What Are Digital Identities in Practice? Initial Insight from Finnish B2B Software Companies

Eerika Peltonen*[0009-0009-6118-8944], Sonja M. Hyrynsalmi[0000-0002-1715-6250], and Kari Smolander[0000-0002-7043-0458]

LUT University, Finland
{eerika.peltonen,sonja.hyrynsalmi,kari.smolander}@lut.fi

Abstract. Digital identities are implemented and used in software products increasingly. They allow businesses to perform a variety of tasks, including managing customer relationships or performing financial management activities. Software companies that offer software-as-a-service products must take growing amount of stakeholder needs and regulatory developments into consideration when implementing or using digital identities in their products.
This research paper presents the initial findings of a qualitative interview study conducted in two software companies in Finland. Both companies offer business-to-business products with a strong role of digital identities. The research goal was to understand the identity provider and software product company perspective on digital identities. This goal was achieved by presenting initial results on the use of the term of digital identity in practice, identify relevant stakeholder priorities, and present both disruptors and accelerators to match these priorities. Some identified stakeholder priorities include security, communication and user experience. Accelerators for matching these include company strategies and communication while disruptors include security concerns and unknown regulative requirements. Research data was collected during Summer 2025 followed by thematic analysis.

Keywords: Digital Identity, Software Product Company, Identity Provider, B2B

1 Introduction

People all around the world have different identities in different scopes. One can have different identity when they are at work, and different identity, or multiple, when they are at home with their family [1]. Due to the rapidly digitalizing world, there simultaneously exists a digital identity, more or less connected to our real world identity [1]. The use of these digital identities extends both on individual level as well as business level. Individuals can use them for healthcare, traveling and e-government. In business context, digital identities can be used for various activities, such as maintaining customer relations or recording working hours.

This worldwide change to digital has caused concerns for the digital identity and its management, such as security, privacy, usability and trust [1]. New technologies to keep digital identities safe are developed while new regulations and laws are set to help

address digital identity concerns. Among other entities, identity providers and software companies share the responsibility of fair and legitimate use of digital identities, while also navigating through the concerns, stakeholder needs and upcoming changes in the identity field.

The aim of this paper is to understand digital identity from the identity provider and software product company perspective. The main research question of this paper is "*How does digital identity appear in a software company setting?*" while the sub questions of this paper include "*How is digital identity as a term understood inside software companies?"* as well as "*From company perspective, what are the priorities of each stakeholder for digital identities?*" and "*What are the current disruptors and accelerators for digital identity related activities in software companies?*". The study in this paper was made in collaboration with two Finnish software companies that offer business-to-business software solutions. Research data was collected through qualitative interviews with people who work in product management, security or as advisors. Collected data was thematically analyzed. Initial findings include understanding the use of term "digital identity" in company setting, identifying digital identity related priorities for stakeholders, and identifying disruptors and accelerators that either slow down or speed up the company's ability to match these digital identity related priorities.

The remainder of this paper is structured as follows: Section 2 provides background on the related concepts while Section 3 outlines the methodology used in this research. Section 4 presents the initial findings, followed by related discussion in Section 5. Finally, Section 6 concludes the paper.

2 Background

Digital identity attributes and credentials can include things such as name, age, an identity number, ID cards, certificates and number sequences [2]. This information can then be used in digital identification process, which consists of three stages to identify, authenticate and authorize a person. Identification refers to the process of establishing digital identifier, which can be alphanumeric string or biometric information [3]. Authentication refers to the process of determining if the user is who they have identified themselves as, while authorization is the mapping of different user identities to organizational policies so that user's access to is regulated [3].

On the regulatory side, one of the biggest current changes for digital identities on European Union (EU) level is the newest instalment of the regulation on electronic identification and trust services. This regulation proposes the concept of European Digital Wallet [4]. The purpose of this wallet is to offer EU-wide access to for citizens and businesses of EU Member States to their national identity as well as proof of other personal attributes, such as diplomas or driving licenses [4].

Stakeholders related to digital identities from the company perspective are presented in Fig. 1. These include customer, software product company, identity provider (IdP), and external stakeholders and regulators. If moving outward from the center of the circle, the first stakeholder is the customer. This refers to the party who buys the product or service from the software company.

