the limitations and validity of the work.

5.1 Future of digital identities in software products and services

As highlighted in the report by Ana et al. (2017), big companies, such as Facebook, Google and Apple leverage their opportunity to collect data from individual customers to predict future needs and attitudes. Therefore, it is plausible that in the future, big companies with limitless amount of data available on large masses of population and huge financial resources, will dominate the field of digital identity innovation, development and adoption rates. This will leave smaller companies dependent on IdP solutions of bigger companies and it will be more difficult or impossible to surpass them in competition. This will inevitably affect the digital identities in software products and services, if big companies remain as the trailblazers of user data and therefore effecting the innovation and development of digital identity options and related requirements as well.

The European Union's regulations, such as GDPR and the new EUDI regulation, will continue to affect the requirements of global software products and services that are offered to customers that live in EU area. After learning about the laws that exist in US through the FTC, it is evident that there are no general and collective laws regarding the digital identity as in EU but instead, there are laws specific to certain industries, such as financial services or healthcare. This fundamental difference with the existing regulations and laws will continue to create difficulties between software products and services, and their use or distribution to either EU or US. Since this thesis limited the geographical focus on mainly EU and US, there could be more difficulties with regulations and laws when looking further

in different countries in the world. In the future, more wider understanding on various regulations and laws around the world regarding digital identities could be gathered through for example, a literature review. As regulations and laws for digital identities prominently dominate how they should be implemented in software products and services, broader understanding could be beneficial for not only researchers of the topic but also for companies who seek opportunities for new markets.

Another aspect of future of digital identities includes interoperability, which turned out to be one common theme as well as future research gap based on the information in the sources. Mentioned in the results many times, interoperability, which refers interconnection of among identity system users, providers and consumers, and permits transmission of digital identity among them in secure and private manner (Gasser and Palfrey, 2007), will be influential topic in the future discussion of identity management systems of software products and services. As mentioned in the results, the EU's new regulation, EUDI, addresses the challenge of interoperability in European Union area by offering EU wide digital wallet that will include citizen's national digital identity by proof of other personal attributes through driving licenses, diplomas and bank accounts (European Commission, 2024b). Besides the regulatory aspect of interoperability, some sources were mentioning future digital identities that would be interoperable or reusable (Gasser and Palfrey, 2007; Salmony, 2018; Liminal, 2022) and were proposing ideas how to build those. If there was a wider adoption of certain type of digital identity and identity management system, similarly what the EUDI regulation is doing in EU, it would benefit companies that offer software products and services since they would not have to spend time and resources solving the current issues and challenges regarding digital identities and its interoperability. It would, however, be extremely difficult to come up with interoperable digital identity that would comply with all the regulations and laws around the world so this can be considered as wishful thinking rather than actual future option for digital identity or identity management system.

5.2 Common themes and future research opportunities

The common themes regarding the use of digital identities in software products and services include interoperability, innovation practices, trust relationships, regulatory compliance, digital identity strategy, challenges in private companies vs. public sector, and end user

involvement and requirements. These common themes can be seen in the information analysis structure (Figure 3), as certain activities are more highlighted than others. For instance, various information regarding the ecosystem management activity was collected from the sources and the activity overall received considerable attention in the information analysis. Other activities that received similar attention were corporate strategy, innovation management, market analysis, and customer insight. Overall, it was surprising to observe how much information attention activities under the Strategic Management responsibility area received. As Strategic Management is seen as more participation responsibility for software product management, instead of core responsibility as defined by Kittlaus (2022), it is surprising how much effect corporate strategy or innovation management has on the responsibilities of the software product manager. On the contrary, some areas of the framework did not receive attention at all, including all activities under orchestration responsibility and many of the singular activities inside the core and participation responsibilities of software product manager. Similarly, Product Planning responsibility area did not receive any company challenges but instead, was emphasizing future research directions. Limitation and validity section discusses that more sources could have balanced out the information analysis structure to include more information on other parts of the ISPMA framework. However, with the time restrictions of the thesis, some activities can be seen highlighted with considerate amount of information in the structure while some were heavily neglected.

The primary research question in this thesis addresses the future research gaps. As discussed in more detail in the last section of the results chapter, the key research gaps related to digital identities in software products and services include interoperability, innovation, trust relationships, digital identity strategy, and involvement of end users and their requirements. There can be seen direct relationship between the most popular activities of the information analysis structure and the key research gaps addressed in the primary research question. Those activities that received considerate amount of information often included some opportunities for future research, as addressed in the third sub-question. Therefore, it is possible that there could be more research gaps outside the ones identified in this work, but as sufficient amount of information was not found on all activities, the lack of information proposes difficulty to discuss related research gaps. However, looking at the information analysis structure (Figure 3), there could be more research done on specific activities or

responsibility areas of the framework to further connect digital identities to software product management.

