Managing change in a dominant infrastructure for digital identification

Bazarhanova Anar
Managing change in a dominant infrastructure for digital identification

Bazarhanova Anar

A doctoral dissertation completed for the degree of Doctor of Science (Technology) to be defended, with the permission of the Aalto University School of Science, at a public examination held at the lecture hall TU1 of the school on 5 June 2020 at 12.

Aalto University
School of Science
Computer Science
Supervising professor
Professor Kari Smolander, LUT University, Finland

Preliminary examiners
Assistant Professor Benjamin Eaton, Copenhagen Business School, Denmark
Professor of Practice Tomi Dahlberg, University of Turku, Finland

Opponent
Professor Marko Seppänen, Tampere University of Technology, Finland
Abstract

Enterprise information systems and applications no longer exist as stand-alone entities, but instead, they interact with other information systems inside and outside the company boundaries. The success of many businesses is dependent on their ability to leverage the innovations coming from the outside, which are often global, remote and dynamic. The challenge attributed to industry platforms is that when they become dominant, integration with them is critical to the thriving of smaller, non-focal organizations.

This thesis studies the case of a digital identity management (IdM) platform as an example of a dominant digital infrastructure. IdM is a crucial component in any software-based service that needs to identify, authenticate and authorize the access of its users and it is an important step towards the successful advancement of digital services in a society. The goal of this thesis is to identify the factors that affect the dynamic phenomenon of change in dominant digital infrastructures. The question is observed through the case of BankID infrastructure in Finland. Empirical research methodologies are applied in the study. The data has been collected through case studies and semi-structured interviews with practitioners and policymakers.

This thesis consists of three phases and four sub-problems. First, the study explores the issue by analyzing the characteristics of the dependencies upon a dominant digital infrastructure. Second, the study gives a comprehensive account of the evolutionary dynamics of a dominant infrastructure by explaining how they transform. Next, the study concentrates on extracting the governance lessons learned from the Finnish IdM case. Lastly, the study proposes the overview of architecturally significant components when managing the development of IdM infrastructures.

The results of the study reveal that as platforms gain dominance, they often become the de facto choice in the market. Furthermore, given the recursive relation between platforms and infrastructures, industry platforms that fail to anticipate wider ecosystem needs and adapt to them, evolve into industry infrastructures. The governance of the successful transformation of dominant (IdM) infrastructures requires cooperation and dialogue between the stakeholders. In addition, the following architecturally significant criteria can be used as an evaluative framework when assessing the design and development of large-scale, dominant IdM infrastructures: technology choice, identity provision, human-user integration, provider choice and the business model, governance structure and strategy in relation to the digital heritage.

The results help advance current knowledge in the management of large-scale IdM infrastructures from both technology and organizational perspectives and could be used by software architects, business professionals, executive management as well as policymakers.

Keywords digital identity management, IdM, electronic identification infrastructure, eID, platform ecosystem
Acknowledgements

Even at the risk of sounding cliché, I must say this thesis would have not been possible without the help of these people.

Firstly, I would like to express my sincere gratitude to my advisor Professor Kari Smolander for his continuous support, encouragement, and guidance throughout the years. Thank you, Kari, for giving me the opportunity to do this in the first place, for always challenging my thinking and believing in me. I owe special gratitude to Dr. Jesse Yli-Huumo for actively advising me on my research when I just started my doctoral studies. Jesse’s positive attitude in everything has always encouraged me to get things done and raised my spirits in times of frustration.

I am enormously grateful to the examiners of my thesis, associate Professor Benjamin Eaton and Professor Tomi Dahlberg, for their insightful comments and suggestions to improve this work. Further, I would like to thank Professor Marko Seppänen for the honor of being my opponent, especially in such unusual circumstances.

I have been lucky to work together with other excellent researchers, particularly, Dr. Juho Lindman, Dr. Johan Magnusson, Dr. Andreas Nilsson, Eric Chou and Dr. Ilkka Lähteemäki who I want to thank for our fruitful collaboration. I would also like to thank my fellow colleagues José Carlos, Abheeshta, Juho and all the former colleagues on the second floor in the CS department for the good times we spent together. Our lunch-, coffee-, ice-cream-breaks and afterworks have helped me to feel part of a team. I would especially like to thank Professor Marjo Kauppinen for stepping in as my advisor in the later stages of my research and for always keeping my best interests at heart. You are an extraordinary colleague that makes the work environment so inclusive and friendly.

To all my friends from everywhere — Arpine, Sasha, Shola, Ornela, Ashraf, Dimitar, Sumeet, Balnur and many others — I am thankful for all the great time we spent together that gave me the energy to complete this project. Thank you, guys, for making me smile when I needed it the most.

Next, I would like to thank my family: my parents Sandugash and Omirzhan thank you for always having my back when I had my lows and making me believe that I can do anything and
everything in life. A special thanks go to my little sisters: Gauhar, Ulzhan and Zhansaya, for your unconditional love and bringing out the best in me almost always.

Last but not least, my partner Niklas, thank you for the countless hours you spent reviewing my drafts, listening to my talks and for helping me understand and appreciate my own worth. You have been my biggest fan throughout this journey and I am so grateful for you in my life.

Espoo, April 10, 2020

Anar Bazarhanova
Contents

Acknowledgements ............................................................................. 1
List of Abbreviations and Symbols ................................................. 7
List of Publications ........................................................................... 8
Author’s Contribution ........................................................................ 9
1. Introduction ................................................................................. 11
2. Theoretical foundations ............................................................. 15
   2.1 Digital platforms and infrastructures ...................................... 15
   2.1.1 Platform ecosystem and governance ................................ 17
   2.1.2 Platform and infrastructure evolution ................................ 19
   2.2 Identity management (IdM) infrastructures ............................ 20
   2.2.1 Literature on IdM ............................................................ 21
   2.2.2 Provision of IdM infrastructures ....................................... 22
   2.2.3 Integration of IdM infrastructures ..................................... 24
   2.3 Summary ............................................................................... 25
3. Case description ............................................................................. 27
4. Research problem and methodology ........................................... 31
   4.1 Scope of research and research problem ................................. 31
   4.2 The research questions .......................................................... 33
   4.3 Paradigms of qualitative research .......................................... 34
   4.4 Selection of research methods ................................................ 35
   4.5 Research process ..................................................................... 37
   4.5.1 Data collection .................................................................. 38
   4.5.2 Data analysis ..................................................................... 42
   4.5.3 Reporting .......................................................................... 42
   4.6 Summary ............................................................................... 42
5. Results .......................................................................................... 45
   5.1 Publication I: How do Practitioners Understand External Platforms and Services? A Grounded Theory Investigation .. 45
5.1.1 Research objectives .............................................................. 45
5.1.2 Results ................................................................................. 45
5.1.3 Relation to the whole ........................................................... 46

5.2 Publication II: Love and Hate Relationships in a Platform Ecosystem: A case of Finnish Electronic Identity Management 49
5.2.1 Research objectives .............................................................. 49
5.2.2 Results ................................................................................. 49
5.2.3 Relation to the whole ........................................................... 50

5.3 Publication III: From platform dominance to weakened ownership: How external regulation changed Finnish eID... 51
5.3.1 Research objectives .............................................................. 51
5.3.2 Results ................................................................................. 51
5.3.3 Relation to the whole ........................................................... 52

5.4 Publication IV: Explaining an eID Framework Implementation using Dialectics .............................................................. 53
5.4.1 Research objectives .............................................................. 53
5.4.2 Results ................................................................................. 53
5.4.3 Relation to the whole ........................................................... 54

5.5 Publication V: Blockchain-Based Electronic Identification: A Cross-Country Comparison of Six Design Choices 55
5.5.1 Research objectives .............................................................. 55
5.5.2 Results ................................................................................. 55
5.5.3 Relation to the whole ........................................................... 56

5.6 Publication VI: The Review of Non-Technical Assumptions in Digital Identity Architectures ................................................ 58
5.6.1 Research objectives .............................................................. 58
5.6.2 Results ................................................................................. 58
5.6.3 Relation to the whole ........................................................... 59
5.7 Summary of results ................................................................. 60

6. Discussion and implications .............................................. 61
6.1 The dependence upon a dominant digital infrastructure ...... 62
6.2 The infrastructure transformation: Case of IdM in Finland... 64
6.3 The governance of dominant IdM infrastructures ............... 65
6.4 The architecturally significant components of IdM ......... 66
6.5 Implications for practice .......................................................... 68

7. Conclusions .............................................................................. 71
7.1 Summary of contributions ....................................................... 71
7.2 Validity and limitations ............................................................. 72
7.3 Future research ................................................................. 74

References .............................................................................. 76

Appendix A: Publications ..................................................... 85
# List of Abbreviations and Symbols

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IdM</td>
<td>Identity management</td>
</tr>
<tr>
<td>eID</td>
<td>Electronic identification</td>
</tr>
<tr>
<td>IS</td>
<td>Information Systems</td>
</tr>
<tr>
<td>IdP</td>
<td>Identity provider</td>
</tr>
<tr>
<td>SB</td>
<td>Service broker</td>
</tr>
<tr>
<td>SP</td>
<td>Service provider</td>
</tr>
<tr>
<td>RP</td>
<td>Relying party</td>
</tr>
<tr>
<td>IAM</td>
<td>Identity &amp; access management</td>
</tr>
<tr>
<td>eIDAS</td>
<td>Electronic identification, authentication and trust services</td>
</tr>
<tr>
<td>FTN</td>
<td>Finnish Trust Network</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>KYC</td>
<td>Know your customer</td>
</tr>
<tr>
<td>PKI</td>
<td>Public key infrastructure</td>
</tr>
<tr>
<td>SAML</td>
<td>Security assertion markup language</td>
</tr>
<tr>
<td>SSO</td>
<td>Single-sign-on</td>
</tr>
</tbody>
</table>
List of Publications

This doctoral dissertation consists of a summary and of the following publications. The rights have been granted by the publishers to include the papers in the thesis.


In this thesis, these publications are referred to as Publication I, Publication II, Publication III, Publication IV, Publication V, and Publication VI.
Author’s Contribution

**Publication I:** How do Practitioners Understand External Platforms and Services? A Grounded Theory Investigation.

The candidate participated in the planning and execution of the data collection, data analysis and reporting as the main responsible contributor. The empirical research was based on semi-structured interviews, which were conducted together with Yli-Huumo. Smolander and Yli-Huumo contributed to all sections of the article, reviewed and provided feedback throughout the writing process.

**Publication II:** Love and Hate Relationships in a Platform Ecosystem: A case of Finnish Electronic Identity Management.

The candidate participated in the planning and execution of the data collection, data analysis and reporting as the main responsible contributor. The empirical research was based on semi-structured interviews, which were conducted together with Yli-Huumo. Smolander and Yli-Huumo contributed to all sections of the article, reviewed and provided feedback throughout the writing process.

**Publication III:** From platform dominance to weakened ownership: how external regulation changed Finnish e-identification.

The candidate participated in the planning and execution of the data collection, data analysis and reporting as the main responsible contributor. The empirical part of this article was based on the data in Publication II and additional interviews. Smolander and Yli-Huumo contributed to all sections of the article, reviewed and provided feedback throughout the writing process.

**Publication IV:** Explaining an E-Identification Framework Implementation using Dialectics.

The candidate participated in the planning and execution of the data collection, analysis and reporting as the main responsible contributor. The research was conducted with semi-structured interviews, for which the candidate designed, organized, carried-out, transcribed and analyzed all the interviews. Lähteenmäki helped in finding the contacts for interviews and provided comments throughout the writing process. Smolander contributed to all sections of the article, reviewed and provided feedback throughout the writing process.

**Publication V:** Blockchain-Based Electronic Identification: Cross-Country Comparison of Six Design Choices
The candidate participated in the planning and execution of the data collection, data analysis and reporting as the main responsible contributor. The empirical research was conducted with semi-structured interviews and secondary data collection, for which the candidate designed, organized, carried-out, transcribed and analyzed the interviews. Chou & Nilsson participated in the data collection sessions and provided comments throughout the writing process. Magnusson & Lindman contributed to all sections of the article, principally theoretical framing and contribution parts, reviewed and provided feedback throughout the writing process.

**Publication VI: The Review of Non-Technical Assumptions in Digital Identity Architectures.**

The candidate participated in the planning and execution of the data collection, data analysis and reporting as the main responsible contributor. The empirical research was based on secondary data for which Bazarhanova designed, organized and analyzed the data of the systematic literature review. Smolander contributed to all sections of the article reviewed and provided feedback throughout the writing process.
1. Introduction

The integration of enterprise information systems is a complex and difficult problem as there can be hundreds of information systems in one large organization (Gericke et al., 2010; Kähkönen, 2017). Enterprise applications and systems no longer exist as stand-alone entities, but instead, they interact with other information systems inside and outside the company boundaries (Linthicum, 2000). As there is no single system or solution to solve all the integration problems in an organization, the integration also is an expensive problem. It has been estimated that companies can spend over 35% of their IT budgets to manage and develop the interfaces of enterprise applications (Gericke et al., 2010). Integrating systems within the company and utilizing external services and products has become a common necessity to satisfy customers in modern collaborative business environments.

The success of many businesses is dependent on their ability to leverage innovations coming from the outside, which are often global, remote and dynamic. Google’s Android, Apple’s iOS, and Tencent’s WeChat social networking sites serve as examples of contemporary industry platforms. Platform strategies have become increasingly important for how organizations innovate, develop their digital infrastructure and interact with networks of heterogeneous organizations. Therefore, studies on platforms have received increasing attention in the information systems (IS) literature (de Reuver et al., 2017; Eaton et al., 2015; Rolland et al., 2018; Selander et al., 2013; Tiwana et al., 2010; Yoo et al., 2012).

The challenge attributed to industry platforms is that when they become dominant, integration with them is critical to the thriving of smaller (non-focal) organizations. A recent article from WSJ is a good case in point: it reports on Amazon’s potential tweaking of their search result ranking algorithm that supposedly features listings that are more profitable for the company (Mattioli, 2019). This puts smaller retailers in a difficult position as they compete with the larger producers.

Although the research focusing on the dependence on dominant digital platforms is scarce (for an exception see (Rolland et al., 2018)), its importance cannot be overestimated. When the integration with a platform is done to extend enterprise capabilities, the platform becomes part of the user-enterprise’s infrastructure. The implications of dependencies upon such dominant industry platforms and infrastructures — in the light of the complex, recursive relations between platform and infrastructure definitions — is not yet well understood. In today’s highly competitive, fast-paced business environment, non-focal organizations struggle to make the right decisions when choosing the platforms to integrate with. Furthermore, platforms can grow to a significant scale that can sometimes lead to the abuse of their leadership position and sudden changes of rules in their use. An example of a public API program shutdown at Netflix demonstrates the high volatility of platform offerings1. Moreover, the dynamic phenomenon of

1 https://techcrunch.com/2014/06/13/netflix-api-shutdown/
change and evolution in digital platforms and infrastructures is essential in understanding the platform strategy implications over time and how platforms evolve and react to their environmental or internal disruptions.

This thesis studies the case of a digital identity management (IdM) platform as the example of a dominant digital infrastructure. IdM is a crucial component in any software-based service that needs to identify, authenticate and authorize the access of its users and it is an important step towards the successful advancement of digital services in a society. A shift to digital government is also dependent on well-established digital infrastructures, where electronic identification (eID) solutions have evolved as one of the cornerstones of the above-mentioned infrastructures. Offering the functionality of scalable identification, these solutions provide several functions including fraud prevention, implementation of customer due-diligence processes, generation of electronic signatures etc., and these facilitate the continued digitalization of society as a whole (Agbede, 2018; Husz, 2018).

However, IdM architectures have often been investigated from isolated perspectives, for example, from the view of technical interoperability, usability, the political aspects etc., but not much from a broad integration perspective. The problem of a global and universally trusted digital identity system, or more specifically, the lack of it, is a well-known problem. The literature on IdM systems shows a variety of approaches ranging from cryptographic protocols to various architectural designs and functioning, yet, disconnected infrastructures. While the ultimate goal may be to achieve a global Internet-based and user-centric digital identity solution, having one unique solution architecture dominating the global market is highly unlikely. This means that there will be a need for inter-domain integrations. The uptake of an IdM system is dependent on many factors: the solution should be technically sound, scalable, economically viable, convenient for humans-users and should recognize organizational integration aspects. These inter-organizational aspects range from infrastructural, system-level integrations, to higher-level strategic, business, liability and trust aspects. Thus, the challenge of building a large-scale digital identity system is an integration problem that requires more attention focused on business, legal, technical, operational and human linkages of its components.

The Nordic countries hold the position of being the most advanced digital economies in Europe (European Commission, 2018). Well-established eID infrastructures are justifiably regarded as one of the main contributors to this success. A special type of market procured IdM infrastructure is widespread in the region, which is provided by a private sector, mainly through banks and large telecommunication providers. This thesis studied the reliance on a dominant eID infrastructure provided by the banks (BankID) in the case of a national IdM platform in Finland. The Finnish BankID ecosystem has a 30-year history and is a closed proprietary service platform. It is the dominant eID method with more than 90% market coverage in Finland. In an effort to break the near-monopoly of the banks as identity providers and to comply with the EU and local regulations, the government created a framework for IdM which has led to ecosystem level platform change. As a result, the transformation of the Finnish IdM provides a unique case of a forced platform ecosystem shakeout.

The main objective of this thesis is to identify the factors that affect changes in dominant digital infrastructures. The question is examined through the case of IdM infrastructure in Finland. The research focuses on the dynamics of the IdM infrastructure from organizational, business and technology perspectives, with the aim to theoretically explain the dependence on external platforms and infrastructures and to derive theory-advised instructions for managing
IdM infrastructures using the example of a dominant digital infrastructure. A broad theoretical approach adopted in this dissertation is the conceptualization of infrastructural change in terms of the installed base, governance and architectural factors. Installed base is referred to as the existing “set of ICT capabilities and their users, operations and design communities” together with existing institutional and organizational components (Aanestad et al., 2017; Hanseth & Lyytinen, 2010).

The main objective was divided into four research questions. First, the study explores the conceptualization of the problem by answering the question (1) what are the characteristics of dependency on a dominant digital infrastructure? Second, the study gives a comprehensive account of the evolutionary dynamics of a dominant infrastructure by answering the question (2) how are dominant digital infrastructures transformed? Next, the study concentrates on extracting the governance lessons from the Finnish IdM case as a response to the question (3) what are the important factors in the governance of dominant IdM infrastructures? Lastly, the study proposes the overview of important components when managing the development of IdM infrastructures and answers the question (4) what are the architecturally significant aspects in the development of IdM infrastructures?

To address these research objectives, case studies and grounded theory approaches have been chosen as research methods using interviews with practitioners and secondary data. The results of this thesis are of broad relevance to software architects, business professionals and policy makers. The findings provide the guidelines for managing the development of large-scale IdM infrastructures and increase the understanding of the role of dominant infrastructures that becomes obsolete.

This thesis comprises two main parts, a summary and an appendix. The summary consists of seven chapters. Chapter two introduces the background literature and presents important concept definitions and theoretical perspectives. Chapter three describes the case of IdM development in Finland along with a short historical overview. Chapter four formulates the research problem, describes the research process and defines the research questions and research methodology. Chapter five presents the findings of the scientific publications included in this thesis. Chapter six discusses the contributions and implications for research and practice. Chapter seven summarizes the contributions, points out the limitations, outlines possible future research topics and concludes the thesis. The appendix comprises six publications.
2. Theoretical foundations

This chapter introduces the context of the thesis and presents the important concepts and definitions that form the background of this thesis. The thesis belongs to the information systems scientific field that “addresses the range of strategic, managerial, and operational activities involved in the gathering, processing, storing, distributing, and use of information and its associated technologies in society and organizations” (Avison & Elliot, 2006). The study of information systems is an interdisciplinary area of science which spans many disciplines, but at its core it bridges business (social sciences) and computer science (natural science).

In this chapter, we first we outline the key concepts from the literature on digital platforms and infrastructures. Next, we introduce the foundations of identity management research. The link between these two domains is the conceptualization of the change in digital platforms and infrastructures that is investigated within the identity management domain. A broad theoretical approach adopted in this dissertation is the conceptualization of infrastructural change (evolution) in terms of an installed base, governance and architectural factors.

2.1 Digital platforms and infrastructures

The rich tradition of research on platforms and infrastructures originates from multiple disciplines, including information systems, strategic management, and economics. Prior studies from these communities provide separately developed conceptualizations on platforms due to the roots from different research traditions.

