Lilly Schmidt

The Diffusion of the German eID Scheme

A Case in Which Resource Richness Collides with Implementation Deficiencies

Master Thesis

at the Chair for Information Systems and Information Management
(Westfälische Wilhelms-Universität, Münster)

Supervisor: Joep Crompvoets

Presented by: Lilly Schmidt

Date of Submission: 2022-08-04

Acknowledgements

When I first applied for the Pioneer Master of Science, I already knew that I was going to enter a world that was both fascinating and challenging at the same time. Even though Public Sector Innovation is such a niche topic, l was able to meet so many interesting people along the way.

That being said, I want to thank my supervisor Joep Crompvoets who has helped me find my way through my thesis and way always there to give tips and connect me to relevant experts.

Besides my supervisor, I want to thank all members of the Pioneer program, that taught me more that I could have ever learned on my own. All three universities, KU Leuven, WWU, and TalTech, have contributed heavily to my academic journey. So much, that I'm even entering the academic career after I graduate. This profession path would have never been on the table if it wasn't for the excellent teaching skills of the Pioneer Family.

I also want to thank the interview partners that took an extensive amount of time to talk to me over the course of the last two years. All of them were able to shed light into current and past developments of the eID diffusion process. Through them, I was able to contextualize decisions by the government and service providers.

At last, I want to thank the research project "Schaufenster Sichere Digitale Identitäten" that I am working at. Only due to their expertise in eID diffusion, the experiences I was able to collect during working there, and by being able to use quantitative data collected during the project, I was able to further contextualize the government and service provider levels. What I couldn't have done without the project was to focus on the end user level, as only through the survey I could analyze that level.

Abstract

Germany has been struggling to diffuse their electronic identification scheme since its rollout in 2010. Even though the country spends a lot of money on innovation and implementation projects, there has so far not been a successful implementation of eID use cases. With a lack of innovative mindsets and coordination in the German public sector, the private sector players keep having difficulties to enter the current existing eID ecosystem. ID solutions that already exist are managed by companies that have tight ties to the public sector, while others are excluded from integration the sovereign eID into their own solution. All that is happening while big tech platforms like Apple and Google begin entering the eID market globally. The EU is currently attempting to counteract to those movements by introducing a cross-border ID wallet solution. Since that has started in 2021, the big platform companies are moving at a pace that the EU struggles to keep up. So far, Germany has not contributed towards efficiency nor impact, but rather acted as a blockage to new developments.

This research analyzes the impact that contextual and acceptance factors of three chosen stakeholder groups (government, service provider, and end user) have on the diffusion of the eID scheme in Germany. The major finding is that the government level has so far had the biggest impact on the lack of diffusion in Germany. As both the creator and executer of regulatory frameworks, the German government level doesn't act towards easing the creation of positive network effects. Before the service providers of the private sectors begin to invest into the complex authorization process, the government level has to integrate the ePA into their own systems first. Following the general struggle of digitalizing the public sector in Germany, the ePA diffusion has so far not been successful.

Content

Figures

Tables

Graphs

Screenshot

Abbreviations

eID	electronic Identification
nPA	neuer Personalausweis
DOI	Diffusion of Innovation
TAM	Technology Acceptance Model
RP	Relying Party
SP	Service Provider
GDPR	General Data Protection Regulation
NFC	Near Field Communication
BMI	Bundesministerium des Innern
BMWK	Bundesministerium für Wirtschaft und Klimaschutz
BVA	Bundesamt für Verwaltung
BDr	Bundesdruckerei
BSI	Bundesamt für Sicherheit in der Informationstechnologie
BMDV	Bundesministerium für Digitales und Verkehr
SME	Small to Medium Enterprise
PKI	Public Key Infrastructure
LSP	Large Scale Pilot

1 Introduction

Digital identity is an often barely perceptible key technology of the networked society. It is a prerequisite for the trustworthy use of digital services and the basis of every digitization project - whether in public administration or in the private sector (Skierka, 2021a). While advancing digitization, identity systems are in a state of upheaval. According to a study by the McKinsey Global Institute, countries can increase their gross domestic product by 3 to 13 percent by 2030 by introducing a national digital identity.[1] Examples from countries in Northern Europe, such as Denmark or Sweden, Estonia, or even Singapore, show that the successful digitization of government and business is built on a cross-sector and widely used digital identity solution (Skierka, 2021a). During the Covid 19 pandemic in particular, it became clear to citizens and organizations how fundamental digital identities are for the provisioning of convenient and secure services in the digital space (Skierka, 2021a).

Germany has so far lacked uniform, cross-sector and broadly deployable digital identity solutions. The core of the German eID system is the electronic ID card and the associated infrastructure. However, the eID is neither widely used nor does it provide access to many applications. Other scholars refer to this as a negative network effect. With an unbalanced cost-benefit balance, the number of use cases low. Though for the benefit to rise, it needs more use cases (Poller et al., 2012). Since then, the usage and acceptance of the German eID scheme has not risen in a way that can be called successful (Skierka, forthcoming). In general, without helpful and relevant services, end users are hesitant to spend time and money to learn new technologies. Nonetheless, without a sizable user base, service providers are unlikely to develop and invest in a developing new service. Even though Germany has already introduced their eID scheme in 2010, the diffusion has not yet been successful. How that makes the German case interesting to research will be presented underneath.

1.1 Research Motivation and Research Problem

While the German eID scheme has reached more attention during the last years, especially on a political and societal level (e.g., pwc Study on electronic identities in 2021 or the public hearing at the German Bundestag on July 4th, 2022), a basic assessment of the reasons for the adoption or non-adoption and diffusion has not yet been done while looking at all three stakeholder levels. With a unique data set at hand, the contextual and acceptance factors affecting the diffusion of the German eID scheme of today can be extensively researched.

[1] McKinsey Global Institute (2019). “Digital Identification: A key to inclusive growth.” https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth

The factors that influence the rejection or acceptance of an emerging information technology artifact such as the German eID scheme have long been of interest to information systems researchers, but they remain difficult to apply at a generalized level (Benbasat et al., 2008; Van Cauter, 2016). Numerous theoretical models have been developed as a consequence of research on technology adoption (Davis, 1989; Homburg & Dijkshoorn; Venkatesh et al., 2013; Williams et al., 2012) However, a smaller number of studies have been conducted on eID adoption (Alkhalifah & D'Ambra, 2012; Alkhalifah & D'Ambra, 2013; Khatchatourov et al., 2015). In general, the academic literature has paid little attention to looking at contextual and acceptance factor influencing the diffusion of eID schemes (Seltsikas & O'Keefe, 2010; Vries et al., 2018; Williams et al., 2012).

Although a growing number of studies have discovered and proposed various criteria and metrics associated with eID adoption (Fensel et al., 2007; Harbach et al., 2013; Homburg & Dijkshoorn; Klischewski & Ukena, 2010; Lips et al., 2021; Nortal, 2020a, 2020b; Poller et al., 2012; Söderström, 2016; Stepanaia & Jerman, 2018; Tsap et al., 2020; Valtna-Dvořák et al., 2021; Zefferer & Teufl, 2015), only one researcher team focus on three stakeholder levels in the network (Government , Service Provider, and End User) (Brugger et al., 2015). It demonstrates the disconnect of research between the technical implementation of eID systems and their adoption by service providers and end users. When it comes to end users, research indicates that the status of acceptance of a national eID varies significantly among countries. Reasons for that are mainly the country context. As they already researched the German case until 2010, this study is an excellent follow up(Kubicek & Noack, 2010)

1.2 Research Questions

Resulting from the research problem above, the following research question(s) will lead the following thesis:

What impact do contextual and acceptance factors (X-Variable) of the government, service providers, and end users have on the diffusion (implementation and use) (Y-Variable) of the eID scheme in Germany since its rollout in 2010?

Resulting from the leading question are the following sub-questions:

1. Which factors mutually affect all stakeholder groups in the diffusion of the eID innovation in Germany?

2. How do the stakeholder groups affect each other in the diffusion process?

3. Which stakeholder group has the highest impact on the diffusion of the eID scheme in Germany?

1.3 Scope of this Research

Because the chosen case is complex and has relevance on multiple levels, three different stakeholder levels are researched. Before doing so we need to go one level higher and look at adoption barriers of service providers and reasons why there aren't many use cases until today. On the other hand, the existing eID scheme can only be understood by looking at the government level. All three levels are influenced by a certain context. The exact variables will be explained in Chapter 2. The technological specifications and cryptographic keys will not be looked at during this thesis as they are out of scope and the one element of the eID scheme that has remained stable since the beginning in 2010 (see Chapter 5). The primary goal of this thesis is to assess the reasons for Germany's damped eGovernment (so the electronic provisioning of public services as well as online-authentication) project success while focusing on the eID project as a case.

1.4 Outline of the Thesis Structure

With the research questions in mind, the thesis will continue with presenting the two theory schools of Roger's Diffusion of Innovation and Technology Acceptance and the composed theoretical framework by Brugger et al. (2015) in Chapter 2. Following that is the presentation of the literature review in Chapter 3 and the chosen research design in Chapter 4: The German case in presented in Chapter 5. Then the theoretical framework is applied onto the case in Chapter 6 as well as directly discussion the results that were found to increase readability. Chapter 7 will conclude with final remarks and a critical reflection on the work of the researcher.

2 Theoretical Framework

To research the German case, a mix of two theories is used. Both look at the introduction of an innovation/technology and its consequences afterwards. While Rogers et al. (2014) created the diffusion of innovation theory (DOI), they focused on the entire process of preparation to an innovation, the launch, and its rollout in mind. The technology acceptance theory by Davis (1989) looks at reasons for the adoption and expected behavior. At first the diffusion of innovation theory is presented, followed by a Chapter on the technology acceptance theory by Davis and other authors looking at technology acceptance. In the third part the used theoretical framework by Brugger et al. (2015) that combines both theoretical schools is presented.

2.1 Roger's Diffusion of Innovation

Even though, Roger already established the factors of how innovations are diffused in a society in 1995 it remains highly relevant until today. As the Figure 1 shows below, the scope of a research project focusing on DOI is different depending on the focused areas. As this thesis is looking at the diffusion of the eID scheme, the prior stages will not be covered. The following Chapter presents factors affection the diffusion and adoption of the innovation as some users will adopt the innovation right from the beginning while others are "lagging behind" (Rogers, 1995).

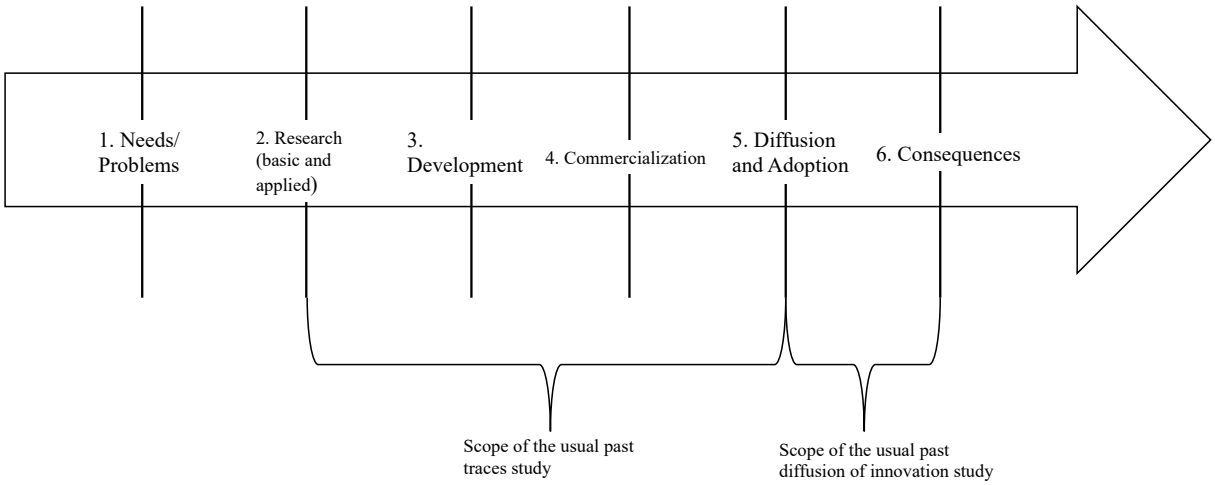


Figure 1 The six stages of the innovation-decision process by (Rogers, 2003, p. 170)

Rogers' central topic is how innovations propagate via social systems and what factors impact the diffusion of an innovation. His paradigm for the adoption process includes actor characteristics (e.g., values, skills, status), situational perception (e.g., social norms, economic constraints), perceived innovation characteristics (advantage, compatibility, complexity, divisibility, and communicability), and information sources (Aichholzer & Strauß, 2009).

An innovation can be a notion, a body of information, a belief or social norm, a product or service, a technology or process, or even a culture, as long as it is considered original (Rogers et al., 2014). Inventions are communicated verbally, with one individual telling another, as well as through a variety of other means, such as magazine advertisements and personal observation. Diffusion is the social process by which an innovation is transmitted within a communication network or social sector over time(Rogers et al., 2014).

Typically, we first become aware of innovations through impersonal, mediated communication channels, but we only decide to adopt an invention for ourselves after seeking the opinion or witnessing how someone we know, trust, or regard as an expert is using the innovation. Rogers identified these individuals as "opinion leaders"(Rogers et al., 2014). The diffusion curve is accelerated by the social influence of opinion leaders, exerted either verbally or by example. They are also responsible for the failure of innovations to diffuse by ignoring them (passive rejection) or speaking out against them (active rejection). The S-shaped curve seen in Figure 2 has been demonstrated by numerous studies to be a predictable pattern of innovation diffusion over time.

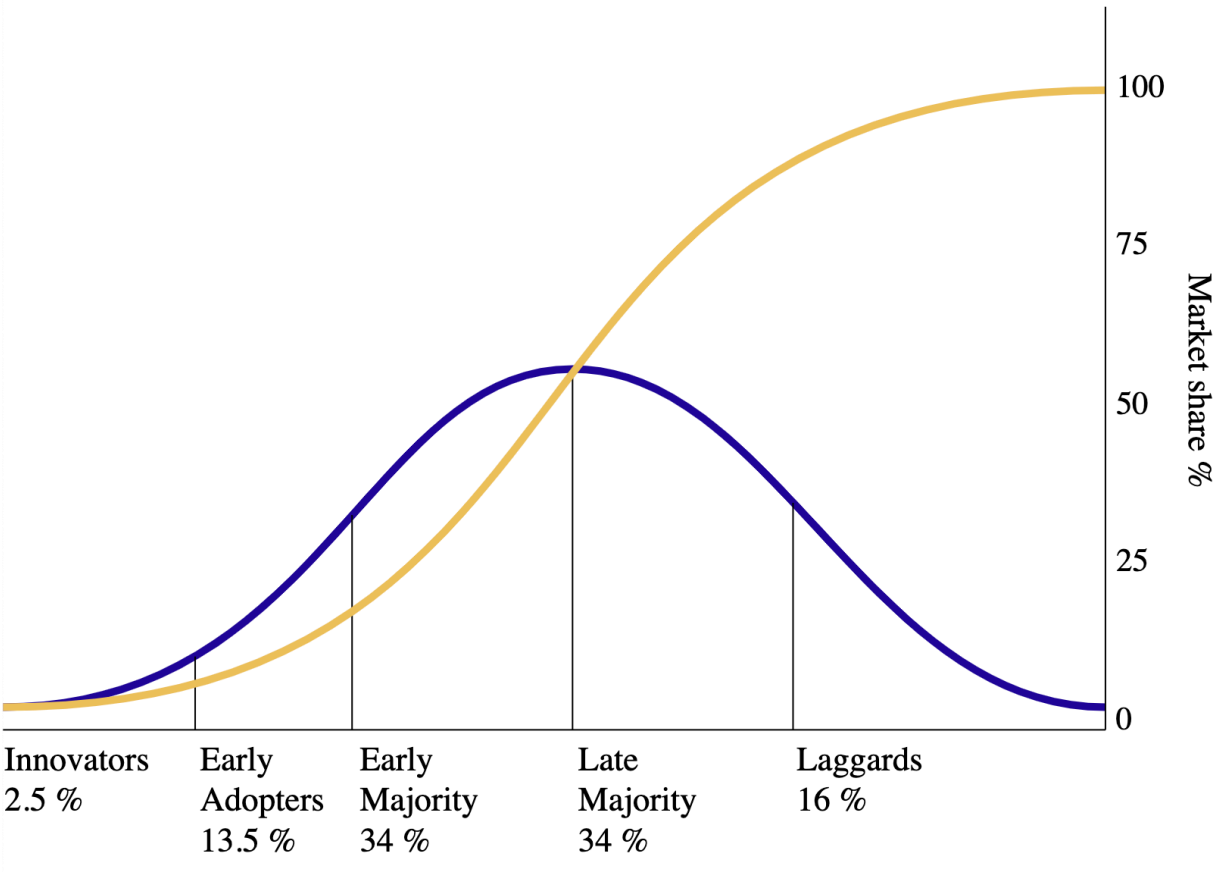


Figure 2 Roger's Diffusion of Innovation S-Curve

The typical view of diffusion expresses the high influence of adopters' perceptions on their decisions (Rogers et al., 2014). These features of innovations are codified by Rogers et al. (2014) as *complexity, relative advantage, compatibility, trialability, and observability* and depicted in Figure 3. They indicate the perceived benefits and costs of a good adoption decision. Relative advantage is the degree to which an innovation is perceived to be superior to the status quo. In this context, quality improvements, time savings, and cost-effectiveness may play a role. Complexity refers to the subjectively perceived complexity of a technology, such as how challenging it is to comprehend or use. Additionally, the compatibility of a technology with experiences, values, and needs, as well as its trialability, such as through test apps, play a significant influence (Rogers, 2003). Rogers et al. (2014) present additional variables that influence the rate of the adoption. The first one is the "type of the innovation-decision", in which the approach to the innovation determines adoption. It can be either an optional, a voluntary or co-creative approach. "Communication Channels" also play a big role as the chosen approach, either to use mass media or to approach end users on an individual level determines how end user feel about the innovation. The next variable focuses on the social context of the system that the innovation is introduced to. If there is already a high traction of interconnections and interdependencies, the innovation can be adoption quicker than if those factors first need to build up from the ground (Rogers et al., 2014).