5.3 Limitations and validity

The most significant limitation of this thesis was its resources. The thesis got allocated the standard resources for master's thesis, but it turned out that the amount of information and the analysis process would have required more resources to perform comprehensively. With more resources, more sources could have been included and analysed in more detail. Additionally, due to resource limitations, this study did not include validity or bias assessment on the sources before including them as part of the analysis. Related to limited resources, the sources analysed in this thesis were heavily focused on the European Union or US software products and services with digital identities in them as some areal delimitation had to be done. US and EU were easy to include as focus areas as they both have different approaches to digital identities while also having some similarities. In the future, research could address this areal limitation and explore the relationship between digital identity and software product management globally.

As briefly discussed in previous section, another crucial limitation of this research includes the information analysis and number of sources collected for it. As can be seen from Figure 3, not every activity or responsibility area of the framework received information from the sources related to digital identities. On the contrary, some activities and responsibility areas received significant attention, including Strategic Management responsibility area, which received overall most information. According to the sources utilized in this work, information regarding digital identity in software product management clearly focuses on certain areas, at least when utilizing the ISPMA framework. With a larger number of sources, it could have been possible to balance out the information on different activities within the framework. However, due to available resources, it was not feasible to include such an extensive range of sources. Therefore, the information analysis done on connecting digital identity related information on the ISPMA framework is not exhaustive. In the future, similar research could be done with more sources included, and this way the different areas and activities in the framework would receive more evenly distributed attention. Alternatively, different method or framework could be utilized for information categorization.

Lastly, limitations of the research method include not properly performing the fourth stage of Arksey and O'Malley's (2005) original scoping review framework, which involves charting key details of each source, such as authors, year of publication, aims of the study and methodology. Instead, reference details and relevant information regarding the sources were recorded to Zotero. Each source was also accompanied by brief notes on its potential usefulness for the analysis and the general description of information that each source offered. As highlighted by Arksey and O'Malley (2005), scoping reviews face some difficulties, such as inability to assess the quality of the evidence from primary research reports. Scoping reviews tend to provide more of a narrative or descriptive account using the available research rather than in-depth analysis (Arksey and O'Malley, 2005). Moreover, the nature of scoping reviews, combined with the fact that some sources were found from Google Scholar, which personalizes search results based on previous searches, makes it difficult, if not impossible, to replicate the research. In the future, adopting a more structured and systematic approach including validity and bias assessment, would be beneficial. However, due to time constraints, certain compromises needed to be made, with methodology and the source validity suffering the most.

6 Conclusions

The purpose of this thesis was to explore the key research gaps related to digital identities within software products and services. This was achieved by examining the current state of research and practice, identifying company challenges in implementing digital identities in software products and services, and outlining the future research directions. In addition to identifying these research gaps, potential solutions to address them were presented. Using an explorative literature study based on a scoping review framework, several key research gaps were identified in a relation to the activities outlined in the ISPMA framework for software product management. These key research gaps include challenges related to digital identity interoperability, company innovation practices, trust relationships in digital identity ecosystems, strategy for digital identity, and the involvement of end users and their requirements.

This thesis represents the first exploration of the relationship between digital identities and software product management. With the recognized key research gaps of the thesis, more research can be conducted to support companies, and especially software product managers, in successfully and responsibly implementing digital identities into their software products and services. Despite the valuable insight, this thesis was subject to several limitations, the most significant being time-related constraints. These limitations impacted the amount, validity and bias of the analysed sources, as well as the depth of the information analysis. Future research could continue the work done in this thesis by addressing the identified key research gaps more comprehensively. In conclusion, this thesis takes important first steps towards understanding digital identities in software products and services. As the global adoption of digital identities continues to grow, the findings of this thesis provide insightful foundation for future research related to the field.

References

Alpár, G., Hoepman, J.-H. and Siljee, J. (2013) ‘The Identity Crisis Security, Privacy and Usability Issues in Identity Management’, *Journal of Information Systems Security*, 9(1), pp. 23–53. Available at: <https://doi.org/10.48550/arXiv.1101.0427>.