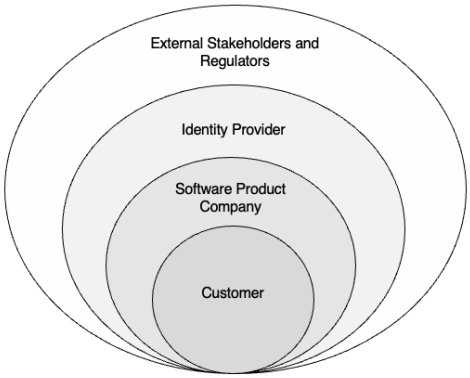

Fig. 1. Stakeholders related to digital identity in business-to-business software context

The next stakeholder, a software product company, is responsible for offering products for other businesses to improve or accelerate their operations. This research will be focusing on business-to-business (B2B) software product company offering software-as-a-service financial management product. The third stakeholder, an identity provider, supplies identities to subjects and have four essential responsibilities of generating, assigning, binding and arranging identity attributes [2]. Lastly, regulators can include national regulators that make sure that the product is compliant with the current regulations and laws while external stakeholders can refer to different institutions or unions that overlook related activities.

3 Methodology

3.1 Data collection

Research data for this paper was collected through semi-structured interviews. Semi-structured interview refers to a type of an interview where questions are planned beforehand but are not necessarily asked in the same order [5]. Interviews, with a conversation approach [6], were chosen as an approach as it allows to explore personal experiences and collect rich data. In the conversation interview approach, the interview is viewed as a conversation and is seen as to construct meaning rather than confirmation of facts [6]. All interviews were held in Finnish and both recorded and transcribed. After each interview, a Finnish transcript was generated and anonymized. Then, the transcript was translated to English and language match was checked. English translation was created since the research findings will be reported in English. Therefore, analysis and reporting will be easier with English transcripts. Location-wise, two of the interviews were held on premise, four remotely. Interviews lasted 60 to 90 minutes. In Table 1, background information about interviewees can be observed, including their roles and location between the two companies. Interviewees were recruited through an external contact, who passed on the email information of the interviewees to be contacted after inquiring them of their interest.

Table 1. Roles and companies of interviewees

Company	ID	Role
1	1	Senior Advisor
1	2	Product Manager
1	3	Information Security and Data Privacy Director
1	4	Product Manager and Portfolio Lead
1	5	Business Specialist
2	6	Product Manager

As can be observed from Table 1, the interviewees have varying roles. Some work more on the product side while some emphasize more security or business. Five of the interviewees work in the software product company (Company 1) and one interviewee work on the external identity provider side (Company 2). All interviewees were informed of anonymity of the data and consent at the beginning of interviews, and they were given a detailed description of the research project and its purposes before the interview.

3.2 Analysis

We followed the practical guide of thematic analysis created by Braun and Clarke [7]. The thematic analysis includes six major phases: (1) Familiarizing yourself with data, (2) Coding, (3) Generating Initial themes, (4) Developing and reviewing themes, (5) Refining, defining and naming themes, and (6) Writing up [7]. The first phase consisted of immersing oneself with the data through listening and (re-)reading the recordings and transcripts of interviews. In this phase, for each interview, general notes on analytic ideas and insight were written. The second step, coding, done only by the researcher herself, included inductive approach to go through the dataset and identify segments that could be interesting and labeling them. Next, the initial themes were generated by outlining of the end results through a mind map, including themes such as the "difficulty of the term", "challenges", "opportunities". These initial themes were then developed further in the fourth step. Fifth step included returning to the dataset and making further developments and adjustments while also collecting suitable quotes to be included as part of the results. The sixth phase of writing concludes in this research paper.

4 Digital identities in a software company setting

4.1 Use of the term

When a user of a work-related software product logs in, they are often identified through their identity as an employee. The information for the identification and authentication activities can include things such as work credentials, an employee number, and even biometrics. As Interviewee 4 expressed on the use of digital identity:

> "Digital identities, are they based on things that can be cracked with raw computing power, or does it have to be something that I also own?"

To answer the first sub research question of the research "*How is digital identity as a term understood inside software companies?"*, inside software companies, people often

refer to more specific activities related digital identities instead of using the term "digital identity" itself. As highlighted by Interviewee 6 on the matter:

> "We haven't really talked about digital identities. It goes to the level of concreteness quite often. We talk about authentication, login, user roles, rights and more."

These all are components connected to digital identity. This way of using digital identity in the company setting makes it appear very much like a practical concept.

4.2 Stakeholder priorities

Different stakeholders related to digital identities from the software company perspective were presented in Fig. 1. To answer the second sub research question of this research "*From company perspective, what are the priorities of each stakeholder for digital identities?*" key stakeholder priorities for each digital identity related stakeholder are presented in Fig. 2.