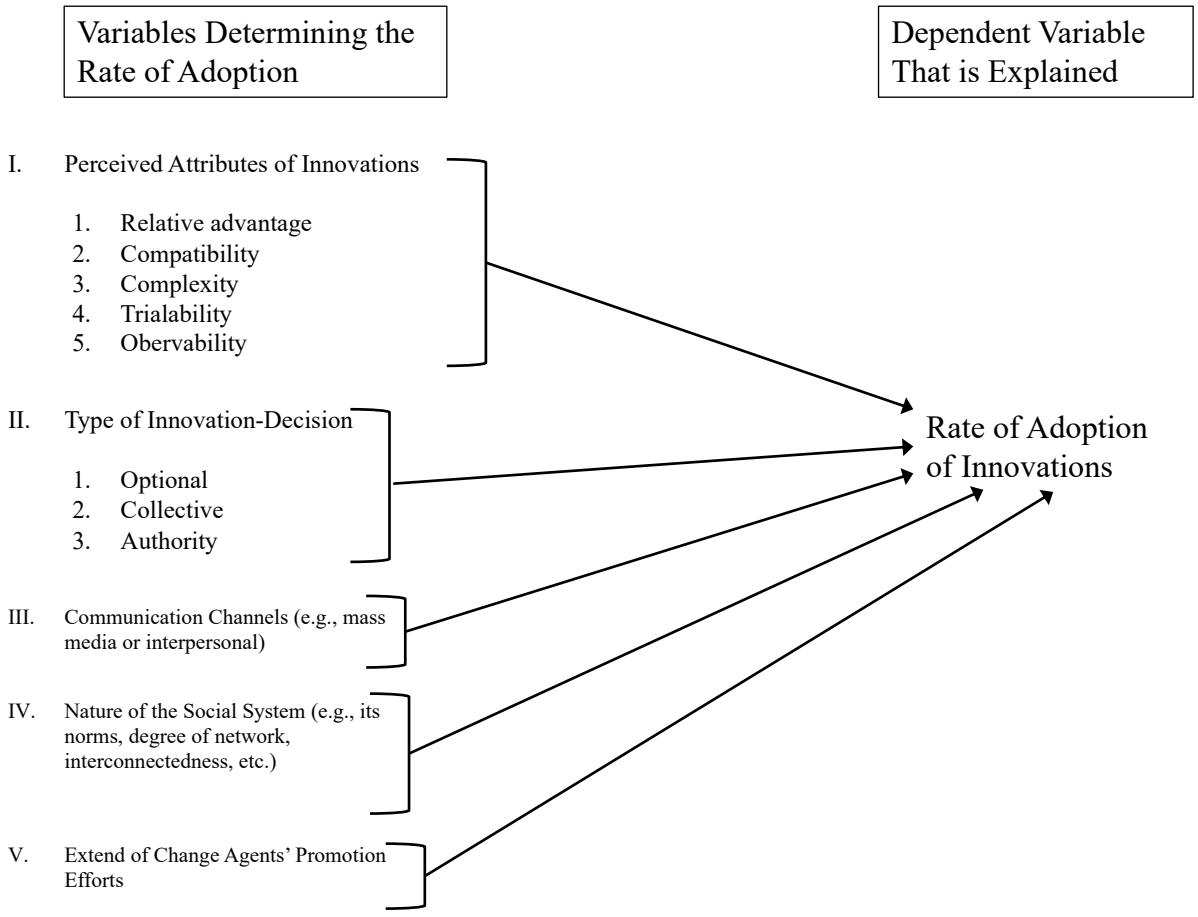


Figure 3 Variables determining the rate of adoption (Rogers, 2003, p. 222)

Other researchers have suggested incorporating image, trust, or visibility into Roger's strategy (Barnes & Huff, 2003).

- Image: the extent to which adoption and use of the invention are perceived to improve one's image or standing.
- Trust: the amount to which an innovator's adopter perceives him or her to be dependable.
- Visibility: the degree to which others can observe the results of a concept.

To summarize, the conventional concept of diffusion, which emphasizes (1) the critical role of centralized change agencies and those they fund as innovation providers, (2) the importance of potential adopters' impressions of an invention's qualities in reducing uncertainty about what the innovation is and can do, and (3) the significance of personal influence in communicating to potential adopters that an innovation merits attention, is consistent with prevalent local social norms.

Limitations

Compatibility and comparative benefit are two qualities that have been analyzed successfully to explain the goal of IT adoption (Taylor & Todd 1995; Karahanna, Straub & Chervany 1999; Wu & Wang 2005; Yang et al. 2012). Others are more difficult to evaluate. Variables from other models, such as Davis's (1989) Technology Acceptance Model, provide theoretical connections between beliefs, attitudes, intentions, and behaviors; they are a good addition to increase the understanding user adoption decisions (Aichholzer & Strauß, 2009).

2.2 Technology Acceptance

The Technology Acceptance Model (TAM) (Davis, 1989) is the most prominent theory on technology acceptance. It focuses on the adoption of information technologies. According to TAM, acceptance is affected by perceived usefulness (use enhances performance) and perceived ease of use (usage is free of effort). Both components share a high degree of similarity with the DOI theory's fundamental assumptions (Davis, 1989).

IS System adoption is essential to the success of information systems/information technology applications (DeLone & McLean, 2004). Convenience, user-friendliness, and usability are the most prevalent expressions of perceived usefulness (Davis, 1989; Harbach et al., 2013; Ho et al., 2019; Kalvet et al., 2018; Omar et al., 2011; Williams et al., 2012).

Dhamija and Dusseault (2008) suggested seven aspects that must be considered when assessing the acceptance of eID schemes: the availability of use cases, cognitive scalability, user experience, usability, transparency, and trust. Particularly, the trustworthiness and cognitive scalability of a system are highlighted by other researchers as crucial acceptance determinants

(Aichholzer & Strauß, 2009; Alkhalifah & D'Ambra, 2012; Jensen & Jaatun, 2013). Other researchers have determined that a lack of trust between partners, the challenges and expenses associated with drafting and maintaining contractual agreements between partners, technical complexity, and investment costs are obstacles to acceptance (Ivy, 2010; Jensen & Jaatun, 2013)

Limitations

Technology acceptance is a highly subjective and individual approach. Every actor has their own personal reasons on why they accept a certain technology or not. Nonetheless, the focus on the perceived usefulness and ease of use can contextualize the behavior to a certain extend.

An additional limitation to the technology acceptance is that the main model only considers two variables that influence the acceptance rate of a technology. While other scholars introduce trust as an important addition to technology acceptance, other variables are sure to be influential too. Especially when it comes to contextualizing the perception, only testing two variables is not sufficient. To counter these limitations, a consolidated framework of both theories is presented in the following Chapter.

2.3 Stakeholder and System Acceptance Framework by Brugger et al.

Both just mentioned schools of technology adoption and diffusion provide an ideal starting point for evaluating a national eID program. Using generic acceptance models to address the technology evaluation process with a limited number of stakeholders is useful. However, they do not fully reflect the mutual effect of the actual and expected conduct of the individuals (Brugger et al., 2015). In addition, they usually disregard the structural opportunities and limitations that influence the decision of stakeholders to embrace a certain solution. In the context of national eID programs, the concept of trust not only aids in bridging this gap, but it is also essential. A holistic framework for analyzing the selected case is produced by combining variables from both theories and contextual elements (Brugger et al., 2015).

Based on the above debate, Brugger et al. (2015) selected a set of criteria that match the key stakeholder groups, namely government s, service providers, and end users. Their theoretical approach integrates contextual characteristics that may limit the decision-making options available to the stakeholder groups (Brugger et al. 2015). Government s, public and commercial service providers, who deploy eID-based authentication, and end users who use an eID to access a service are the three distinct stakeholder groups. Most prior studies have focused on public administrations and/or end users as parts of the eID ecosystem. Private service providers, on the other hand, are an essential stakeholder group too.

In electronic contexts, trust relationships are crucial for prosperous cooperation and can span over multiple domains: On the technological front, confidence is linked to data quality and information systems (security and reliability). On the actor side, it refers to those who engage in

the technology's infrastructure (e.g., consciousness of privacy and security issues). Brugger et al. define the operationalization of perceived trustworthiness as "expectations about competence, credibility, good intentions, predictability, and reliability" (Brugger et al. 2015) Unlike typical adoption models, the concept of trust covers not only user expectations of technology, but also user expectations of other actors and a larger emphasis on contextual factors. As with the DOI theory, it implies that external acceptance (trust) is essential to the diffusion process. The provision of identification services must also accurately serve benefits the existing business arrangements of all partners (Brugger et al., 2015).

Brugger et al. selected the variables following variables to analyze perceived value, ease of use, and perceived trustworthiness of system components based on the technological acceptance model and adding trust (Brugger at al., 2015). All three criteria will ultimately influence acceptance decisions and the implementation/use of the respective eID scheme component at each stakeholder level.

The diagram below depicts the initial framework developed by (Brugger et al. 2015). Since their emphasis was on cross-national eID federation and the addition of an interoperability layer (developed by the STORK Large Scale Pilot, which will presented in more detail during Chapter 5 and 6), the framework must be slightly modified to accommodate the national context. Figure 5 illustrates the theoretical framework employed in this thesis.

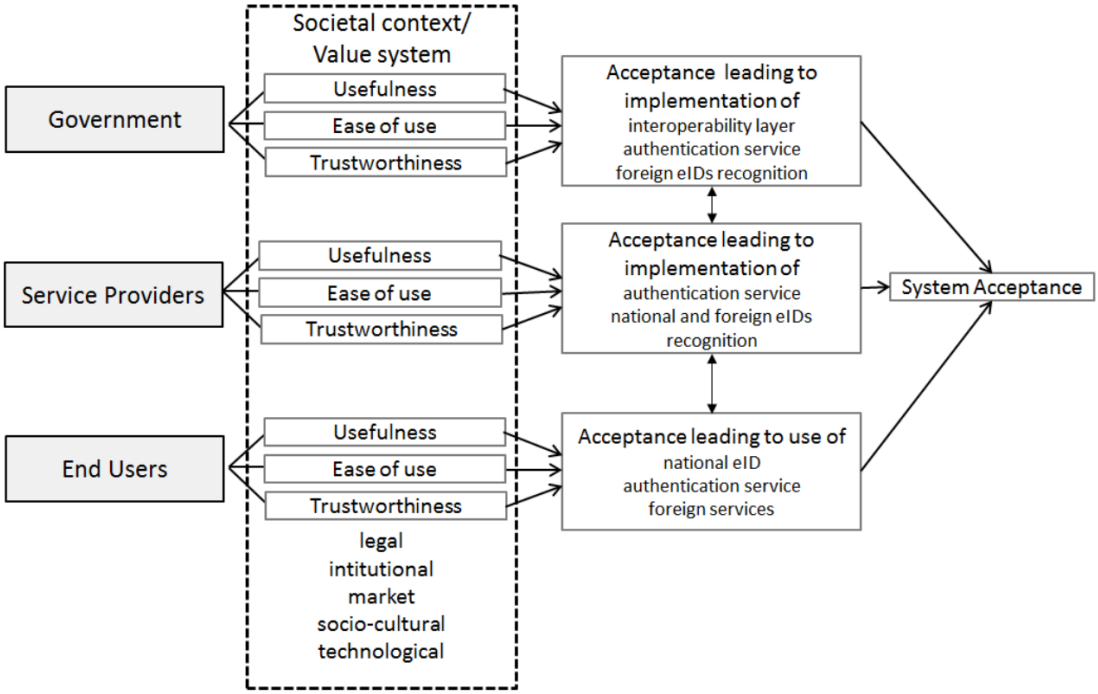


Figure 4 Stakeholder and System Acceptance Framework by Brugger et al. (2015)

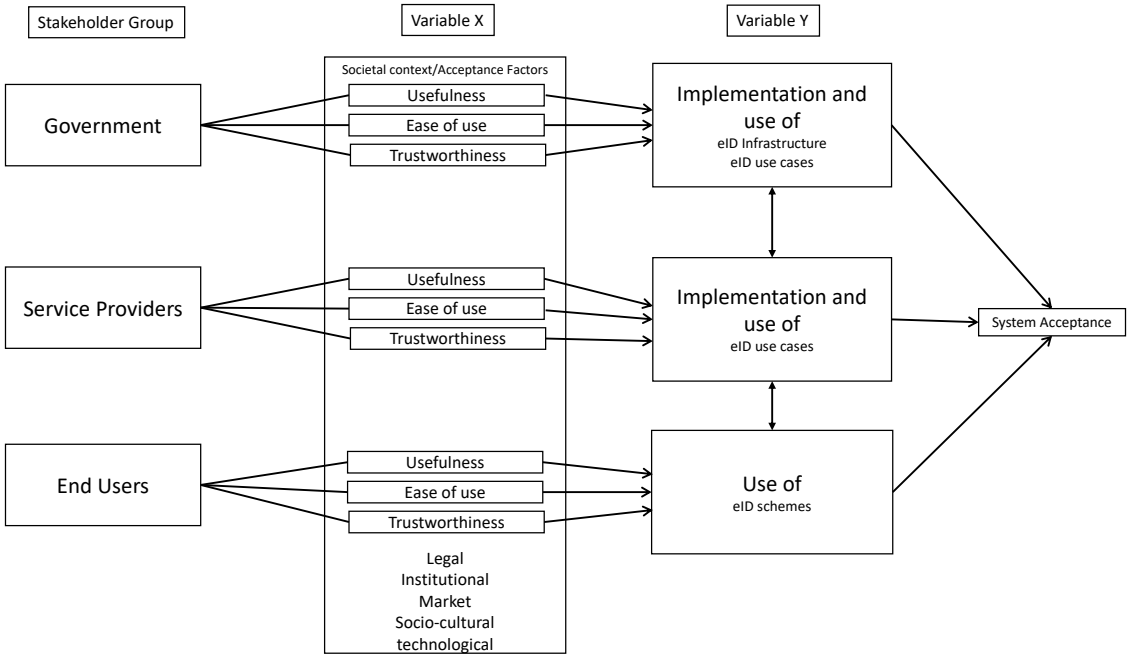


Figure 5 Adjusted Stakeholder and System Acceptance Framework by Brugger et al. (2015)

2.3.1 Stakeholder Groups

Government

Government s perform many roles in an eID program (managing a national eID system, providing eGovernment services that rely on the eID, and establishing the legal framework). Brugger et al. (2015, p.) "concentrate on three major points: the alignment of eID initiatives with regulation, the culture of the public sector, and the value of the services."

Service Providers

The identification data obtained from the eID infrastructure is utilized by service providers to grant access to their systems. The willingness to expend money and commit time and effort in supplying eID services or eID servers can be more or lower depending on the situation.

End Users

From the perspective of the end user, the eID system is frequently a means to a goal, such as simplifying access to specific services. This suggests that consumers frequently go for the path of least resistance (Dhamija & Dusseault, 2008). Users are unlikely to devote substantial time and effort in identity management and control. Consequently, marketing, convenience, and user experience must be considered when diffusing the eID scheme (Poller et al., 2012; Stepanaia & Jerman, 2018; Zefferer & Teufl, 2015).

2.3.2 Variable X: Societal Context and Acceptance Factors

Societal Context:

All external elements that influence stakeholder and system acceptance are contextual in nature. Without context, no process can be comprehended in its entirety. Brugger et al. (2015) identify the following five context-relevant factors:

- Legal: The regulatory framework outlining the decision-making capacity of the ecosystem's participants and the evolution of the legal basis through time;
- Institutional: The institutions involved in a network that is dependent on cooperation, transparency, the national institutional system of the public sector, and the availability of institutional learning;
- Market: The market determines the availability of different business models and value chains for service providers, as well as the cost-benefit ratio;
- Socio-Cultural: The cultural predisposition to invest in innovations, responses to societal pressure, and demographic shifts, and
- Technological: Not only do the technological specifications of the existing eID scheme play a role, but also the relationship to upcoming technologies and how these are affecting the actions of the stakeholder groups are addressed.

2.3.3 Variable Y: Diffusion in Terms of Implementation and Use

Depending on the societal context and acceptance factors, the diffusion rate of an innovation can be higher or lower. Brugger et al. (2015) understand the diffusion process differently on each stakeholder level. While government stakeholders must implement the ID infrastructure and possible eID use cases, service providers need to use that infrastructure to implement use cases. End users on the other side are the last factor that will decide whether the diffusion was successful or not – their use of the eID scheme is essential for the whole ecosystem to work. The current but also expected behaviour of each stakeholder group can have mutual influences on the overall system acceptance rate, as Brugger et al. (2015) have identified.

Limitations

Brugger et al. (2015) have not considered all potential variables and theories that can also have an impact on the diffusion of an eID scheme. As including them is beyond the scope of this thesis, only a few are discussed below and considered while going through the factors that influence the diffusion. Path dependence is an important topic to investigate in relation to the development and implementation of electronic identification. Kubicek and Noack (2010) grouped the routes for four European national e-ID identity management systems into three categories: technological, organizational, and regulatory. Consequently, path-related decisions may involve the technical specifications of an eID system, the organizational structures that support it, and the regulatory pattern (Skierka, forthcoming). Other experts concur with the significance of path dependence (Bednar & Page, 2018; David, 1985).

To summarize, there are two major theoretical schools combined in the used theoretical framework. Both Technology Acceptance and Diffusion of Innovation give extensive explanatory factors for a successful or unsuccessful diffusion of an innovation/technology. The theoretical framework of Brugger et al. (2015) is a great foundation for analysing which acceptance and contextual factors influence the diffusion and overall system acceptance of an innovation. In the following Chapter key terms are defined as well as key success factors for the management of eID project are presented that will serve as accompanying factors for analysing effect of variable X on variable Y.

3 Literature Review

The following Chapter will define central terms such as electronic identification, eID management, and eID ecosystem approaches. The last part of this Chapter will present key success factors of eID introduction projects.

3.1 Definition of eID

The debate over electronic identity (eID) originates from a far older debate about citizenship rights and responsibilities. For instance, during the French Revolution, the livret—a record of work and earnings—was introduced as part of a package of measures intended to create equality between employers and laborers (Garrioch, 2002 in Kubicek & Noack, 2010). It was later dubbed "the instrument of industrial enslavement" since it theoretically greatly restricted an individual's liberty to change occupations (Dunham, 1955 in Kubicek & Noack, 2010).

There are many definitions of identity and eID. The definition that is used for this thesis is the following:

The eID originates from the concept of entity, which is "everything that can be described by a collection of qualities." (Kubicek, 2010). A person, a business, or a computer are all examples of entities. Additionally, identity is the dynamic entirety of an entity's properties. Additionally, the entity may have just one physical identity, but several digital identities since they are subsets of certain qualities. Attributes may be discrete or abstract, quantifiable characteristics of identity, and some are identifiers. Finally, an identifier is a single property or a collection of properties of an entity that uniquely identifies it inside a given context (Kubicek 2010). The eID is available in a variety of formats, including plastic cards, computer data, sim cards in mobile phones, and mobile apps (Söderström, 2016).

Or simpler said:

“Identity is what distinguishes things." (Collings, 2008, p. 62). An online "online identity" refers to a digital representation of one or more distinct principles (Subrahmanyam & Šmahel, 2011). Electronic identification refers to the process of using personal identification data or attributes in electronic form that uniquely represent a natural or legal person (Skierka, 2021b).

If used adequately, eID`s enable electronic transactions using safe, established, and legally legitimate identification information, enable smooth digital procedures by removing the need for paper signatures or human presence for identity verification (Skierka, 2021b). Apart from its usage in eGovernment applications, eID may assist commercial service providers to reduce their expenses associated with identity and access management. The present use, which is limited to the national environment in which the eID’s are issued, imposes a constraint on its potential (Skierka, forthcoming).