Ana, B. *et al.* (2017) *Building Digital Identities: The Challenges, Risks and Opportunities of Collecting Behavioural Attributes for new Digital Identity Systems*. University of Exeter and Coelition. Available at: <http://hdl.handle.net/10871/28297> (Accessed: 9 July 2024).

Ante, L., Fischer, C. and Strehle, E. (2022) ‘A bibliometric review of research on digital identity: Research streams, influential works and future research paths’, *Journal of Manufacturing Systems*, 62, pp. 523–538. Available at: <https://doi.org/10.1016/j.jmsy.2022.01.005>.

Arksey, H. and O’Malley, L. (2005) ‘Scoping studies: towards a methodological framework’, *International Journal of Social Research Methodology*, 8(1), pp. 19–32. Available at: <https://doi.org/10.1080/1364557032000119616>.

Bakhaev, S. *et al.* (2023) ‘Co-Creating Requirements for the Emerging Electronic Identity Management Platform’, in *14th Scandinavian Conference on Information Systems*. Available at: <https://aisel.aisnet.org/scis2023/1>.

Barton Cunningham, J. and Kempling, J.S. (2009) ‘Implementing change in public sector organizations’, *Management Decision*, 47(2), pp. 330–344. Available at: <https://doi.org/10.1108/00251740910938948>.

Bazarhanova, A. (2020) *Managing change in a dominant infrastructure for digital identification*. Doctoral thesis. Aalto University. Available at: <https://aaltoodoc.aalto.fi/handle/123456789/44024> (Accessed: 3 September 2024).

Bazarhanova, A. and Smolander, K. (2020) ‘The Review of Non-Technical Assumptions in Digital Identity Architectures’, in *53rd Hawaii International Conference on System Sciences*. Available at: <https://doi.org/10.24251/HICSS.2020.785>.

Bertino, E. and Takahashi, K. (2010) *Identity Management: Concepts, Technologies, and Systems*. Norwood, United States: Artech House. Available at: <http://ebookcentral.proquest.com/lib/lut/detail.action?docID=634511> (Accessed: 8 July 2024).

Bertot, J., Jaeger, P. and McClure, C. (2008) ‘Citizen-centered e-government services: Benefits, costs, and research needs’, in *9th Annual International Digital Government Research Conference*. Available at: <https://doi.org/10.1145/1367832.1367858>.

Cabinakova, J., Ostern, N. and Krönung, J. (2019) ‘Understanding Preprototype User Acceptance of Centralized and Decentralized Identity Management Systems’, in *27th European Conference on Information Systems*.

Cambridge Dictionary (2024a) *Ecosystem* | *English meaning*. Available at: <https://dictionary.cambridge.org/dictionary/english/ecosystem> (Accessed: 6 September 2024).

Cambridge Dictionary (2024b) *Software* | *English meaning*. Available at: <https://dictionary.cambridge.org/dictionary/english/software> (Accessed: 9 September 2024).

Caribou Digital (2016) *Private Sector Digital Identity in Emerging Markets*. Farnham, Surrey, United Kingdom: Caribou Digital Publishing. Available at: <https://www.cariboudigital.net/publication/private-sector-digital-identity-in-emerging-markets/> (Accessed: 6 September 2024).

Cullen, R. (2009) 'Culture, identity and information privacy in the age of digital government', *Online Information Review*, 33(3), pp. 405–421. Available at: <https://doi.org/10.1108/14684520910969871>.

Dahlqvist, A.P. (2005) *Important Factors for a Successful Integration of Product Data Management and Software Configuration Management Systems*. Sweden: Mälardalen University. Available at: http://www.es.mdu.se/pdf_publications/889.pdf (Accessed: 2 September 2024).

Domingo, A.I.S. and Enríquez, Á.M. (2018) *Digital Identity: the current state of affairs*. Spain: BBVA Bank. Available at: https://www.bbva-research.com/wp-content/uploads/2018/02/Digital-Identity_the-current-state-of-affairs.pdf (Accessed: 6 September 2024).

European Commission (2024a) *eIDAS Regulation* | *Shaping Europe's digital future*. Available at: <https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation> (Accessed: 19 July 2024).

European Commission (2024b) *European Digital Identity (EUDI) Regulation*. Available at: <https://digital-strategy.ec.europa.eu/en/policies/eudi-regulation> (Accessed: 19 July 2024).