While some research streams embrace a technological view of digital platforms, see for example the definition by Ghazawneh and Henfridsson (2015), as “the extensible codebase of a software-based system”, the literature from the economic perspective refers to platforms as two-sided markets, or multi-sided platforms (Rochet & Tirole, 2003). As defined by Armstrong (2006), two-sided markets involve two groups of agents interacting via the platform, where the benefit gained by one group from joining a platform depends on the size of the other group joining the platform. The focus from the engineering perspective is on the platform itself, and the economic perspective is concerned more with business models, strategies and value creation (de Reuver et al., 2017). Further, Gawer (2014) bridges the two dominating perspectives and outlines a third perspective on platforms — termed organizational — as “evolving organizations or meta-organizations” (Gawer, 2014; Rolland et al., 2018). Table 1 summarizes three perspectives on digital platforms from the literature and their corresponding definitions.

This thesis follows the call for adopting a more integrative perspective in research (de Reuver et al., 2017), and a socio-technical view on digital platforms is taken, which is defined as “a
sociotechnical assemblage encompassing the technical elements (of software and hardware) and associated organizational processes and standards” (de Reuver et al., 2017; Tilson et al., 2012).

Table 1. Digital platforms in IS research from (Rolland et al., 2018)

<table>
<thead>
<tr>
<th>Perspective</th>
<th>Definition</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Engineering: as technical artifacts</td>
<td>Digital platforms are software based external platforms consisting of the extensible codebase of a software-based system that provides core functionality shared by the modules that interoperate with it and the interfaces through which they interoperate.</td>
<td>(C. Y. Baldwin &amp; Woodard, 2009; Boudreau, 2010; Ghazawneh &amp; Henfridsson, 2015; Tiwana et al., 2010; Yoo et al., 2010)</td>
</tr>
<tr>
<td>Economic: as markets</td>
<td>Digital platforms are the components used in common across a product family whose functionality can be extended by applications and is subject to network effects.</td>
<td>(Ceccagnoli et al., 2012; Eisenmann et al., 2006; Song et al., 2018; Tiwana, 2014)</td>
</tr>
<tr>
<td>Organizational: as innovation practices</td>
<td>Digital platforms are sets of assets organized into a common structure which acts as a foundation upon which other firms, loosely organized in an innovation ecosystem, can develop complementary products, technologies or services.</td>
<td>(Eaton et al., 2015; Gawer, 2014; Ghazawneh &amp; Henfridsson, 2013) (Gawer &amp; Cusumano, 2014)</td>
</tr>
</tbody>
</table>

Research on digital platforms often comes with the larger and more multifaceted concept of digital infrastructures (Table 2). In line with Constantides et al. (2018), this thesis discusses platforms in tandem with infrastructures — one of the emerging themes in the IS field. Digital infrastructures are shared, open, unbounded and evolving socio-technical systems that consist of a set of IT capabilities and their users, operations and design communities (Hanseth & Lyytinen, 2010). In this thesis, digital infrastructures are also referred to as “heterogeneous collection of sociotechnical components that are essential or contribute to the functioning of a system, organization or industry” (Henfridsson & Bygstad, 2013; Tilson et al., 2010).

Table 2. Digital platforms infrastructure definitions

<table>
<thead>
<tr>
<th>Concept</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digital platform (sociotechnical view)</td>
<td>Technical elements (of software and hardware) and associated organizational processes and standards (Tilson et al., 2012).</td>
</tr>
<tr>
<td>Digital infrastructure</td>
<td>The computing and network resources that allow multiple stakeholders to orchestrate their service and content needs (Constantinides et al., 2018).</td>
</tr>
</tbody>
</table>

The concept of digital infrastructures has proven to be instrumental to the IS field, as it helps to change the perspective and unit of analyses from single organizations to organizational networks and from systems to infrastructures, “allowing for a global and emergent perspective on IS” (Bygstad, 2008), as the perspectives can also be adjusted to different contexts: enterprise, industry, economy, national, regional, and global levels (Tilson et al. 2010). One of the central works defining the relation between platforms and infrastructures, is the work by Hanseth & Lyytinen (2010) that notes that the differences between these two models lie in their overall increasing complexity, in how they relate to their design and use environments, and how they behave over time in relation to those environments. Digital infrastructures are “recursively composed of other infrastructures, platforms, applications and IT capabilities” (Hanseth & Lyytinen, 2010) and, hence, whether the artefact under study should be considered an industry platform or the infrastructure really depends on the context of its use and the perspective of the analysis.

One of the main premises of the information infrastructures literature — a parent notion of digital infrastructures — is the role existing practices, conventions, tools and systems, so-called installed base that impact the evolution of infrastructures (Øvrelid & Bygstad, 2019). Following the discussion of (Aanestad et al., 2017), the notion of an installed base can be seen more than a collection of specific elements but also as a sense-making tool that helps to answer the following questions: “when and how some element of an existing reality becomes significant
[in the evolution process], for whom, with what effects? In what way do the different elements become significant, are they working as triggers, as resources, as competitors, as alternatives?" (Aanestad et al., 2017). A central rationale for taking this perspective is acknowledging the path-dependency of infrastructural changes (Aanestad et al., 2017; Øvrelid & Bygstad, 2019).

2.1.1 Platform ecosystem and governance

When discussing the evolution of digital artifacts, such as platforms and infrastructures, it is important to describe various roles involved in the ecosystem — a digital platform together with the larger number of organizations around it (Table 3). Such systems in which various actors and artifacts are organized around a central digital platform can be considered as a more captivating object of inquiry than the platforms alone in isolation.

A platform orchestrator (platform owner) dominates and exercises control over the innovation network of its ecosystem (Rochet & Tirole, 2003). Orchestrators define software interfaces and rules of use (boundary resources) allowing complementors to use the core platform functionality to build applications. Orchestrators regulate the flow of resources and knowledge within the network and subsequently define the types of innovations created in the ecosystem (Eck & Uebernickel, 2016). Recent studies on exercising power from the software engineering perspective on ecosystems recommend that orchestrators need to work on exerting the power-dependence relationships in a way to ensure not only their own success, but also the success of the entire ecosystem (Alves et al., 2017). Moreover, the notion of an ecosystem itself is sometimes referred to as a distinct form of governance which is different from other business arrangements such as markets, alliances or hierarchically managed supply chains (Jacobides et al., 2018). Coming from strategic management literature, scholars theorize that ecosystems consist of a set of distinct yet interdependent organizations that are coordinated without full hierarchical order or customized contractual agreements with each other (Jacobides et al., 2018).

In the scope of this thesis, the focus is on an industry platform, as opposed to product platforms, following Gawer & Cusumano’s (2014) differentiation of internal or company-specific platforms and external or industry-wide platforms. Internal (product) platforms are a set of assets organized in a common structure from which a company can efficiently develop and produce a stream of derivative products (Gawer & Cusumano, 2014). Internal platforms are best understood in the context of new product development and incremental innovation around reusable components or technologies. External or industry platforms are sets of assets organized into a common structure that act as a foundation upon which external innovators can develop their own complementary products, technologies, or services.

Industry platforms have essential differences compared to product-platforms. First, there is the existence of complementors (or third-party developers), who are various firms that develop complementary products as platform capability extensions. Complementors together with the platform, create an ecosystem in which the participants are dependent on each other to some extent (Cusumano, 2010; Viljainen & Kauppinen, 2011). Second, industry platforms have relatively little value to users without complementary products or services (Cusumano, 2010). Such platforms are ubiquitous: the Microsoft Windows and Linux operating systems (OS); Intel and ARM microprocessors; Apple’s iPod, iPhone, and iPad iOS operating system, iTunes and AppStore; Google’s Internet search engine and Android OS; Facebook, LinkedIn, and Twitter; video-game consoles; and the Internet (Gawer & Cusumano, 2014).
Platform orchestrators employ various strategies that help them to coordinate the ecosystem players and contribute to a growth of the platform. Platform governance includes the decisions on procedures and processes by which an orchestrator controls, changes or maintains its current and future position in an ecosystem (Jansen & Cusumano, 2013). Platform governance also entails the establishment of ecosystem-wide mechanisms (Huber et al., 2017) and how these mechanisms influence the evolutionary dynamics of the ecosystem and modules in platform settings (Tiwana et al., 2010).

Platform openness refers to the extent to which platform boundary resources support complementors and has certain tradeoffs. By following a fully open strategy, the platform owners run into the risk of reducing their share of profits and control by lowering the entry barriers to complementors, but on the other hand, boosting the wide adoption of the platform (Boudreau, 2010). Increased adoption triggers positive feedback cycles, that in turn further increase the usefulness of the platform (de Reuver et al., 2017). Direct network externalities refer to when the value of the platform depends on the number of users in the same user group, e.g., social-media platforms (Katz & Shapiro, 1994). Indirect network externalities refer to the platform value increase depending on the number of users in different user groups, e.g., gaming platforms with content creators and players (Katz & Shapiro, 1994). An example case of when network externalities provide benefits to users and third-party developers is the popular messenger application WeChat (China’s App for everything) that operates as a platform for providers of payments, bookings management, transport and other services.

An increased interest in platform thinking has resulted in cumulative knowledge on platform ecosystems and their governance (Eisenmann et al., 2009; Huber et al., 2017; Tiwana, 2014). The focus of recent research has been on investigating how big tech organizations such as Google (Karhu et al., 2014), Amazon (Venkatraman et al., 2014) and Apple (Eaton et al., 2015) orchestrate their ecosystems. Consequently, there are fewer attempts in the literature to investigate companies that are not dominant players (Ghazawneh & Henfridsson, 2013; Huang et al., 2009; Lindgren et al., 2015) but that need to integrate with various infrastructures and platforms, not to develop platform capability extensions, but to sustain or extend their own business capabilities (Selander et al., 2013). These non-focal firms, from the viewpoint of platforms, are platform-utilizing organizations that wish to extend their own capabilities by combining resources from external platforms (Selander et al., 2013). Such resources can be data, unique competences (knowledge), services (methods and algorithms) or people (customer base) that are valuable, rare, inimitable and non-substitutable (Barney, 1991). The need for such integrations may happen when the number of reasonable platform choices in the

<table>
<thead>
<tr>
<th>Concept</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software ecosystem (organizational view)</td>
<td>A collection of firms that are interlinked by a reciprocal interest in the prosperity of a digital platform for materializing their own product or service.</td>
</tr>
<tr>
<td>Software ecosystem (technical view)</td>
<td>A collection of complements (apps) to the core technical platform, mostly supplied by third party developers.</td>
</tr>
<tr>
<td>Boundary resources</td>
<td>Software tools and regulations facilitating arms’ length relationships between the involved parties.</td>
</tr>
<tr>
<td>Platform openness</td>
<td>The extent to which platform boundary resources support complementors.</td>
</tr>
<tr>
<td>Direct network externalities</td>
<td>The value of the platform depends on the number of users in the same user group.</td>
</tr>
<tr>
<td>Indirect network externalities</td>
<td>The value of the platform depends on the number of users in a different user group.</td>
</tr>
<tr>
<td>Platform orchestrators</td>
<td>The platform owner that dominated and exercises control over the innovation network of its ecosystem.</td>
</tr>
<tr>
<td>Third-party developers</td>
<td>Various firms that develop complementary products as platform capability extensions.</td>
</tr>
<tr>
<td>Non-focal firms</td>
<td>Platform-utilizing organizations that wish to extend their own capabilities by combining resources from external platforms.</td>
</tr>
</tbody>
</table>

Table 3. Definitions of core concepts related to digital platform ecosystems adapted from (de Reuver et al., 2017)
market falls to one or only a few. In such cases the only reasonable choice become the de facto standard, which is also known as a dominant design (C. Baldwin & Clark, 2000).

One of few the studies that addresses the issue is the research by Rolland et al. (2018) who investigate the problem of the management of external industry platforms as part of a user organization’s (non-focal) digital infrastructure and work processes. The authors found that organizations are increasingly adopting external digital platforms, “such as Google’s G Suite and Microsoft’s SharePoint, as central components of their digital infrastructures to support work processes and innovation efforts” (Rolland et al., 2018). As a result, a certain capability provided by an external platform becomes a critical part of the organization’s infrastructure. The relationships between non-focal businesses and platform orchestrators are asymmetric (Pfeffer & Salancik, 2003), and non-focals are forced to continuously accommodate quick adjustments to changes introduced by platform owners (Altman, 2016). Various forms of dependencies and long-term consequences arising from integrations with platforms are not always fully anticipated. The governance implications of such ecosystems are not well understood from the orchestrators’ perspective, nor from the perspective of non-focal organizations.

2.1.2 Platform and infrastructure evolution

An interesting outlook on the relation between platforms and infrastructures is proposed by (Kazan et al., 2018), where the authors theorize that platforms within network economies vary in their modularity and consist of two strategic architectural dimensions: (1) value creation, and (2) value delivery. Starting from the assumption that digital platforms are created and cultivated on top of digital infrastructures (Constantinides et al., 2018), the authors theorize that digital platforms compete through architectural configurations. Value creation architectures, as defined by Kazan et al. (2018), are modular components of digital platforms that can be exploited by third parties to develop value-added derivatives. Thus, platforms practice modularity in their value creation architectures (i.e., at the platform level), where they compete within value networks by offering the best resource configuration, i.e., a stable core and flexible derivatives. Similarly, platforms also practice modularity in value delivery architectures (i.e., at the infrastructure level) to deliver derivatives in a standardized format (Kazan et al., 2018). This second strategic dimension refers to the efficient diffusion of derivatives across their value network, where platforms rely on access to technological backbones in the form of digital infrastructures (e.g., the Internet).

These strategic dimensions are important conceptualizations, as they guide the discussion in unfolding the complex relationship between digital platforms and infrastructures. The layered architectures perspective is built on the notion that infrastructures fuel the platforms while also acknowledging the existence of a recursive relation between them. Furthermore, for the purpose of analysis, it is possible to consider a platform ecosystem as a form of organizational structure, with change comprising an inherent part of organizational structures. Describing and explaining the scope, drivers and dynamics of the change processes is challenging as the change processes include entities that, although they change somewhat as a result of their interactions, remain largely stable and analytically distinct from each other as well as from the processes in which they are embedded (Langley & Tsoukas, 2016).

Platforms and infrastructures are volatile and sensitive to changes in technology, regulation, and customer preferences. The evolution capacity of a system is a result of its generativity, defined as “a capacity to produce unanticipated change through unfiltered contributions from
broad and varied audiences” (Zittrain, 2008). There exist two outlooks in the IS literature on
the generativity concept: generative capacity due to artifact (i.e., platform or infrastructure)
characteristics or due to artifact evolution (Eck & Uebernickel, 2016). This thesis draws
attention to the second perspective — evolutional generativity, which emphasizes the
interactions between individual ecosystem entities (Eck & Uebernickel, 2016).

As the platforms literature has focused mostly on guiding firms to become platforms (Gawer
& Cusumano, 2008; Leijon et al., 2017) and organizational decisions to adopt platform
strategies (Ghanam et al., 2012), so-called “platformization” has become a popular topic
leading many firms to tap into this model of value creation (de Reuver et al., 2017). Platform
evolution is not a new research direction and is in line with the call for research on the
“neglected problem” of how platform owners’ choices and the exogenous environment
influences the evolutionary dynamics of an ecosystem (Tiwana et al., 2010). Similarly, when
studying infrastructural evolution, it is advised to bear in mind the inherent characteristics of
infrastructures as a sociotechnical artifacts and to view them as perspectives of paradox of
control (i.e., opposing logics around centralized and distributed control) and paradox of
change (i.e., the need to enable stability of components but allow flexibility across layers)
(Tilson et al., 2010). Moreover, “infrastructures do not grow de novo” but always through the
change of an installed base, inheriting its strengths and weaknesses (Star & Ruhleder, 1996).
Under the contextual conditions that infrastructures identified with decentralized control and
loosely-coupled architectures, Henfridsson & Bygstad (2013) identify the generative
mechanisms of digital infrastructures (innovation, adoption and scaling) that lead to successful
(or not) evolution outcomes.

Our empirical case is an extreme example of an industry platform becoming almost a
monopoly, the Finnish BankID platform, which was unsuccessful in anticipating changes and
proactively adapting to them. Finnish BankID is a proprietary platform that many
organizations depended on as the primary industry– and country–wide dominant eID
infrastructure for organizations in both public and private sectors. This thesis demonstrates
how external drivers, in the form of regulations specified by the European Union (EU) and
Finland, led to changes in the platform and the ecosystem surrounding it, affecting the roles,
relations and power structures of incumbent ecosystem participants.

2.2 Identity management (IdM) infrastructures

The history of identification dates back to human prehistory when the physical details of a
person, display of decorative jewelry, tattoos and skin markings were used to distinguish
individuals or to determine their role in society². Since then, the evolution of identity
verification has come a long way and new methods of verification have been created that
eliminate common human error. Identification in the modern physical world is done using
national ID cards, passports, driving licenses etc. With an increasing number of services
provided online, digital identification plays an important role in societies.

A digital identity is defined as “a collection of electronically captured and stored identity
attributes that uniquely describe a person within a given context and is used for electronic
transactions” (Natarajan et al., 2018, p. 21). An electronic identification (eID) is the act of
making an entity known, a process representing unique attributes used for authentication and
authorization in an electronic public or private service context (Söderström 2016). The

² https://www.trulioo.com/blog/infographic-the-history-of-id-verification/
acronym “eID” is also used to refer to “electronic identifiers”. Söderström (2016) lists the following identity sub-concepts:

- **Identity** – a unique combination of attributes;
- **Identification** – a representation of attributes;
- **Authentication** – an assessment of attributes;
- **Authorization** – permission based on attributes;

Electronic (digital) identity management (IdM) system are attributes of systems and processes that manage the lifecycle of individual digital identities (Natarajan et al., 2018). IdM incorporates all four sub-concepts from the sub-concepts above (Söderström 2016). Additionally, an IdM infrastructure is a combination of technical systems (such as databases, IT infrastructure) and business systems, policies, and processes that are used to establish identities, govern, and synchronize the collection, utilization of identity information and to safeguard it (Stevens, 2018; The World Bank Group, 2017).

In Europe, eIDAS — the regulation on sets of standards for electronic identification and trust services for electronic transactions in the European Single Market (European Commission, 2014) — provides guidelines to be used for electronic authentication on the web. It defines the process that allow for the electronic identification of a natural or legal person across the EU member states. The eIDAS regulation defines 3 assurance levels (Table 4) on the basis of various level of assurance (LoA) criteria (European Commission, 2015).

In this thesis, the scope of eID solutions is confined to official systems for authentication of citizens within a national scope that are used both in private and public sectors and which refer to strong customer authentication (SCA) methods and ‘substantial’ and ‘high’ assurance levels. SCA is defined as an “authentication based on the use of two or more elements categorized as **knowledge** (something only the user knows), **possession** (something only the user possesses) and **inherence** (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data” (European Banking Authority, 2019).

<table>
<thead>
<tr>
<th>Assurance level</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Limited degree of confidence in the claimed or asserted identity of a person. The purpose is to <strong>reduce</strong> the risk of misuse or alteration of the identity.</td>
</tr>
<tr>
<td>Substantial</td>
<td>Substantial degree of confidence in the claimed or asserted identity of a person. The purpose is to <strong>decrease substantially</strong> the risk of misuse or alteration of the identity.</td>
</tr>
<tr>
<td>High</td>
<td>Higher degree of confidence in the claimed or asserted identity of a person. The purpose is to <strong>prevent</strong> misuse or alteration of the identity.</td>
</tr>
</tbody>
</table>

Furthermore, the main concern of this thesis is consumer IdM systems (Hardjono & Pentland, 2018) in contrast to enterprise IdM. Organizational needs and requirements in IdM are very different from requirements for a global, more permanent, digital identity system. Enterprise IdM entails a central administrator who manages the needs of an organization, which initiates and provisions users with credentials and privileges in a company environment. The lack of such a central authority makes the problem of a ubiquitous digital identity more challenging.

### 2.2.1 Literature on IdM

The concept of digital identity is complex and resides at the interplay between information systems, security, usability and human-computer interaction (Whitley et al., 2014). Scholars from different fields have investigated policy, technology and societal issues in a wide variety
Theoretical foundations

of ways. The vast majority of studies have analyzed public sector eIDs by laying out technological (Marsalek et al., 2017), organizational (Melin et al., 2016) and legal dimensions (Lentner & Parycek, 2016) as well as the emergence factors of national eID schemes (Söderström & Melin, 2012) and policy options for the regulation of electronic identity (Hoikkanen et al., 2010). As pointed out by scholars (Whitley et al., 2014), an absolute analytical separation of technological and societal issues of digital identity is proving to be increasingly unhelpful in studying contemporary practices.