3.2 eID Management Approaches

As stated above, individuals, organizations, and objects can utilize digital identification to identify themselves to an information technology system. In the context of information technology, they are collections of attributes that are presented differently based on their usage context. In principle, a digital identity can be issued by any online service provider with which a user opens an account (Skierka, forthcoming). The spectrum of digital identities is vast, encompassing anonymous, pseudonymous, and confirmed identities. A verified identity verifies that the information presented (claims), such as the user's genuine name, corresponds to the actual person, such as by using an official identification document (Lips et al., 2021; Poller et al., 2012 in Skierka, 2021b). The unit of description and analysis is initially a national digital or eID management system (eIDMS). This broadly relates to

1) the identification, registration, authentication, and authorisation of persons, objects, and organizations

2) about the utilization of public and commercial digital services

3) with national validity tokens

4) considering the technical, organizational, and regulatory factors (Kubicek & Noack, 2010; Skierka, forthcoming).

The following components of an eIDMS can be defined:

Registration identifies an individual and/or verifies other aspects of their identity. The entity is allocated a partial identity for a certain context because of registration. In the future, the entity can be authenticated using this credential (Sedlmeir et al., 2021 in Skierka, 2021b).

Authentication is the digital validation of a stated set of qualities or facts about a person, with a predetermined or acknowledged level of confidence. Authentication entails determining the veracity of the presented information. Authentication precedes it (Aichholzer & Strauß, 2009; Alkhalifah & D'Ambra, 2012 in Skierka, 2021b).

Digitally granting specific privileges is referred to as authorization. It refers to 1) the permission of an authenticated entity to perform a defined action or use a defined service/resource, and 2) the process of evaluating the applicable permissions of an entity and determining, based on that evaluation, whether an authenticated entity is granted access to a specific resource. A permission is frequently related with an entity's authentication (Dhamija & Dusseault, 2008; Poller et al., 2012 in Skierka, 2021b)

In the sense of information, an identity is a collection of attributes associated with an entity (whether person, object, or organization). People and things, or robots and organizations, require identities in the digital environment. An identity system must aid in mapping these various items and their usage settings (Söderstrom, 2016 in Skierka, 2021b).

Services and software programs: Individuals can identify themselves to an information technology system using a digital identity. Therefore, digital identities are a precondition for the use of trustworthy digital services and the foundation of any digitization effort, whether in government, transportation, education, or industry. 4.0. It is possible to make a fundamental distinction between public services in the realm of eGovernment and those provided by private providers in business and society. In certain application domains, such as the financial and banking industry, public administration, and the healthcare industry, identity providers are subject to certain regulatory obligations. Services can manage digital identities in isolated, federated, or decentralized forms (see below) (Homburg & Dijkshoorn; Kubicek & Noack, 2010; Lips et al., 2021; Stepanaia & Jerman, 2018; Zefferer & Teufl, 2015 in in Skierka, 2021b).

Token: Tokens serve as the medium for user identification and authentication. They incorporate the credentials and properties of objects. Tokens can be composed of both hardware and software components. Tokens include, for instance, the smart card of the German eID card, USB tokens or the RFID chip, a secure SIM card, security element in the smartphone, or a hardware- or software-based One-Time Password (OTP) generator (Jones et al., 2007; Kallinikos et al., 2013 in Skierka, 2021b).

Standards: No global standard for identification and authentication has yet been created. Instead, numerous technical standards, such as SAML, OAuth 2.0, and OpenID or FIDO, have arisen during the past few decades (Tietz et al., 2017 in Skierka, 2021b). OpenID Connect is a widely used open standard that enables the seamless exchange of identity data. The dependence of users on identity providers or other central entities is a characteristic shared by all existing standards. On the other hand, decentralized approaches to self-sovereign identification (SSI) are based on standards in development (e.g., DIDs in the W3C), which do not grant any institution a central role (Lips et al., 2021 in Skierka, 2021b).

Identity management databases: In systems like directories and databases, such as registers, identity information must be saved and handled. In accordance with the notion of self-determined identity, they can also be stored in digital "wallets" on the user's devices or in the cloud (Laurent & Levallois-Barth, 2015 in Skierka, 2021b).

A national eIDMS is always embedded in an organizational and regulatory structure and consists of technological infrastructures and software components (Dabrowski & Pacyna, 2008; Torres et al., 2013 in Skierka, forthcoming).

3.3 eID Ecosystems

When many stakeholder networks are merged, a self-sustaining system known as an identity ecosystem is produced.

Participating actors and their roles

The issuer is responsible for the accurate and reliable fabrication of identities and for assuring the accuracy of claimed identities and claimed identity characteristics. In the real world, examples are sovereign documents, certificates, and plastic cards. These can be expressed digitally using digital proofs of identification that are cryptographically safe (Skierka, forthcoming).

There are several roles to be clarified in the ecosystem:

1) **Identity Providers** are a subset of service suppliers that authenticate subjects on behalf of other stakeholders in an identity ecosystem, including service or attribute providers. identity providers are responsible for issuing identities. Individuals may use self-issued identities for purposes such as entering websites. Credit card firms may issue identities that enable payment. IdPs validate the user's security and identifying information and permit the use of legitimate information credentials (Cameron, Posch & Rannenberg 2009 in Alkhalifah, 2013).

2) **Attribute Providers** are responsible for the procedures associated with the generation and maintenance of a subject's attributes. Attribute suppliers convey assertions of attributes to individuals and other stakeholders, especially service providers (Bernabe et al., 2017 in Skierka, forthcoming).

3) **Users** are often referred to as individuals who utilize digital services. Subjects may act independently (as citizens or customers) or inside organizations, businesses, or government s. In addition, users may be businesses that register on many websites and create company accounts (Skierka, 2021b).

4) Individuals and organizations are known as **Relying Parties (RPs) or Service Providers (SPs**). An Organization or service that manages access to and the modification of services based on claims made about a user by a claim’s provider. SPs are also subscribers of identity providers, enabling the Internet retrieval and input of identification information. These service providers keep user information on a Web server and secure networks (Bertino & Takahashi 2010 in Skierka, forthcoming). Both the service provider and the user limit access to specific information on a user's identity.

Actors are natural or legal beings who, depending on the circumstances, assume one or more of the just mentioned roles. As a real person, the user frequently functions as both owner and subject, as most of the ID attributes he manages belong to themselves. Legal entities (organizations) are also permitted to utilize the platform, as they engage in legal transactions and require a verified identity. Additionally, organizations may operate consumer-facing applications. This application's properties determine whether it is a publisher or an acceptor. Owners may also be applications that must display special qualities to the user (Ehrlich et al. 2021 in Van Cauter, 2016). Governance in identity ecosystems must be collaborative and not centralized to be advantageous for all stakeholders. This will require defined guidelines for the development of multi-stakeholder principles (World Economic Forum, 2019).

The possessor obtains these credentials and manages them in a wallet software or physical wallet. The holder retains full control of these credentials. The topic of an identification token is the referenced entity. This could refer to a controlled object or a person for whom the holder is accountable or authorized. However, in many circumstances, the topic and the holder are identical (Van Cauter, 2016).

The acceptance point (verifier) is a software application, an online service, or a physical entity that receives evidence of specific ID features from the holder to verify his identity or credentials (Van Cauter, 2016).

The authentication technique grants users access to the resources of service providers utilizing the same platform (Bertino & Takahashi 2010 in Van Cauter, 2016).

Infrastructures are defined as shared, open, limitless, and evolving sociotechnical systems comprising of a collection of information technology capabilities and their associated users, operations, and design communities (Hanseth and Lyytinen 2010). The concept of digital infrastructures has contributed significantly to the subject of information systems, since it has helped to move the perspective and unit of analysis from single organizations to organizational networks and infrastructures, "enabling for a global and emergent perspective on IS" (Bygstad 2008 in Van Cauter, 2016).

3.4 Key Success Factors of eID Acceptance

It is crucial that service providers (applications) and their users diffuse, accept, and use the system. Rogers, as noted in Chapter 2, stated that the diffusion of a technology is contingent on five factors: visibility, relative advantage, complexity, compatibility, and trialability (Rogers, 2003, (Van Cauter, 2016).

The most important element for eID acceptance is that as many people as possible utilize the eID scheme without being deterred by cumbersome procedures. Nonetheless, users must be distinctly recognizable to execute legally compliant transactions: If done right, all approved users are

provided access without the requirement for additional registration. Users are identified in a unique manner for secure online services. Verification of identity and management of personal data require minimal effort. Integrating and utilizing an identity management solution is inexpensive. What was just described can be understood as an ideal scenario situation.

Identity management service providers must be as appealing as possible to users and to succeed in the market. There is a positive network effect between the number of acceptance and the number of users: the higher the acceptance of a service, the more attractive it is to prospective users, and the more users a service has, the more likely its operator is to maintain it (Laurent & Levallois-Barth, 2015; Laurent, 2015 in van Cauter, 2016).

Lack of organizational collaboration in inter-organizational efforts or programs is a significant obstacle that must be addressed (Kubicek and Hagen, 2000). In general, agencies operate too independently; their programs are frequently poorly coordinated (Irani et al., 2007, (Van Cauter, 2016). Throughout the history of national e-ID development, this weakness has existed (Gronlund, 2010; Soderstrom and Melin, 2012 in Van Cauter, 2016). It has been established that administering eGovernment projects presents a variety of challenges. Numerous causes of failure have been identified (Sarantis et al., 2011 in Van Cauter, 2016), including the following:

- a lack of internal ownership;
- a weak strategy and/or vision;
- poor project management (including technology management);
- a technological infrastructure that is incompatible; and
- data transfer problems (Van Cauter, 2016).

In order to avoid delays, failures, and blockages in the development of eGovernment, Kubicek and Hagen (2000) identified six important barriers to overcome. As other scholars confirmed, a crucial area is a lack of organizational coordination, the second is a lack of legislative limits, the third is the required zone of preconditions for technology, and the fourth is human factors (Van Cauter, 2016). The final obstacle is insufficient funding and political support. Reel (1999) also published indicators of project failure and they appear to be prominent in contemporary e-service development (Heeks and Stanforth, 2007; Melin and Axelsson, 2009 in Van Cauter, 2016).

These indicators are consistent with the previously described eGovernment trends. Included are the following examples:

- the project scope is unclear;
- project modifications are inadequately handled;

- the chosen IT changes;
- business demands change;
- timelines are unreasonable;
- users are reluctant;
- project sponsorship is lost; and
- the project lacks individuals with the required capabilities (Heeks and Stanforth, 2007; Melin and Axelsson, 2009 in Van Cauter, 2016).

To summarize, electronic identification has many ways to be defined and therefore agreeing to one definition for the duration of the research has been reached. The ways of how to manage eID data is also diverse, but important to understand before looking at the German eID scheme. The same goes for eID ecosystem approaches and key success factors or failure factors of eID implementation projects. Especially the eID success and failure factors will serve as a great explanatory baseline for the results that were found (see Chapter 6).

4 Research Design

To follow a thorough research design, the research onion by Sauer (2008) serves as the ideal guidance tool. The approach is to choose one or more principles per "layer" and then follow their steps accordingly. The following Chapter will present the different approaches chosen for each layer of the onion.

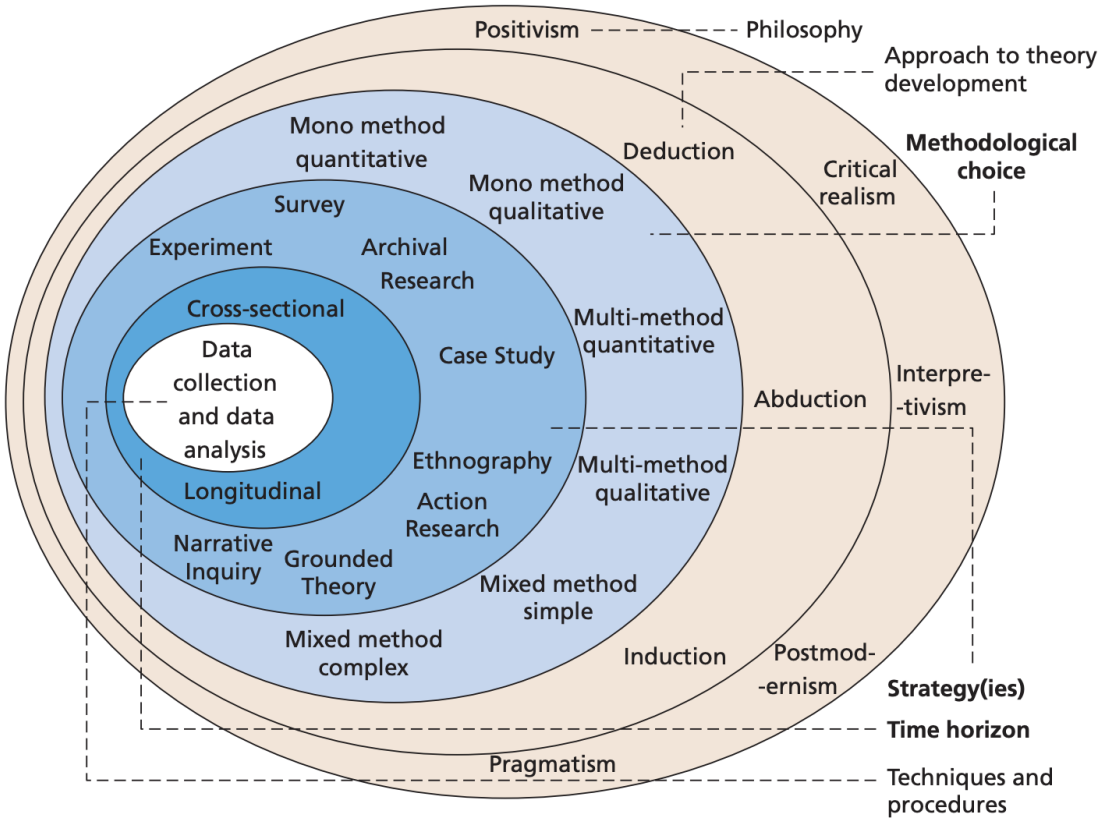


Figure 6 The Research Onion by Saunders et al. (2019)

4.1 Research Philosophy

Interpretivism

As this thesis is using contextual factors and social groups as in stakeholder groups, the most appropriate philosophy to start scientific considerations is interpretivism. This philosophical approach is focusing on "the way we as humans attempt to make sense of the world around us" (Saunders et al., 2019). While trying to understand the ways in which the societal context and acceptance factors of the eID scheme have so far failed to diffuse in society – interpretivism makes the most sense to use.

4.2 Research Approach

Exploratory

With an exploratory study, the topic of interest is explored with open questions. Typical research questions ask a "What" or "How" question. As this thesis is trying to explore the influence of acceptance factors and societal contexts on the diffusion process, the exploratory approach is most appropriate (Saunders et al., 2019). In that sense, the contextual and acceptance factors serve as the X-Variable. Their influence on the diffusion and overall system acceptance is then tested. Therefore, the diffusion in terms of implementation of the ID infrastructure/use cases and usage serve as the Y-Variable. The techniques to collect data also followed the suggestions by Saunders et al. (2019). Literature Research and expert interviews with semi-structured questions were used. The questions used in the survey were also of exploratory nature.

4.3 Research Strategy, Choices, and Time Horizon.

Case Study

When a topic is researched in a "real-life setting" and there are clear boundaries to which it is researched, it is called a case study (Saunders et al., 2019; Yin, 2018). As this study is researching the diffusion of the eID scheme in Germany (ePA) and its consequences on three levels, the appropriate research strategy is a case study. Other strategies do not have the same focus on the real-life setting of a topic and are therefore not an as a "good fit". The choice of Germanys eID introduction as a case has been done due to its international relevance and unique phenomenon of a country that should have all financial (and other) resources to successfully diffuse an innovation but having struggled the way it has for almost 13 years and counting.

Mixed Method:

A mixed-method choice means to use both qualitative data as well as quantitative data (Saunders et al., 2019). As this thesis has first used semi-structured expert interviews for its qualitative data collection method and then used a survey as a quantitative data collection method, it can be characterized a sequential explorative mixed method research design. The initial set of findings that were collected during the interviews was therefore expanded with the survey so that all three interest groups of the theoretical framework could be analysed.

In this thesis, the qualitative research method is dominant as more topics were being covered – therefore more in-depth data was collected. On the other side, the data from the survey covered less topics, though the quantity of participants was considerable higher as is described in the section on the survey in 4.4. All findings were triangulated to research mutual effects on the diffusion of the eID scheme on all three stakeholder groups and to fill gaps that could not be

researched with just one method (interview for government and service provider level and survey for end user level).

Cross-Sectional Study

A cross-sectional study is done while looking at a phenomenon or topic during a particular point in time or time-span (Saunders et al., 2019). As this thesis is looking at a specific timespan from 2010 until today, this time horizon makes most sense. Data was mostly collected during one time – making the data collected of cross-sectional and not of longitudinal nature. Some interviews were already collected in 2020, though not everyone who was interviewed was available again in 2022. Hence, this study cannot be a longitudinal study. To fill the gap of interviewee availability, an additional batch of new interviews were conducted. Hereby focusing more on the service provider level.

4.4 Data Collection and Analysis

The data that was used is collected in three steps. First an extensive document analysis is conducted as it serves as a basis for the questions being asked at step two. Step two are semi-structures expert interviews. The information that was gathered with documents and the theoretical framework at hand leads the way that the questions are asked. The deductive method then leads into an inductive third step as new information is gathered through a survey. The specific steps are described in detail underneath the figure.

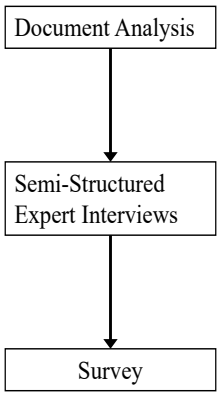


Figure 7 Data Collection Strategy

Document Analysis

This thesis is using both scientific and grey literature as a source for triangulation and contextualizing the data that was gathered through the mixed-method approach (Saunders et al., 2019; Valtna-Dvořák et al., 2021; Yin, 2018). Especially for clearing central definitions and the state of the art on current eID research, the document analysis data collection technique was used. Findings of such are presented during Chapter 3. The document research technique is always reliant to the researcher's collection technique. One thing that is sure is that the collected

documents will never be fully complete, as some documents are not accessible to the researcher. Some documents at hand also weren't public and could only be used in a limited way. The public documents that were analysed, were systematically researched via the limo.libis.be and google scholar platforms with the following keywords being used by themselves or in combination with each other: "eID", "electronic identification", "eIDMS", "eID ecosystems", "technology acceptance", "diffusion of innovation", "Elektronische Identität", eGovernment in Detuschland", etc.

Semi-structured expert interviews

The benefit of expert interviews is that they provide researchers with access to extensive insider information about the research object (Meuser & Nagel 1991: 442). Expert interviews can "supplement statistical data with context" (Pickel & Pickel, 2009).

Semi-structured interviews are the optimum way for obtaining the most information from experts since the interviewer can modify the questions and adapt to impromptu events in real time (Pickel & Pickel, 2009). As the thesis is using a theoretical framework as its basis, the themes of the questions were deducted from the framework. The questionnaire can be found in Appendix B is German and its English translation. In practice, the questions at hand were only used as a guidance, while the interview followed a much more open character to react to the information given by the expert in real time.