European Commission: Directorate-General for Communications Networks, Content and Technology (2023) *2030 Digital Decade – Report on the state of the Digital Decade*. Publications Office of the European Union. Available at: <https://data.europa.eu/doi/10.2759/318547> (Accessed: 2 May 2024).

European Data Protection Board (2023) *1.2 billion euro fine for Facebook as a result of EDPB binding decision*. Available at: https://www.edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en (Accessed: 11 September 2024).

European Parliament and the Council of the European Union (2016) *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)*. Available at: <http://data.europa.eu/eli/reg/2016/679/oj> (Accessed: 22 July 2024).

Federal Trade Commission (2024) *Division of Privacy and Identity Protection*. Available at: <https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/our-divisions/division-privacy-and-identity> (Accessed: 22 July 2024).

Gasser, U. and Palfrey, J.G. (2007) 'Case Study: Digital Identity Interoperability and eInnovation', *Berkman Center Research Publication No. 2007-11* [Preprint]. Available at: <http://dx.doi.org/10.2139/ssrn.1070061>.

Goniwada, S.R. (2024) *Introduction to One Digital Identity: Strategies, Innovations, and Future Trends*. 1st edn. Apress Berkeley, CA.

Hagi, S. (2005) *Engineering e-Business Applications for Security*. Canada: IBM Corporation. Available at: <https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=3f3e25a94cec345df01b8583b10789cfe30d7bde> (Accessed: 7 June 2024).

Institute for Work & Health (2008) *Grey literature*. Available at: <https://www.iwh.on.ca/what-researchers-mean-by/grey-literature> (Accessed: 23 August 2024).

Kitchenham, B. and Brereton, P. (2013) 'A systematic review of systematic review process research in software engineering', *Information and Software Technology*, 55(12), pp. 2049–2075. Available at: <https://doi.org/10.1016/j.infsof.2013.07.010>.

Kittlaus, H.-B. (2022) *Software Product Management: The ISPMA®-Compliant Study Guide and Handbook*. 2nd edn. Berlin, Heidelberg: Springer Berlin / Heidelberg. Available at: <https://doi.org/10.1007/978-3-662-65116-2>.

Landrigan, M., Wilson, S. and Fraser, H. (2024) 'Why Are There So Many Digital Identities?', *Law, Technology and Humans*, 6(1), p. 18. Available at: <https://doi.org/10.5204/lthj.3096>.

Lee, S.M., Olson, D.L. and Trimi, S. (2012) 'Co-innovation: convergenomics, collaboration, and co-creation for organizational values', *Management Decision*, 50(5), pp. 817–831. Available at: <https://doi.org/10.1108/00251741211227528>.

Liminal (2022) *The Market Opportunity for Reusable Identity and How to Get There*. Liminal. Available at: <https://liminal.co/reports/the-market-opportunity-for-reusable-identity-and-how-to-get-there/> (Accessed: 29 July 2024).

Maler, E. (2009) 'The design of everyday identity', *Online Information Review*, 33(3), pp. 443–457. Available at: <https://doi.org/10.1108/14684520910969899>.

Miro (2024) *Miro | First Idea to Final Innovation — It All Lives Here*. Available at: <https://miro.com/product-overview/> (Accessed: 5 September 2024).

Mueller, M.L. *et al.* (2006) 'Digital identity: How users value the attributes of online identifiers', *Information Economics and Policy*, 18(4), pp. 405–422. Available at: <https://doi.org/10.1016/j.infoecopol.2006.04.002>.

Natarajan, H., Appaya, M.S. and Balasubramanian, S. (2018) *G20 Digital Identity Onboarding*. World Bank Group. Available at: <http://documents.worldbank.org/curated/en/362991536649062411/G20-Digital-Identity-Onboarding> (Accessed: 29 July 2024).

Pesch, R., Endres, H. and Bouncken, R.B. (2021) 'Digital product innovation management: Balancing stability and fluidity through formalization', *Journal of Product Innovation Management*, 38(6), pp. 726–744. Available at: <https://doi.org/10.1111/jpim.12609>.

Rahman, B. (2024) *Conflicts between passkeys and European e-ID scheme*. Master's thesis. LUT University. Available at: <https://lutpub.lut.fi/handle/10024/168189> (Accessed: 2 September 2024).

Rose, J., Rehse, O. and Röber, B. (2012) *The Value of Our Digital Identity*. Boston Consulting Group. Available at: <https://www.libertyglobal.com/wp-content/uploads/2022/08/The-Value-of-Our-Digital-Identity.pdf> (Accessed: 29 July 2024).