The state-of-the-art on electronic identification (eID) architectures contains a plethora of insights into existing designs. Therefore, systematic literature reviews in the domain of IdM are very common: see, for example, a survey on authentication methods (Halunen et al., 2017), their classification, usability and drawbacks (Barkadehi et al., 2018), recommendation framework for authentication schemes (Velásquez et al., 2018), a review of authentication using behavioral biometrics (Stylios et al., 2016). Such reviews prevail, partly, because of the rapid pace of technological innovation in the domain, ever changing regulatory guidelines and the importance of identity management for the functioning of society. IdM reviews have also been performed in various contexts, e.g., on the Internet of Things (Pal et al., 2018), within the e-government services (Dubey et al., 2015), from privacy-specific perspectives (Khan & Mustafa, 2017) and in cloud environments (Indu et al., 2018).

In recent years, research on federated IdM architectures (linked eIDs across multiple IdM systems) have been widely investigated, these are federated identity management (FIM) in the cloud (Shere et al., 2017), FIM challenges (Jensen, 2012) and security issues of FIM in the cloud computing (Ghazizadeh et al., 2012). User-centric and self-sovereign identity are thought to be next phases of Internet identity development after FIM (Allen, 2016). Another recent trend in IdM is the application of blockchain methods (Dunphy & Petitcolas, 2018). Hence, publications have appeared in recent years conceptualizing essential components of self-sovereign identity (Muehle et al., 2018), user-centric identity built on blockchain (Augot et al., 2017) and counter arguments exposing some of widely-held misconceptions on blockchains as a new trust mechanism (Auinger & Riedl, 2018).

2.2.2 Provision of IdM infrastructures

There exist several outlooks on the supply and ownership of digital identity solutions; the infrastructures can be provided by organizations from public or private sectors, or be a joint venture (Berg et al., 2017). IdM implementations may vary considerably from simple password-based solutions, to the use of tokens such as smart-cards, one-time-passwords (OTPs) to smartphone-based and hybrid systems, and may include the involvement of various actors such as governmental officials, telecommunication providers, post offices and Internet providers.

**Governmental IdM implementations**

In many countries, the government is considered the natural electronic identity provider for the citizens (Suoranta et al., 2015). In a study about India’s Aadhar system, which is the world’s largest biometric identity platform, the role of platform ecosystem theory is explored in scalable e-government services delivery (Mukhopadhyay et al., 2019). The Indian government encouraged a network of heterogeneous private organizations to use the capabilities of the platform and develop the innovative services because the platform owners’ goal in this case was not to extract maximum revenue, but rather to increase wider societal benefits. It is also
possible that when governments establish identity infrastructures in order to optimize processes and enable the digitalization of services, market participants may be seen to free-ride off the government-provided identity technologies (Berg et al., 2017).

Among the research on success factors for the introduction of national eIDs is the work by McGrath (2016). Through a comparative case study of identity verification in Nigeria and other more successful cases in Bangladesh and the UAE, the authors tackle the question as to why some countries achieve the desired development outcomes from the provision of identity verification services while others do not (McGrath, 2016). Distrust in the government’s motives around the issues of security and privacy was found to be one of the main reasons affecting trust, which is in line with the findings by (Seltsikas & O’keefe, 2010). On the other hand, the Estonian case is a prime example of a governmental success in the provision of successful IdM, with a state-issued smartcard-based solution. According to a study about a recent and major incident in Estonia due to eID card encryption vulnerability, well-maintained public-private sector partnership relations were reported to be one of the key crisis-management factors (Lips et al., 2018). These examples are in line with the results of the OECD report from 2010, in which it was found that the national IdM strategies generally adopt an evolutionary approach based on existing offline identity regulations and practices (OECD, 2011). In other words, IdM strategies are country-specific and there is no generic ‘one-fits-all’ solution (Kubicek & Noack, 2010).

Nowadays, the goal of governments has shifted towards enabling cross-domain (cross-border) and interoperable eID schemes. Aligned with regulatory developments, there have been numerous EU projects on integrating national IdM infrastructures. For example, eSENS — towards stronger data security in an IdM (Berbecaru et al., 2017), ABC4Trust project — attribute-based credentials (Rannenberg et al., 2015), CREDENTIAL project — digital identity wallet (Kostopoulos et al., 2017), are among many initiatives with the goal of enabling cross-border recognition of electronic IDs, personal data exchange and to allow citizens and business to share their identity data when necessary.

Non-governmental IdM implementations
Alternatively, identity infrastructures could be provided by private actors and consequently used by other market participants and public sector organizations. An example of identity solutions that meet the requirements of SCA provided by non-governmental organizations could include 3D Secure methods offered by payment-card associations such as Mastercard and Visa. However, these identity solutions are not traditionally utilized in national contexts, i.e., public services. Due to the presence of complex public-private relationship between actors, particular attention has been paid to examining market-procured eID solutions (Medaglia et al., 2017a, 2017b). For example, the SwissID digital identity solution is a joint venture between the most influential public and private organizations in Switzerland (SwissID, 2017), which is also the second attempt after a previously unsuccessful attempt (SuisseID) to launch a nationwide electronic IdM (Mettler & Gündüz, 2019). In the Nordics, the same bank-specific identifiers that the customer uses in the bank’s own services have been reused for national services as well. Studies about Danish (Hoff & Hoff, 2010), Norwegian (Murphy, 2014) Swedish (Grönlund, 2010; Söderström, 2016) and Finnish (Rissanen, 2010) IdM infrastructures provide examples of developed economies and the presence of high trust in societies (Medaglia et al., 2017a). The societies in these countries have adopted the use of bank identifiers (or some hybrid form of it) as a form of electronic identification for a wide variety
of private and public services that vary from payment applications, tax declaration to making appointments for social and health services.

2.2.3 Integration of IdM infrastructures

At a meta-level, IdM ecosystem consists of three roles: identity providers (IdPs), human-users, relying parties (RPs) or service providers (SPs), where each actor has their own set of requirements. The RP needs a certain level of assurance to provide the service, the human-users want to be in control of their personal data, and the IdP requires certain diligence in the process of handling the data (Schwartz & Machulak, 2018).

The classification of IdM systems has long adhered to paradigms and models conceptualized in (Cao & Yang, 2010). Paradigms refer to the implementation and deployment of the system and can be network-, service- or user-centric. Models refer to where identity data is stored and delimits the responsibility of each party. This includes isolated, centralized and federated models (Carretero et al., 2018). More detailed conceptualization on the paradigms and models can be found in (Cao & Yang, 2010).

The research on user-centric designs has attracted much attention from researchers and practitioners, though many proprietary solutions are based on service-centric paradigms (e.g., services from Google, Facebook etc.). However only limited federation of identity data is possible with platforms such as Google (i.e., Single Sign-On (SSO), and there is limited user control on what data is shared. Existing and functioning networks of identity systems (in research, education, companies, countries, etc.) cannot be easily modified (Carretero et al., 2018). Thus, the digital identity landscape consists of numerous non-integrated silos of infrastructures and the real challenge is to “connect” them and allow the inter-federation of trust.

Existing inter-federation architectures, i.e., approaches that enable multi-party federations, can be grouped into three types: a hierarchical root of trust, a mesh-based federation and a proxy-based design (Schwartz & Machulak, 2018). The root of trust design enables hierarchical services, with the most common examples such as Eduroam which provides international network access for users in research and higher education (Eduroam – World Wide Education Roaming for Research & Education, n.d.) and Domain Name Service (DNS) (Mockapetris & Dunlap, 1988) often criticized for its centralization drawbacks. The second model is a metadata aggregate publication (mesh-based federation), in which the federation participants do not need to negotiate agreements with each other individually but agree on a standard contract. An example of a mesh-based federation is InCommon, which is a federation of U.S. higher education institutions, that currently has approximately 10 million users and 760 educational institutions. InCommon also has an inter-federation agreement with eduGAIN, the EU higher education federation (Schwartz & Machulak, 2018). The third model, the proxy federation service, is beneficial to RPs and IdPs because it requires only one point of integration, but, on the other hand, implies a high dependence on the proxy. OpenConext — an open source identity federation and educational collaboration platform in the Netherlands — is an example of a central proxy-based model implementation of, also referred to as the “hub & spoke model”.

In order to build a large-scale inter-federation using any of the ecosystem designs above, it would take considerable effort to define legal agreements, federation policies on governance, as well as agreements on protocols, data structures and vocabularies. Regardless of the multiparty federation design, the goal is to facilitate and encourage integration. The challenge
of building a global digital identity system, thus, is an interconnection problem that requires more attention to be focused on the business, legal, technical, operational and human integration of its components.

2.3 Summary

This chapter presented the theoretical foundations of the literature on digital platforms and infrastructures. The problem of the management of dominant external industry platforms as part of a user organization’s (non-focal) digital infrastructure has been identified as a research gap. Overall this thesis is concerned with digital infrastructure evolution, and it is seeking to explain this change process in terms of governance, architectural and installed base factors of IdM infrastructure. The research problem of the evolution of digital infrastructures was exemplified in a case of a nation-wide national IdM platform. The platform change perspective serves as an analytical lens for studying the dynamic phenomenon of the IdM evolution. This thesis is confined to large-scale consumer IdM systems that are used as official systems for authentication of citizens on a national scale and that are used both in private and public sectors. Such a market-procured approach involves a number of challenges, namely market dynamics, technological changes, as well as the regulation and political interests that influence the power relationship between the government and private organizations when negotiating a common approach to the governance of an eID infrastructure. Therefore, the nation-wide IdM infrastructure provided by financial organizations is an ideal case to study the evolutionary dynamics of the ecosystem.
3. Case description

This chapter describes the main case studied in this thesis. The story described in this chapter was studied during the period from October 2016 until October 2019. BankID is a proprietary platform and is the dominant industry- and country-wide infrastructure for organizations from public and private sectors in Finland.

Existing strong customer authentication (SCA) methods in Finland include online banking identifiers (BankID), mobile certificates from telecom operators (MobileID) and state-issued certificate cards from the Population Register Centre (FineID), the shares of which in public services transactions were 96%, around 3% and less than 1% percent respectively in 2017. Identification method providers (IdP), bank and telecommunications companies, provide both public and private sectors with SCA solutions, such as bank identifiers or mobile certificates. MobileID is a PKI-based (public key infrastructure) authentication method developed by Finnish telecommunication operators in 2011. In contrast to the Finnish BankID, MobileID represents full collaboration between telecom operators in Finland and allows cross-carrier identification. It requires a specialized SIM card with an embedded certificate and a contract with the mobile operator. MobileID can be used to access all public e-services, as well as many private services. The main barrier to a wider MobileID take-up was the classical “chicken-egg” problem between service providers and users (Murphy, 2012). Drawbacks slowing down MobileID expansion included a monthly fee and onboarding practices: customers needed to visit a telecom office for the first-time identification.

The Tupas protocol — the name of a protocol and a household name for the Finnish BankID platform — was jointly specified by the Federation of Finnish Financial services (FFI), a consortium of Finnish banks, more than 30 years ago, as illustrated in Figure 1. A group of large banks decided to standardize the electronic authentication service, whereby service providers could identify customers through a bank-specific identification method that the customers would use within the bank’s internal services. The method quickly became popular among other e-service providers, allowing the banks to generate additional revenue streams by opening the eID service to other participants. Tupas is the protocol that is used to establish citizen authentication and identity and the protocol is accepted as a standard by Finnish banks. It is based on a combination of username, password and one-time codes that can be generated by a token generator, mobile app or printed on paper. The official name of the service is the “Tupas identification service”. In this thesis, we distinguish between these terms by using “Finnish BankID platform” as the more generic service name for the Tupas enabled eID method.

It is important to emphasize that the banks have agreed to common standards but not to a shared infrastructure. Each bank has been running their own authentication solution independently since the beginning and there are no cross-bank eIDs and no single eID
platform, but instead each bank has their own eID platform enabled by Tupas. Nevertheless, from the perspective of eID utilizing organizations and users, the service “looks and acts” like an external platform (with multiple owners of various platform components). Therefore, for the sake of simplicity, we view the Finnish BankID platform as a single platform jointly owned by separate banks.

Figure 1. Timeline depicting the evolution of the Finnish eID ecosystem.

Although the state introduced non-mandatory FINEID cards in 1999 to replace the older citizen ID card with a machine-readable smartcard chip, citizens did not take the technology into use. In retrospect, experts attribute the failure of FINEID to high upfront costs of card-reader devices, the learning effort involved in learning to install and use the certificate, user experience (UX) issues, and a historically well-disseminated BankID (IDABC, 2009). It was shortly debated whether FINEID card readers should be distributed free of charge to citizens, as had been done in neighboring Estonia. However, the government decided not to promote FINEID in such a way (IDABC, 2009). This view was clearly expressed in the Act on the Openness of Government activities, which stated that the governmental policy “does not include any exceptions favoring eID solutions. Any favoritism towards one solution is deemed contradictory to higher principles of openness of public services”. To support their stance, the government gave equal legal acknowledgment to the Finnish BankID in 2003 for accessing e-government services, which boosted the overall e-service usage throughout the country but made the FINEID method irrelevant. FFI, as a representative consortium of the financial sector, has been the owner and regulator for BankID. Back then, smaller banks expressed their concerns that they would prefer “a single government-provided standard which would guarantee similar competitive opportunities for all players” (Kallio et al., 2004). As the last sign of a Finnish BankID “victory”, the largest bank in Finland terminated FINEID support in 2009. Although FINEID cards are still in use, they have a very specific niche, mostly for governmental, healthcare, and social welfare workers, and the government has not expressed its will to terminate or expand their use.

In August 2018, the Ministry of Finance in Finland announced the government’s decision to explore alternative methods of electronic identification for citizens after 2020. So far identification in Finland has been dominated by the bank-provided eID solutions, with a total
number of 125 million transactions in 2018. The decision to explore alternative identification methods was preceded by two rounds of partially successful public procurements in 2017 and 2018, where some banks as IdPs and the public sector as a procuring entity could not agree on mutually acceptable pricing models. In the most recent (the third) procurement in October 2018, agreement was finally reached between the banks and public sector. However, the use of bank-provided eID solutions is secured temporarily and only for the period of 2019 - 2020.

The need for a renewed procurement was created by budget limitations (a maximum of 5 million EUR per year) to cover the identification costs for the public sector; and the newly introduced e-identification framework, the Finnish Trust Network, FTN (Finnish Transport and Communications Agency (Traficom), 2019) that came into force in mid-2017. The FTN framework, which was created in compliance with the EU Regulation on electronic identification and trust services (eIDAS), has introduced a number of architectural and business changes to the eID ecosystem. eIDAS promotes electronic identifier reuse and interoperability across services in the EU. It came into force in 2014 and required that all EU member states comply with its specifications by 2016. One of the main goals of eIDAS is to ensure that people and businesses can use their own national eID schemes to access public services in other EU countries where eIDs are available. Most importantly, eIDAS data security requirements made it impossible to continue to use the Tupas protocol, thereby increasing the need for larger changes. Finland’s Act on Electronic Identification and Electronic Signatures was amended to correspond to EU legislation and boost market competition in the eID market (Finnish Transport and Communications Agency (Traficom), 2019).

The FTN specifies the role of service brokers who are allowed to resell eID solutions in Finland using a standardized service contract. The idea behind the FTN framework creation was to help relying parties to acquire the eID services via a single proxy, i.e., one point of technical integration and simplified contractual agreements, thus, expanding the use of eIDs. The most important impact of FTN concerns contractual agreements, which previously required service providers to sign agreements with each of the banks (9 in total). Firms interested in becoming service brokers need to meet the requirements for strong customer authentication laid down in the legislation. The list of registered providers includes banks, telecom operators, and incumbent service brokers. The change has had major implications not only on the platform and its role in the ecosystem but also on other ecosystem participants.

Moreover, the framework has put a price cap on BankID identification transactions. The reduction was from about 0.5 to 0.1 EUR. It has also authorized the chaining of electronic identifiers, i.e., the recreation of new eIDs (e.g., MobileID, a competing solution provided by telecoms) based on existing strongly authenticated eIDs (BankID method) in return for a fee of 2.5 euros max.

It is important to mention that when this research commenced, Finnish banks had already been only maintaining the TUPAS infrastructure and regarded TUPAS as a “fee-income cash cow”. Furthermore, by the time the regulation came, Finnish banks had lost their interest to defend TUPAS with the same vigor and energy they had done that when establishing TUPAS in the early 1990s and promoting its use in private and public sector electronic services.

Finland follows a market-procured model similar to other Nordic countries where the IdPs can offer their audited and qualified solutions to the public sector. In Sweden, the e-identification service is provided by the private sector, mainly through banks and large telecommunication providers. Although at the beginning the Swedish BankID was launched

---

independently by the banks in 2003. However, by 2011 they realized that the cooperation between banks and mobile operators on a shared eID services infrastructure would be advantageous to all stakeholders (Eaton et al., 2017). The public sector in Sweden is also dependent on market-procured e-identification solutions. Concerning the other Nordics, Norway’s approach is similar to the Finnish approach (Murphy, 2014). Norwegian citizens have a choice between four commercial eID alternatives, among which is BankID which started to be operational in 2004 (Eaton et al., 2014). At the beginning, the Norwegian government was indecisive about whether to adopt a commercial solution or not for two reasons: there were disagreements on security protocol specifications and due to ideological reasons. The process of finding a compromise, though catalyzed by public frustration (Eaton et al., 2017), was settled in 2012. The Danish way can be characterized as more proactive and government-driven: the national eID infrastructure is controlled by the state and operated by private service brokers (Eaton et al., 2017).
4. Research problem and methodology

This chapter outlines the research problem, the scope of the research and presents the research questions. Next, the chapter describes the research approach taken in this study, as well as the corresponding research process. In addition, the descriptions of the participating organizations and interviewees are provided.

4.1 Scope of research and research problem

The dependence upon a dominant digital infrastructure. Present-day activities and transactions are increasingly happening in a digital context (Van Alstyne et al., 2016) on software-based platforms such as Facebook, Google, WeChat, AliPay and various industry-specific platforms. There is a wealth of studies on the platforms themselves and their evolution (Henfridsson & Bygstad, 2013; Tilson et al., 2010), and on platform governance (Jansen & Cusumano, 2013) and leadership (Gawer & Cusumano, 2008) of keystone players such as Google (Iyer & Davenport, 2008; Karhu et al., 2014), Amazon (Venkatraman et al., 2014), Apple (Eaton et al., 2015) and organizations’ decisions to adopt platform creation strategies (Ghanam et al., 2012). However, we lack understanding of how not-owner enterprises should approach external integration. This thesis investigates platform ecosystems and external integration from the other end, i.e., from the perspective of enterprises that do not own the platform but need to integrate with it because, e.g., their customers and business partners increasingly access services and business transactions through the platform. These enterprises, i.e., non-focal actors of the platforms, are required to continuously develop their external integration and strategies and align themselves with internal integrations. Often there are no alternatives, as global infrastructures have a tendency to form monopolies because of the winner-takes-it-all economics (Eisenmann et al., 2006), such as is the case with Google and Facebook. As there will not be many global winners, we consider that most Finnish and European enterprises belong to this non-focal role in relation to external platforms. Understanding external integration and being successful in its implementation is essential for the future of enterprises in Europe and Finland. There is neither any clear scientific advice nor instructions for practitioners available on how enterprises could optimally choose the platforms and implement, manage and maintain their external integration. This research area offers potential for research and practice because of lacking earlier research and there is high potential for economic and scientific impact. The research context combines technical and organizational domains and requires understanding of software architectures, information systems and organizational management.
The dominant infrastructure evolution. Current research on platforms has focused on guiding firms to become platforms (Gawer & Cusumano, 2008; Leijon et al., 2017). Amrit Tiwana’s seminal book on orchestrating software platforms suggests that businesses must learn to leverage the power of platform business models in order to remain competitive (Tiwana, 2014). Firms are increasingly opening up their products and services to create developer ecosystems around their services. Digital platforms are digital artifacts and thus they are volatile and sensitive to changes in technology, regulation, and customer preferences. However, few studies have addressed the implications of the termination phases of the platform or the periods following their dominance. An increasing use of platforms among businesses creates dependencies that we need to understand better. After integrating with externally developed and managed solutions, little is known concerning the consequences when the platform ecosystem is transformed or disrupted. Due to the rise of platforms spanning geographies and industries, it is pivotal to understand what happens to “defeated” platforms. Do they simply disappear, disintegrate or diminish? In order to gain answers to these questions, this thesis engages in an extensive case study of a nation-wide platform and focuses primarily on the latest phase of its evolution. In relation to studies of change, digital platforms have mostly been studied as enablers for transformations within organizations, markets or industries (Resca et al., 2013). Platform evolution has also been explored in the context of a platform’s ignition, or how the platform materializes in the first place (Sandberg et al., 2014). In our study, we have had the opportunity to look at the exceptional phenomenon of a transformation within a platform ecosystem that also involved a change in its materiality. Our empirical case is an extreme example of an industry platform which achieved an almost-monopoly-like status and whose orchestrators were unsuccessful in anticipating changes and proactively adapting to them.