The expert interviews were conducted during a period of two months. Some expert interview built up on past interviews that were done with the same expert in 2020, when the researcher first looked at the topic of eID in Germany during their bachelor thesis. Due to codification and anonymity of the data gathered, it was possible to use the same date from back then and conducting more interviews during this research period. The experts that were interviewed can be found in Table 1. A more detailed table on the specific organisation, date, and duration of the interviews can be found in Appendix A. The transcripts are provided via a separate folder in Toledo. Some interviews were not allowed to be taped, therefore only notes exist. As all documents are in German, a translation may be requested.

Code	Position, Field of Expertise
IPG1	Member of the Ministry of Economic Affairs, Department of Research & Development in the Field of Digitalization (Interviewed in 2020)
IPG2	Head of Unit: BSI (Interviewed in 2020)
IPG3	Head of Unit: BVA (Interviewed in 2020 and 2022)
IPG4	Director of Secure Systems Engineering at Fraunhofer Institute for Applied Integrated Security (AISEC), former project leader of nPA Project at Ministry of Interior (Interviewed in 2020 and 2022)

IPS1	CEO of ID Service Provider, Former Director of IT in Ministry of Interior (Interviewed in 2020 and 2022)
IPS2	CEO ID Technology Provider (Interviewed in 2020 and 2022)
IPS3	Director at IT-Consultancy (Interviewed in 2022)
IPS4	Director Identification-as-a-Service Provider (Interviewed in 2022)
IPS5	Director ID-Server Provider (Interviewed in 2022)
IPS6	Director ID Trust Service Provider (Interviewed in 2022)

Table 1 Experts that were interviewed

Survey

While qualitative research is meant to bring in-depth insights, surveys can bring results from a much broader audience (Saunders et al., 2019; Yin, 2018). The questionnaire created by the researcher during research conducted in the research project that they are part in, was created following the outputs of prior conducted expert interviews. While the questions during the expert interviews were directed at the government and service provider stakeholder groups, the questionnaire for the survey was more generic and directed at the end user level. Questions were either multiple choice or one choice only and followed four major themes. It was sent over the Internet and was able to reach between 5001-5003 participants during a time span of four days and spread by CIVEY[2]. Only by doing so, data on end users was conductible, since planning focus group interviews or other lengthy techniques were out of the time scope of this research. The questionnaire of 10 questions can be found in Appendix C, the raw data is provided via a separate folder in Toledo (with Password: LSMS22).

Thematical Coding Technique

The data at hand comes mainly from interviews that were allowed to be recorded and were transcribed. Some were not allowed to be recorded and hence only have written notes serve as their source for data. Transcripts of the recorded interviews are provided via a separate folder in Toledo to save space of this document. The transcripts are in German and can be translated on request. The interviews were analysed and thematically coded by themes that were deducted of the theoretical framework, employing arrays of dimensions established in the framework and literature review, such as contextual, acceptance and key success factors. Themes that have been analysed are therefore placed and classified in the appropriate dimension category. The steps for analysing the data from the interviews are transcription/note reading, coding, analysis, and writing (Braun & Clarke, 2006). The coding of transcribed interviews was done in Microsoft Excel and is also provided in separate folder in Toledo (with Password: LSMS22). During the coding process, theoretical thematic analysis is chosen. Passages from the interviews are sorted

[2] Company for Market Research and Professional Surveys

according to the respective themes of the theoretical framework. Themes in that sense are the variables and topics that count as sub-variables that came up in during the interviews.

4.5 Limitations and Implications

As interpretivism is highly reliant on the data collected by the researcher, the context from which the interview partners came from must be carefully considered. Other philosophies were rules out as they did not take the context and social groups into account. A limitation of the survey approach is the reliance on the quality of information contained by experts or participants of the survey. Surveys are mostly unable to contextualize the answers of its respondents apart from socio-economic factors as age, gender, income, etc. (Venkatesh et al., 2013).

Additionally, since the topic of eID is not widely known as it has already been proven numerous times, answers of respondents often showed that they simply didn't know what the question was asking as shown in Chapter 6.3 (Arkwright, 2022; Podgorelec et al., 2022; Saunders et al., 2019; Skierka, forthcoming). These possible shortcomings can be handled by an extensive document analysis process. As other approaches handle more concrete ways of asking questions and are narrower from the start, they did not fit the research goal of this thesis. When looking at the keywords being used for the document research it must be noted that the list is not expensive as some papers were found through the snowball technique when going through the references of relevant publications. A document list can never be complete as access and knowledge of other possible literature sources is limited.

Since this thesis is focusing on one case, the generalizability is lower. On the other hand, the questions used in the semi-structures interviews and survey could be asked differently. So far, the theoretical framework has not been applied to a pure national context, hence the adjustment to the framework is exposed to bias of the researcher. The chosen interview partners are also limited to availability and do not cover every stakeholder that is involved in the ecosystem hence the data does not cover all possible implications.

The method of expert interviews has some downsides as well. The sample selection of the researcher determines the overall body of data. To be able to identify the suitable experts for a research topic, one must have collected sufficient knowledge in that area (Pickel & Pickel, 2009). Choosing expert interviews as a data collection strategy also requires a substantial expenditure in the production of the interviews themselves (Pickel & Pickel, 2009).

In summary, the research onion is a great way to structure someone's research design. All layers were presented and chosen approaches of each layer properly explained Discussions on scientific and subjective limitations lay an appropriate baseline for the following research.

5 The German eID Case

5.1 General Facts of Germany

Germany has 83,2 million citizens. The political system is a parliamentary democracy with 16 states and one federal government. The public sector belongs to the continental-European federalist profile by Kuhlmann and Wollmann (2019). While the federal government writes most general laws, the states are responsible to impose them and can decide how exactly they want to do it. The broadband coverage, therefore access to the internet has reached 95%, while 89,8% use the internet (KPMG, 2022). The median age in Germany is 45,9 years old (KPMG, 2022). The AusweisApp2 has been downloaded 2,2 million on iOS, 2,5 million on Android, and 3,8 million on a computer (Windows, MacOS), which equals to 8,5 installed AusweisApp2's (IPS2). As of today, 97% own an ePA, while only 35% have an activated online-authentication function (Monitor, 2021).

5.2 Chronological Events of the Diffusion of the eID Scheme 1997-2022

eSignature and Preparation to nPA pre-2010

The first attempts at electronic features on identity cards were made by the signature alliance[3], not the "elektronischer Personalausweis" (ePA) back in 1997. After the Signature Act was passed, the data records' ID attributes were removed, but the necessity to identify individuals in administrative procedures prevailed. In 1999 the European Parliament followed the German directive and passed the eSignature Act "on a Community Framework for Electronic Signatures"[4]. In the same year (the current German government coalition consisted of the Green Party and the SPD) the first eGovernment program was drafted: BundOnline2005.

Then the first electronic passport discussions began in Germany and the then-responsible Ministry of Economic Affairs chose to incorporate the eID functionality into the identity card. In 2003, the effort to introduce an electronic identification card began from "scratch" (Kubicek & Noack 2010, p. 89). To achieve the highest possible security standards, the Federal Office for Information Security (BSI) was consulted as the appropriate technical authority for technical issues (related to the Ministry of the Interior). The Ministry of the Interior's plans to introduce new travel documents with eID tokens were greeted with resistance from the Ministry of Economic Affairs, which insisted on digital signatures. As a result, the nPA incorporates both the chip and the e-Signature certificate. Before 2005, the "Deutsche Industrieforum für Technologie" (DIF)[5] founded a specialization unit for eID solutions.

[3] The Signature Alliance was responsible for bringing forward the most prominent digitalization projects in the 90's.
[4] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31999L0093
[5] The DIF serves as a platform for technological technologies and coordinating force in order to collect expertise on emerging technologies

Until then eID solutions weren't on the radar of the German government. After the BundOnline2005 program was finalized, it was clear that not much happened in the eID area. Then the ruling cabinet (Green Party[6] and SPD[7]) started a new program that focused on the ID card: "eCard Strategie" (Kubicek & Noack, 2010). The program was supposed to help with the interoperability of the existing federal card project and an upcoming new ID card. As a result, the German Ministry of Interior created a new unit (IT4) that would be responsible for passports, ID cards and registration matters.

After the federal elections in 2005, a new coalition was formed with the SPD and CDU[8]. The new coalition took the matter of eGovernment reforms into their hands as well and started the eGovernment 2.0 program, which also focused on the new ID card and an eID concept. During the discussions on the elements of the ID card, the prior decision of adding mandatory fingerprints onto the smartcard (a result of the 9/11 attacks in NYC) was rejected by parliamentary groups (Kubicek & Noack, 2010). At the same time the so-called STORK Project was started as a large-scale pilot (LSP) by the European Commission (EC) groups and member states. Project was supposed to build an interoperability layer in order to connect national eID schemes of Member States (Brugger et al., 2015).

The application testing focused on integrating the eID function into services of application system from, (Kubicek & Noack, 2010, p. 93). The project members anticipated that NFC[9] interfaces would eventually be available on most mobile devices and integrated it as their chip interface. The members of the project believed that once the eID-card was introduced, electronic services would automatically be created. At the time, requirement engineers and project managers did not prioritize the user perspective - the field of User Experience (UX) had not yet been an established area (IPG3+4).

In 2009, the grand coalition of SPD and CDU passed the nPA bill shorty before the federal elections. The grand coalition thereafter disbanded, and a new one was formed of the CDU and FDP[10]. As the new coalition member, the FDP opposed the project, resulting in a complete cut of the marketing budget of the 2010 nPA rollout. Official testing of the new identity card and possible use cases began one year prior to the deadline by the end of 2010. The chip and interface were not fully developed until after it was launched in November 2010. As a result, the project team had no time for necessary improvements before it entered the market.

---

[6] The Green Party aka Bündnis90/Die Grünen is a federal party of the German parliament. https://www.gruene.de/
[7] = Sozialdemokratische Partei Deutschlands is a federal party of the German parliament: https://www.spd.de/
[8] = Christlich Demokratische Union Deutschlands is a federal party of the German parliament: https://www.cdu.de/
[9] NFC = Near Field Communication – _ "it enables short-range communication between compatible devices" _ (androidautority.com viewed 22.6.2020 https://www.androidauthority.com/what-is-nfc-270730/)
[10] = Die Freie Demokratische Partei Deutschlands – Liberal Party of Germany

Test + Rollout Phase of nPA 2010-2013

As of 2010, the nPA served three purposes: as an eID, a machine-readable travel document, and as a National Identity card (Alkhalifah & D'Ambra, 2012). The eID card had an optional online-authentication function, that needed to be activated by the end user when picking up their new ID-card (also called Opt-In approach). For potential service providers to enter the eID scheme, they had to be authorized by the Bundesamt für Sicherheit in der Informationstechnik (BSI). The requirements to be met were written by their data security experts. At that point one use case needed one authorization certificate. To use the ePA, potential users had to purchase an external card reader. During the first year, that measure was subsidized by the German state.

Because the marking budget was cut, there was never a true product launch. Municipal office employees were unable to receive professional training to be able to consult interested citizens on the nPA (Kubicek & Söderström 2015: 6). By the beginning of the rollout phase, there were three trusted partners that were authorized to give out authorization certificates to new interest groups as their service: The Bundedruckerei (BDr), The German Postal Office, and the German Telekom[11]. As no uptake of ePA usage numbers was detectable by 2011, the first private sector service providers withdrew. During the rollout phase, there were many attempts to cooperate with the banking sector, as their use case was more common than the use of German public sector services. No cooperation was succeeded during that time (until today).

By the end of 2012, the STORK Project was finalized and by the beginning of 2013 the STORK2.0 was started. In the 2.0 version, the project focused much more on standardization and possible solutions to bring national eID schemes to the next level (Brugger et al., 2015).

Europeanisation + Simplification 2013-2017

As of 2013, there were 147 (40% public, 60% private) services that supported the eID authentication (Fromm et al., 2013). They could be used for a wide variety of daily purposes. On the other hand, a common reluctance among private sector service providers was detected to build such eID-supporting services, particularly when the current solutions (for example, bank authentications) already successful (Fromm et al., 2015). In the same year a study investigated the reasons why the end users didn't activate their online-authentication option. 70% opted out of the activation due to a lack of consultation by public servants as they picked up the card (IPG4).

[11] The Bundesdruckerei is a private company that is 100% owned by the federal government and prints ID cards and other printable credentials for the German state. https://www.bundesdruckerei.de/de

The application that served as the gateway from the nPA to another device (AusweisApp) was taken over by Governikus in 2013. During that time, experts at the OmniCard Conference[12] agreed that the nPA will never move onto the smartphone. On the other side, the Ministry of the Interior, Federal Administration Office, Federal Printing Agency, and the Agency for Information System Security, began their first consultations on bringing the nPA onto the phone just one year later as the predominance of mobile phones couldn't be ignored anymore (IPG2+4). As a result, to the talks, the Fraunhofer Institute conducted a feasibility study.

In 2014, the EC passed the eIDAS bill[13]. The Agency for Information System Security was a major influence on the security standards that were set during that bill (IPG2). Due to the new high standards, other countries that already established their eID schemes had to make heavy adjustments (Skierka, 2021a).

Prior to the start of the new legislation period in 2017, the German parties FDP, Greens, and CDU discussed the creation of a Digital Ministry. When the negotiations broke down and a new coalition government was established with the SPD and CDU, the idea of a Digital Ministry was deleted from the coalition treaty. Rather than that, the government determined that prior to establishing a digital ministry, the public administration must be digitalized. As the new cabinet, the topic of digitalization was put on the agenda again, as with the other coalition formations.

Second Simplification Phase: 2017-2020

Resulting from the just mentioned decision, the newly formed cabinet (SPD + CDU) passed the Online Accessibility Act (OZG), committing the country to digitalize all public administrative services by the end of 2022 (OZG, 2017). However, previous studies demonstrated that Germany has historically struggled to undertake effective digital projects due to its cross-sectional nature (Kubicek & Noack, 2010; Nortal, 2020b). In the same year, Governikus introduced the AusweisApp2 as an app for mobile phones (first on android only) which made the card readers obsolete. The AusweisApp2 was a first step of bringing the nPA and mobile phone closer together. Later that year, Apple also allowed their NFC interface to be used for reading the ePA. By the end of 2017, the cabinet adjusted the nPA bill, now citizens had to actively decide against the online-authentication function of the nPA (also called opt-in). Otherwise, it would be activated by default. The local readability option was introduced. Through this, end users were able to use their ePA at banks or other areas without needing to know their PIN. Even though this hurdle was resolved, the resetting of the PIN fee remained at 6€.

[12] A conference for anything smartcard. Is called OmniSecure today: https://omnisecure.berlin/
[13] = on electronic identification and trust services for electronic transactions in the internal market

During this time, there was no central coordinating agency for the management and development of electronic identification (Nortal, 2020a). Even though the German government was increasing its investments in public-private partnerships, the multilevel eGovernment was hampered by federalist structures and an inflexible public administrative culture (Kuhlmann & Wollmann, 2019). Especially since the technical implementation of federal law like the OZG or nPA bill has been entirely up to the municipalities (IPG3+4).

Pandemic and MobileID Phase 2020-today

By the beginning of the Covid Pandemic there was still no established eID scheme nor use cases that could have supported the public infrastructure during lockdown phases. This is where the entire topic of eGovernment reached its peak in popularity (pwc, 2021). That factor will be covered in the results Chapter while looking at the different stakeholder groups. Due to its political popularity, the German chancellery attempted to introduce an ID Wallet with the driver's licence as their showcase use case. Because, they didn't properly consult data security experts and built their technology based on blockchain, they opened the security walls to hacking attacks by the hacktivists[14]. After 72 hours and officially naming server overloads as the reason of failure the chancellery took the ID Wallet app out of App Stores.

Today, among the federated identities are the electronic identification card (ePA) with electronic ID (eID), the electronic residency permit, and the electronic passport. This identity is not managed by an identity management system, but is a sovereign authentication mechanism with an added digital representation (Skierka, forthcoming). Germany does not centrally maintain identification data. Rather than that, a specialized ID infrastructure (eID server) is employed to send the eID data from the ID card to the acceptance point. To do this, the user must have an electronic ID document with the eID feature active and the AusweisApp2. Through that, the owner of the identity can validate themselves digitally without having to re-register (Pohlmann 2019 in Skierka, forthcoming). Identification with the nPA meets the highest trust level which is set by eIDAS. As of today, eGovernment services make up 40% of authorization certificates, while e-Business services account for 60%, nothing has changed since 2014. After eight years of operation, the rate of implementation, or the activation of the online identifying function, is around 50% (Skierka, forthcoming). Still, the ePA implementation is regarded as one of the greatest IT projects undertaken by the German government (IPG3+IPG4). More than 60 million German citizens now have access to the ID infrastructure. More than 23,000 personnel from more than 5,300 government agencies have been trained in the nPA working procedures (Thales, 2020).

[14] German hacktivists, mainly come from the Chaos Computer Club (CCC) and represent the interests of hackers and data security experts on all topics related to personal data, digitalization of the public sector, etc.

In 2021 the last federal election took place, and the big coalition was replaced by the SPD, Grüne, and FDP. With the new coalition the digitalization and nPA issue was taken up again and specifically written into the coalition treaty (Regierung, 2021). As a result, the mobile eID project called “Smart eID” was launched by Federal Administration Agency, the Federal Printing Agency, Agency for Information System Security, and the Ministry of the Interior (as well as other stakeholders). With this project, the online authentication option of the nPA can be derived onto the secure element, which is an independent hardware token on the mobile phone. The project is part of an analysed variable in Chapter 6, hence less detail at this point.

To summarize, the history of eID in German public and private sector dates to the mind 90’s. Back then, Germany was one of the first in Europe to think about the electronic presence of one’s identity. Since then, Germany has not been able to hold its pole position in being a pioneer. The country has had to fall back to the lower quarter of digitalization rankings (Commission et al., 2021). Many factors have played and still play a role in the struggle to diffuse the ePA. Today, the ePA still is neither accepted by end users nor adopted by service providers. The figure below shows a detailed timeline of legal and sectoral events that have played a role in the creation of today’s eID scheme. Consult the legend for the respective color codes.