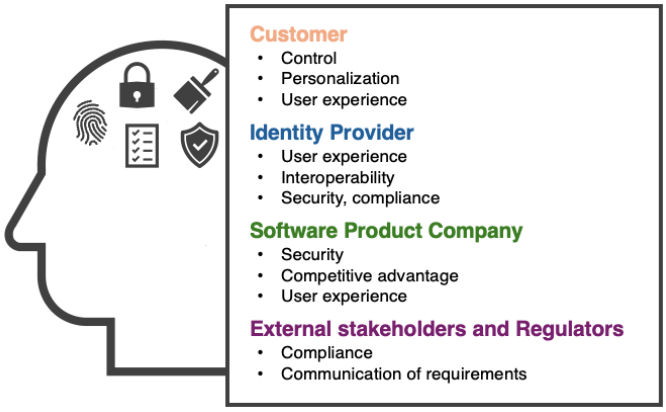

Fig. 2. Stakeholder priorities related to digital identities

Customer priorities include the control over their own identity, meaning that the user can choose what information they want to share. Another customer priority is personalization. This can refer to using certain digital identity type to log into the system or choosing background color or the theme for the system. As said by Interviewee 6:

> "I'm thinking that the trend is personalization. You want the product to feel like your own."

The third and the last priority for the customers is the user experience. For customers, it is important that they have good experience when using the system. One of the priorities for **Identity Provider** is also user experience. As highlighted by Interviewee 6 on the user experience:

> "We want to make it as easy as possible for the user to log in or create an account. It actually starts from the user's need."

Closely related to the use of different identity types is interoperability, which refers to the ability to use one digital identity type across different systems. Lastly, security and compliance are important priorities for identity providers. As Interviewee 6 stated:

> "Starting to support a standard is a matter of examining quite carefully what you are going to support in the first place. It can't be just anything."

To ensure interoperability, security and compliance, technological standards related to different identity types must be examined carefully and any regulative requirements must be followed. **Software Product Company** follows similar priorities with the identity provider. In a software product company, there is constant seeking for balance between the security measures and the user experience. As described by Interviewee 3 on the balance of security, regulations and user experience:

> "Often, it alone poses challenges to understand what the right requirements are, which ones come from legislation, which ones come from customers, which ones are internal requirements, and to ensure that all those requirements are met in a way that is not too difficult for the user."

On top of security and user experience, competitive advantage is one of the priorities. However, as expressed by Interviewee 2 in relation to competitive advantage:

> "Competitive advantage must not be sought from taking a shortcut in the requirements of information security or by shortening some process."

This highlights the importance between the security and competitive advantage. Lastly, for **External Stakeholders and Regulators**, compliance and communication are the key priorities. Regulators and other external stakeholders have the responsibility to oversee the regulative aspects and other requirements. Both parties are also responsible for communicating them to all relevant parties.

4.3 Disruptors and accelerators for matching the priorities

To answer the third and last sub research question of this paper "*What are the current disruptors and accelerators for digital identity related activities in software companies?*", identified disruptors and accelerators are presented in Fig. 3. Disruptors refer to aspects that slow down the ability to match the priorities of stakeholders. Identified disruptors include security concerns, interoperability issues, unknown regulative requirements and lack of standardization.

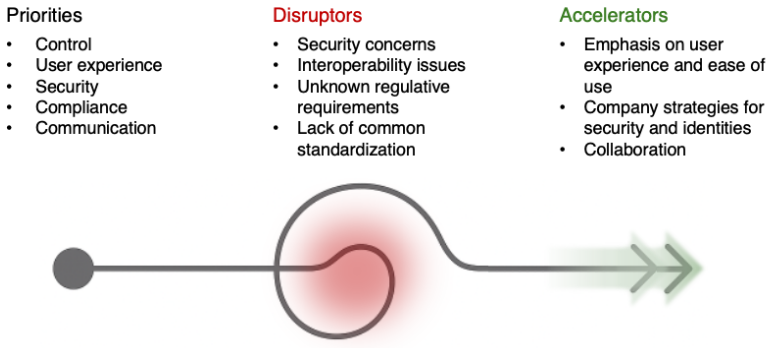

Fig. 3. Disruptors and accelerators for matching stakeholder priorities

Accelerators speed up the ability or processes to match the priorities. Identified accelerators for matching digital identity related priorities include emphasis on user experience and ease of use, company strategies for security and use of identities, and collaboration with stakeholders.