The case of a national IdM infrastructure and its governance. Electronic identification solutions have evolved as one of the cornerstones of digital infrastructures. Offering the functionality of scalable identification, these solutions facilitate the continued digitalization of society (Husz, 2018). At the same time, previous research highlights that the design, realization and implementation of such solutions are fraught with difficulty (Eaton et al., 2014; Hoff & Hoff, 2010). As it was described earlier, the eID services in Finland are procured on the open market with bank identifiers as the de facto method of e-identification both in the private sector and for e-governmental services. Despite being a pragmatic solution, the market-procured approach involves a number of challenges, namely market dynamics, technological changes, regulation and political interests that influence the power relationship between the government and banks (in the Finnish case) when negotiating a common approach to the governance of the eID infrastructure (Medaglia et al., 2017b). The use of bank identifiers as a national eID infrastructure have been criticized for their technical weaknesses and vulnerabilities in (Espelid et al., 2008; Gjøsteen, 2008), but the benefits have also been emphasized (Eaton et al., 2014). The banks’ ownership of the identification infrastructures has also been criticized for hindering competition and for taking advantage of their dominant market position (Murphy, 2014). Among other criticisms is the geographical limitation of the method, which has inherent limitations in scaling into a global system (Teigland et al., 2018). Therefore, research that can extract the lessons learnt from the “receding” Finnish BankID case would be valuable in the governance of similar IdM infrastructures.

The architecturally significant components in IdM infrastructures. The literature on IdM solutions is abundant and solutions vary according to the technology components and other
non-technical requirements. Although there is a need for exchanging identities across domains and borders which requires interoperable solutions and flexible architectures, studies on how to systematically build such infrastructures is still lacking. To the author’s knowledge, very few publications can be found that give an overview of IdM infrastructure architectures and extract important development features at the ecosystem level. Here, we refer to the concept of architecturally significant requirements that are used in software design to drive and justify architectural decisions. Such design choices can be based on organizational, business, human and technological factors. Through the identification of these architecturally significant components of infrastructures, it is possible to discuss their potential real-life inhibitors. Issues such as ownership, responsibility and architecture (Söderström, 2016) have proven difficult to manage, resulting in substantial failures and costs (Beynon-Davies, 2011). The research problem of building dominant IdM infrastructures, and especially focusing on the important design choices, is an open problem that has considerable implications on the digitalization of services.

4.2 The research questions

The research carried out in this thesis uses empirical research methods to help understand the problem of external platforms and infrastructures in the context of IdM and for developing theory-advised instructions for practitioners. The main research question is: What factors affect changes in dominant digital infrastructures?

The main objective is to theoretically explain the nature of dependencies upon external platforms and infrastructures, the dynamics of their evolution and to derive practical instructions for managing dominant digital infrastructures, illustrated as an IdM infrastructure in this thesis. This main research question was divided into four sub-questions that are addressed fully or partially in each corresponding publication (Table 5). Each research sub-question tackles an individual aspect of the main research problem: installed base factors (RQ 1 and RQ 2), governance (RQ 3) and architecture (RQ 4). Note that these four research sub-questions are high level re-conceptualizations of the research questions reported in the publications.

RQ 1 focuses on defining and conceptualizing the dependence upon a dominant digital infrastructure and asks: What are the characteristics of dependency on a dominant digital infrastructure? The question is answered in Publication I and Publication II.

RQ 2 focuses on conceptualizing the process of dominant infrastructures evolution where the IdM infrastructure in Finland serves as an example case, asking: How are dominant digital infrastructures transformed? Here, the transformation process is directly related to the evolution concept. The question is answered primarily in Publication III and partially in Publication II.

RQ 3 focuses on understanding the governance aspects in the transformation of dominant (IdM) infrastructures and asks: What are the important factors in the governance of dominant IdM infrastructures? Here, the question is answered in Publication IV and covers the governance aspects of a specific type of nation-wide IdM infrastructure which is a result of public-private sector cooperation and resistance.

RQ 4 focuses on deriving the features of IdM infrastructure architectures that are crucial when developing and managing the development of such infrastructures and asks: What are the architecturally significant aspects in the development of IdM infrastructures? Here, the
viewpoints include organizational, business and technology perspectives. The question is answered in Publication V and Publication VI.

This dissertation is seeking to explain the infrastructural change process in terms of the installed base, governance and architectural factors. The perspective of the installed base brings a process-oriented understanding which emphasizes “tracing and analyzing the historical sequence of events and decisions that shape the forming of infrastructures” (Aanestad et al., 2017). The governance aspect and architectural factors contribute to the domain-specific knowledge of identity management infrastructures.

Table 5. Research questions addressed by the publications in this thesis

<table>
<thead>
<tr>
<th>Research sub-questions</th>
<th>Objectives</th>
<th>Publication</th>
</tr>
</thead>
<tbody>
<tr>
<td>What are the characteristics of dependency on a dominant digital infrastructure?</td>
<td>To understand the dependence upon a dominant digital infrastructure.</td>
<td>Publication I, II</td>
</tr>
<tr>
<td>How are dominant digital infrastructures transformed?</td>
<td>To explain the process of dominant infrastructure transformation.</td>
<td>Publication II, III</td>
</tr>
<tr>
<td>What are the important factors in the governance of dominant IdM infrastructures?</td>
<td>To identify the governance aspects of dominant IdM infrastructures.</td>
<td>Publication IV, V</td>
</tr>
<tr>
<td>What are the architecturally significant aspects in the development of IdM infrastructures?</td>
<td>To identify the key dimensions of IdM infrastructure architectures.</td>
<td>Publication V, VI</td>
</tr>
</tbody>
</table>

4.3 Paradigms of qualitative research

Prior to proceeding with the description of the research methodology chosen for this research, it is important to cover the fundamental ideas of research. Although there are multiple ways to conduct research, the approaches can be grouped by their philosophical assumptions regarding the nature of the phenomena studied and different views on knowledge. We follow Orlikowski and Baroudi’s (1991) distinction between three different paradigms: positivist, interpretive and critical. Each paradigm is based on explicit assumptions that are mutually consistent and shared within various communities of researchers.

The positivist perspective is commonly used in natural sciences. In the positivist worldview, reality is given objectively and can be described by measurable properties that are independent from the observer (Orlikowski & Baroudi, 1991). The purpose of a positivist inquiry is explanation and finding general laws and causal connections. In this paradigm, a set of basic beliefs, questions or hypotheses are proposed and then tested or verified empirically to generate falsifiable statements (Guba & Lincoln, 1994). However, such a strict worldview creates inconsistency when applied in social sciences where the understanding and interpretation of human activity is at the center.

The interpretive perspective suggests that the access to reality is possible only through social constructions such as language, consciousness and shared meanings. An ontological assumption is relativism, i.e., that there exist multiple socially constructed realities not governed by any natural, causal or other laws (Lincoln et al., 2011). The goal of knowledge generation is to understand phenomena through the meanings that people assign to them (Avenier & Thomas, 2015). Within the IS field, studies in the interpretive tradition attempt to understand the context of the information systems and how such systems influence and are influenced by the context (Walsham, 1993).

The critical perspective assumes that the reality is historically constructed, produced and reproduced by people. Research from a critical perspective seeks to evaluate, challenge and transform existing social systems (Orlikowski & Baroudi, 1991). Its main task is the search for a social critique, where “the restrictive and alienating conditions of the status quo are brought
to light” (Myers, 1997). It also incorporates the idea of totality, which is the interdependence of parts with the whole, in which, e.g., in our case information systems cannot be studied in isolation of the organization, industry, economy in which they operate.

### Table 6. Research paradigms used in each publication

<table>
<thead>
<tr>
<th>Publication</th>
<th>Paradigm</th>
<th>Method</th>
<th>RQ1</th>
<th>RQ2</th>
<th>RQ3</th>
<th>RQ4</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>Interpretive</td>
<td>Grounded Theory</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>II</td>
<td>Interpretive</td>
<td>Case study</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>III</td>
<td>Interpretive</td>
<td>Case study</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>IV</td>
<td>Interpretive</td>
<td>Case study</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>V</td>
<td>Positivist</td>
<td>Case study</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VI</td>
<td>Positivist</td>
<td>Systematic literature review</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
</tr>
</tbody>
</table>

Any research takes place within an explicit or implicit philosophy of knowledge, and the research presented in this dissertation is no exception (Avenier & Thomas, 2015; Van de Ven, 2007). The overall philosophical paradigm regarding the entire research is interpretivism. Two of the philosophical perspectives described above (that resulted in separate publications) underlie the research presented in this thesis, demonstrated in Table 6. Although the variability of philosophical assumptions indicates a paradigm shift, we believe it also binds the publications in the thesis together. The shift from the interpretive towards a more positivist paradigm manifests the shift in the author’s own research interests and predispositions, or in other words “remaining open to the possibility of other assumptions and interests” (Orlikowski & Baroudi, 1991).

### 4.4 Selection of research methods

Here, the selected research methodologies applied in this research are presented. A research method is defined as a strategy of inquiry that “moves from the underlying philosophical assumptions to research design and data collection” (Myers, 1997). The study belongs to the IS domain which is closely related to social sciences, unlike the IS research within the computer science and engineering traditions that has its roots in natural sciences (Orlikowski & Baroudi, 1991).

The selection of research methodologies was influenced by the main objectives of this thesis. The main interest was in studying the interaction of information technology and organizations. Qualitative research methods are designed to help researchers understand social phenomena, whereas quantification often loses these contexts. Qualitative research findings illustrate the phenomena studied in real-life settings. Well-designed qualitative studies not only bring richer semantical meanings to the understanding of the problem, but also can act as an effective benchmarking method to evaluate methodology or technology usage, which can then be transferred into industrial practice.

Myers (1997) specifies that action research, case study research, ethnography and grounded theory are all qualitative methods that are essential in the IS field. In *Publication I* the selected method was the grounded theory. The studies reported in *Publications II and IV* were performed as case studies with the data analysis based on grounded theory. *Publication III and V* followed case study designs with qualitative data analysis techniques, while *Publication VI* was a systematic literature review. In the following goes the description of the methods used in this thesis, see Table 7.

A *case study* is “an empirical enquiry that investigates a contemporary phenomenon within its real-life context, especially when the boundaries between the phenomenon and context are not clearly evident” (Yin, 1981). A case study is a commonly used research method in social
sciences and in IS research the object of inquiry is the information systems within organizations (Myers, 1997). The literature offers extensive methodological guidelines for interpretive field studies drawn from the IS literature (Klein & Myers, 1999). Runeson and Höst (2008) outline five main steps when conducting a case study. These consist of: (1) the case study design, in which the objectives are defined and the case study is planned; (2) preparation for data collection, in which the procedures and protocols for data collection are defined; (3) collecting evidence, which includes the execution of data collection for the studied case; (4) analysis of collected data and (5) reporting. Alternatively, a roadmap for building theories from case studies from Eisenhardt (1989) is a blend of previous work on Yin’s design of case study research (Yin, 1981), grounded theory (Glaser & Strauss, 1967) and qualitative data analysis methods (Miles & Huberman, 1984). Eisenhardt (1989) extends these works by introducing an a priori specifications of constructs and researchers’ triangulations and emphasizes the role of the extant literature in generating the theory. The process is similar to other empirical methods, yet there are a significant number of iterations. The roadmap proposed by Eisenhardt (1989) differs from Runeson and Höst’s (2008) model by including steps on shaping hypotheses and the overall process flow and procedure in both models are comparable, except for terminological variations.

Grounded theory is an inductive, theory-forming methodology that is grounded in empirical observations (Glaser & Strauss, 1967; Strauss & Corbin, 1990). The analysis procedure in Grounded theory (Strauss & Corbin, 1990) follows three steps:

- Open coding: “the process of breaking down, examining, comparing, conceptualizing, and categorizing data” (Strauss & Corbin, 1990, p. 61).
- Axial coding: “a set of procedures whereby data is put back together in new ways after open coding, by making connections between categories. This is done by utilizing a coding paradigm involving conditions, context, action/interactional strategies and consequences” (Strauss & Corbin, 1990, p. 96).
- Selective coding: “the process of selecting the core category, systematically relating it to other categories, validating those relationships, and filling in categories that need further refinement and development” (Strauss & Corbin, 1990, p. 116).

The main difference between case studies and a grounded theory is that in case studies, theories or concepts can be defined a priori to guide the research. Grounded theory focuses on developing a theory that emerges from the data (Myers, 1997). Another major trait of grounded theory methods is the continuous interplay between data collection and analysis, where data can be anything that is collected for the purpose of the study.

**Table 7. Summary of the approaches in each publication**

<table>
<thead>
<tr>
<th>Publication</th>
<th>Empirical data</th>
<th>Method</th>
<th>Data analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Publication I</td>
<td>8 Organizations, 24 semi-structured interviews</td>
<td>Grounded Theory (Strauss &amp; Corbin, 1990)</td>
<td></td>
</tr>
<tr>
<td>Publication II</td>
<td>8 Organizations, 24 semi-structured interviews</td>
<td>Case study (Yin, 2011)</td>
<td>Grounded Theory techniques</td>
</tr>
<tr>
<td>Publication III</td>
<td>31 semi-structured interviews and secondary data</td>
<td>Case study (Yin, 2011)</td>
<td>Qualitative content analysis</td>
</tr>
<tr>
<td>Publication IV</td>
<td>11 semi-structured interviews and secondary data</td>
<td>Case study (Yin, 2011)</td>
<td>Grounded Theory techniques</td>
</tr>
<tr>
<td>Publication V</td>
<td>11 semi-structured interviews and secondary data</td>
<td>Case study (Eisenhardt, 1989)</td>
<td>Qualitative data analysis</td>
</tr>
<tr>
<td>Publication VI</td>
<td>Secondary literature</td>
<td>Systematic literature review</td>
<td>(Kitchenham et al., 2009)</td>
</tr>
</tbody>
</table>

A third method that needs to be introduced is a **systematic literature review (SLR)**. An SLR is a methodologically rigorous review of research results (Kitchenham et al., 2009). Reviews in
the field of IS are challenging due to the complexity of assembling a review in such an interdisciplinary field (Webster & Watson, 2002). While the objectives of conducting reviews may differ, the main idea is to aggregate the empirical evidence on the topic of interest. SLRs can be performed as part of outlining a theoretical background, identifying the related literature and the state-of-the-art or answering specific research questions (Okoli & Schabram, 2010). Literature reviews are most commonly included as the introductory chapter of dissertations, in this thesis, Publication VI reports the results of an SLR that constitutes original research of its own (ibid.).

4.5 Research process

The research presented in this thesis was performed in three phases. This research is part of the DINE project — Digital Infrastructures and Enterprise Integration, with funding provided by the Academy of Finland. DINE focused on the use of digital infrastructures, possibly provided by global Internet giants, as strategic assets. Figure 2 depicts the connections between publications, that can be theoretical (referring to the publications that share their theoretical framing or concepts used to analyze the data) or empirical, which means that the link between the publications is a shared empirical case (i.e., Finnish IdM or IdM in other contexts). While each publication is designated for a specific phase, the work on each publication and the final publication date may differ. The knowledge acquired in each phase had a significant influence on the viewpoints and formulation of research problems that were used as guidance in consecutive research phases. Phase one can be seen as a preliminary one with a broad scope, the findings of which helped to identify the main case analyzed comprehensively in phase two of this thesis. After the saturation has been reached in phase two, it led to phase three, where the aim was to “triangulate” the case context.

Figure 2. Phases of research and publications.

Phase 1 of the research presented in this thesis started in October 2016 and started with a preliminary literature review on the topic of platform ecosystems, digital infrastructures and enterprise architectures within the IS discipline. Phase 1 resulted in Publication I that was
published in 2018. The focus of phase 1 was to identify the cases of integrations with external platforms and infrastructures as well as defining the research focus from a narrower perspective.

Phase 2 began in June 2017 and it started with the identification of a specific case of an external platform and infrastructure and the submission of Publication II. The article was submitted in May 2017 and presented at a conference in early 2018. Publication II was invited for revision and extended to a journal article in early 2018 and was submitted in May 2018, which resulted in Publication III that appeared online in early 2019. In March 2018 the research problems and ideas were presented at Gothenburg University (GU). From August to September 2018 was the period of a research visit at GU and where the data for Publication V was collected.

Phase 3 began in October 2018. At the beginning of that phase, Publications IV and V were written simultaneously and submitted to a conference in late 2018. October 2018 included a data collection visit to Taiwan – which formed the primary data for Publication V. In spring 2019 Publication I was invited for revision and published as a separate volume of the Lecture Notes in Information Systems and Organization series (version included in this thesis). From early 2019 until summer 2019 the work reported in Publication VI was performed. Publications V and VI are the outcomes of phase 3.

4.5.1 Data collection

Both primary and secondary data were collected in this research. In addition to collecting different views from banks, the government, and other organizations, we collected secondary data from official publications, press releases, reports and news found online.

<table>
<thead>
<tr>
<th>Organization</th>
<th>Industry sector</th>
<th>Size (employees)</th>
<th>Number of interviewees</th>
<th>Data used in Publication</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. A</td>
<td>Telecommunications</td>
<td>1,700</td>
<td>10</td>
<td>x x x x</td>
</tr>
<tr>
<td>2. B</td>
<td>Finance</td>
<td>2,500</td>
<td>6 x x x x x x</td>
<td></td>
</tr>
<tr>
<td>3. C</td>
<td>Governmental organization</td>
<td>360</td>
<td>5 x x x x x x x</td>
<td></td>
</tr>
<tr>
<td>4. D</td>
<td>IS for the government</td>
<td>130</td>
<td>3 x x x</td>
<td></td>
</tr>
<tr>
<td>5. E</td>
<td>Academia</td>
<td>52</td>
<td>6 x</td>
<td></td>
</tr>
<tr>
<td>6. F</td>
<td>Software development</td>
<td>20</td>
<td>1 x x x</td>
<td></td>
</tr>
<tr>
<td>7. G</td>
<td>Software development</td>
<td>10</td>
<td>1 x x x</td>
<td></td>
</tr>
<tr>
<td>8. H</td>
<td>Governmental organization</td>
<td>38,000</td>
<td>2 x x x x</td>
<td></td>
</tr>
<tr>
<td>9. I</td>
<td>Regulatory authority</td>
<td>240</td>
<td>2 x x x x</td>
<td></td>
</tr>
<tr>
<td>10. J</td>
<td>Bank</td>
<td>12,000</td>
<td>2 x x</td>
<td></td>
</tr>
<tr>
<td>11. K</td>
<td>Bank</td>
<td>28,990</td>
<td>1 x x</td>
<td></td>
</tr>
<tr>
<td>12. L</td>
<td>Finance</td>
<td>55</td>
<td>1 x x</td>
<td></td>
</tr>
<tr>
<td>13. M</td>
<td>Financial regulatory authority</td>
<td>200</td>
<td>1 x x</td>
<td></td>
</tr>
<tr>
<td>14. N</td>
<td>Finance</td>
<td>380</td>
<td>1 x x</td>
<td></td>
</tr>
<tr>
<td>15. O</td>
<td>Finance &amp; Legal</td>
<td>12</td>
<td>1 x x</td>
<td></td>
</tr>
<tr>
<td>16. P</td>
<td>ICT</td>
<td>13,000</td>
<td>1 x x</td>
<td></td>
</tr>
<tr>
<td>17. Q</td>
<td>Non-profit organization</td>
<td>6 (600 members)</td>
<td>2 x x</td>
<td></td>
</tr>
<tr>
<td>18. R</td>
<td>Governmental organization, Sweden</td>
<td>490</td>
<td>1 x x</td>
<td></td>
</tr>
<tr>
<td>19. S</td>
<td>Security company</td>
<td>80</td>
<td>1 x x</td>
<td></td>
</tr>
<tr>
<td>20. T</td>
<td>Governmental organization, Sweden</td>
<td></td>
<td>1 x x</td>
<td></td>
</tr>
<tr>
<td>21. U</td>
<td>Fintech</td>
<td>10</td>
<td>2 x x</td>
<td></td>
</tr>
<tr>
<td>22. V</td>
<td>Financial Media and Financial Technology Taiwan</td>
<td>130</td>
<td>2 x x</td>
<td></td>
</tr>
<tr>
<td>23. W</td>
<td>Research</td>
<td>1</td>
<td>1 x x</td>
<td></td>
</tr>
</tbody>
</table>

The research included semi-structured interviews conducted with experts in relevant fields. The interview protocol was prepared before each interview round. Each interview began by asking the interviewee’s position, background, experience and projects/products/services they
managed. Next, there was a discussion on the specific topic of the interview: existing utilizations of external platforms or experiences with the IdM platform. The interviews followed the funnel model principle, moving from open to more specific questions (Runeson & Höst, 2008). The initial set of organizations at the beginning of phase 1 included A, B and C only (shown in Table 8). Then, the list was expanded to include other organizations after discovering the magnitude and degree of dependence on the Finnish IdM countrywide. A snowballing technique was used in order to acquire new contacts or organizations for the interviews. At the end of each interview the interviewee was asked to refer to a colleague who could possess relevant knowledge on the case/topic of the interview.