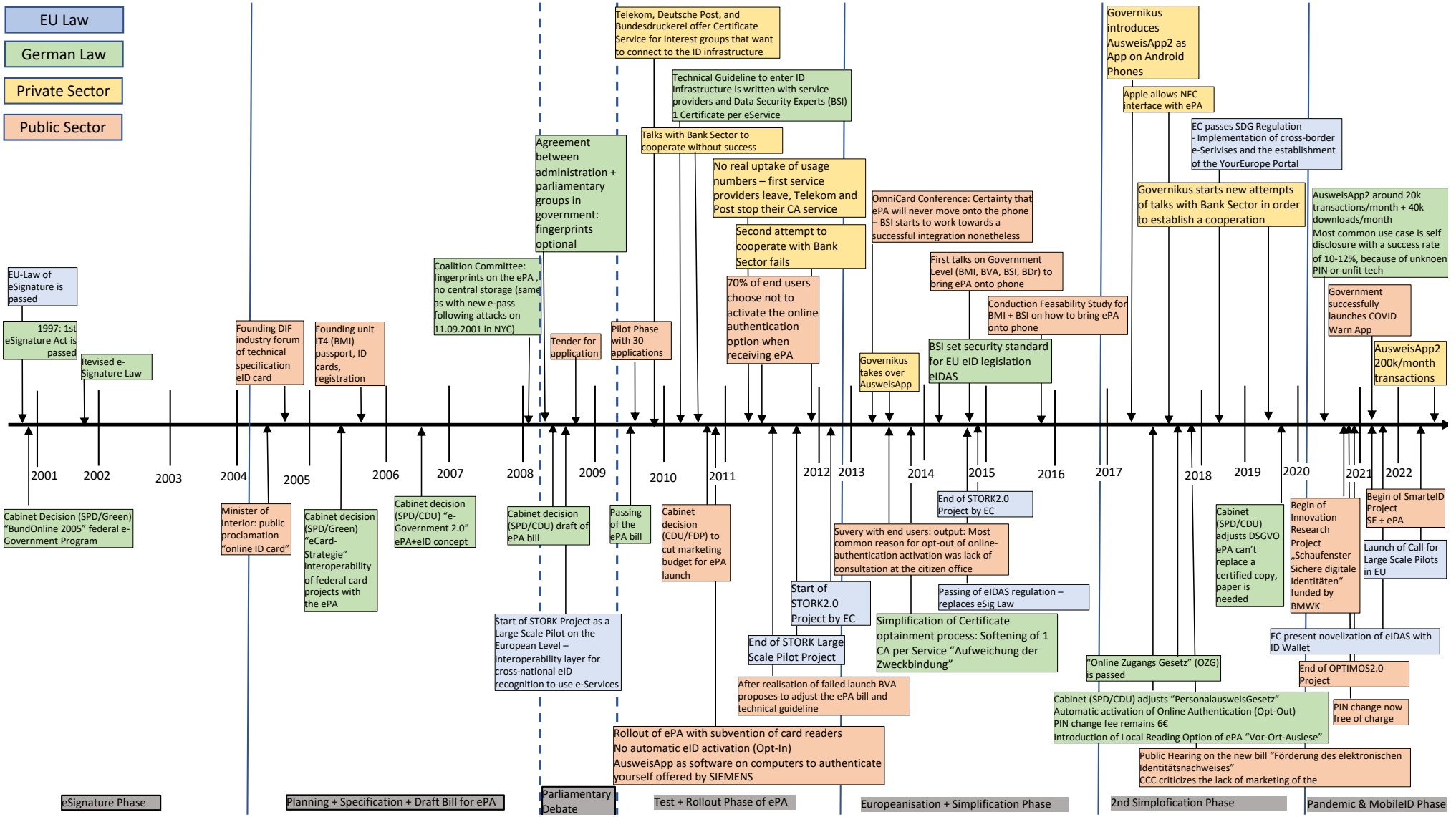


Figure 8 Timeline of eID focusing on EU (blue) and German (green) Law as well as Public (orange) and Private (yellow) Sector events 1997-2022

6 Results and Discussion

The following Chapter looks at the three stakeholder groups following the theoretical framework by Brugger et al. combining TAM and DOI. At first contextual factors are presented, followed by acceptance factors. The Chapter will end with looking at “mutual influences of acceptance and success factors” (Brugger et al. 2014) as it was done in the work of Brugger et al. To increase readability and doubling of content, the results and discussion section are synthesized and combined into one Chapter.

6.1 Government Stakeholders

Government stakeholders are both part of the legal and implementation side of the eID scheme. As they are responsible for the well-being of the ID infrastructure and the production of new solutions, they showcase an interesting stakeholder group. During their daily work, they need to solve issues like product management or how the needs of service providers can be aligned with the IT infrastructure. Even though government stakeholders are responsible for the diffusion of the nPA, it seems as if basic product management concepts are not applied. Following Roger’s DOI one measure is weather mass media, or an individual approach is chosen as the communication channel. In retrospective, the initially chosen diffusion strategy on an individual basis had a limiting influence on the ePA diffusion. The individual approach doesn’t lead to an increase of acceptance. Because of that path dependence, public servants aren’t trained, the nPA isn’t properly introduced on the first encounter, and the key success factors mentioned din Chapter 3.4 aren’t met. Registration offices and immigration offices, as well as consulates and other locations, don’t contribute to an increase in the diffusion.

During the first encounter advertising happens and citizens decide whether the nPA meets their expectations on an innovation (so complexity, relative advantage, compatibility, trialability, and observability as well as acceptance factors). Since 2010, many showstoppers have been abolished. Examples are the automatic activation and the free PIN changing service. The next step is to focus on onboarding and utilization. Once that is fixed, and citizen offices use their capability of properly introducing the ePA, a major hurdle of the so far negative network effect will be solved. One way this is that the citizen offices offer the automatic installation of the AusweisApp2 and the nPA onto the phone once the Smart eID is established (IPG3). Before that, the staff must realize that demonstrating and advertising the municipality’s’ digital capabilities is a win-win situation for everyone. If the ePA offers a benefit to the process that existed before, it will dissolve.

So far, no change agent is officially and publicly responsible for the diffusion of the ePA. A central determinant of the acceptance rate is not given and hence no communication channel can be found that is in force. For a successful diffusion and efficient communication channel, a “face” from the political leadership is needed. That person needs to represent the eID efforts permanently. The federal CIO is a possibility to become a representative of this (IPS1). In practice though, the CIO must adhere to political interests (IPG3+IPS1). Another issue with the CIO is that they represent not just eID efforts but all information system project in Germany. The role of the CIO is placed in the Ministry of the Interior and is rather meant for representation but not connected to power. They still need to coordinate a multitude of interests. When five ministries express different opinions on how to diffuse the ePA, the practice of doing it is much more complicated (IPG3).

On the other side, the public administration has so far not taken a leading role in the diffusion of the ePA. After all, the ID card is a sovereign document issued by the state and is mainly used for administrative use cases or in highly regulated areas such as banking and insurances. However, so far, the most public administration offices have not integrated the nPA into their own systems (IPG4).

So far, the government level has not prioritized the ePA diffusion and spent their resources elsewhere. Even with a public household increase of 40% during Angela Merkel's years as a chancellor. Therefore, the argument that there are insufficient resources does not follow up and is merely an issue of prioritization (IPS2). Currently, the Ministry of Economics, the Ministry of Transport, the Ministry of the Interior, and the Chancellor's Office are dealing with some aspect of the eID scheme in Germany. Considering the key success factor of having one coordinating force during the diffusion process, the current practice is much different. Through that resources are wasted. The present Digital Ministry inside the Ministry of Transport, which looks at digitalization subjects such as digital identities or data, as well as other overarching social issues, has no real authority. Even though it was initially given a coordinating role; the specific themes are handled by other ministries and the Ministry of the Interior took over that responsibility. Multiple prior presented factors that will lead to a diffusion failure have so far been met (Van Cauter, 2016):

1. a lack of internal ownership;
2. a weak strategy and/or vision;
3. poor project management (including technology management); and
4. project sponsorship is lost.

To summarize, there are currently too many stakeholders, with too many competing interests. New actors also attempt to enter the ecosystem accompanying federal funding projects. All agree that digitalization is an important problem, but in-depth knowledge in this area is lacking (IPG3+IPG4). Everyone wants to have a say. Through that it ensures that the diffusion of the eID scheme will is not successful. Every five years, strategy sessions are held, with the statement, "We have a chicken egg problem.". As the most recent effort, the Ministry of the Interior has taken over the primary responsibility for digital IDs. As the German government level is diverse and the complex to analyse, it makes sense it makes sense to look at specific contextual and acceptance factors.

6.1.1 Contextual Factors

Legal Context

Back in 2010, the challenge was that there was very little interpretation of **mutual authentication**. To solve that, the service providers and data protection experts got together and developed common legal and technical guidelines (IPG3; IPG4+IPS1). As the guidelines were drafted, involved service providers applied them (see also Chapter 5). Since then, work has been carried out in accordance to these guidelines (BSI, 2017). Because of the two classic instruments of data protection: eligibility and purpose limitation, initially each service would get its own certificate. After only three months, it became clear that the prices demanded by certificate authorities were too high for small municipalities (IPG3). Since then, minor changed have been made such as the easing of binding certificates. Other than that, the BSI has no plans to loosen the technical requirements (IPG3).

Today, there are **different regulatory requirements** depending on the sector. In addition to the public sector, these include identification and authentication in the financial sector (cf. § 12 (1) and § 13 (1) GWG15 and Art. 97 PSD2-RL16), in the healthcare sector (cf. § 291 a SGB V17), telecommunications sector (cf. § 172 TKG18) or identification within the framework of qualified electronic trust services (cf. Art. 24 (1) eIDAS19) (Skierka, 2021b).

Everything that specifies nPA technology is written into laws and technical guidelines (Kubicek & Noack, 2010). So, if a member of the government level wants to **alter the legal grounds**, the cabinet need to rewrite the entire legal foundations, which takes time. Technological guidelines are difficult frameworks to alter since expertise on technical specifications and the cyber thematic are hard to find in the public sector (IPG3). When someone tries to explain to the lawyer

[15] https://www.gesetze-im-internet.de/gwg_2017/
[16] https://www.bundesfinanzministerium.de/Content/DE/Downloads/Gesetze/2017-07-21-G-z-Umsetzung-d-Zweiten-Zahlungsdiensterichtlinie.pdf?__blob=publicationFile&v=3
[17] https://www.gesetze-im-internet.de/sgb_5/
[18] https://www.gesetze-im-internet.de/tkg_2021/__172.html
[19] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=DE

who is responsible for said alteration, that technological advances are significantly faster than the creation of legal foundations it mostly doesn't speed up the process (IPG4).

The **eIDAS Regulation** establishes a technical and legal framework for the mutual recognition of state-notified eID systems (Skierka, 2021b). As already mentioned in Chapter 5, it sets requirements for three different levels of trust of identification systems: "low," "substantial," and "high." The exact requirements for achieving the trust levels are specified in the Implementing Regulation (EU) 2015/150227. The BSI has outlined the fulfilment of the trust levels of the identification through the ePA up to "high" (BSI, 2017). eIDAS is supplemented at the national level by the Trust Services Act (VDG), which specifies the implementation of the eIDAS regulations for trust services. It defines the Federal Network Agency (BundesNetzAgentur/BNetzA) as the supervisory body for trust services at national level (Skierka, 2021b) In the perception of government experts, the amendment of the current eIDAS Regulation makes sense, because the eIDAS Regulation currently does not achieve a European solution for digital identities (IPS1+IPG1). So far, only weak recognition rules have been written into the regulation, which in recent years has not led to a uniform European identity or to interoperability of identities in Europe. There is a patchwork of digital identities that correspond to some trust levels, but so far there is no movement towards interoperability and unification (IPG1+IPS1; (Skierka, 2021a).

Simultaneously, the **big platform companies** (Apple + Google) are beginning to occupy the issue of digital identity (Shekar, 2021). If there are no European steps towards unification, the platform companies will take over most of the market of low and substantial assurance levels, because of the need for unified solutions that is prevalent among users (see also Chapter 6.3.1). Therefore, the move of the European Commission to proceed into the direction of unified European identities or interoperable systems is a logical step in accordance with current market regulations such as the Digital Markets/-Service Act (IPG4+IPS1).

Another cross-sector regulation is the EU **General Data Protection Regulation (GDPR**). With the passing of the DGPR, processors are obliged to ensure the security of data processing in accordance with the "state of the art" (Skierka, forthcoming). A negative example from the GDPR, it says that you can't scan anything electronically. Now you must submit a certified copy. That would also not be a problem, if you could replace this copy with the ePA, but it doesn't say that. So, a lot of potential is lost through false adjustments. The same thing is currently happening in the Verification Act. Employment contracts must be signed in paper form (Schulze, 2022). Instead, a rule exception system is needed: written form should only be required if it is justified.

In that sense, the German government level both needs to follow German but also European regulations that specify how to handle the personal data of their citizens. This comes with the price of an **overspecialization** when it comes to data privacy, since Germany has a unique commitment to data security. When looking back at the success factors and factors influencing

acceptance and diffusion, this is the one factor that is given: Trust, a technological infrastructure that is working; and data transfer security (see Chapter 2 and 3).

The **cross-border use of eID** was not seen as relevant by German government stakeholders in 2020 when the first batch of interviews were conducted (IPG1). This has since changed. The focus on user-friendliness gained importance in Germany since eIDAS. Now it's just a matter of implementing it. European rankings are leading to greater pressure on the German government, as Germany does not score particularly well on average (Commission et al., 2021; IPG2+4).

Digitization as a topic become more important in the last two years (IPG2). The **OZG** is more of an effect than a cause though. The cause is that digitization has a completely different status than when the nPA first attempted to diffuse in 2010. At its baseline, when one reconstructs an administrative process, you always come back to the identification issue. The OZG is a tool for pushing digitization through in the public sector (IPG2). There is a lot of criticism on the topic of the OZG implementation. In connection to eID, the procedures that are linked to user accounts, are automatically linked to the eID. To use the ePA is voluntary. So, if a municipal administration makes use of it is not guaranteed. Therefore, the key success factor of a unified strategy is not met. Due to the OZG there now is no de facto barrier to using the eID for public services by the public sector. One way to tackle this issue is the introduction of a digital suitability check with a duty of disclosure on how much is invested in digitalization and how much savings potential is realized. If members of the public office are not able to prove either of these, budget is cut by the savings potential. The same idea is already written down in the coalition contract of the current cabinet, though in practice it has not yet been implemented[20] IPG3).

Let's now focus on **communication channels**, which is an essential factor of a diffusion process. The ones that exist for digitization projects and laws are in urgent need for improvement. Especially the ones specifically meant for the nPA (IPG2+IPG4). It is not enough to write everything on an nPA portal, as it has been practiced so far (IPG3, 2020). So far, the public administration understands the nPA as a product. As it's a product, public servants are not allowed to market it. Now that it is clear, that the ePA is not going to diffuse by being automatically turned on, the communication from the responsible stakeholders needs to be intensified. This means marketing campaigns, education programs, substitutions projects, leap innovation programs, and much more need to implement as soon as possible and without a deadline. As technological developments will not stop proceeding, the German states is responsible for a constant investment into education of their citizens.

More **administrative personnel** realize that eID and digitization are not bad. That change is taking place unsystematically (IPG3). As stated before, in eGovernment, there is still no legal

[20] The Coalition Treaty can be found here (in German): https://www.bundesregierung.de/resource/blob/974430/1990812/04221173eef9a6720059cc353d759a2b/2021-12-10-koav2021-data.pdf?download=1

obligation to integrate the ePA. In that respect, the federal government needs to decide to enforce that (IPG3). However, there are 17 different parties at the table for such decisions. 16 federal states and the federal government. In the context of the administrative system in Germany that means that city state has the same saying as big states like North-Rhine-Westphalia. Finding a common ground complex, as some states don't see digital identification as a central measure to be met. On the other side, the federal ministries, agencies, and institutions don't improve the situation as their role division is strategy-less (IPG3). In general, no national ePA strategy can be detected, which also means that that key success factor is not met.

Institutional Context

As already introduced during Chapter 5 and the legal context, the German government level has to deal with a **complex and multilevel institutional landscape** following a top-down approach. A multitude of path dependencies adds to that. In its basic understanding, the state is responsible for the nPA project. The BMI is the political arm, the BSI is the technical arm, the BVA authorizes the certificates, and the Bundesdruckerei hands them out. The fact that the overall responsibility lies within a ministry means that it plans in terms of 4-year legislature periods (IPG2). The government level is responsible for the ePA. The procedures have legislative deadlines, which means that funding is lost before a project can be implemented in its entirety. Work in the IT area cannot function in this way (IPG4).

Let's first zoom into the institutional context of the **technical arm** on the one hand. The BSI will not claim that a pragmatic, semi-secure eID solution is secure. If the solution is hacked, the BSI loses its reputation. On the other hand, something like this is already being done in other areas. Private sector projects are started with a usable solution, and it is readjusted as needed (automotive industry or occupational safety) (IPS1). In IT security, the German government level has become accustomed to saying that they want to have the highest security, the BSI gold standard (IPS1). By doing so, no other players are allowed to enter the nPA infrastructure. Additionally, to that, there is no central IT instance that coordinates digitalization projects of the public and private sector as mentioned before. Each sector builds its own eID solutions (eGov, Health, Work). Hence, the key success factor presented by Kubicek and Hagen (2000), that there needs to be interorganizational coordination, is not given. If such an instance is introduced, it must be associated with power in Germany for it to become effective (IPG2+IPG3).

The importance of **municipal employees** for the marketing of the nPA is underestimated. In 2013/14 the feedback was received that it was often due to the lack of or wrong advice that the online authentication function was not activated. No consequences were drawn. To date, no new project has been launched for the individual clarification of administrative staff on the ePA. Online training courses with eLearning modules are offered but aren't successful (IPG3). The eLearning modules don't have the effect of actively promoting the nPA in citizens' offices. Cities that offer solutions for online services have a much rate of uptake. These employees see that it

is a useful function (IPG4). However, in the vast majority, employees in administration don't perceive the nPA as personal progress but rather as additional work and more complicated procedures (IPG3).

Federalism is another obstructing force in the diffusion of the eID scheme in Germany. One great example is the insistence on the 6€ fee for the re-setting of the PIN nPA until 2021. The BMI first tried to abolish the costs 2017 and the nPA law was revised accordingly, so that municipalities would be able to choose whether they wanted to ask for a fee or not. After reviewing the states got the passage to be taken out again in the Bundesrat. The presented argument was that it could imbalance the states. Municipalities that would still take the 6€ could then come under pressure. Since 2021, the PIN reset is free for everyone (IPG2). Debates like these, with the power of municipalities, are a strong component of the lack of diffusion of the German eID scheme. So far, federal structures and digitization projects do not go well together. Naturally, it is challenging when 17 different interests must be considered. On the other side, the federal government also consistently involves five different ministries in the issue of the eID diffusion (IPG3).

Market Context

German citizens have about 1.7 **contacts with public services** per year, of which one is the tax declaration. The low frequency is due to the unattractive eGovernment use cases. The demands that people now place on eGovernment are much greater (eGovernment Monitor, 2021; IPG4+ IPS3). For example, from the point of view of the OZG, it is important to be able to simply submit a building application online. End users also want to regularly check the status of the application. One application would immediately trigger 5-6 visits to the "office". The background systems in the authorities are not yet equipped for this. And cannot communicate with each other. Much more needs to be done to make eGovenment services more attractive and sustainable both on the frontend and backend. This shortcoming is not because there are no electronic identities, but because the IT systems are not prepared (IPG4). When looking at the diffusion theory, the trialability of the nPA is not given, since there are no mass use cases with which the innovation can be tried on (Rogers et al., 2014).

Considering the market context, the government level choses to either invest in public-public partnerships or public-private partnerships. One attempt to move towards public-private partnerships is to cooperate with banks. During the first discussions on a **cooperation with the banking sector** before the nPA launch in 2010 the banks expressed their openness to cooperate. They expressed one condition: To put the nPA on their EC-cards or print their logo onto it. The nPA smartcard was seen as a competitor to their own electronic systems. Especially in the banking sector it is crucial that the customer has a card in their hand where the bank logo is

printed onto it. Since this would have led to external dependencies, the cooperation was not pursued (IPG2). With the new Payment Services Directive[21] of today, banks realize that they have higher regulated and more regular customer identification processes. Currently, solutions like VideoIdent[22], that come from the private sector, are still being used even though they don't meet the security standard of the nPA. Banks aren't as profitable as they used to be, and VideoIdent isn't cheap. In theory, the ePA integration can save them a lot of money. Every failed fraud attempt cost money, too. That's where the ePA-Banking cooperation is ideal (IPG3; IPG4).