Salmony, M. (2018) 'Rethinking digital identity', *Journal of Payments Strategy & Systems*, 12(1), pp. 40–57. Available at: <https://doi.org/10.69554/HGWP9250>.

Sedlmeir, J. *et al.* (2021) 'Digital Identities and Verifiable Credentials', *Business & Information Systems Engineering*, 63(5), pp. 603–613. Available at: <https://doi.org/10.1007/s12599-021-00722-y>.

Smith, P.G. and Reinertsen, D.G. (1992a) 'Developing Products in Half the Time', *Small Business Reports*, 17(1), pp. 65–68.

Smith, P.G. and Reinertsen, D.G. (1992b) 'Shortening the Product Development Cycle', *Research Technology Management*, 35(3), pp. 44–49.

SpyCloud (2024a) *SpyCloud Annual Identity Exposure Report 2024*. Austin, Texas: SpyCloud. Available at: <https://engage.spycloud.com/rs/713-WIP-737/images/spycloud-2024-identity-exposure-report.pdf> (Accessed: 8 August 2024).

SpyCloud (2024b) *We disrupt cybercrime*. Available at: <https://spycloud.com/company/> (Accessed: 8 August 2024).

Tate, M. *et al.* (2018) 'Managing the "Fuzzy front end" of open digital service innovation in the public sector: A methodology', *International Journal of Information Management*, 39, pp. 186–198. Available at: <https://doi.org/10.1016/j.ijinfomgt.2017.11.008>.

The Economist (2017) 'The world's most valuable resource is no longer oil, but data', *The Economist*, 6 May. Available at: <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data> (Accessed: 4 September 2024).

The International Software Product Management Association (2024) *Learn about our values, our work, our people and more*. Available at: <https://ispma.org/about/> (Accessed: 9 September 2024).

Uhlemann, T.H.-J., Lehmann, C. and Steinhilper, R. (2017) 'The Digital Twin: Realizing the Cyber-Physical Production System for Industry 4.0', *Procedia CIRP*, 61, pp. 335–340. Available at: <https://doi.org/10.1016/j.procir.2016.11.152>.

Utesheva, A. (2020) *Designing Products for Evolving Digital Users: Study UX Behavior Patterns, Online Communities, and Future Digital Trends*. 1st edn. Berkeley, CA: Apress L. P. Available at: <https://doi.org/10.1007/978-1-4842-6379-2>.

Wohlin, C. (2014) 'Guidelines for snowballing in systematic literature studies and a replication in software engineering', in *18th International Conference on Evaluation and Assessment in Software Engineering*. Available at: <https://doi.org/10.1145/2601248.2601268>.

World Economic Forum (2018a) *Digital Identity on the Threshold of a Digital Identity Revolution*. Davos-Klosters, Switzerland: World Economic Forum. Available at: https://www3.weforum.org/docs/White_Paper_Digital_Identity_Threshold_Digital_Identity_Revolution_report_2018.pdf (Accessed: 8 July 2024).

World Economic Forum (2018b) *Identity in a Digital World - A new chapter in the social contract*. Available at: https://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf (Accessed: 10 May 2024).

World Economic Forum (2021) *Digital Identity Ecosystems: Unlocking New Value*. World Economic Forum. Available at: https://www3.weforum.org/docs/WEF_Guide_Digital_Identity_Ecosystems_2021.pdf (Accessed: 9 July 2024).

World Economic Forum (2023) *Reimagining Digital ID*. World Economic Forum. Available at: https://www3.weforum.org/docs/WEF_Reimagining_Digital_ID_2023.pdf (Accessed: 17 May 2024).

World Economic Forum (2024a) *Digital Trust: Supporting Individual Agency*. World Economic Forum. Available at: https://www3.weforum.org/docs/WEF_Digital_Trust_Supporting_Individual_Agency_2024.pdf (Accessed: 8 July 2024).

World Economic Forum (2024b) *Our Mission*. Available at: <https://www.weforum.org/about/world-economic-forum/> (Accessed: 7 August 2024).

Zotero (2024) *Zotero | Your personal research assistant*. Available at: <https://www.zotero.org/> (Accessed: 3 September 2024).

Zwitter, A.J., Gstrein, O.J. and Yap, E. (2020) 'Digital Identity and the Blockchain: Universal Identity Management and the Concept of the "Self-Sovereign" Individual', *Frontiers in Blockchain*, 3(26). Available at: <https://doi.org/10.3389/fbloc.2020.00026>.