The organizations that participated in this research included small, medium-sized and large organizations. A summary of the participating organizations in this research and the information on which interviewee data was used in which publication is presented in Table 8. A short description of each organization is presented below.

- **A** is a telecommunications operator and a major cable operator, a pay TV provider in both cable and terrestrial networks. The company employs around 1,600 people and serves around 2.7 million customers.
- **B** is a large payment service provider. The customers of B are banks, businesses, merchants and the public sector. B employs approximately 2,400 employees in six countries and, according to recent statistics (2016), served a network of more than 300,000 merchants and 240 banks. B’s services also include payment and authentication bundle services.
- **C** is part of the Finnish government. C prepares the government’s economic and financial policy as well as the budget, and acts as a tax policy expert. One of the tasks of C is the general steering of public sector agencies’ information management. Their ambition, together with other ministries in Finland, is to boost the e-services market in Finland.
- **D** is a governmental organization that operates under the authority of C. D’s task is to develop, support and manage the usage of electronic data contained in governmental and public information systems.
- **E** is the IT services department of a university in Finland, who are responsible for IS support of research and teaching staff.
- **F** is a small payment service operator that resolves bureaucratic complexities in salary payments as an Internet service. Their cloud-based service provides a suite of open APIs and support services for any company or individual to integrate payroll features and salary payments, including integrations between insurance companies, tax agencies, pension companies, employment foundations and banks.
- **G** is a software-development company founded in 2015. Their main service is a native mobile app for students that integrates study records, campus restaurant menus, indoor positioning guide maps, various news and feeds, in other words all the essential information needed by students in their daily university life.
- **H** is a municipality that represents the local level of the administration. The H council is the main decision-making organ in local politics, dealing with issues such as city planning, schools, health care, and public transport. H operates the portal for e-services where citizens can make appointments and manage documents electronically.
- **I** is a regulatory agency in Finland that prepares the technical specifications and supervises their compliance in telecommunications.
- **J** is a large banking group operating in Finland and the Nordic countries.
- **K** is a large financial services group operating in over 1,400 branches in northern Europe.
- **L** is a representative organization of the banks and the Finnish financial sector and its core function is the provision of high-quality lobbying. The office employs 55 financial sector
requirements. L represents the majority of banks, insurers, finance houses, securities dealers, fund management companies and financial employers operating in Finland.

- **M** is the authority for the supervision of Finland’s financing and insurance sectors with about 200 employees. The entities supervised by the authority include banks, insurance and pension companies as well as other companies operating in the insurance sector, investment firms, fund management companies and the Helsinki Stock Exchange. The activities of M are supervised by the Parliamentary Supervisory Council.

- **N** is the ‘bank of banks’ in Finland and safeguards liquidity in the domestic financial system. It implements the Euro system’s monetary policy in Finland by conducting monetary policy operations with Finnish counterparties, generally banks. N is responsible for oversight of the financial system and assesses risks to the system jointly with the M.

- **O** is an e-commerce and electronic signatures company, which is an incumbent service broker in the eID ecosystem.

- **P** is an IT software and service company providing IT and product engineering services, with approximately 15,000 employees, active in around 20 countries.

- **Q** is an open community, which promotes project pilots and shares knowledge and resources. The aim is to develop national and internationally scalable interoperability models for personal data management.

- **R** is a governmental organization in Sweden that is responsible for matters relating to infrastructure, digital policy, post issues and energy. The division for digital government prepares the policies for digital identity.

- **S** is an international IT security company that provides innovative security solutions for banking, government and businesses worldwide. S creates solutions for the protection of digital identities and information.

- **T** is a government authority in Sweden that serves as a hub for digitalization of the public sector. T promotes and coordinates electronic identification and signature for the public sector e-services.

- **U** is a Nordic Fintech company that is committed to introducing Nordic financial technology to Taiwan, and through cooperation with local partner manufacturers assists financial institutions and corporate customers to quickly bring new applications to production. Their focus areas include blockchain platforms, insurance technology, electronic payments, information security, and digital forensics.

- **V** is a financial media and financial technology provider in Taiwan and Hong-Kong. Their service portfolio includes providing a global financial information, investment decision advice, asset management and funds, and stock trading services.

- **W** is a book author and an R&D representative in the field of information systems (business informatics), information science, API design and developer experience.

The total number of experts interviewed was 55. The total number of interviews was 51, because 4 interviews were conducted together with 2 experts. More detailed information on each interviewee’s position is summarized in Table 9.

Most of the interviews were performed in person in the participating organization’s premises. An asterisk (*) in Table 9 indicates that two interviewees from the same organization were interviewed together. Interviews 51 and 52 were conducted in Taipei, and interviews 53 and 54 were in the form of a workshop and an ethnographic observation. Interviews 48, 49 and 50 were conducted over Skype during the author’s research visit to Sweden. Interviews 15 and 16 were conducted over Skype. Interview 47 was conducted over the phone. A recording device was used in all the interviews.
Before commencing each interview, the interviewer followed a protocol of asking for permission to record and utilize the data. In addition to using the recorder, the candidate also took notes during the interviews concerning non-verbal observations and remarks. During the data collection, there was only one organization that did not allow the recording of the discussion due to company regulations. In both cases, the author had a second interviewer (research team member) who helped by taking notes which were promptly discussed and

Table 9. The roles of the interviewees who participated in this research

<table>
<thead>
<tr>
<th>#</th>
<th>Organization</th>
<th>Role in organization</th>
<th>Data included in Publication #</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>A</td>
<td>Manager, data services</td>
<td>I, II, III</td>
</tr>
<tr>
<td>2.</td>
<td>A</td>
<td>Director, corporate solutions (1)</td>
<td>I, II, III</td>
</tr>
<tr>
<td>3.</td>
<td>A</td>
<td>Director, corporate solutions (2), (*)</td>
<td>III</td>
</tr>
<tr>
<td>4.</td>
<td>A</td>
<td>Chief digital officer</td>
<td>I, II, III</td>
</tr>
<tr>
<td>5.</td>
<td>A</td>
<td>Head of enterprise architecture (1)</td>
<td>I, III</td>
</tr>
<tr>
<td>6.</td>
<td>A</td>
<td>Head of enterprise architecture (2)</td>
<td>II, III</td>
</tr>
<tr>
<td>7.</td>
<td>A</td>
<td>Development manager (1)</td>
<td>I, II, III</td>
</tr>
<tr>
<td>8.</td>
<td>A</td>
<td>Development manager (2)</td>
<td>III</td>
</tr>
<tr>
<td>9.</td>
<td>A</td>
<td>Head of online performance</td>
<td>I, II, III</td>
</tr>
<tr>
<td>10.</td>
<td>A</td>
<td>Vice president, broadband and entertainment business</td>
<td>I, II, III</td>
</tr>
<tr>
<td>11.</td>
<td>A</td>
<td>Development manager, corporate solutions (*)</td>
<td>I, II, III</td>
</tr>
<tr>
<td>12.</td>
<td>B</td>
<td>Head of point of sale, software engineering (1)</td>
<td>I, II, III</td>
</tr>
<tr>
<td>13.</td>
<td>B</td>
<td>Head of point of sale, software engineering (2)</td>
<td>I, II, III</td>
</tr>
<tr>
<td>14.</td>
<td>B</td>
<td>Head of quality assurance, merchant services</td>
<td>I, II, III</td>
</tr>
<tr>
<td>15.</td>
<td>B</td>
<td>SVP digital innovation (*)</td>
<td>I, II, III</td>
</tr>
<tr>
<td>16.</td>
<td>B</td>
<td>Senior manager - digital practices, (*)</td>
<td>I, II, III</td>
</tr>
<tr>
<td>17.</td>
<td>B</td>
<td>Enterprise architect</td>
<td>IV</td>
</tr>
<tr>
<td>18.</td>
<td>B</td>
<td>Account director</td>
<td>III, IV</td>
</tr>
<tr>
<td>19.</td>
<td>C</td>
<td>Development manager</td>
<td>I, II, III</td>
</tr>
<tr>
<td>20.</td>
<td>C</td>
<td>Main architect</td>
<td>I, II, III</td>
</tr>
<tr>
<td>21.</td>
<td>C</td>
<td>Service manager</td>
<td>I, II, III</td>
</tr>
<tr>
<td>22.</td>
<td>C</td>
<td>Service manager</td>
<td>III, IV, V</td>
</tr>
<tr>
<td>23.</td>
<td>C</td>
<td>Financial markets in Finland</td>
<td>III, IV</td>
</tr>
<tr>
<td>24.</td>
<td>D</td>
<td>Development manager</td>
<td>I, II, III</td>
</tr>
<tr>
<td>25.</td>
<td>D</td>
<td>Product owner</td>
<td>II, III</td>
</tr>
<tr>
<td>26.</td>
<td>D</td>
<td>Director</td>
<td>Not used in any publication, but used in thesis discussion</td>
</tr>
<tr>
<td>27.</td>
<td>E</td>
<td>ITS manager</td>
<td>I</td>
</tr>
<tr>
<td>28.</td>
<td>E</td>
<td>Main architect</td>
<td>I</td>
</tr>
<tr>
<td>29.</td>
<td>E</td>
<td>Architect</td>
<td>I</td>
</tr>
<tr>
<td>30.</td>
<td>F</td>
<td>Managing director</td>
<td>I, II, III</td>
</tr>
<tr>
<td>31.</td>
<td>G</td>
<td>CTO (*)</td>
<td>I, II, III</td>
</tr>
<tr>
<td>32.</td>
<td>G</td>
<td>CEO (*)</td>
<td>I, II, III</td>
</tr>
<tr>
<td>33.</td>
<td>H</td>
<td>Project Manager, Head of eservice Program</td>
<td>I, II, III</td>
</tr>
<tr>
<td>34.</td>
<td>H</td>
<td>Main architect</td>
<td>II, III</td>
</tr>
<tr>
<td>35.</td>
<td>I</td>
<td>Main lawyer</td>
<td>II, III</td>
</tr>
<tr>
<td>36.</td>
<td>I</td>
<td>Director</td>
<td>IV, V</td>
</tr>
<tr>
<td>37.</td>
<td>J</td>
<td>Product manager (1)</td>
<td>III</td>
</tr>
<tr>
<td>38.</td>
<td>J</td>
<td>Product manager (2)</td>
<td>IV</td>
</tr>
<tr>
<td>39.</td>
<td>K</td>
<td>Product manager</td>
<td>IV, V</td>
</tr>
<tr>
<td>40.</td>
<td>L</td>
<td>Finance expert (*)</td>
<td>IV, V</td>
</tr>
<tr>
<td>41.</td>
<td>L</td>
<td>Legislation, senior expert (*)</td>
<td>IV</td>
</tr>
<tr>
<td>42.</td>
<td>M</td>
<td>Senior advisor</td>
<td>IV</td>
</tr>
<tr>
<td>43.</td>
<td>N</td>
<td>Adviser, financial markets and statistics</td>
<td>IV</td>
</tr>
<tr>
<td>44.</td>
<td>O</td>
<td>Chief legal officer</td>
<td>III</td>
</tr>
<tr>
<td>45.</td>
<td>P</td>
<td>Blockchain solutions consultant</td>
<td>IV</td>
</tr>
<tr>
<td>46.</td>
<td>Q</td>
<td>My data</td>
<td>IV</td>
</tr>
<tr>
<td>47.</td>
<td>Q</td>
<td>Ex-bank executive, My Data, industry advisor</td>
<td>Not used in any publication, but used in thesis discussion</td>
</tr>
<tr>
<td>48.</td>
<td>R</td>
<td>Head of section, division for digital government - Sweden</td>
<td>V</td>
</tr>
<tr>
<td>49.</td>
<td>S</td>
<td>CEO</td>
<td>V</td>
</tr>
<tr>
<td>50.</td>
<td>T</td>
<td>Senior advisor</td>
<td>V</td>
</tr>
<tr>
<td>51.</td>
<td>U</td>
<td>Fintech partner</td>
<td>V</td>
</tr>
<tr>
<td>52.</td>
<td>U</td>
<td>Fintech partner</td>
<td>V</td>
</tr>
<tr>
<td>53.</td>
<td>V</td>
<td>Project stakeholders (1)</td>
<td>V</td>
</tr>
<tr>
<td>54.</td>
<td>V</td>
<td>Project stakeholders (2)</td>
<td>V</td>
</tr>
<tr>
<td>55.</td>
<td>W</td>
<td>Industry expert</td>
<td>IV</td>
</tr>
</tbody>
</table>

(*) two interviewees from the same organization were interviewed together
registered upon the completion. The author or the professional service company that has a contractual relationship with Aalto University transcribed the recorded interviews. The interview transcriptions were not shared with any of the interviewees. Instead, the interviewees were given a chance to give feedback on the analyses of cases in the form of article drafts.

### 4.5.2 Data analysis

The data analysis in the publications followed either a grounded theory method as an overall approach and methodology (as in *Publication I*) or used the grounded theory techniques in combination with the case study approach (as in *Publications II, IV*). We analyzed the data in three phases: open, axial and selective coding. The data analysis started after all interviews had been conducted. The gathered data was analyzed with a qualitative data coding and analysis tool, Atlas.ti. This systematic approach to the qualitative inquiry helped us to deal with the rich data we collected which was full of diverging perspectives, opinions and insights (Strauss and Corbin, 1990).

The first step was open coding, where we went line-by-line through each interview or secondary data document and labelled the pieces of information by extracting the quotes that we believed were relevant regarding the research topic. The next step was axial coding, where we systematically browsed through the open codes to find the relations between them and merged or disaggregated relevant concepts. The goal was to let the understanding of the phenomenon emerge from the data. Finally, in the selective coding phase we selected and described the central phenomenon in the light of the core categories. The goal in the selective coding phase was to integrate and refine the degree to which the central concept varied in its dimensions. The coding process continued iteratively until a strong understanding of the phenomenon emerged.

### 4.5.3 Reporting

All the publications included in this thesis were written by a group of researchers, including the author as a doctoral candidate. The primary co-authors are the supervisor of this thesis, Professor Kari Smolander (all publications except *Publication V*), and D.Sc. Jesse Yli-Huumo (*Publication I, II, III*). *Publication IV* was written with a colleague from Aalto University, Department of Industrial Engineering. The study reported in *Publication V* was a collaboration effort between colleagues from Gothenburg University and industry practitioners.

### 4.6 Summary

This chapter articulated the four research questions, the research methods and the research process used in this thesis. The research process was divided into three main phases, which are summarized in Figure 3.
Figure 3. Research process.

Phase 1
- Brief literature review
- Study on understanding external platforms and infrastructures
  *Publication I*

Phase 2
- Study on relations in an IDM platform ecosystem transformation
  *Publication II*
- Study on IDM platform to infrastructure transformation
  *Publication III*
- Study on conflicts in IDM infrastructure transformation
  *Publication IV*

Phase 3
- Study on cross-country comparison of IDM implementations
  *Publications V*
- Study on assumptions of IDM infrastructure architectures
  *Publications VI*
5. Results

This chapter presents the most important findings of the study included in this thesis. The study results can be found in six publications attached as an appendix. Publications I, II, IV, V, and VI have been published in peer-reviewed scientific conferences. Publication III has been published in a peer-reviewed scientific journal. This chapter summarizes each publication’s research objectives, main findings, and relation to the overall objective of the thesis.

5.1 Publication I: How do Practitioners Understand External Platforms and Services? A Grounded Theory Investigation

5.1.1 Research objectives

This publication introduces the research problem of external platforms and infrastructures utilization as well as the non-focal role of organizations in a platform ecosystem. We address this gap by analyzing how practitioners give meaning to their integrations with external platforms. The meanings and definitions of external platforms among stakeholders within and across organizations are interpreted into higher level conceptualizations. Initially, we wanted to investigate how the utilization of external platforms could be explained. During the data collection and analysis we recognized the emerging phenomena of differing understanding among interviewees. Thus, the findings reported in this manuscript answer the following research question: How do practitioners understand external platforms utilized in their firms? The meanings and definitions of external platforms of the stakeholders within and across organizations are interpreted into higher level conceptualizations using the grounded theory method. We interviewed twenty-four practitioners from eight organizations of various sizes in Finland.

5.1.2 Results

The main result of this publication is that practitioners across units and sectors perceived the notion of external industry platforms differently. We identified four categories in the interpretations of external platforms. These were: externally deployed, externally developed, externally managed and external platform-based dependence. The four categories are discussed below.

The first category were externally deployed industry platforms. This was the most common understanding of an external platform and refers to the physical deployment of the underlying infrastructure where the platform is hosted. A platform was understood to be external when it was not running in house, but outside of the organization’s premises. The second category were
externally developed platforms. The majority of practitioners associated any software system originating from predominantly large vendors, e.g., SAP, Salesforce, Oracle, SAS, etc. as external platforms by default. The third category were externally managed platforms. The respondents affiliated the black box services developed for the organization as external service platforms, such as when a service is built and maintained by another organization. The fourth category were externally deployed, developed, managed and shared platforms. This refers to the existence of some voluntary-compulsory dependencies on certain services provided by other firms. These can be legal enforcements or constraints imposed by industry monopolies. This category refers to monopoly-like platforms and implies a combination of three preceding attributes together with shared simultaneous use of the platform (Table 10). Figure 4 below shows how the four categories were obtained from the codes in Table 10. The boxes labeled as “A_Number” are the axial coding outcomes and the network view in Figure 4 demonstrates the end result of core categories selection process.

Table 10. Four categories of interpretations of external platforms, Publication I

<table>
<thead>
<tr>
<th>External platform interpretation</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Externally deployed</td>
<td>Software instances physically running outside company’s premises, a system hosted remotely</td>
</tr>
<tr>
<td>Externally developed</td>
<td>Labelled products from predominantly large vendors, e.g., SAP, Salesforce, Oracle, or SAS</td>
</tr>
<tr>
<td>Externally managed</td>
<td>Instances not developed and maintained by the company, an outsourced black box service</td>
</tr>
<tr>
<td>Externally deployed, developed, managed and shared</td>
<td>Monopoly-like platforms, often legally enforced integrations or the only platform choice</td>
</tr>
</tbody>
</table>

Integrations with external platforms can be seen as a means to manage the complexity in the company, similarly to the adoption of cloud services or systems maintenance outsourcing. Schneider and Sunyaev (2016) define a cloud-sourcing decision as “the decision of the organization to adopt and integrate cloud services from external providers into their IT landscape”. We commit to the view of IT outsourcing as a predecessor of cloud computing models and extend this continuum with external platforms. Based on their comparison of cloud computing to IT outsourcing (Schneider & Sunyaev, 2016) we reuse the determinant factors (Table 11 Column 1) to contrast cloud computing (Table 11, Column 2) and IT outsourcing (Table 11, Column 3) with external platforms. The categories from our findings descriptively correspond to the cloud sourcing models presented in Table 11: externally developed primarily (but not exclusively) refers to cloud computing models, externally managed for IT outsourcing, and externally deployed to all.

The variance of what the interviewees identified as external platforms indicates the absence of agreement within the community of practitioners on various criteria of systems utilized in their organizational operations.

5.1.3 Relation to the whole

This publication presents the results of the first phase of the thesis. In the first phase we interviewed industry experts with the objective of finding specific cases of external industry platforms. The study reported in this publication is of a broad scope and is considered to be a starting point for exploring the next, more specific topics of the thesis. One of the examples of an external industry platform we identified in this Publication I was the Finnish IdM infrastructure. In consecutive Publications II, III and IV we study the case in greater detail.
This publication was also a first step in understanding the specifics of the topic: different experts within the same organization characterized the same systems differently. Moreover, the existence and extensive diffusion of external industry platforms has been questioned by some experts. One can argue that the dependency to external platforms is rare, because organizations hesitate to outsource business-critical resources or functions. However, the utilization of intangible resources, e.g., technological or managerial knowledge (Teece et al., 2008) or tangible IT resources, i.e., software, and data (Dreyfus & Iyer, 2008) coming from outside the enterprise boundaries is more common. Organizations of different sizes, for example, allow the use of external platforms for non-critical activities or as complementary solutions. For example, the use of social media platforms for boarding ticket distribution by airline companies, where, e.g., Facebook’s Messenger app is one option among other distribution channels (e.g. email, SMS etc.). In our work, we denote the integrations with external industry platforms as a contemporary, emerging service model.

Table 11. Publication I findings embedded in the literature.