5 Discussion

5.1 Interpretation of results

As was identified in this research, the use of the term "digital identity" is not common in the software company setting. Instead, more practical terms related to digital identity are used, such as authentication or logging in. As identified in [8], digital identity is used as a proxy for single sign-on, also known as SSO. Therefore, confusion can be detected when using the terms "digital identity" or "identity" itself. As what to comes to the multifaceted aspect of identity in this research, people in general have multiple identities, some lasting throughout person's life and some just for limited time [1]. Every identity a person has, there are corresponding identifiers for each [1].

Next, user experience was identified spawning over multiple stakeholders as one of their priorities (Fig. 2), including customer, identity provider and software product company. This user-centricity of systems has been at the center of previous research. For example, when co-creating user requirements for digital identity enabled platforms users identify aspects such as efficiency of the identification process, usability and interoperability as important [9].

Lastly, security and privacy are one of the overarching themes in the initial findings. Previous research shows strong social contract between the supplier and buyer, and that data breaches cause negative effects on trust and dissatisfaction of customers [10]. Identified also in [9], security is one of the concerns of the users towards the identity management platforms. The previous research further emphasizes the importance of security.

5.2 Implications

This research draws attention towards software companies and presents initial findings. Different stakeholders and their priorities around the digital identity field and priorities for each are identified. Furthermore, disruptors and accelerators are for matching these priorities are identified. Future research will include governmental actors and other relevant entities in the digital identity field.

5.3 Limitations

The limitations include the number of interviewees, which in this case includes six individuals. Despite that, we believe that the current results already provide important insight to those that integrate digital identities into software products. Research in that area is rare and therefore new insights are needed.

6 Conclusions

This research sheds initial light on the software company perspective on digital identities through interviews with two Finnish software companies. Thematic analysis was utilized to understand the use of "digital identity" in software companies and identifying relevant stakeholders and their key priorities. These include compliance, user experience, security and communication. To understand the company's ability to match these priorities, disruptors and accelerators were identified. Some of the disruptors include interoperability issues and security concerns while accelerators include company strategies and collaboration. Future research aims to expand on these initial findings, by including more stakeholders in the identity field in Finland, such as governmental actors.

Acknowledgments
This work has been supported by FAST, the Finnish Software Engineering Doctoral Research Network, funded by the Ministry of Education and Culture, Finland. We also thank all interviewees for making this research possible.

References

1. Alpár, G., Hoepman, J-H., Siljee, J.: The Identity Crisis Security, Privacy and Usability Issues in Identity Management. Journal of Information Systems Security, **9**(1), 23–53 (2013). https://doi.org/10.48550/arXiv.1101.0427
2. Natarajan, H., Appaya, M.S., Balasubramanian, S.: Digital Identity Onboarding (2018)
3. Mueller, M.L., Park, Y, Lee, J, Kim, T-Y.: Digital identity: How users value the attributes of online identifiers. Information Economics and Policy, **18**(4), 405–22 (2006). https://doi.org/10.1016/j.infoecopol.2006.04.002
4. European Commission: European Digital Identity (EUDI) Regulation, https://digital-strategy.ec.europa.eu/en/policies/eudi-regulation, last accessed 2024/7/19
5. Runeson, P, Höst, M.: Guidelines for conducting and reporting case study research in software engineering. Empirical Software Engineering, **14**(2), 131–64 (2009). https://doi.org/10.1007/s10664-008-9102-8
6. Schultze, U., Avital, M.: Designing interviews to generate rich data for information systems research. Information and Organization, **21**(1), 1–16 (2011). https://doi.org/10.1016/j.infoandorg.2010.11.001
7. Braun, V., Clarke, V.: Thematic analysis: a practical guide. SAGE Publications, London (2022)
8. Grayson, T.R.D.: Philosophy of Identity, https://timothygrayson.com/PDFs/PhilosophyOfIdentity.pdf, last accessed 2024/11/18
9. Bakhaev, S., Naqvi, B., Wolff, A., Smolander, K.: Co-Creating Requirements for the Emerging Electronic Identity Management Platform. In: 14th Scandinavian Conference on Information Systems, pp. 1-15. AIS, Porvoo, Finland (2023). https://aisel.aisnet.org/scis2023/1
10. Swani, K., Labrecque, L., Markos, E.: Are B2B data breaches concerning? Consequences of buyer's or firm's data loss on buyer and supplier related outcomes. Industrial Marketing Management, vol. 119, 43–61 (2024). https://doi.org/10.1016/j.indmarman.2024.03.007