Regarding the prices for the **authorization certificates** for service providers, the costs are too high. The price is around 2000€ for all participants and hasn't changed since 2010 (IPG3). Today, only one player offers the service of giving out certificates to service providers, the BDr. Because there is only one central provider of certificates, there are no market effects happening, like customer convenience. Potential service providers have already opted out of integrating the nPA after being offered only a flyer as consultation service (IPG3). This practice isn't just detectable on the government level towards the service provider but also towards the end user (IPG4+IPG4). So far, the government level doesn't see themselves in need of marketing and proactively increasing their customer base.

Socio-Cultural Context

The German government level **invests** a lot of money through OZG and funding projects such as the "Secure Digital Identities" showcase project (IPG4+IPS1). The challenge here, is consistent funding. Public services that must be digitalized with OZG must be completely digitized from A to Z. From the first initial ignition of the data to the end point of the service. All of that in a user friendly and convenient way as being proven by Davis (1989) and Rogers et al. (2014). The understanding at Germany's government level is that a service/solution can only be promoted and diffused if it is one hundred percent safe and ready. But there is nothing that anyone can be one hundred percent sure of. This culture in the governmental level is a blockage to diffusion. To counteract this culture, an Agency for Leap Innovation[23] is currently implemented (IPG4).

In addition, a new consortium has been formed by the BMI with various departments that have expertise in eID matters. There are enough people that want to implement the eID. But they all encounter the same problem: they don't have the enough **resource prioritization** towards an eID diffusion. To properly manage the diffusion of the ePA, you need a team that does nothing else but taking care of this topic as recommended by Roger et al. (2014) and Kubicek und Hagen

[21] https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_en

[22] "VideoIdent is an online procedure that allows you to identify yourself via video, regardless of your location. Identification via VideoIdent is possible with a smartphone, tablet, PC, or laptop and via all common web browsers or apps. This makes VideoIdent an easy-to-use alternative to the PostIdent procedure at the post office." https://www.weltsparen.de/glossar/videoident/

[23] https://www.sprind.org/de/

(2000). One possibility is to establish a Start-Up. Participants take care of this topic apart from political decision makers and only call in a steering committee when it comes to strategic and political decisions. Otherwise, no ministry gets involved. They get a budget and must show that they can do it (IPG3).

Another factor that plays a role is **demographic change**. In the next 3 years, there will be a big shift in personnel in the German administration. A whole generation (also called boomer generation) will no longer be working. While the budget remains the same, the personnel won't be there to spend it for the good of society. There is a gap of about 15 years, in which hardly anyone was hired into the public sector, because of radical cutbacks. Trends like New Public Management were triggers for that. As a side effect, no new positions are created (Hood, 2011). Therefore, if the German government level doesn't digitalize themselves now, future generations will pay the price (IPG3). One the one side, attempts to digitalize the public sector are blocked by unit leaders that will retire soon, on the other side the benefits of digitization are not being exploited. An obligation to the nPA introduction can be one possible step into the right direction (IPG4).

Technological Context

When looking at the technological context at the government level, it makes sense to focus on technical specifications of the nPA considering technological trends that the government deals with. Since it is out of scope, the following technologies will not be discussed in depth from a technological viewpoint, but rather how their stance has influenced the diffusion of the eID scheme in Germany.

For instance, the nPA has a **contactless interface**. Already during the preparation phase, it was clear that users would not buy an extra card reader. At that time though, the NFC technology was constructed as a card replacement and not as a card reader (Apple Pay/Google Pay). As shown in Chapter 5, the relevant stakeholders were convinced that the NFC interface would become the first step of using the mobile phone as a card reader (IPG4). When looking at Roger's DOI, this is where Germany became an innovator, as no one else had included the NFC interface in their chip. As already mentioned in Chapter 5, while ePA experts were convinced that the online authentication function will not move onto the smartphone, the government stakeholders still incorporated the NFC interface. For years, NFC was exclusively reserved for payments. Additionally, to that, there was also an interoperability problem at the time: the standardization of the different NFC technologies. Once that issue was succeeded, the nPA team took up conversations with Apple and Google again. As a result, NFC was opened for ID card usage on the phone (IPG3).

Self-Sovereign Identity

The topic of Self Sovereign Identity (SSI) has gained popularity in the last couple years due to its connection to blockchain in mainstream discussions. When looking at the underlying principles of SSI[24], it gets clear that there is no obligation to use blockchain in order to meet the principles nor that these are set laws that have to be met – they rather serve as a guidance tool (Allen, 2016). The failed ID Wallet project by the Chancellery also tried to connect SSI principles with blockchain, which heavily backfired as major security gaps were found by earlier mentioned hacktivists (see Chapter 5). One major issue that the hacktivist group Chaos Computer Club criticized about the project is the lack of mutual authentication (CCC, 2021). If you don't know who you're talking to or who you're giving your data to, that is a big problem. When looking at acceptance factors, the factor trust would have been given if the project would have been launched properly. Another issue that has been expressed not just by the CCC but also by other actors is that in principle, the already existing technology underlying the nPA meets SSI recommendations. The end user is always in power of their data, there is no way to access one's personal data unless it is justified, etc.

Everyone must oblige to **multilevel data protection laws.** If someone does not oblige to these laws, there are severe penalties. For some experts that baseline is to be enough to start introducing more convenient ID solutions. They might have a lower assurance level than "high" according to eIDAS (IPG4+IPS1), but the convenience can get higher.

Electronic credentials such as diploma certificates or master's certificates don't have to be handled with the same BSI gold standard logic as electronic identifications. A certification can be copied for example. If party A gives party B an electronic copy of a credential, then it can be proven to a third-party counterpart, that party A has a diploma in e.g., political science. What you can't prove is that party A has an identity. It's just an authentication and identity mean that party A is certainly party A and by the way, they also have a diploma in political science. First you need to prove the authenticity of the diploma and then to prove one's identity. The differentiation of credential vs. identity has not arrived in the common minds of the government level as it was shown in the most recent public hearing on digital identities at the German Bundestag on July 4th, 2022[25] The biggest issue that experts see with the emerging technologies

[24] The principles are: "Existence — Users must have an independent existence, Control — Users must control their identities, Access — Users must have access to their own data, Transparency — Systems and algorithms must be transparent, Persistence — Identities must be long-lived, Portability — Information and services about identity must be transportable, Interoperability — Identities should be as widely usable as possible, Consent — Users must agree to the use of their identity, Minimization — Disclosure of claims must be minimize, Protection — The rights of users must be protected" https://medium.com/metadium/introduction-to-self-sovereign-identity-and-its-10-guiding-principles-97c1ba603872

[25] During the hearing, nine experts from areas of eID and nPA were invited to talk about the current state of the eID diffusion and were asked questions by Parliamentarians. Link to the hearing and statements (only in German) https://www.bundestag.de/ausschuesse/a23_digitales/Anhoerungen/899386-899386

that try to reach the SSI principles is that they do not comply with established technologies and much rather make us of blockchain (IPG4; (Kahlo, 2022). The following paragraph will focus a little more on blockchain.

Blockchain

To meet the expectations of SSI, latest technology projects implemented the blockchain technology. With that technology data is managed decentralized and transparency is given (Mahula et al.). After the ID wallet failure by the Chancellery, the critiques of blockchain technology have gained popularity. With the underlying principles of the ePA, GDPR, and eIDAS, the end user has the right to forget and be forgotten. That right does not fit with blockchain. Even storing the public key in a blockchain is reconstructive and there is no recall mechanism. Therefore, that public key is on the network forever. Even if the end user or public servant has called it back, it will always be in the network. Some new attempts to combine the current eID projects with blockchain were to introduce a semi-public key chain, though that makes blockchain technology obsolete (IPG3).

6.1.2 Acceptance Factors

After looking into the different context areas, the focus now moves onto acceptance factors. For a successful diffusion of the eID scheme, the government level also needs to accept the technology. The following Chapter will look at perceived usefulness, ease of use and the aspect of trust. Afterwards on those factors affect the implementation of the ID infrastructure.

Usefulness

The government level wants to include as much as possible into their projects (e.g., ePA, ID Wallet, or OZG). That approach does not agree a successful diffusion though. Small and manageable portions are better (IPG2). According to the key success factors presented in Chapter 3.4 realistic deadlines and clear deadlines must be given. Even if there is a great technology at hand, there are no appropriate applications for it and vice versa (IPG1). In terms of usefulness, the government level is both the problem and solution of the diffusion of the eID scheme. As the instance to set legal guidelines and regulations, the government level is blocking true process. Due to this issue the government level is affecting the three levels mutually. This will be covered in Chapter 6.4.

The one factor in which the government level must deal with perceived usefulness is the issue of teaching public servants **the benefits of integrating the nPA** into their public services. Once this hurdle is broken, the self-evidence of the usability of the nPA becomes eminent. The government experts are sure about the following steps that need to be taken to increase the perceived usefulness for the rest in their group:

1. Increase and intensify eID educational courses for public servants;
2. Make integration of nPA mandatory for all public services with “high” assurance level according to eIDAS;
3. Make sure that municipalities properly understand the benefits of an nPA integration;
4. Properly explain the issue of demographic change and that digitalization is the only way to save future generation’s well-being when it comes to the provisioning of public services; and
5. Make sure that municipalities properly explain the benefits of the nPA to citizens when they pick up their ID card – once the Smart eID is established. Offer to install it at the spot or if there’s is a European ID Wallet, to do the same with that (IPG1-5).

Ease of Use

When looking at the ease of use, the **integration process** itself has been identified as being one of the major hurdles to tackle (IPG4). Especially if the integration of the nPA is not mandatory, the process to do so anyway cannot be difficult or at least more difficult than the existing solutions. Following the basic principles of technology acceptance and the diffusion of innovation – any new technology must bring a benefit from the one before (see Chapter 2). So far, there are only prospective benefits but no direct benefits that can be presented about the ePA. Hence, no public servant will deal with a “maybe-benefit” if the integration process is as resource drenching as it is now. Public servants also need to be seen as customers whose needs need to be satisfied. If that is not given, the diffusion will not take up pace on the government level (IPG4). While there were 20.000 transaction/month on the AusweisApp2 in the first years it’s only risen to 1 million transactions/month in 12 years (IPS2). There have been positive changes to the process in the last years, though these changes have not had a real effect on the total diffusion of the eID scheme in Germany (IPG2+3). There needs to be a cultural shift on both sides at the government level. The provider level needs to see the receiving level as an asset rather than an opponent must deal with (IPG 2 + IPG 4).

Trustworthiness

The high level of **data protection sensitivity** in Germany has already been discussed. What is missing is some form of pragmatism on the government level. Data protection and IT security requirements are always taken extremely seriously and are enormously hyped. It costs speed, interoperability, and usability (IPG 4). Since trust effects all three levels mutually, the factor will be discussed in more detail in Chapter 6.4.

... leading to the implementation of an ID Infrastructure

Infrastructures never occur naturally and are always planned. Examples from the physical world are highway networks, fibre optics, or cables. There always must be someone who connects the components and who connects the various business models with each other. It needs someone who has the overall responsibility, e.g., a security update and who can enforce the usage of the infrastructure. In other words, writing a regulatory framework that describes the details of how the infrastructure is supposed to work. When it comes to the ID-infrastructure in Germany, there are the ID card and the ID card infrastructure. It is financed, secure, always updated, internationally recognized, legally regulated and responsibilities are clearly divided. Beyond those specifications, there is no additional infrastructure. Expanding the infrastructure in such a way that all possible service providers are included would cost their innovative flexibility (IPS1). Service providers need to be able to develop innovative services in the infrastructure, develop them further, incorporate new innovations, etc. (IPG3+IPS1). And in this respect, an infrastructure is the core, and the various providers around it forms the ecosystem.

From the perspective of the government level, the acceptance is high enough for them to implement the ID infrastructure. Resulting from the positive effects of earning the status of being an innovator in the 90's. With the eSignature Act, the baseline was set for an efficient construction of the ID infrastructure. As the specifications of the ID infrastructure were set by the included stakeholders of the government level, the status of being an innovator was lost (IPG 3+IPS 1). Somehow, the innovative spirits got lost on the way and were replaced by an unrealistic perfectionism that provides the **most secure eID schemes** that has ever been created. Since then, Germany has been a laggard country, though an extremely secure one (more on this in Chapter 6.4 as this factor affects all three levels mutually).

As the ID infrastructure is already set and stable in Germany, the analysis will also investigate **eID ecosystems**. In contrast, an ecosystem can't be built up in a planned manner. Rather the ecosystem has its own dynamics. Services must be attractive. Business models must pay off somehow. The networking of different players must offer advantages for both sides, i.e., a win-win situation is needed. It can't be that one partner has to pay the other for something. For such an ecosystem effect or also positive network effect, the government level can only give incentives. In the case of the eID, the infrastructure is very small and there is no such thing as an ecosystem. Instead, there are a lot of players who don't relate their technology or ID solutions to each other properly. This problem cannot simply be solved through coordination because ecosystems are not coordinated per se. Ecosystems coordinate themselves because there are stable interests. Therefore, it's more a matter of sharpening interests for eID, to drastically increase the demand for eID solutions. For example, because there are enough providers. One expert provided three steps for an increasement of demand by the state:

- The state could align its own procurement policy more strongly.
- The state can promote the nPA fiscally; and
- The state can prescribe certain use cases (IPG3+IPS1).

In general, the **mood regarding digitization** has changed drastically (IPG2). Now that more people are talking about the topic, the German state needs to think carefully about what the role of the state is. One possibility is that the role of the state in a sovereign domain remains narrow and stays aways from economic activities, innovation, and market dynamics. Through that, the state in the digital space would be that of a framework setter rather than a market actor. Another option is the one that most experts see the State moving towards is that it will offer services. Once the government level is doing so, they must do it the way any company does it. With user expectations, dynamics, usability, feedback loops (IPG1-4). As of today, Germany has attempted to tackle the eID diffusion issue in three implementation projects after the ePA project in 2010. The following part focuses on all three.

OPTIMOS

Chronically speaking, the first one is OPTIMOS project. It achieved the standardization and interoperability of NFC interfaces. Through that achievement, the nPA identity card can be used with the mobile phone as a card reader (IPG1). OPTIMOS 2.0 is the follower of the OMTIMPS project and the predecessor of the Smart eID project as it already began with working on secure element[26] interfaces. When OPTIMOS 2.0 was finalized, the research project on secure digital identities was launched. As both OPTIMOS 2.0 and the research project are financed by the Ministry of Economics, the ministry made sure that at least one project attempted to integrate a use case with the secure element solution. In practice, that measure was quite naïve. Today's Smart eID infrastructure integrates the nPA with the SE while excluding any other player than Governikus as its technological interface (IPG4).

While that is the current situation in the technological context of the government level, platform providers such as Apple and Google increasingly recognize the importance of identification on a secure level. As a result, state ID documents and driver's licenses in the US are compatible with IOS devices and Android devices and the providers for Apple & Google use trusted platforms on which they can store credentials (pilots have started in the US, not in Europe). It does not work (which was a misjudgement of BMI at that time) that the private providers integrate the state ID in their technology. Big platforms are needed to deliver trustworthy state

[26] A secure element is a hardware token in the mobile phone that is not connected to the phone producer but can be used by other entities to save secure credentials. For doing so, the tech producer needs to open up their interface to the respective partner, which is challenging to begin with.

documents, that are valid for a certain time, that offer marketing on the internationally standardized technical level and solve design problems (IPS1).

ID Wallet Project of Chancellery 2021

The ID Wallet project was highly politicalized. The execution had major flaws that were never solved. Not just data security-wise, but also from a coordination point of view of the different stakeholders. Essential elements of the ID infrastructure weren't involved, like the BSI or other security experts. Before the federal elections, nobody was interested in the introduction of an ID wallet. Then, the Chancellery publicly claimed to have solved the eID issue (Bundesregierung, 2021). From the view of the government level, the failed launch damaged their reputation (IPG3). The ID wallet used blockchain technology. As mentioned during the technology context, the integration of blockchain technology does not align with the legal framework from the governmental level point of view (IPG3+IPG4). In general, the government level perceives fast paced attempts like the ID wallet one to be a side effect of a lack of a learning process of included institutions. The same discussion is held over and over again with every occurring novel project (IPG3, IPG4, IPS1). When looking at the involved actors that were included until the end, they were private companies that wanted to reduce costs through regulations. Those actors came from the hotel industry and telecommunications. There were none there that wanted to create a good ID solution for their use cases (IPS1). They solely wanted to achieve that regulatory requirements from the state would be lowered for the use identification methods (IPS1, IPS3).

Smart eID

The technical challenges of the Smart eID project that must be overcome in order to achieve nationwide coverage for eID's are still quite great (IPG3). Also, from an organisational point of view, the project has been highly politicized from the first setting of the deadline for the launch in 2021(IPG3). The current approach of using the secure element of the mobile phone for deriving the nPA onto the phone will not play a major role by the end of 2022 (IPG3). The software-based solution not only has legal hurdles, but also major technical hurdles. In principle, the Smart eID initiative is seen as a step forward as all services are moving onto the mobile phone (IPG4, IPS4-6).

The Federal Ministry of the Interior is still reluctant to publicly market their new ID solution, as they don't want to receive bad press. This reluctance is an effect from the ID Wallet "disaster" that was looked at above. Alternatively, the use of the secure enclave as the secure interface is presented. This development will only be looked at in detail after the first results come back from the current user tests with the SAMSUNG phones (IPS1). Apple for instance, will only allow the Secure ID on the Secure Enclave. The only question now is how the highest assurance level can be met without using the SE but the Secure Enclave. So far, the BSI has believed the Secure

Enclave is not high, that it is perhaps substantial. With that decision, the nPA can naturally not be save on the Secure Enclave (IPS2).

To summarize, government stakeholders have been implementing the ID infrastructure and made some adjustments to its regulatory framework throughout the years. Government services are also developed to help diffuse the eID scheme. Not one is successful so far.

6.2 Service Providers

As shortly presented in Chapter 2.3, Service Providers can both be part of the public and private sector. They offer either identification services or host clients' data on their ID servers. They are reliant on all levels of the ID infrastructure and are the creators and essentials parts of a working ID ecosystem. Without service providers, especially the one's coming from the private sector, there will be no successful way out of the negative network effects, since they will be the one's offering use cases that are used more often than once a year.

The following Chapter will first investigate the contextual factors. In doing so, the legal and market context is presented in one, as the market is heavily influenced by the legal guidelines that are provided by the government level.