<table>
<thead>
<tr>
<th></th>
<th>IT outsourcing Externally managed</th>
<th>Cloud computing Externally developed</th>
<th>Shared external platforms</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Decision</strong></td>
<td>Vendor selection prior to decision on degree of outsourcing. Top management as decision makers.</td>
<td>Vendor selection bound to product selection. SaaS by business department, IaaS/PaaS by IT department.</td>
<td>The platform is valuable, rare, inimitable and non-substitutable enough to represent nearly the only smart choice. Top management as decision makers.</td>
</tr>
<tr>
<td><strong>Asset specificity</strong></td>
<td>Custom-tailored IT services, may include software development, datacenter or desktop maintenance, help desk.</td>
<td>Standardized software (SaaS) or cloud infrastructure (IaaS/PaaS).</td>
<td>Standardized, dynamic platform offering with volatile boundary resources (APIs, SDK, contracts).</td>
</tr>
<tr>
<td><strong>Customizability</strong></td>
<td>Individually negotiated configurations.</td>
<td>At a minimum, some limited user-specific application configuration settings.</td>
<td>Non-existent configurational tuning capability at none of the OSI stack layers.</td>
</tr>
<tr>
<td><strong>User-to-system utilization cardinality</strong></td>
<td>One-to-one relationship between user-organizations and individual system instance, i.e., each user-organization has exclusive access to its own instance.</td>
<td>Non-existent configurational tuning capability at none of the OSI stack layers.</td>
<td></td>
</tr>
<tr>
<td><strong>Externally deployed</strong></td>
<td>Outside or in-premises.</td>
<td>Usually outside, broad network access and dependence.</td>
<td>Outside.</td>
</tr>
<tr>
<td><strong>Ownership</strong></td>
<td>Varies with the type of outsourcing.</td>
<td>Ownership of the data stored on the service provider’s system and the rights to get it back usually belong to the customer.</td>
<td>The platform, its derivatives and sometimes even the associated data are owned by the provider.</td>
</tr>
<tr>
<td><strong>Contractual mode</strong></td>
<td>Usually long-term strategic partnerships preferred.</td>
<td>Standardized terms of use.</td>
<td>Non-negotiable SLAs, strategic decisions on platform development or service discontinuity, interfaces availability are made by the provider.</td>
</tr>
<tr>
<td><strong>Substitutability or abandonment options (Saya et al., 2010)</strong></td>
<td>Moderate to high number of alternatives. Outsourcing market is well established with numerous experienced providers.</td>
<td>Moderate to high number of alternatives. Volatile and immature market.</td>
<td>Number of alternatives is non-existent or extremely limited. Market in its nascent stage, uncertain legal issues.</td>
</tr>
<tr>
<td><strong>Examples</strong></td>
<td>Software development subcontractors.</td>
<td>SaaS, e.g., Salesforce. PaaS, e.g., Microsoft Azure. IaaS, e.g., Amazon Elastic Cloud.</td>
<td>e.g. CRM integration with Facebook, Google AdWords in marketing business.</td>
</tr>
</tbody>
</table>
Figure 4. Network view of codes from Atlas.ti, Publication I.
5.2 Publication II: Love and Hate Relationships in a Platform Ecosystem: A case of Finnish Electronic Identity Management

5.2.1 Research objectives

This objective of this publication is to provide observations on the implications of dependencies. The lack of in-depth studies tackling organizations’ dependencies on external platforms and infrastructures indicates an insufficient understanding of this phenomenon, consequently making it an important research direction. The following research questions were formed: *How do the changes in the platform ecosystem affect non-focal firms? How can the non-focal actor's relations towards the dominating platform be characterized?* To answer these questions, we engaged in a case study of seven Finnish organizations that utilized the BankID platform and their views on the changes. Using the interviews with the non-focal Finnish firms, we describe the platform ecosystem transformation concerning organizational and technology aspects. The empirical analysis of this publication is based on the same 24 interviews used in *Publication I*.

5.2.2 Results

In this publication, we illustrated how the changes took place in a platform ecosystem in the context of an IdM platform decline. This publication is considered to be the first introduction of the Finnish IdM story which was the central case study in this thesis. This publication illustrates how the EU eIDAS regulation N°910/2014 on electronic identification and trust services influenced the ecosystem architecture, and affected the roles, relations and power structures of the incumbent ecosystem participants.

The results can be seen as a compilation of both technology-centric and social aspects of the platform ecosystem transformation. These views were compared in the light of changes concerning how the eID services in Finland operated before and after the regulation came into force. The first two themes belong to the platform and its focal role in the ecosystem, which has a great influence on the ecosystem development. The next three themes cover non-focal firms’ resisting and accommodating attitudes towards the dominating platform, especially the reconfiguration of their roles and relations along with the power redistribution between ecosystem participants caused by the legislation change. The themes are discussed below.

- **Internal to external platform evolution.** In this theme, we find that Gawer and Cusumano’s (2014) distinctions between internal and external platform do not fit the case of the Tupas platform as it is internal and external at the same time. Banks first established the Tupas platform for their internal use, and consequently they opened it to other heterogeneous actors. Thus, this case serves as an example of a platform that was used first by the banks only, i.e., it was internal, and it evolved and became part of other firms’ infrastructure, i.e. external.

- **From dominance to deterioration.** The success and sustained dominance of the Tupas platform was contingent on the resources they possessed (i.e., their customer base), which is valuable and hard to imitate (Barney, 1991). The Tupas case exemplifies how governmental endorsement contributed to the authentication platform’s sustained dominance and how the regulation changes in the ecosystem recursively lead to the platform’s deterioration. The lesson learned from this theme is that the platform orchestrators must manage the delicate balance of generativity and control in the platform (Yoo et al., 2012). Banks in Finland exercised too much control over the Tupas platform, with the risk of driving out third-party developers, thus possibly preventing the generativity of the platform.
• **Resistance and accommodation.** The definition of co-opetition (Nalebuff & Brandenburger, 1997) is “competing without having to kill the opposition and cooperating without having to ignore self-interest”. A coopetitive attitude towards the platform was observed among firms that owned a competitive authentication method (FINEID, MobileID). We could also observe the acquiescence, i.e., reluctant acceptance of the platform dominance among smaller organizations. The views of non-focal organizations interviewed were complex and came to some degree with a negative perception of the platform owners’ dominance and the forced utilization of the platform. This theme points that the concept of the actors’ interest in the ecosystem’s health and prosperity (Selander et al., 2013) may not always be true. Such relations towards the dominating platform can occur when the platform becomes “the only choice”.

• **Power distribution.** This theme is about how regulation can disrupt the roles of actors and disseminate the cumulative power of platform ecosystems. In the Tupas case, the banks still own the platform, but have been forced to open access to it to service brokers. That is to say, that the cumulative power in the ecosystem is the same, but due to changes in regulation it is more distributed among actors. The banks’ position has been weakened while service brokers have gained more control.

• **Roles and relations reconfiguration.** This theme refers to how regulation can affect the roles of ecosystem participants — the introduction of the service broker role to the ecosystem affected the Tupas ecosystem organizations. Relations between firms are not always linear; firms may be partners in one market and competitors in another. One example is company A (telecommunication provider) which had a service broker firm that managed technical integrations, and after the eIDAS took place — from having partnership relations they became direct competitors.

5.2.3 **Relation to the whole**

The theoretical framing of this publication is associated with the previous *Publication I*. While narrowing down the focus to a specific case, *Publication I* sets off with the perspective of a non-focal role in a platform ecosystem. This article also introduces more extensive considerations of the relations between the platform and infrastructure concepts. This discourse is a stepping-stone to the consecutive *Publication III*, which was an invited submission based on the results of *Publication II*.

The contribution of this publication can be seen as the compilation of initial research results, which are then analyzed in greater detail in the consecutive *Publications III and IV*. *Publication III* continues the discussion on (1) internal to external platform evolution as well as the theme (2) from dominance to deterioration. *Publication IV* examines the themes (3) resistance and accommodation, (4) power distribution and (5) roles and relations reconfiguration.
5.3 Publication III: From platform dominance to weakened ownership: How external regulation changed Finnish eID

5.3.1 Research objectives

The main objective of this publication is to investigate the post-dominance phase of the dominant platform — a nation-wide platform with the primary focus on the latest phase of its evolution. The research question was: how does the dominant platform respond to external regulation? The case study used real-time observations for a year and a half and 31 interviews in the period from 2016 to 2018. The interviews constituted 24 interviews used in Publication II and an additional 7 interviews. A retrospective approach was taken by examining public documentation related to the case, such as government reports, case studies, and reports from news media and organizational archives found online. The secondary data comprises 24 specification items and reports, 16 news articles, 10 blog posts and 2 documented case studies.

5.3.2 Results

The main result of this publication is the theorizing of what happens to defeated external platforms. We find that the introduction of intermediaries between the platform and its users contributes to a weakening of the dominant platform owners. Here, it is important to re-introduce the conceptualizations of Kazan et al. (2018) on strategic dimensions of value creation and value delivery architecture, to discuss the architecture of the Tupas ecosystem before and after undergoing regulatory changes.

Value creation architectures (VCAs) are modular components of a digital platform that can be exploited by third parties to develop value added derivatives (Kazan et al., 2018), which is the “service” layer in the Finnish BankID architecture in which third party platform users, service providers and end-users together with service brokers integrate with the platform via boundary resources to create value-added services. Value delivery architectures (VDAs) are defined as omnipresent digital infrastructures that operate as technological backbones of value networks to facilitate the efficient delivery of standardized platform derivatives among stakeholders belonging to the same value network (Kazan et al., 2018). In Tupas, this layer includes the entire process of customer onboarding, i.e., bank account opening, first-time identification as part of know your customer (KYC) requirements, as well as distribution and maintenance of Internet banking identifiers. Prior to the eIDAS and FTN regulation changes, these two strategic dimensions of VCA and VDA were closely imbricated, i.e., they overlapped.

In their original case examining mobile payments (Kazan et al. 2018), VDAs, such as MasterCard or VISA, were exemplified as established payment infrastructures, which power the processing of financial transactions. Likewise, the VCA dimension includes the interaction between payers and payees to make payments together with the provision of boundary resources, such as APIs and SDKs. In other words, the banks in the Finnish IdM were in charge of the platform ecosystem orchestration by coordinating the eID service creation and delivery, i.e., they had exclusive control over the entire value chain.

Figure 5 illustrates the Finnish BankID ecosystem after the change, which has disintegrated the VCA & VDA architectures. This happened due to entity layering, i.e., the introductions of external orchestrators and service brokers around the platform. Thus, the Finnish BankID platform seems to more vividly exhibit the strategic dimension of value delivery architecture, i.e., the infrastructure level that functions as a pipeline to deliver value in a standardized...
format. Its value creation architecture dimension is then the layer where the service brokers are entitled to exploit the modularity and create value-added derivatives by re-configuring the resource. This is possible due to legally enforced access to a critical national infrastructure.

The Finnish regulation (FTN), which was altered to be compatible with broader EU requirements (eIDAS), changed the principles of electronic identification by adding a layer of service brokers into the scheme of the eID, thereby driving the transformation of the platform into an industry infrastructure. Such entity-layering, i.e., the introduction of intermediaries between the platform and its users and external orchestrators on top of platform owners, can be seen as a pervasive phenomenon among dominant platforms that fail to anticipate ecosystem needs and adapt, pushing them to act as the backbone and enabler for the ecosystem. The finding that platforms can transform into industry infrastructures has an important implication for our understanding of the dynamics underlying digital platforms.

5.3.3 Relation to the whole

This publication constitutes one of the central contributions of this thesis. Here, we explicate the platform evolution process, from a phase of dominance with centralized control structures to a more federated governance approach. This publication was invited as a revised extension of Publication II. While the findings sections of the two publications are based on the same information, Publication III includes a deeper analysis of the platform-to-infrastructure evolution phenomenon together with better theoretical framing. The data in this publication was analyzed through a process theory lens. A more detailed description of the differences between the manuscripts and their data analysis phases can be found in the “Data collection and Analysis” section of Publication III.
5.4 Publication IV: Explaining an eID Framework Implementation using Dialectics

5.4.1 Research objectives

The main objective of this article is to understand the internal conflicts and contradictions among the actors involved in the transformation of a nation-wide IdM infrastructure. In this article, we describe the governmental effort to diminish the role of the banks in the Finnish eID ecosystem. In order to answer this question, we break it down into a dialectic between opposing views on the eID infrastructure, with the government and regulators representing the thesis, and banks the antithesis.

- **Thesis**: The government should fully control the eID infrastructure.
- **Antithesis**: The market is the best guarantor for a cheap and reliable eID infrastructure.

Dialectical process research seeks to explain how dialogue and confrontation emerges, develops, and diminishes over time. In a dialectical process model (Van de Ven and Poole, 1995) the process can result in four different outcomes: synthesis, pluralism, thesis or antithesis. An outcome may lead to another contradicting antithesis that sets off another dialectical process. We chose a qualitative case study approach for this study (Yin, 2011). We use the abductive approach with the dialectics lens in mind and the data analysis was based on grounded theory (Strauss and Corbin, 1990). Semi-structured interviews (Yin, 2011) with eleven experts on the Finnish eID ecosystem were conducted and the total interview time was 9 hours 45 minutes. In addition to collecting different views from banks, government, and independent organizations, we collected secondary data from government reports, press releases, reports and news found online.

5.4.2 Results

The main findings of this publication is the dialectical process model explaining the root cause and effects of the challenges in the Finnish eID transformation (Figure 6).

![Figure 6. Main dialectical process model.](image_url)

The root cause of the problems with the FTN arose from the conflicting goals of the government and the banks; that is, the regulators’ interest in creating more competition in the market, to achieve cost savings, and to reduce the dependence on banks vs. the objectives of the banks to maintain the status quo. The dual role of the BankID as a proprietary platform and a national eID infrastructure also contributes to the conflict. The framework implementation practices, such as the hard enforcement strategy, inherent infrastructuring mindset and communication...
problems, considerably contributed to further conflict development. Divergent views on the framework architecture and the pricing models are the outcomes of the confrontation. The thesis and antithesis consist of two contradictory assumptions and goals. The government employed regulatory mechanisms to achieve their goals and encountered resistance from the banks. The two sides engaged in a dialogue on budgetary, business and technological aspects. Three procurement rounds led to a synthesis, which appears to be temporary, while the pluralism of opposing views dominates.

Overall, this publication answers the question on the reasons for the difficulties in implementing changes in the Finnish IdM system. Our theoretical contribution is a nuanced understanding of how the dialectics played out in the transformation process. While the dialectical situation in Finland will change over time, the thesis and antithesis on whether the government or private sector should fully control the eID infrastructure will remain. In other words, considering the dialectical elements on legitimacy (goals and power to regulate) as a constant, changing variables on the implementation practice (communication, power and an infrastructuring attitude) and solution features (architecture and pricing model) could result in different outcomes. This study forms a base case for future research on digital infrastructure evolution as a result of dialectical dynamics in public-private sector relationships.

5.4.3 Relation to the whole

This publication is a third integral part of the contribution to the Finnish IdM case in phase 2 of the research. While Publication II is an introductory description of the case from the non-focal perspective, Publication III is a more conceptually developed theorizing of the case, Publication IV can be considered a follow-up and progress update on the case together with a root-cause analysis. The findings of this publication serve as the motivation for the study in Publication V, in which the alternatives of BankID infrastructure development are studied. This publication also concludes the narrow scope phase of the research before proceeding to the wider part of the funnel, i.e., “zooming out” on the scope of the research.
5.5 Publication V: Blockchain-Based Electronic Identification: A Cross-Country Comparison of Six Design Choices

5.5.1 Research objectives

The objective of this research was to make a cross-country comparison of IdM approaches. The majority of traditional examples of eID initiatives from the literature have relied on centralized or federated architectures, in line with the technological development of their time. With the introduction of distributed ledger technology (DLT), decentralized alternatives are currently becoming increasingly technologically feasible and interesting. The research question that this study aimed to answer was what advantages does blockchain bring to eID compared with previous designs? The study was conducted through a comparative case study of three eID initiatives in Sweden, Finland and Taiwan. The method applied in the study was a comparative qualitative interpretative case study using primary and secondary data sources with 11 interviews and secondary documents. While the research question features the notion of blockchain as a central concept, the goal of this publication was to compare the Finnish IdM story with the approach in neighboring Sweden. The Taiwanese example, which had the objective of replicating the success story of the BankID system as a national IdM infrastructure, added an interesting contrast. We searched for indications of benefits, tensions and solution peculiarities in six dimensions of comparison between the Finnish and Swedish eID implementations.

5.5.2 Results

The main result of this publication is that within the design space of IdM implementations, several different configurations and design choices are possible. These architectural variations reveal different strategies to managing the tensions and conflicts. In the comparison of Finland and Sweden the following aspects were noted:

Solution architecture. Swedish BankID is a PKI infrastructure implementation, a technology based on asymmetric cryptography that involves the use of two different keys for encrypting and decrypting data. While a consortium of banks governs the Swedish BankID infrastructure, Finnish banks run their Tupas implementations separately.

Tensions. PKI implementation involves a costly operational burden across the full life cycle of certificates. Symmetric key encryption is used in the Finnish BankID system, which is simpler to administer because there is no need to maintain the CRL infrastructure between multiple banks. The problem with the latter implementation is that the banks act as independent certificate authorities and do not accept each other’s keys, which prevents the reuse of certificates.

Data control. In both cases, personal data is revealed with the users’ consent only. However, personally identifiable data is limited and includes the users’ social security number and name, which are shared with the relying party along with the digital certificate. Thus, only limited personal information can be shared, and the identifiers cannot be reused outside the ecosystem.

Tensions. In addition to the lack of selective disclosure, banks act as central authorities that “own” and control that data.

Initial identification. The very first step of acquiring an eID is the initial registration process, namely binding the digital identifier with the real legal entity or natural person. Normally, this requires the user to visit a designated government registration authority (RA), such as the police office or a bank branch office, where the applicant’s personal details are collected, and
their identity is verified. As banks become digital and have fewer offices this creates difficulties for BankID providers and entry barriers to newcomers.

**Tensions.** Countries worldwide may differ in their legal requirements, but universally, the initial identity verification process is concerned with linking the physical entity with the digital identifier, which requires a physical presence or must be done remotely with the help of software. The main distinction of bank-procured eID solutions is that the identity verification processes are regulated by law. One-time identity verification removes the need for consecutive visits to bank offices and enables not only online banking but also the use of identifiers in e-government and ecommerce services.

**eID chaining.** In order to create more competition in the market, Finland has mandated eID chaining, i.e., creation of new eIDs based on existing ones. The process is considered to subsidize newcomers and is not allowed with the Swedish BankID.

**Tensions.** The chaining of identifiers is a powerful way to overcome the challenge of onboarding and bootstrap user identities. However, some important issues arise from the chaining, including the threats of identity theft and questions concerning responsibility. If business negotiations permit, chaining could also help to expand the user base, include various customer groups and reduce exclusion.

**Ecosystem architecture.** The Finnish ecosystem and its changes have been described in detail in two previous publications. These measures were aimed at increasing the competition as well as boosting the innovation in the market. Three optional systems cover the need for eID in the public sector in Sweden, where the arrangements provide a comprehensive supply of well-established and new eIDs in public sector e-services that do not prevent any existing solutions, but rather create opportunities for the use of existing as well as future eID solutions. The price for eID transactions involving BankID in Sweden and Finland is 0.017 EUR and 0.1 EUR accordingly.

**Tensions.** In both cases, the BankID method is used as the main identification device in the G2C and G2B use cases, which creates the need for governments to regulate the infrastructures. However, the governments’ involvement in regulating market-procured eID solutions differs significantly.

**Strategy.** The governments in both countries understand the limitations of relying on an almost monopoly of bank-provided solutions. The Finnish government conveys a clear message that the BankID solution has become too expensive for the use in public services, which is why strategies to change the de facto role of the BankID were created, and state agencies are exploring alternatives for citizens’ eID (see Publication V for more details). However, Sweden’s approach to stimulating the market differs. A distinct example is the recent proposal on the police and banks collaborating in the process of the initial identification.

**Tensions.** One explanation of cooperative and non-cooperative practices could be the maturity stages of the two solutions; i.e., in Finland the banks could not achieve the same close collaboration and a common infrastructure that the banks have in Sweden. There is also less distance and more understanding between the BankID providers and regulators in Sweden than in Finland.

**Publication V** further explains how the tensions identified in the Swedish and Finnish cases are mitigated in the design of a BankID-like solution in Taiwan.

### 5.5.3 Relation to the whole

This publication is the first result of phase 3 of the research presented in this thesis. The previous results presented in Publication II, III and IV constitute a detailed analysis of the Finnish IdM development case which was a narrow-focused perspective. The results presented in this Publication V contribute to the broader view on the development of the IdM infrastructure. It includes a description of alternative IdM infrastructure implementations in contrast with the Finnish case. While the title and the research question feature the concept of
blockchain, the contribution of this publication is of a more generic nature, i.e., a configuration model of design choices. This opens up interesting avenues of interpretation and future research, for example, whether there is a causal hierarchy of factors in the underlying model of analysis. The results of this Publication V influenced the research motivation and objectives of Publication VI, where we take an even broader perspective on IdM infrastructure implementations.
5.6 Publication VI: The Review of Non-Technical Assumptions in Digital Identity Architectures.