6.2.1 Contextual Factors

Legal and Market Context

In order use the ePA, service providers must apply for an **authorization certificate** from the state authorization certificate issuing office at the BVA and must design their service to be DSGVO- and eIDAS-compliant. Once the service provider has gone through the process**,** they are officially a notified identity system of the eIDAS network and are accessible to users throughout the EU (Skierka, 2021a). Under the eIDAS regulation public authorities of EU Member States are obliged to recognize the notified identification systems of other Member States. However, this obligation only applies to the public sector. The private sector is exempt from the mutual recognition obligation. However, private services can connect to the eIDAS network (Skierka, 2021a). Providers of private identification systems can propose their solutions for eIDAS notification to the EU Commission via the BMI. The prerequisite for this is a conformity assessment by the BSI (Skierka, forthcoming).

In 2017, the nPA bill was simplified for the use and acceptance of the nPA by service providers. Among other things, it now allows the approval of identification service providers offering electronic identification services to third parties as "eID-as-a-Service". Service providers can use these identification service providers to integrate the eID into their online service. Through that, company such as Authada were able to begin offering such services and begin a new business value stream in their value chain (IPS4).

As the Process of obtaining an authorization certificate is a bit longer, it makes sense to investigate it in a bit more detail than just mentioning it has done above:

1. Applying for the authorization certificate at the BVA: filling out the form on the online portal. The processing time is approximately 1 week. For applying, the BVA takes a fee of 102 EUR.

Afterwards the following requirements need to be met:

2. Declaration of data protection and data security concept

3. For identification service providers: proof of compliance with the technical security guidance of the BSI and their auditing by a notified body (such as a TÜV). Going through the procedure can take 6-12 months and is very costly (IPS4-6)

4. Integration of the authorization certificate:

    a. Only provider on the market is Bundesdruckerei (D-Trust)

    b. The Fee for authorization certificate to CA (D-TRUST of BDr) is not public. As they publicly claimed at the hearing on electronic identifications at the German Bundestag on July 4th, 2022, the fee amounts to a four-to-five-digit sum, depending on the size of the organization.

    c. The Price per transaction is between 0.5€ and 5€ (the fewer authentications, the more expensive it gets)

For small to **medium-sized enterprises** (SME), these costs are often not worthwhile compared to the relatively small benefit for users (IPS4-6). Identification service providers such as Authada offer an alternative to unattractive authorization process by offering to integrate the nPA as a service into the clients' infrastructure. Naturally though, this service also incurs costs. Overall, there is lack of diversity and competition in the ecosystem. The consequence is that many potential service providers abandon the German eID scheme and stick to paper-based, on-site procedures or VideoIdent technology. Other potential big players opt to move their business outside of Germany and offer eID service for other EU member states as the integration and authorization is lower (Skierka, 2021a).

The interviews with service providers have shown that the predominant business model is a **transaction-based model** (IPS2-6). This means that the prices for using the online authentication function of the ID card are dependent on the number of transactions. This model creates a barrier to getting involved as a service provider. SMEs and non-profit associations are particularly affected by this business model. For the manageable number of service providers, this results in the challenge of creating a value chain that guarantees competitiveness. All value chains available to us are currently not linked to any profit, except for one stakeholder. This uncertainty is also automatically a hurdle for potential interested parties to offer a service.

Governikus has by far the largest market share in the public sector. As a business model, they sell their technology to the public sector at very clear, fixed prices, which are distributed among the states according to the so called "Königstein Key": Large states pay more money for the same software than small states. This business model is only established in the public sector as they couldn't do a business model like this anywhere else. A second market that Governikus is focusing on is the banking industry. There, calculations are based on transactions (IPS2).

So far it hasn't worked out to look for customers by offering the ID card alone from a **price-benefit** point of view. Nonetheless, there are service providers like IDnow[27], WebID[28], that offer identity services and are now also relying on the ePA, in some cases more and more intensively due to regulatory adjustments (Skierka, forthcoming) (IPS2). One negative example is the current adjustment of the Proof Act (already mentioned in the legal context of the government level). As of right now, the adjustment means that the use case of signing work contracts online, which is offered by WebID, will be forbidden again.

All those use cases so far are mainly on the onboarding/registering stage of the value chain. But if the nPA had to be marketed in all sectors, that would be a major challenge. Therefore, it is good that IDnow and WebID are already successfully working together in these specific areas. In contrast, Governikus offers itself as a technology provider with the AusweisApp2 for customers who have the highest **security requirements**, such as the public sector. If another sector also has this requirement. It can integrate the solution into their system. With lower requirement customers can also use VideoIdent or other solutions with assurance levels lower than "high" according to the eIDAS regulation (IPS2).

Established players in the German eID ecosystem are also focusing more and more intensively on entering the **consulting** business, as they realize that they have know-how that other consulting firms will never have. A very product-related, market-related, or technology-related knowledge. On the other hand, according to their contracts with the administration, Governikus has determined that they are the only ones being allowed to consult their customers on matter of their own technology. The combination of that requirement and being the only authorized company to offer the upcoming Smart eID solution (all with an unlimited contract with the German state), makes it sound like a monopolist position. When being asked about it, the experts that profit from the conflict situation named reasons why it is not the case: they can't dictate prices, must consult with states on pricing models on a regular basis, and they don't have many customers to dictate their business model onto as their only real customer is IT-Planning-Council (IPS2; Hearing on electronic identifications, 2022). In contrast, experts that do not profit from the current market situation are assured that they need to deal with some sort of monopolist

[27] Provider of VideoIdent solutions and other identity solutions on their own platform: https://www.idnow.io/idnow-vision/

[28] Money Laundering Act-compliant identification with WebID Video Ident: https://webid-solutions.de/solutions/?lang=en

structure, as they are actively excluded from integrating their own eID infrastructure with the upcoming Smart eID solution (IPS4-6). This situation leads to the fact that no other company can establish itself in the public sector, because the product of Governikus (AA2) is the only recognized one for the integration of the nPA (IPS2).

According to today's **market situation**, there are not many service providers left that have an integrated nPA and the few private sector ones must consider annually if they can still keep up that business stream, as it is not profitable (IPS4-6). The openness of the market does not run as it is intended according to Roger's diffusion variables. To date, there is no return on investment. Players like Governikus and BDr can remain calm in these situations since they are either owned or commissioned by the public sector. As mentioned above, in the Smart eID project, companies such as the Bundesdruckerei and Governikus have received the pole position and are the only certified players to offer the mobileID version of the ePA. But even with a prime position such as Governikus has, they needed 22 years to accumulate at least enough profit to recoup their equity (IPS2).

Socio-Cultural Context

Currently there is **no implementation project** in Germany, there are only research projects. Because it is so complicated and hard to enter the German market, many German companies have been extending their business onto the whole European market. In Europe, there are real eID solutions in use in many countries. It also works and has often increased in use in recent years due to the pandemic, as in the Scandinavian countries or in Belgium with ItsMe (Skierka, forthcoming). This development could not be pushed in German market since no functioning solution is commonly accepted (IPS1).

Germany has been too strongly **fixated on government and public administration**. What does not seem to have reached the government level to this day, is that the masses of identification processes that citizens have every day are carried out in the private sector. There is little the state can do about it, except where it is regulated: banks, account openings, or mobile phone contracts. These are also not mass user actions. On the one side, there is still no solution for mass transactions. On the other side, no one wants to be regulated by law, because being regulated also means having costs in order comply to regulations. There is no interoperable solution in Germany until today (IPS1).

Private sector service providers need to both deal with global socio-cultural factors according to customer needs and very specific German customs coming from the public sector. While many have tried their luck at offering the next big and profitable eID solution, not one has been able to survive and increase their business. Players like Verimi have also had to deal with the inconsistency of the just mentioned conflict of pragmatism vs. regulatory standards. Other

players that are part of the research project on secure digital identities, have to find ways to make use of use cases that don't need the highest assurance level to integrate any use case at all.

Technological Context

From a technological point of view many Start-Ups have a hard time in Germany, because they **can't get access to data**. When it comes to personal data, the German regulations and GDPR are setting extremely high standards (IPS2). As already discussed, other approaches, like SSI, are gaining more traction in recent years. However, establishing them is complicated. And if it gets too complex, it becomes less likely to be adopted by the market. Implementation projects become more and more protracted and expensive. Still the factor of citizens explicitly agreeing to their data being accessed is an essential base line to begin with. The whole consensus management issue though is extremely complex to implement technically (IPS3).

Let's now analyse how the private sector service providers view **blockchain technology**. Digital credentials are filed in registers and produce certificates, e.g., bank statements, child support certificates, birth certificates, school reports, etc. Afterwards, the credential is handed over to the citizen/user and they can use it for whatever purpose. Then the state is out of the picture. The only thing that is still needed at that point is that you have to be able to verify the authenticity of these certificates. In the area of certifications, there is an undefined large circle of interested parties or of potential users who want to verify the certificate. That means it would also be hard to do a public key infrastructure[29] (PKI)-based solution (IPS1). In contrast to the perceived usefulness of blockchain on the government level. Service Providers from the private sector (even if they offer services in the public sector) have a different view on Blockchain (IPG3+4 vs. IPS1).

Even though there are many criticisms of Blockchain, they are perceived as being superficial because people don't look at the solution (IPS1). The problem with storing any information in the blockchain is that it is not erasable. Therefore, the simple solution is to not write personal data on the blockchain. Otherwise, personal data must be able to be deleted under certain conditions. If you can't, you can't store it there in the first place. But that is not necessary for the verification of certificates. So even in the very much criticized blockchain-based school certificates from the BDr[30], not the certificates, their content nor the grades are stored on the blockchain. It's just a key that's stored through a hash function[31], which is not reversible. In that

[29] "A public key infrastructure (PKI) is a set of roles, policies, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption." https://en.wikipedia.org/wiki/Public_key_infrastructure

[30] The project of school certificates has been receiving heavy criticism from all kinds of expert. Especially security experts, as they condemn blockchain technology in itself. E.g., an article on that matter (only in German): https://www.heise.de/news/Schlechtes-Zeugnis-fuer-Zeugnisse-in-der-Blockchain-6370807.html

[31] "a mathematical function that converts a numerical input value into another compressed numerical value. The input to the hash function is of arbitrary length but output is always of fixed length." https://www.tutorialspoint.com/cryptography/cryptography_hash_functions.htm

sense, it’s not different from a PKI with different functions or from digital documents in which an eSignature is used. In any case, you can't pull out the personal data. Therefore, you can then implement the diffusion of the eID scheme for one part (digital certificates) in the blockchain. It doesn't always have to be blockchain. But from the organizational principle of ensuring availability, redundancy, and resilience (as are also the underlying principles that the BSI golden standard is trying to achieve) by having many, is not unattractive for private sector service providers. Any other form of public infrastructure that guarantees something like that would have to be built with a complex backup and resilience system, that has to be managed. In contrast, you don't have to do that with blockchain (IPS1). As it’s now been shown, there are relevant arguments coming from both sides. From a practical point of view, which would also support the diffusion of the eID scheme, the topic of blockchain should not be “abolished” right away.

In summary, the service provider level has to deal with contextual factors that are mostly set by the government level while trying to satisfy customer needs that were created by big tech platforms. This conflict has mostly remained unsolved or even gotten worse throughout the past years. Regulations were either adjusted to exclude the service providers from coming up with new services or the regulations that were adjusted to “help” service providers were always lagging behind the reality of the pace of technological change.

6.2.2 Acceptance Factors

Not just the government level but also the service provider level needs to accept the technology at hand in order for them to start investing in new solutions. As presented above in the legal and market context, service providers need to meet numerous requirements before being able to offer their eID service. The following Chapter will look into the perceived usability, ease of use and trust of the eID scheme by service providers.

Usability

When looking at usability from the perspective of the service provider level, **opportunities** to use the eID scheme is not usable for the vast majority. Only institutions that have been sticking around since 2010 are now established enough so that the eID scheme is working in the favour of Governikus and BDr (IPS2). New players on the other side have almost no chance to enter the ecosystem connected to the nPA and establish usable services (IPS4-6).

Therefore, an **open market** is not existent that could bring positive network effects (the positive/negative network effect is discussed in Chapter 6.4 as it mutually affects all three levels). Apart from Governikus and BDr, there is no perceived usability to be detected from other service providers (IPS4-6). Consequently, the responsibility of investing resources into improving the usability of the eID scheme is moved to the government level. Since the eID scheme is one of the most heavily regulated fields in the German system, there is almost no room for innovations

without a close cooperation with the public sector. Unfortunately, the public sector has so far chosen to cooperate exclusively with Governikus and BDr (IPG3 + IPS2).

Ease of Use

If a service provider does choose to **invest** into integrating the nPA technology into their system, the perceived ease of use is still not given. In parallel to the government level, there has not yet been a direct profit of integrating the nPA from the existing identification measures such as VideoIdent (IPS4-6).

Key success factors that were presented during Chapter 3.4 have not been met on the level of service providers to change the ease of use of the eID scheme. Therefore, service providers have had to struggle to keep up their business model and have to stay in the black (IPS4-6). As the responsibility to improve the ease-of-use lays within government level, service providers need to lobby for the consideration of their needs. Detectable approaches of bringing both parties closer together are the research project on secure digital identities and conferences like the OmniSecure Conference every annually in Berlin. When looking at the research project though, it is highly dependent on the contextual factors that were just presented Chapter 6.1.1.

Trustworthiness

So far, the only aspect of the ID ecosystem that has reached the trust of service providers is the ID infrastructure itself. On the other side, as the market is neither open nor planned, the different players don't necessarily trust each other. The research project on safe digital identities aims on fixing that issue by combining stakeholders on all levels into projects. In that case, there are even more levels represented than the three that are being looked at, which is a limitation of the theoretical framework itself.

Other than that, the cooperation between service provider stakeholders is limited. It is more likely for ID service providers to merge businesses than cooperating (IPS1-6). So far, only "island solutions" have been developed in the sense that they do integrate the nPA but offer entirely different user experiences.

… leading to the Implementation of ID use cases

Current eID solutions are being developed **without the customer in mind.** The healthcare sector offers a good example. It is in the interest of insurance company that everyone has their own system since it leads to a lock-in effect.[32] The same is practices in banking sector. It's a restriction of competition. European laws, such as the Digital Markets Act and the Digital Service Act were passed precisely because of such practices (IPS3).

[32] "The Lock-In Effect is a strategy for keeping customers by making it hard for them to leave." https://modelthinkers.com/mental-model/lock-in-effect

Verimi, for example, is a private provider of legally compliant identities that is substantively endorsed for the eIDAS trust level for public administration services under the OZG and provides Money Laundering Act-compliant (GWG) know-your-customer (YKC) identities for the financial and credit industries (Skierka, forthcoming). Another example is the private sector identity provider “Yes”, which provides federated identification from many banks, is also a private GWG-compliant identity supplier (Skierka, 2021a, 2021b).

There are also several other identity suppliers that issue identities with varying assurance levels according to eIDAS. One example is the "single sign-on" solution that allows a cross-app authentication (Skierka, forthcoming). Single sign-on solutions are available from American platforms such as Google, Apple, Facebook, and Amazon. They provide clear added value to their users and greatly benefit from network effects. The market for identity suppliers in Europe is fragmented, and no overarching tech platforms on the scale of the big tech companies as mentioned above have developed from Europe (Skierka, 2021a, forthcoming).

Coming back to **big platform companies**, for example Apple with their Apple Wallet, it can be seen that even market providers say a digital identity and credentials are becoming more and more important. Providers for digital identities not only need the unique identification and authentication of a person, but identity comes in different forms. However, the fact that the EU requires some sort of unified digital identity wallet is questionable. Each member state must issue a wallet to citizens. It doesn't have to be one, it can be completely different ones. That's exactly the challenge. Therefore, if you look at the regulation of platforms, we have an opening regulation through the Digital Markets Act. The platform companies have to open up their platform, have to disclose interfaces, and allow independent software solutions for payment, identities, and so on (IPS1). This means that we are now breaking open these markets, but at the same time we need an anchor of trust for this or a trust environment for this, so that certain credentials whose authenticity is important for people are nevertheless secured by someone. If Apple or Google are told that their wallet technology also has to be opened, a piece of overall security will be lost. This deficit must then be made up in some other way. That means at least something like a security framework for identity wallets is needed in any case (IPS1).

Nonetheless, the **EU ID Wallet project,** it is a logical development. There is already a plenitude of electronic identities. The state issues one, the bank issues one, etc. In other words, each of us is a human being, but we all have different electronic identities. The occurring questions now is just, how do we want to organize those in the digital world? Through these EU projects and their large-scale pilots, only standards are being developed, but each country will issue its own wallet. There will then be a German wallet and a wide variety of identities from different sectors will fit into it (IPS2). With a trust framework and open market competition, the service provider will also increase their acceptance of the eID scheme. Through that, the diffusion can move to the next level.

To summarize, service providers have so far not been actively included in the creation of the ID infrastructure and were therefore not successful in building up the ID ecosystem. Once some of those path dependencies are solved, like the regulatory fragmentation, the acceptance will rise.

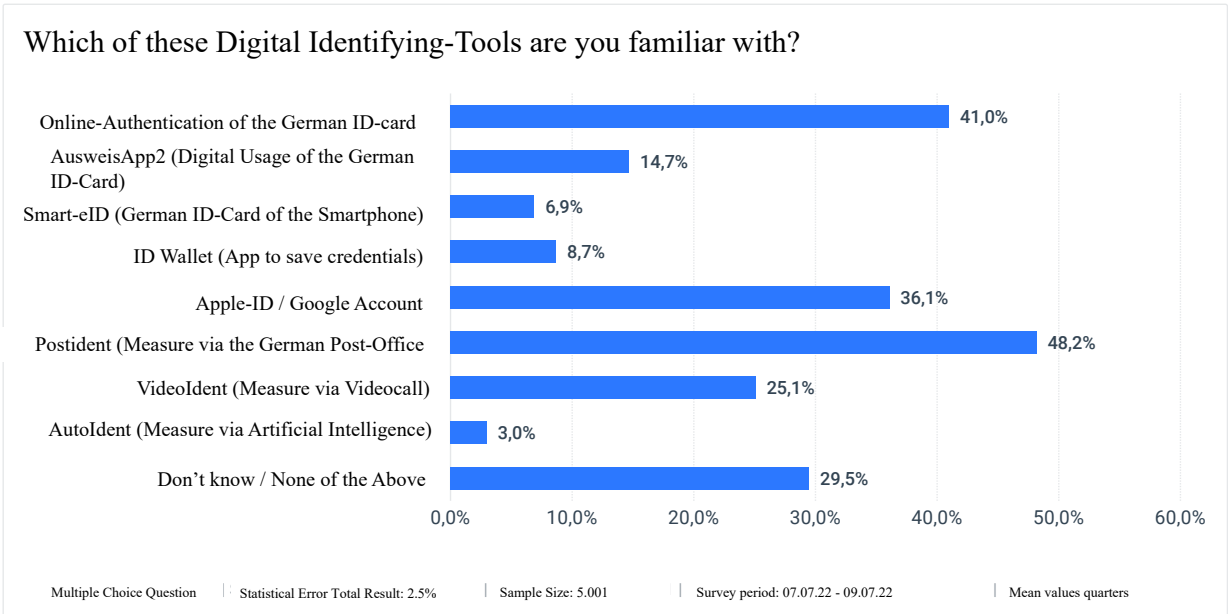
6.3 End Users

Even though end users have been extensively studied in terms of technology acceptance, the end user of the eID scheme of Germany is a unique group of inconsistent views and priorities. The following Chapter will present the cumulated data from the survey conducted during the research project that the author is part of. Even though end users are also influenced by the same context areas, the data doesn't show enough specific references in order to presenting them in detail. Therefore, the following Chapter will focus on overarching outputs of the surveys in the areas that fit the theoretical framework.