5.6.1 Research objectives

In this publication, we investigate the current state of IdM research and elicit implicit architectural assumptions in the proposed designs. The motivation is that the solutions that span organizational boundaries usually require changes of various degrees that involve coordinating multiple actors. These inter-organizational aspects range from infrastructural, system-level integrations, to higher-level strategic, business, liability aspects and trust. The research question is what are the non-technical assumptions in the proposed solutions? A systematic literature review was performed by following the guidelines for conducting literature reviews in software engineering. The search was conducted in five databases: IEEE Xplorer, ACM Digital Library, Web of Science, Scopus and the AIS eLibrary. The search string used was as follows: ((digital OR electronic OR online OR federated OR self-sovereign OR user-managed) AND identity architecture).

5.6.2 Results

The analysis of 62 digital identity designs from the literature resulted in the following dimensions. Category A — whether the solution requires a change to infrastructural components, and/or a completely new infrastructure; Category B — whether the solution implies a trusted third party (trusted intermediary, semi-trusted agents); Category C — whether the solution assumes the users are ready to take more control and responsibility over “something they have”, or requiring an increased user understanding and training. Table 12 lists the assumptions identified in the articles reviewed.

Table 12. A compilation of assumptions found in the articles reviewed, Publication VI.

<table>
<thead>
<tr>
<th>General Assumptions:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uptake and support of the solution by organizations, users and governments.</td>
</tr>
<tr>
<td>Once adopted in an e-government scenario the same technology will spread to other consumer cases (if the solution is in e-government context).</td>
</tr>
<tr>
<td>Easy and cost-efficient distribution of tokens (if solution implies tokens).</td>
</tr>
<tr>
<td>The process of digital identity provisioning is optimized.</td>
</tr>
<tr>
<td>Necessary inter-organizational collaborations are achievable.</td>
</tr>
<tr>
<td>Sustainable business models exist; new model brings cost savings.</td>
</tr>
<tr>
<td>A: Relation to Legacy Infrastructures:</td>
</tr>
<tr>
<td>It is trivial to make integrations with, e.g., IDPs and RPs.</td>
</tr>
<tr>
<td>Scalability is achievable.</td>
</tr>
<tr>
<td>The proposed governance structure is feasible.</td>
</tr>
<tr>
<td>B: Trusted Institution:</td>
</tr>
<tr>
<td>A Trusted third party (TTP) can be trusted (e.g.,unlinkability of identities is guaranteed, key recovery not possible). TTPs are the intermediary institutions, except for the identity provider, such as manufacturers of secure hardware (e.g., trusted platform module (TPM), trusted execution environment (TEE), metadata proxies and other agents.</td>
</tr>
<tr>
<td>C: Human-User’s Responsibility:</td>
</tr>
<tr>
<td>Users understand the importance of not compromising the security.</td>
</tr>
<tr>
<td>Users would like to use their smartphones as security tokens.</td>
</tr>
<tr>
<td>Smartphones are secure.</td>
</tr>
<tr>
<td>Users vouch that no one else has access to their tokens.</td>
</tr>
</tbody>
</table>

General assumptions, i.e., not IdM-specific, that were extracted varied from having no discussions on the potential actors involved and their motivations in participating, to those that propose involving new agencies that are close to the user, such as insurance companies, banks, postal offices and local shops for identity provisioning. A viable economic model and considerations of the incentives for the participation are crucial in attracting the private sector.
In relation to existing IdM infrastructures (A), articles can be grouped into those proposing changes of various degrees in legacy infrastructures, such as improvements of PKI, or mechanisms for managing untrusted IDPs such as Google, Facebook, etc. Others propose that there is a need for completely new infrastructures, such as private or public blockchains. Even though, ultimately, the “winner” models should be integrated into existing infrastructures without significant changes, integration efforts and their complexity are addressed explicitly in only a few articles.

Articles that belong to dimension (B) are based on one or more trust anchors that can be intermediaries that operate federation metadata, proxies, trusted hardware providers or personal data store agents. A trusted third party is an institution that facilities the process; or operates a software service that manages things on behalf of the user (e.g., Dropbox, and Google Drive are used as personal data stores). Given the involvement of a TTP in an IdM scheme, complex governance techniques, including standards, best practices, and auditing must be managed. Building and operating TTPs is also costly and TTPs are subject to liabilities. Nevertheless, articles especially within the e-governmental context stress the need for operating a governmental TTP.

At the other end of trust-in-institution spectrum, there is (C) human-users’ readiness and/or willingness to take responsibility over their digital identity. Here, we refer to designs where, for example, smartphones would be central to the operation of credential wallets (IdM mobile applications); hardware modules or physical eID cards would be used for storing and accessing sensitive cryptographic key material and other private data that users must keep secure. Advocacy for full human-user control essentially requires users to understand the importance of safekeeping the keys or managing backups.

The findings show that solution designs can be based on trust in an institution or based on human-user responsibility along with assumptions on infrastructural deployability. These assumptions have various implications, and, more importantly, they manifest the research gap. For instance, the concept of human-user’s readiness to take responsibility involves more than user experience; and the role of various institutions and businesses in IdM is not entirely understood.

5.6.3 Relation to the whole

The results of Publication V inspired the framing for Publication VI. Overall, we were interested in identifying the fundamental issues potentially inhibiting the establishment of large-scale IdM systems. This study shows that at the high abstraction level, in order to achieve a well-functioning IdM system, human subjects must either trust in institutions such as IdPs, stewards or operators, or they must take more control, and consequently, they must take responsibility over their digital identities.
5.7 Summary of results

Publication I is an introduction to the topic of platforms and infrastructures and is based on the interviews with all participating organizations that were available at the beginning of the study. The main result of Publication I is a discussion on the understanding and the role of external industry platforms, where the Finnish IdM platform was identified as one of the cases. Publication II delves deeper into the case and provides an umbrella view on the case while still connecting the non-focal theoretical perspective to the empirical case. Publication III, as a more mature revision of Publication II, provides a theoretical discussion on the relation between industry platforms and infrastructures. While Publication IV explains the further development of the Finnish IdM case and performs a root-cause analysis of the events, Publication V offers a broader outlook on the case with a cross-comparison with the approaches of IdM governance from Sweden and a blockchain-based initiative in Taiwan. Publication VI takes an even broader perspective on the IdM infrastructure case and identifies the factors important to take in consideration when developing and managing the large-scale nationwide IdM infrastructures.
6. Discussion and implications

This chapter discusses and summarizes the main contributions of this thesis. The answer to the four research sub-questions can be summarized as the following:

- **RQ 1**: What are the characteristics of dependency on a dominant digital infrastructure?
  
  **Answer**: Although there exist variances in the understanding of what external platforms and infrastructures are, non-focal organizations are careful in integrating with them and creating dependencies they cannot control. The need for such integrations happens when the number of reasonable platform choices in the market falls to just one or only a few, then the only reasonable choice becomes the de facto standard.

- **RQ 2**: How are dominant digital infrastructures transformed?
  
  **Answer**: Dominant industry platforms may evolve into industry infrastructures through entity-layering, which means the introduction of intermediaries between the platform and its users and/or additional external orchestrators along with platform owners. This evolution scenario can be seen as inevitable for dominant platforms that fail to anticipate ecosystem needs and adapt, pushing such platforms to act as the backbone and enabler for the ecosystem.

- **RQ 3**: What are the important factors in the governance of dominant IdM infrastructures?
  
  **Answer**: Firstly, IdM infrastructures become dominant when successful public-private sectors cooperation is accomplished. Second, in order to achieve mutual benefits in such ventures, openness in the dialogue of the involved parties and a strong (neutral) leader organization to coordinate the actors within the groups and across the ecosystem are essential.

- **RQ 4**: What are the architecturally significant aspects in the development of IdM infrastructures?
  
  **Answer**: The key design choice categories that affect the development of dominant IdM infrastructure are: the technology choice, the identity provision process, human-user integration, the choice of providers and business model, the governance structure (as in the level of public-private cooperation) and the strategy for handling relations with the digital heritage (i.e., existing eID methods).

The model below (Figure 7) presents four areas of contributions in line with the overall theoretical approach taken in this thesis. Specifically, it helps to unpack the infrastructural change process of Finnish BankID in terms of its installed base factors: the specifics of its dominance position built over the years and the dominant platform’s transformation into industry infrastructure; governance factors: strategies of platform owners and levels of cooperation among public and private actors; and architectural factors: key design choices that affect the success of IdM infrastructure development.
The chapter includes further discussions and covers implications for practice.

6.1 The dependence upon a dominant digital infrastructure

The first goal of the study presented in this thesis was to understand the characteristics of relying on dominant digital infrastructures. RQ 1 “What are the characteristics of dependency on a dominant digital infrastructure?” was answered in Publication I by investigating practitioners’ understanding of their dependence on external digital platforms and in Publication II describing the implications of such relations.

An interesting theoretical framing of the issue was recently proposed by Rolland et al. (2018) in which they also investigated digital platform-based innovation from a user-organization perspective. In their 17-year longitudinal study, the authors theorize the progression between digital options (i.e., the capabilities that digital platforms bring) and digital debt (i.e., a cumulative buildup of technical and informational obligations) during an organization’s digital platform management in relation to its infrastructure and work processes (Rolland et al., 2018). Similarly to our views, the authors start with the observation that the literature on digital platforms is predominantly owner-centric and has not addressed the interdependence between dominant digital platforms and their role in the digital infrastructure of user-organizations.

The use of the digital options concept is particularly well-suited when analyzing the integrations with external platforms as it refers to an organization’s continuous capability search and redeem (Selander et al., 2013) that generate new value (Svahn et al. 2015). A set of actionable digital options represent desirable and feasible IT capability investments that address relevant business opportunities (Sandberg et al., 2014). For the purpose of discussion, we adopt the extended definition of digital debt from (Kruchten et al., 2012; Rolland et al., 2018) as “a buildup of technical and informational obligations that affect a platform’s maintenance and evolvability as part of a user organization’s digital infrastructure”. This definition is an appropriation of the concept of technical debt which has been studied extensively in software engineering (Kruchten et al., 2012; Yli-Huumo et al., 2016). While the technical debt in software is usually studied mostly at the code level, in this research we are concerned with a broader enterprise-wide view of technical debt.
The results of our study indicate that organizations are careful in accumulating a digital debt. The mental model of managers in companies we interviewed may be seen as trying to avoid dependencies they cannot control, preserve power integrity, gain more power, and secure their position by carefully establishing alliance relationships.

The adoption of and integration with global platforms can be seen as similar to the cloud computing service model in the IT industry (Xin & Levina, 2008). External platform utilization, as well as cloud service adoption or outsourcing, is a means to manage complexity. Similarly, in another study about the motivations in outsourcing of small and medium sized organizations in Finland, the researchers found that companies that mainly acquire external expertise outsource only a limited number of processes within a specific business function (Asatiani et al., 2019). Likewise, exceptional cases that were identified in our case companies arose when established companies allowed the use of external platforms for non-critical activities or as complementary solutions. For example, the use of social media platforms for the distribution of boarding tickets by airline companies where, e.g., Facebook’s Messenger application was listed as one option among other distribution channels (e.g. email, SMS etc.). Rolland et al. (2018) theorize that such hesitancy may at times prevent organizations from realizing otherwise attractive digital options.

Another study by (Penttinen et al., 2018) further investigates the uncharted territory of platforms utilization. The authors examined platform features that firms value the most when selecting between competing platforms and what factors influence this choice in the context of business-to-business (B2B) integrations. Their findings reveal that companies seek user-friendly platforms through which they can reach a sufficiently high number of users; and service customization features (defined as “the nature, scope, and tone of interactions between vendor and buyer of the platform when the platform is adopted and used”) have low importance for both small and large companies (Penttinen et al., 2018). The study (ibid.) was about the selection of e-invoicing connectivity platforms, and it is important to note that there exists a multitude of e-invoicing platform providers. The difference between making traditional IS selection decisions compared to the use of capabilities offered by dominant external platforms is the switching cost and the speed of “how things might go wrong” that can be very abrupt in a dominant platform scenario. In this thesis, we find that firms of various sizes and across sectors exhibit an attitude of resistance and accommodation (“love and hate”) towards the one dominating platform we identified, which was the Finnish BankID platform. Therefore, we hypothesize as part of future research that the distribution of the importance of platform features that firms value the most when selecting between competing platforms would be different for platforms that offer a unique capability.

Nonetheless, the literature on non-focal actors, while far less dense than the platform owner perspective, is slowly gaining more attention (Schreieck et al., 2016). In the industry world there are an increasing number of projects aiming to “fix” the problem of having to rely on global industry providers. One of the examples is the company Dfinity, whose goal is to create a completely “new Internet”, by building an open, decentralized system as a replacement for today’s Internet. The founders of the project advocate for the need of a complete replacement of the current global IT stack because organizations rely on data or other resources from global platforms and infrastructures that are dominated by a few large technology firms such as Google, Amazon, Facebook, LinkedIn (Hanke et al., 2018). Dfinity founders often refer to the
example of Zynga⁴ — a social gaming company that suffered major setbacks in 2012 after Facebook changed its policies concerning third-party complementors. Another example, is SalesforceIQ (formerly RelateIQ) that used various LinkedIn APIs⁵ that were then changed, leading to the company being acquired by Salesforce. Dfinity’s goal is to create a Web 3.0 where the organizations of various sizes are not at the risk “that crucial components of their infrastructure will suddenly change” (Miller, 2019). On the other hand, while projects like Dfinity seem to be part of the race to build “the best blockchain” with decentralized control, the important point is that while the modern platforms and infrastructure service offerings are becoming increasingly monopolized, startups and industry are searching for new innovative solutions to the problem. As the dependence on platforms and infrastructures is mostly an unexplored area from an academic perspective, there is a need for more studies, especially of real-life cases of failure and success.

6.2 The infrastructure transformation: Case of IdM in Finland

The second goal of the study presented in this thesis was to examine the process of dominant digital infrastructure transformation. While Publication II only scratched the surface of the topic, RQ 2 “How are dominant digital infrastructures transformed?” was answered primarily in Publication III by analyzing the Finnish IdM platform change implications at the ecosystem level.

Similar to the need for creating a “new Internet” mentioned above, there exists another inherent architectural flaw — the Internet as we know it was created without the identity layer. With the aim of creating a universally trusted digital identity system, decades of research has built a solid body of knowledge on various architectural designs, cryptographic foundations, and functioning, yet, disconnected infrastructures. Modern eID infrastructures offered by providers from both public and private sectors can be seen as partial remedies. The Finnish IdM ecosystem forms a unique case to describe the platform’s wide adoption followed by nationwide expansion, which then weakens its position. The success and sustained dominance of the Tupas eID method was contingent on the resources possessed by the banks, such as the customer base, which is valuable and hard to imitate (Barney, 1991). Their competitive advantage is also based on large volumes of transaction data and inherent trust from customers. While the case has been mostly studied in the light of a legislative mechanism of change, the regulatory change triggered a set of system-wide modifications. The affected dimensions were business model modifications such as the pricing model, as well as system level changes in technical protocols, infrastructural configurations and organizational relationships. Moreover, the case illustrates an ideal example of an entire platform ecosystem transformation that was possible to study at full length.

Our findings theorize the metamorphic change in nature of a dominant digital platform into an industry (backbone) infrastructure. Comparing ecosystem architectures, we observe that the Finnish BankID platform experienced the process of “infrastructuring”. Constantinides, Henfridsson & Parker (2018) refer to infrastructuring as making digital platforms more “physical”, while expanding their reach and scope into supply chain management. They provide the example of Amazon’s purchase of the Whole Foods supermarket chain as a strategy

---

⁵ https://www.zdnet.com/article/linkedinout-crm-companies-squawk-over-linkedins-api-policies/
to move into supply-chain management and distribution with its Amazon Prime service and Amazon-Fresh unit, while expanding the company’s digital platform strategy. Here, the authors refer to “positive infrastructuring” as a strategy for companies to acquire more control and push for more innovation. Another example is a study of Stockholm’s digital infrastructure for public transportation that established a positive (successful) infrastructure growth case (Koutsikouri et al., 2018). The authors (ibid) explicate the typology of four growth tactics, such as adding services, inventing processes, opening identifiers, and providing interfaces, as a means of adaptation to a changing environment and requirements.

Asymmetrically, the evolution of the Finnish BankID platform into an industry infrastructure could be understood as becoming both the backbone and the back-office. We regard this “negative infrastructuring” as a phenomenon that arises due to entity layering (i.e., the introduction of intermediaries between the platform and its users and/or external orchestrators along with platform owners) as a platform evolution mechanism. The former perspective on positive infrastructuring is in accordance with Constantinides et al. (2018) who argue that the infrastructuring concept implies strengthening the role of the platform, and that dependence on the BankID as an eID method is still strong throughout the industry. In the latter perspective, there is a risk to banks that new competitors will consign them to a limited role as back-office utilities, while non-banks become “the new face of their customers’ financial lives” (Busch & Moreno, 2014). In line with de Reuver, Sorensen & Basole (2017), this thesis also empirically observes that it is the control arrangement that sets digital platforms apart from digital infrastructures.

Teece (2017) argue in their study on digital platform evolution that platforms go through four lifecycle stages: birth, expansion, leadership and self-renewal. In general, we commit to this perspective of development through lifecycle phases. The Finnish BankID case reveals that the self-renewal stage implies a major transformation. Self-renewal could also indicate a shift in decision-making ownership, for example, from being a platform to becoming an infrastructure. We expand the platform lifecycle model (Teece, 2017) by proposing that a platform that does not develop the ability to pursue new businesses while protecting their existing advantages and revenue sources (O’Reilly III & Tushman, 2008), retire (or self-renew) by becoming the industry infrastructures. These propositions can be taken further by platform researchers, as more research into the evolution mechanisms and processes is still necessary to extend our knowledge and understanding of platforms and infrastructures as value capturing, creation and delivery architectures.

6.3 The governance of dominant IdM infrastructures

The third goal of the study presented in this thesis was to investigate the governance aspects of dominant (IdM) infrastructure development. RQ 3 “What are the important factors in the governance of dominant IdM infrastructures?” was answered in Publication IV by scrutinizing the internal motivations, conflicts and contradictions between the actors involved in the transformation of a nation-wide digital IdM infrastructure. Publication V complements the explanation by comparing the evolutionary development of the Finnish IdM with the Swedish case.

The use of a dialectical process model in Publication IV developed the understanding about the conflict roots, mechanisms that created greater conflict between the actors and the consequences. The governance aspect of the transformation was one of the main problems
contributing to the pluralism phase (i.e., different opinions) in the Finnish case. The literature has already pointed out the benefits of creating a neutral body for managing such public-private ventures (Eaton et al., 2014). Clearly, such ecosystems need a strong leading organization to coordinate the actors within the groups and across the ecosystem. As the Finnish government’s view on the case was not necessarily stable over time, there was clearly a need for a strong orchestrator who was capable of regulating the big players, defining clear rules and aligning interests. In a similar study of public-private partnerships in Denmark (Medaglia et al., 2017b), the authors emphasize that for the successful establishment of common e-government infrastructures the parties need to aim to achieve mutual benefits and overcome any legacy thinking. This entails, unsurprisingly, collaboration and openness of the involved parties to envision how they can achieve common goals.

Our findings also raise important questions related to the long-term sustainability of public-private infrastructures. In the early years of digitalization of the e-government services, when the national FineID card proved to be unsuccessful, the solution provided by the banks was a ‘lifesaver’ in Finland. With the transaction volumes growing exponentially, and the transaction fees not decreasing fast enough, the objectives and the mood of the government changed more towards changing the status quo. We observe that the need and importance of absolute control over the infrastructure may change relative to the economic dependence on the said infrastructure. While the tensions we found may indicate the lack of resilient business models in public-private partnerships (Teece, 2018), the Swedish approach to managing BankID infrastructures provides a counterexample. The involvement of the governments of Sweden and Finland in regulating market-procured eID solutions differs significantly. The legislative environments in the two countries vary according to the “tenseness” in relationships: Finland has decided to govern the ecosystem with a rigid framework (FTN) and strict organization, whereas the Swedish eID ecosystem is a result of a gradually evolving heritage built over the years. This indicates a need for future research on policy developments as well as empirical studies investigating the success factors and evolution of similar market-procured infrastructures.

In a similar manner, the Taiwanese initiative on building BankID infrastructure has chosen the coopetitive strategy rather than choosing between (less feasible) full cooperation and competition. This is also supported in the recent research within the platform literature with an increased interest in coopetition as a mode of coordination in platform settings (Adner, 2017; Basole et al., 2015). As found by Tiwana et al. (2010), this increases the complexity of market coordination activities, and puts a significant emphasis on governance. Hence, the issue of how the design choice of coopetition impacts the governance arrangements becomes relevant for future studies.

### 6.4 The architecturally significant components of IdM

The fourth goal of the study presented in this thesis was to identify architecturally significant components in the architectures of IdM infrastructures. RQ 3 “What are the architecturally significant aspects in the development of IdM infrastructures?” was answered partially, in *Publication V* with a comparison of design choices for eID solutions and, primarily, in *Publication VI* by analyzing the digital identity solution architectures from the literature and extracting their inherent non-technical assumptions. The design choices from *Publication V* were used as a basis for a typology including: solution architecture (technology choice), data
control (human-user integration), initial identification + eIDs chaining (identity provisioning), ecosystem architecture (relation to the digital heritage and the choice of providers & business model) and strategy (governance and public-private relationships). The three non-technical assumptions identified in *Publication VI* refer to human-user integration, the choice of the providers and business model and the relation to the digital heritage. Below is the synthesis of the design choice repertoire for IdM solutions as six core components.

1. **Solution architecture.** This design choice refers to the choice of the technology when designing and developing an eID solution. There exist a pluralism of user-side innovation solutions, e.g., smart cards, YubiKey (a small USB and NFC device), multifactor applications for mobile devices that keep improving continuously the usability requirements. However, regardless of choices in the customer facing technology, high-level architectures for large-scale IdM infrastructures fulfilling SCA requirements could be based on PKI, symmetric cryptography, web of trust (arguably) or currently evolving self-sovereign identity methods. Each of these design choices have their strengths as well as limitations. Inherent challenges of PKI infrastructures, which is the most widespread design, include operational and deployment issues, such as certificates issuance, recovery and revocation (Davis, 1996). Another limitation in current implementations is the lack of reusability of the certificates in ecosystems with multiple certificate authorities that do not cross-validate each other's certificates for business reasons. (Dunphy et al., 2018), for example, put forward a research agenda in this regard, to evaluate the blockchain deployability in the light of PKI challenges. Thus, the investigation on how blockchain-based eID systems can “optimally replace, integrate with or disregard principles” from existing architectures is worth pursuing (Dunphy et al., 2018).

2. **Identity provisioning.** Depending on the desired assurance levels (LoA) of identification (2015), users might be required to go through the process of initial identification at least once requiring the physical presence of the user when verifying their identity. In many IdM systems, this onboarding phase is regarded as a bottleneck, especially in highly regulated markets such as banking. There is a clear need to investigate new innovative means of user onboarding. One way to bootstrap a digital identity can be achieved by the chaining of identifiers, i.e., creating new eIDs based on existing (or legacy) methods of identification. Such an approach could solve the potential challenge of identity information locked in silos of organizations that own and control users' digital identity-related information; and to expand the reach of legal identities.

3. **Human-user integration.** End users should be in control of their digital identities, and any personally identifiable information should be revealed only with their explicit consent. In order to offer an increased amount of human-user control, digital identity wallets are thought to be as the next milestone in IdM. Although the web of trust approach, in which human-users have full control over the end-to-end interactions, provides and ensures the most security effectiveness only when used correctly, the integration of the human component is usually the weakest link in the security chain (Whitten & Tygar, 1999). While the interactions between (non tech-expert) human-users and digital artefacts can be made seamless, the fear of the unknown may potentially interfere with the solution acceptance. Especially based on modern service offerings from, e.g., Google where the illusion of human control is given to users, it is important for new self-sovereign solutions to help the users to understand the implications. Thus, the goal should be to increase transparency, make complex cryptographic solutions understandable, provide training for ordinary users and make the implications of the data ownership and control less ambiguous.

4. **The choice of providers and business models.** At the high abstraction level, in order to achieve a well-functioning IdM system, human subjects must either trust in institutions such as IDPs, stewards or operators, or take more control, and consequently, responsibility over their digital identity. Designs that are based on a TTP (excluding a trusted identity or attribute provider) have considerable implications on human-user autonomy, i.e., what is the level of trust by human-users of agents handling their personal data activities? What are the incentives for organizations to provide IdM? When governments cooperate with
businesses in the provision of national infrastructures, the challenge is to define (or create) a business case that also includes adequate funding in the long run (Klievink et al., 2016). Thus, business model formulation is central to the economic sustainability of market-procured national infrastructures (Larsson & Grönlund, 2014).

5. **Governance.** The success of any digital identity initiative depends on the user uptake, and also involves the interaction of heterogeneous groups of stakeholders: governments, public agencies and businesses. IdM infrastructures result from cooperation of various degrees that can be partnerships, competition or coopetition. Generally, cooperating at the infrastructure level while competing at the service level helps to delivery cost savings among private sector participants. Governments nowadays understand the importance of creating a “fertile” environment for a diverse ecosystem of participants (Mukhopadhyay et al., 2019). Public-private partnership initiatives are found to be reliant on the distribution of power dependence between the actors (Medaglia et al., 2017a) and their successful cooperation ventures require clearly defined rules and responsibilities.

6. **Relation to the digital heritage.** Interoperability with legacy eID schemes is not only a mechanism for wide adoption but can also be a strategic decision for initial bootstrapping and enabling the inclusivity of various user-groups. The relationship to legacy infrastructure also includes considerations of the extent of infrastructural changes in existing IdM systems. There is also the need to comply with the local and global regulations. This typology of design choices can be used as an evaluative framework when assessing the design and development of large-scale IdM infrastructures. These findings expose some of the fundamental aspects to keep in mind when developing the IdM systems and aiming for their dominance.

6.5 **Implications for practice**

This section summarizes the implications for practice. The readership may include software architects, business professionals, executive management as well as policy makers.

- External platforms become dominant when they are almost the only choice. Problems occur when such platforms become a critical part of user-organizations’ infrastructure.

The interconnectedness of the enterprise information systems landscape is a manifestation of globalization. This trend is happening at all levels and in all societal activities. The problem of dominance has primarily policy implications concerning competition or antimonopoly regulations. While it is not possible to influence the decisions of dominant platform owners or influence which platforms become dominant, it could be possible for non-focal organizations to take collective action and/or aim to building a unique service or product in conjunction with the platform. There are for example cases when platform owners have made exceptions for non-focal actors: e.g., the change of terms and conditions in Apple’s App Store in 2016 stated that applications should not be dependent on one another. This caused a big problem for Sweden’s most popular mobile payment application (Swish), the use of which required the user to be authenticated with a mobile BankID for authentication and transactions signing. Following the media backlash in Sweden, an exception for the Swedish BankID was made.

- Self-centered strategies of platform orchestrators, unwillingness to resolve technical debt and the inability to align interests in the ecosystem eventually leads to the infrastructuring of the platform.

The environmental disruption caused by external forces in the form of regulatory changes revealed the accumulated conflicts of interests (de-facto control over the important infrastructure) and unresolved tensions (high prices, outdated technology) among participants in the Finnish IdM case. Our findings emphasize the importance of strategic and operational
coherence in the governance of a changing ecosystem with a proprietary platform playing the role of a national infrastructure. Overall, orchestrators should revise traditional closed strategies by building a more sustainable power-dependence relationship when coordinating the players that would ensure their own success as well as the success of other ecosystem participants. This lesson learned from the case can be useful for other longstanding orchestrators confronted with similar changing settings.

The findings also increase the understanding of the role of dominant infrastructures that become obsolete. What happened to Finnish TUPAS could as well happen to a dominant infrastructure and platform that becomes obsolete as a result of mergers & acquisitions or centralization of services. A well-functioning dominant infrastructure may become sacrificed “for a greater good” to merge two enterprises or to replace local services with national, regional or global services.

- The following architectural components: solution architecture, identity provisioning, human-user integration, a choice of providers and business models, governance and relation to the digital heritage can be used as important points for discussion when managing the development of IdM infrastructures.

Designers, developers and business decision-makers should take the big picture into account when designing IdM solutions. First, technology choice is about the architectural design choices that have consequences, as well as the identity provisioning process related to first time user identification, bootstrapping the eID provisioning via the existing eID credentials and/or linking several credentials, e.g., physical or virtual onboarding and “identity chaining”. The technical soundness and interoperability considerations are obviously of utmost importance, however, the non-technical aspects, e.g., organizational integration motivations, should also be considered carefully. Third, the need to increase individuals’ control over their personal data requires human-users’ readiness and/or willingness to take responsibility for their digital identities. On the other hand, in order to not to overburden human users, the solution may include a trusted third party. With the increased focus on user-centrism in terms of data control that is being pushed through regulations, few studies have empirically described the implications of full human-user control of the IdM infrastructures design space. Fourth, when the infrastructure is not government-funded and businesses bear the costs, it requires commonly agreed standards, interface specifications and definitions of financial compensation. Fifth, depending on the types of actors involved in the infrastructure development and service provision, commonly agreed and efficient governance structures need to be agreed upon. There can be variations in the degrees of cooperation between the public and private actors. Lastly, there is a need to assimilate eID schemes into an existing ecosystem and legacy not only in terms of technical interoperability but on the organizational level in relation to existing legal and regulatory frameworks.

The importance of electronic identity management cannot be over emphasized (Walsh et al., 2018). IdM services are the backbone infrastructures of everyday electronic transactions. However, identity management is not the main goal of human-users, it is merely an intermediary service in the process of obtaining other digital services. Therefore, the requirements for successfully building large-scale IdM infrastructures are particularly demanding.
This chapter outlines the limitations and validity of the study and concludes with the summary of contributions and suggests possible directions for future research.

7.1 Summary of contributions

This thesis consisted of three phases which aimed to answer the main research question (which was divided into four sub-questions). The main research question was:

- **RQ**: What factors affect changes in dominant digital infrastructures?
- **Answer**: Given the recursive relation between platforms and infrastructures, platforms become dominant when they are the only rational choice in the market. Industry platforms that fail to anticipate wider ecosystem needs and adapt to them, evolve into industry (backbone) infrastructures. The governance of the successful transformation of dominant (IdM) infrastructures requires cooperation and dialogue between the stakeholders. The following architecturally significant criteria can be used as an evaluative framework when assessing the design and development of large-scale IdM infrastructures: technology choice, identity provision, human-user integration, provider choice and the business model, governance structure and strategy in relation to the digital heritage.

In the first phase of this research the characteristics of the dependencies upon a dominant digital infrastructure were studied (RQ 1). In the second phase the process of dominant infrastructure transformation was studied (RQ 2) and the third topic on the governance aspects were partially addressed (RQ 3). In the third phase, the governance aspects of dominant (IdM) infrastructures were studied (RQ 3) and the architecturally significant components of IdM infrastructures were identified (RQ 4). The main contributions of this research are summarized as follows in Table 13. The results of this thesis provide high-level conceptualizations and guidelines that could be used by researchers and practitioners.

Seamless interactions with digital identity platforms are at the cornerstone of the everyday digital life of users and modern ways of doing business. However, the question of how such infrastructures are developed and who provides and governs them, are still open questions. By accepting the assumption of a recursive nature between infrastructures and platforms, we studied the reliance on a dominant bank-provided infrastructure in the case of a national IdM platform in Finland. The dependence on such dominant infrastructures — the long-term implications of which is not always anticipated and can often be confused with traditional service models — entails that changes in the ecosystems of such infrastructures involve (subsequent, resultant) changes in user-organizations. In this research, we described the implications of relying on external digital platforms and infrastructures; theorized how dominant IdM infrastructures transform when they involve complex public-private sector
In summary, the dependence on dominant infrastructures can be challenging for organizations. In the case when dominant infrastructures exist in the digital identity context, the implications of the reliance entail an even more profound importance to both human-users and organizations of various sizes. While the problem of IdM is not new and various academic, industry and governmental solutions are being proposed and developed, the eID infrastructures are sociotechnical constructs (van Dijck & Jacobs, 2019), which require a holistic outlook concerning their design, development and control arrangements. The results of this research provide a better understanding of the role of dominant infrastructures by focusing on the case of a Finnish IdM case. Practitioners, researchers and policymakers can use the lessons learned from the case of this nationwide platform-to-infrastructure transformation to advance their understanding of the successful development of electronic identification services.

### 7.2 Validity and limitations

The validity of the findings and the limitations of this thesis are analyzed in this section. Publication I was performed following the grounded theory method, with semi-structured interviews as a data collection method. Publications II, III, IV, V were performed following a case study method (Yin, 2011) in which the data collection method consisted of semi-structured interviews. Publication VI followed an SLR method (Kitchenham, 2004) and also falls under the interpretive view of research. In the following, the findings of this thesis are evaluated using the validity criteria proposed by (Maxwell, 1992), namely descriptive, interpretive and theoretical generalizability and evaluative validity.

First, the descriptive validity threat was eliminated by recording and transcribing each interview in true verbatim, to ensure the factual accuracy of the data. As qualitative researchers are not interested in solely describing reality, but concerned with what the phenomenon under
study means, there is an interpretive validity threat. Although there is “in principle no access to data that would unequivocally address this threat to validity”, we attempted to construct our findings closely grounded in the language used by interviewees, their own words and concepts (Maxwell, 1992). We mostly used open-ended questions to allow respondents to elaborate on their answers and avoided using leading questions to achieve a desired response. The next validity threat is theoretical, which is not concerned with factual accuracy and consensus, but rather with the legitimacy of the applications of the concepts to the phenomena and the validity of causal relationships among them. Here, the choice of grounded theory with no a priori theory in mind (Publication I) and an inductive data analysis approach (Publications II, III, IV) and its continuous interplay of data collection and analysis along with incremental open, axial and selective coding procedures spanning several months proved its usefulness. This ensured that the constructs, identifications and their application to the data were not biased and the patterns identified were (as much as possible) theoretically saturated, and that the different types of relations between concepts were identified. Next, as with any other qualitative studies, we cannot claim the internal or external generalizability of the findings as such, but rather their analytical transferability extended to other cases. Furthermore, the empirical evidence we provide may be industry or country specific. Qualitative research findings illustrate specific phenomena studied in real-life settings and are not generalizable to the population as such. The evaluative validity has been addressed by means of scientific peer-reviews.

The studies presented in this thesis have limitations. The first limitation that can be found in Publications II, III and IV is the trade-off between observing a process in real-time instead of relying on retrospective accounts. When conducting real-time observations of a change process as it unfolds, the chances of missing critical events are high (Van de Ven, 2007). The second limitation is the trade-off between temporal duration and granularity of events. Despite providing a retrospective overview of historical events, the study of the Finnish IdM case focused in detail on the evolution process of a relatively short temporal duration. On the other hand, our prolonged involvement with the case had a positive impact by allowing us to employ a snowballing technique in the data collection and access to data from different sources. It is also important to note that we did not have direct access to all the banks in Finland, and our view of the ecosystem evolution was based on the data collected from various ecosystem participants. This limitation was addressed by employing a triangulation approach, i.e., using data from different sources, including secondary data in the form of official press releases from the government, banks, telecoms and other players in Finland, as well as opinion articles advocating for contradictory reactions, diverging viewpoints.

There are two additional limitations in Publication V. First, the combination of different technological regimes that we studied (centralized vs. decentralized) in different institutional settings (Sweden, Finland, and Taiwan) may be considered problematic in terms of the representativeness and generalizability of the findings. As noted by (Bannister, 2007) the transferability of findings from one country to the next is potentially problematic, and in our utilization of three diverse settings, we have made no attempt to sensitize the particularities of the settings themselves. Instead, we considered the empirical selection criteria as instrumental for creating optimal prerequisites for explorative nuance rather than transferability. Second, the bias in the data collection associated with studying two incumbent solutions (Sweden and Finland) and one challenging solution (Taiwan) implies that the comparability of three cases
is limited. At the time of writing, we have not seen a successful adoption of the Taiwanese eID solution, so we could not rely on the same type of data as in the two other cases.

The literature review performed in Publication VI was limited to the research published on the most common information technology (IT) outlets and did not include all publication forums (we did not look into professional sources, only academic publications). A brief overview of non-academic solutions in the discussion of Publication VI was rather superficial and was included in an attempt to provide pointers for further research. Furthermore, we did not perform backward and forward searches in the literature review. Second, we did not differentiate between different purposes of identity management and employed IdM in its broad scope. This includes strong user authentication as well as single sign-on and sharing of attributes in a privacy-friendly way. There was no differentiation made concerning the security achieved, the privacy provided, nor the technology employed. Next, the review in Publication VI focused on non-technical assumptions based on the information provided in the articles only. In (Mamun & Hansson, 2011), the authors point out the difficulties in explicating the assumptions from a system description without having a thorough understanding of the system. Therefore, as part of a call for future research, studies that entail a deeper inquiry involving interviews with key people and stakeholders and the analysis of documentation could be beneficial. Lastly, the generalizability of the findings in Publication VI needs to be investigated in future research due to the small sample of articles in the analysis. Additionally, since there were only three types of assumptions, the list is possibly not yet complete, and the future work may extend it.

On a more fundamental level, the research presented in this dissertation has limitations coming from the scope of information systems (with technical, economics/business and organizational perspectives) as a discipline. Although these perspectives are mainstream in IS research, they are at the same time narrow by limiting out several other factors that influence how digital infrastructures and platforms become dominant, remain or lose their dominant status and how dominance impacts the activities of non-dominant parties.

Examples of economic perspective factors that were left out include governance of business transactions (transaction cost economics theory), efficiency and scale effects, monetizing of platform value, and competition between platforms. Examples of organizational perspective factors left out include theories and research on market development and organization from the emergence of a market through stabilization to stagnation, structure, processes and (coordination) mechanisms used to govern infrastructures and platforms including decision-making rights, and behavior and motives of infrastructure and platform stakeholder groups.

These theories were not investigated in this dissertation (that makes them good avenues for future research) in an attempt of achieving a systemic understanding of the case that requires focusing on a limited number of factors in the execution of research. However, it is important to mention the opportunity of broadening the context of research.

### 7.3 Future research

This thesis explored the topic of platform evolution somewhat partially, demonstrating a need for further research to confirm, refute or develop further the conceptualizations of the platform to infrastructure transformation. These are timely implications considering the upcoming waves of other important changes caused by regulations in Europe. For example, the introduction of the second Payment Service Directive (PSD2), which requires banks to grant
third parties access to customer accounts and payment services following customer consent, is a platform-based business approach which poses various challenges for the banking sector, with the threat of them becoming a back office. On the other hand, it also brings opportunities for innovative service creation. Among other challengers are the big tech platforms, such as Google, Amazon, Facebook, and Apple (GAFA), as well as Baidu, Alibaba, and Tencent (BAT), which constantly look for ways to create value in new industries. There also exists evidence on consumers’ increasing readiness to have their banking services provided by non-traditional financial service companies (Accenture, 2016). Thus, questions concerning the consequences of platforms being challenged by their environments have become one of the most relevant inquiries nowadays. Moreover, change in the external environment is a very broad area to consider. In this thesis, we investigated the entity layering phenomenon as a response to an external regulation — a specific type of external change — that calls for further reflection on different response types in correlation with the types of external change. Other types of change could be of a technological, competitive or organizational nature and adding a layer of service brokers may not be a suitable response to them.

A potential future research avenue in relation to the Finnish case specifically could be taking an in-depth historical investigation about TUPAS. It will be important to understand the wider economic, organizational factors and the detailed history of the case to understand why TUPAS started to lose its dominant position. The questions such as why was TUPAS developed and how did TUPAS achieve its dominant position? Why did the Finnish banks allow TUPAS to become obsolete by not adapting to technology, regulatory and other developments? Why did they allow the build-up of technical debt?

In relation to the particulars of IdM, it is widely acknowledged that trust establishment plays a key role in the scalability of IdM solutions. While there is a clear need for consolidation of distributed and fragmented, currently ongoing and future IdM initiatives, in this thesis, we observe that inter-organizational integrations (that are the background problem to ubiquitous IdM establishment) are a neglected problem both in research and practice. According to earlier research, most of the enterprise systems integration challenges and problems are of a socio-organizational nature (Kähkönen et al., 2017). This calls for better integration management strategies as part of IT governance. We call for future research to bear in mind the non-technical assumptions and to address their implications explicitly. For instance, what are the roles in the proposed solution? What are the potential organizations, and what are the incentives for their participation? Specifically, what innovative business models are required? Why should organizations collaborate and what is the extent of the potential infrastructural change in participating organizations?

The case of China’s social credit rating system (Ramadan, 2018) is a provoking and extreme demonstration of the importance of the dominant IdM infrastructures development. While understanding the inseparability of political, economic, technical and societal contexts in studying contemporary IdM platforms, further research into the problem is essential.


References


References


82


83