6.3.1 Contextual Factors

Awareness of eID

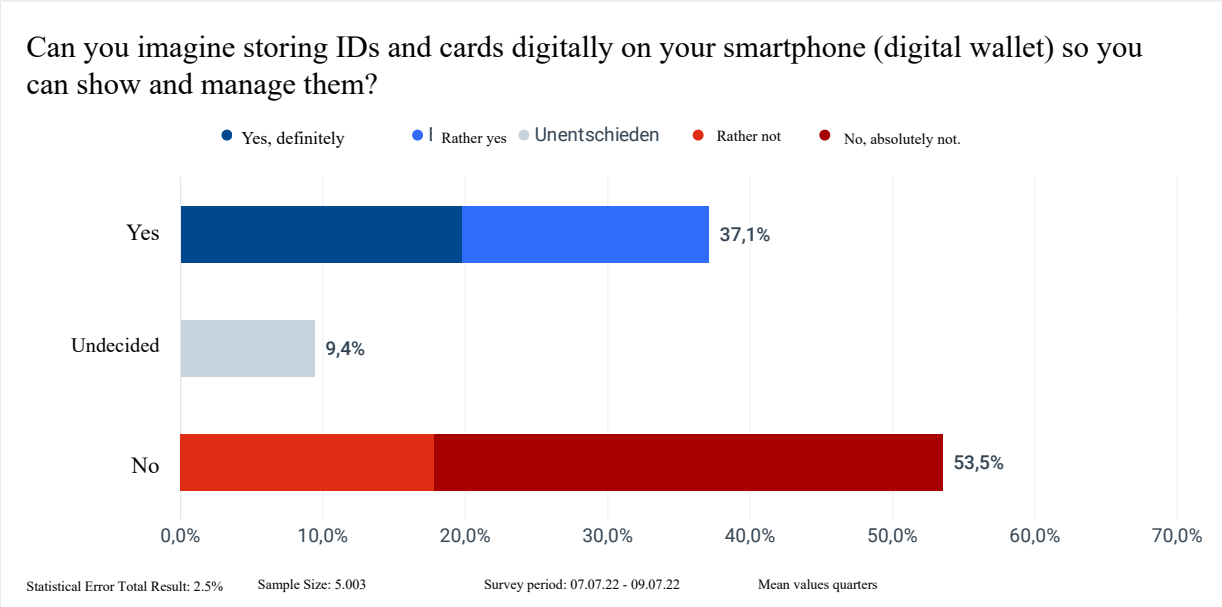
The underlying graph shows the answer to the question: "Which of these Digital Identifying-Tools are you familiar with? By now, the online-authentication function of the nPA its sill unknown by 55% of citizens. The most known tool is PostIdent. This comes as no surprise, since PostIdent was part of a mass-media campaign after it was introduced that prepaid phone buyers needed to identify themselves (IPG3). Surprisingly, the second possible option for purchasing a prepaid phone VideoIdent is much less known. The reason for that difference can't be detected with the data at hand. The assumption, that even with citizens being aware of the online-authentication function of the ePA, due to a lack of trialability and observability, the AusweisApp2 is still not well known. The 30% of end users not knowing any of the before mentioned identification tools also comes of no surprise. In contrast, 70% do know at least one digital identification tool, which means that the general topic of electronic identification has reached most participants of the survey.



Graph 1 Familiarity with eID-Tools, Showcase Project Secure Digital Identities, 2022

Opinion on implementation of eID Solutions

The output of the question underneath, whether participants want to store their ID and other cards on their phone, is surprising. Another survey that was conducted by the consulting firm PwC, came up with an entirely different output in which participants were positively responding to the wallet proposition (pwc, 2021). The most logical reason for the drastic difference is that in the PwC survey, the topic of ID wallets and its benefits was extensively explained before asking the question. While it does lead to a more positive output, it is also made clear that most citizens simply don't know what is meant with a digital wallet when it's just brought up in a question. Therefore, education in eID matters is of central importance to increase technology acceptance and the diffusion of the eID scheme.



Graph 2 Wallet usage, Showcase Project Secure Digital Identities, 2022

To summarize, with the first two questions the researcher was able to investigate the awareness - and preferences on the implementation of the eID solution. A major limitation is the lack of data on the actual contextual factors that are part of the theoretical framework. The data at hand does give some contextual information on socio-economic factors, though looking through all of them is out of scope of this thesis. The following Chapter will look at the output from the last eight questions of the survey and how they fit into acceptance factors at the end user level.

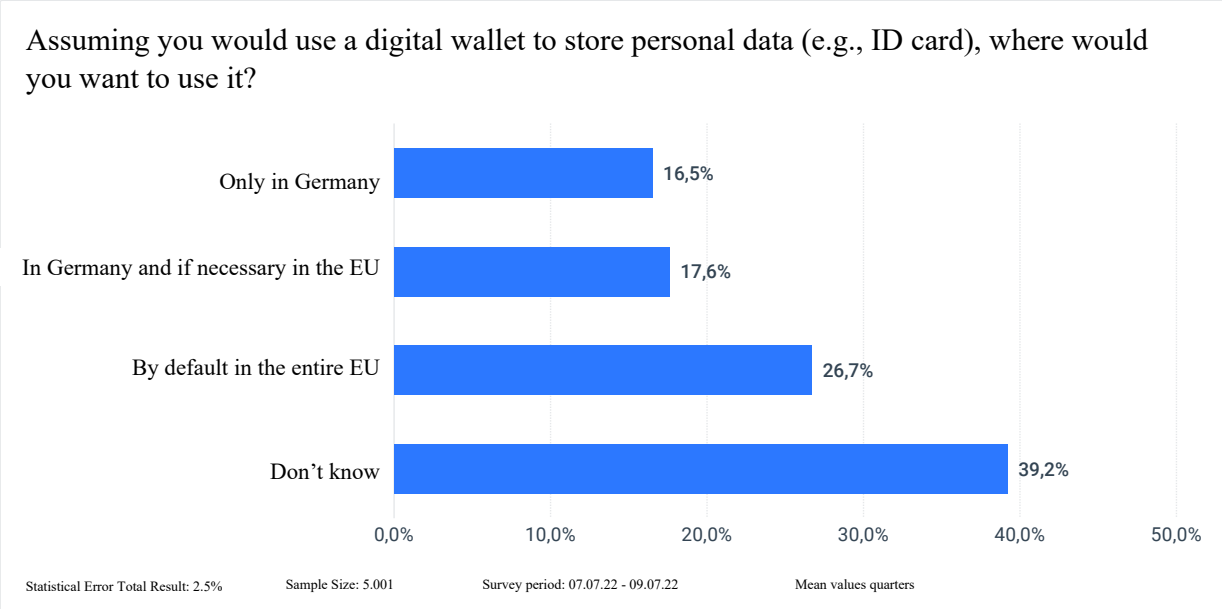
6.3.2 Acceptance Factors

Usefulness

The nPA technology solves exactly the digitalization problem, but nobody uses it. So why doesn't anyone use it? Because it doesn't offer any useful applications. Especially in 2010, when the nPA had a coverage of 5%, there was no way of end users getting used to new technology. The issue though is that most private service providers only start to think about investing when there is a coverage of 50% (IPG4+IPS1). Accordingly, it was misjudged when it was said in 2010 that hundreds of applications would be available from the beginning of the roll-out in 2010 (IPG3).

In terms of usefulness, the survey focused on future prospective for application areas. Unsurprisingly, the majority doesn't know if they want to use their possible digital wallet in only Germany or the entire EU, since they don't have an existing digital wallet to compare it to. Hence, the variable by Roger's (2015) "trialability" is not given. One assuring factor though of the replies is that of the approx. 60% that do know that they want to use a digital wallet, want to

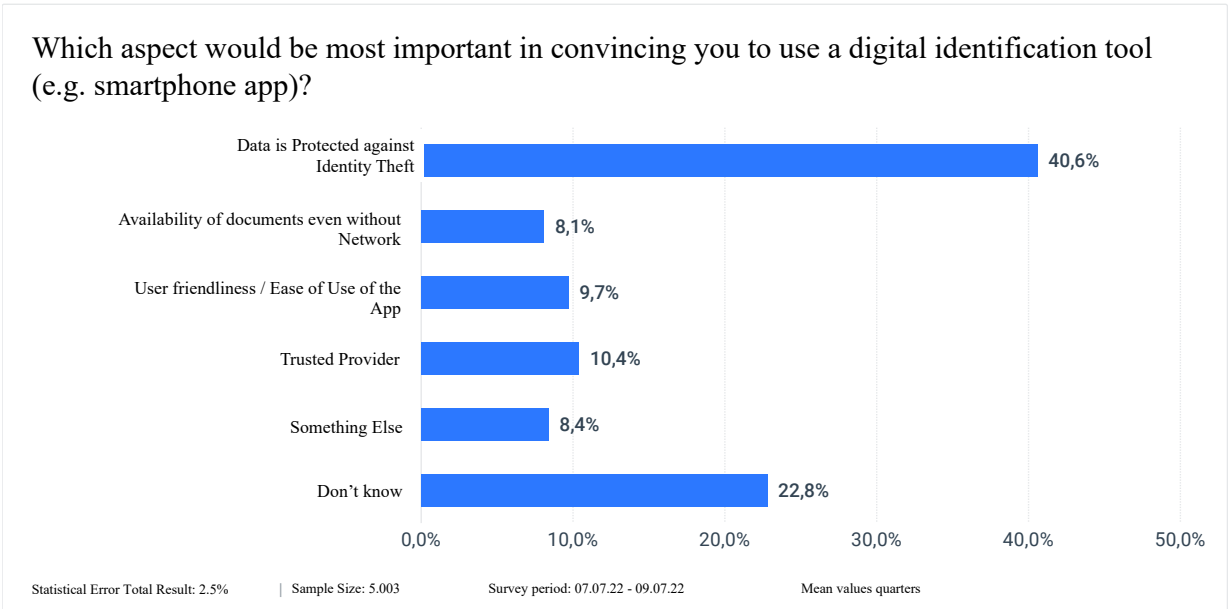
use it across the EU by default. With that, the ID Wallet projects with the LSP currently being planned seem to go into the right direction of meeting their citizens' needs.



Graph 3 Usage of Personal Data, Showcase Project Secure Digital Identities, 2022

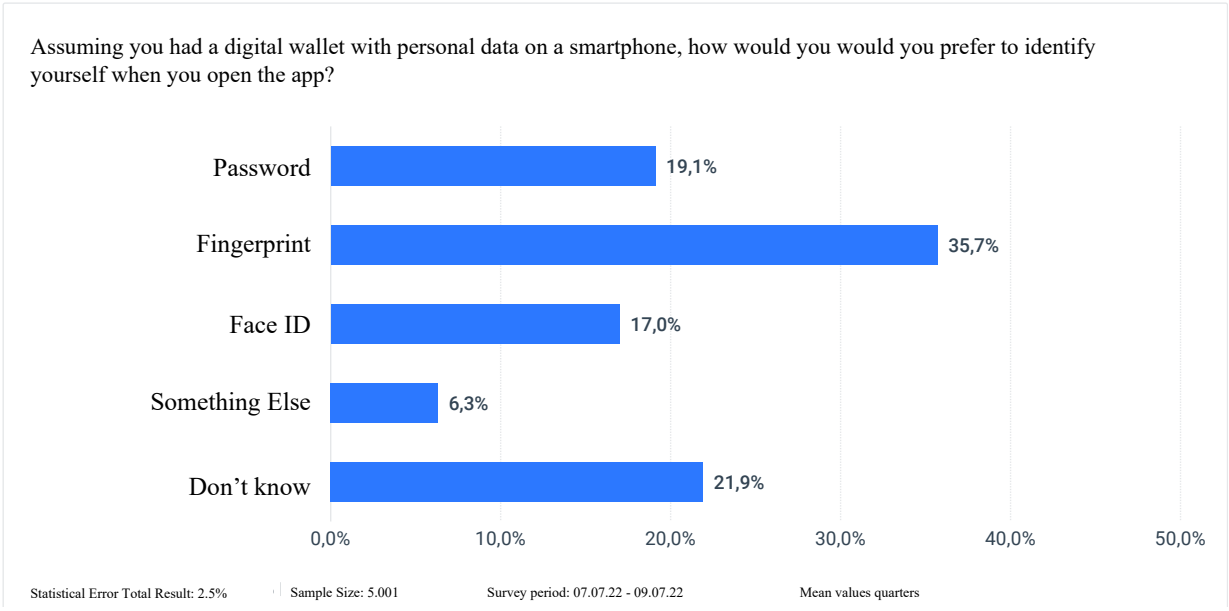
Ease of Use

The reason why German citizens have such a specific and strict understanding of data protection is not understandable outside of Germany. The topic is not just politically hyped. Survey like the one conducted during this thesis prove that end users perceive data protection in Germany as especially important (40%). The inconsistency though starts as soon as one looks into the data sharing rate by big platforms to which most global citizens are enrolled in (Aichholzer & Strauß, 2009). The Graph 4 underneath shows how much more important perceived data protection is vs. other aspects of possible ID solutions. The availability of documents, user friendliness, and the management by trusted providers each score a maximum of 10,4%.



Graph 4 Reasons to Use an eID, Showcase Project Secure Digital Identities, 2022

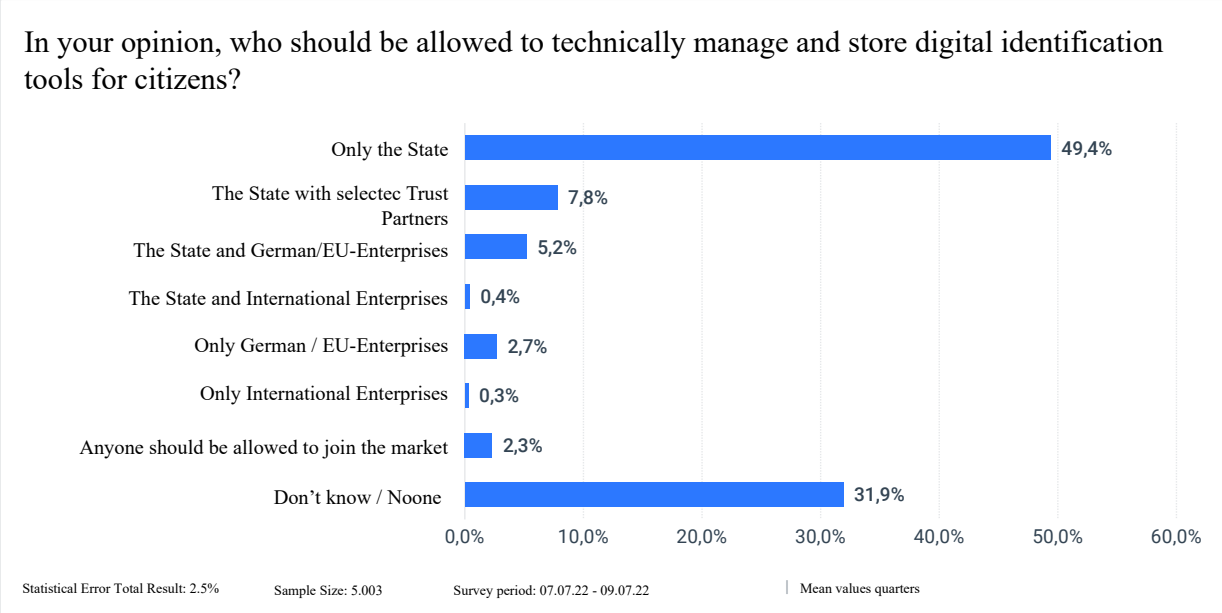
Another interesting development of the acceptance of other technologies that the usage of the eID scheme needs to use are the ways to login to an eID solution. Both the fingerprint and face ID have gained much more popularity, since they were established by big technology providers such as Apple or Samsung for their login technologies (Lawler, 2013). This shows that even if technologies are heavily criticized in the beginning of their diffusion process, if they still offer an improvement/higher convenience it will gain in popularity and diffusion pace.



Graph 5 Preference on Login Method, Showcase Project Secure Digital Identities, 2022

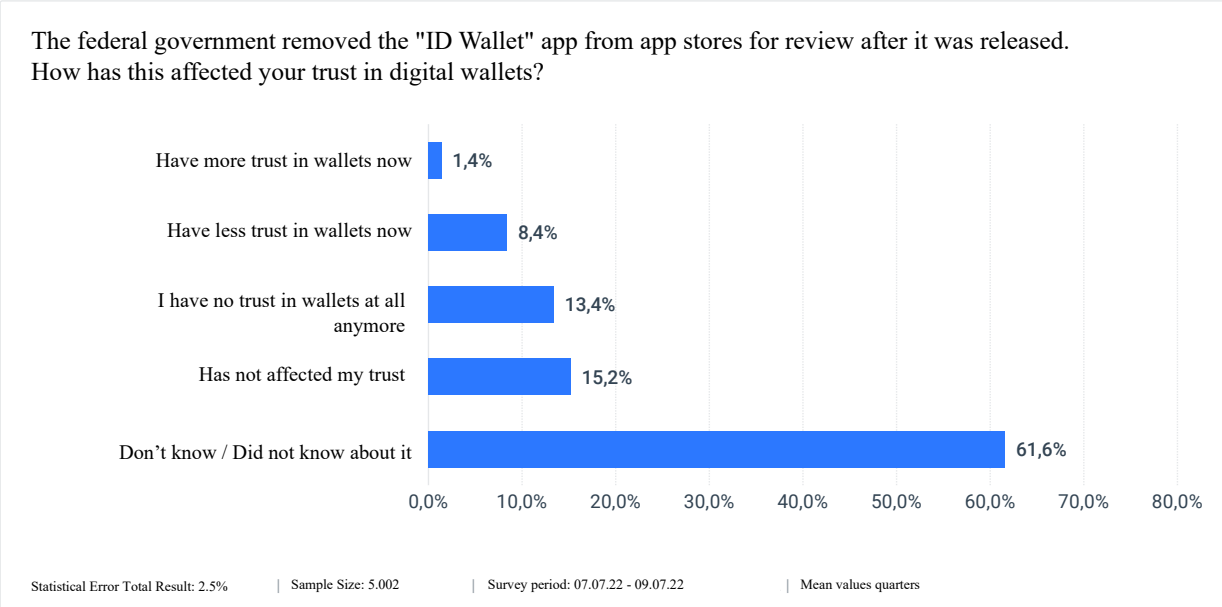
Trustworthiness

Another important factor for the acceptance of an emerging technology is trust. An interesting development is the gain of the state's trust by the end users. While end users traditionally mistrusted the state, especially in handling of personal data (Kubicek & Noack, 2010), the underlying output show a turnaround in trust. One explanation that could serve as explanation is the successful implementation of the Covid-Warn-App during the Covid-Pandemic (IPG4).



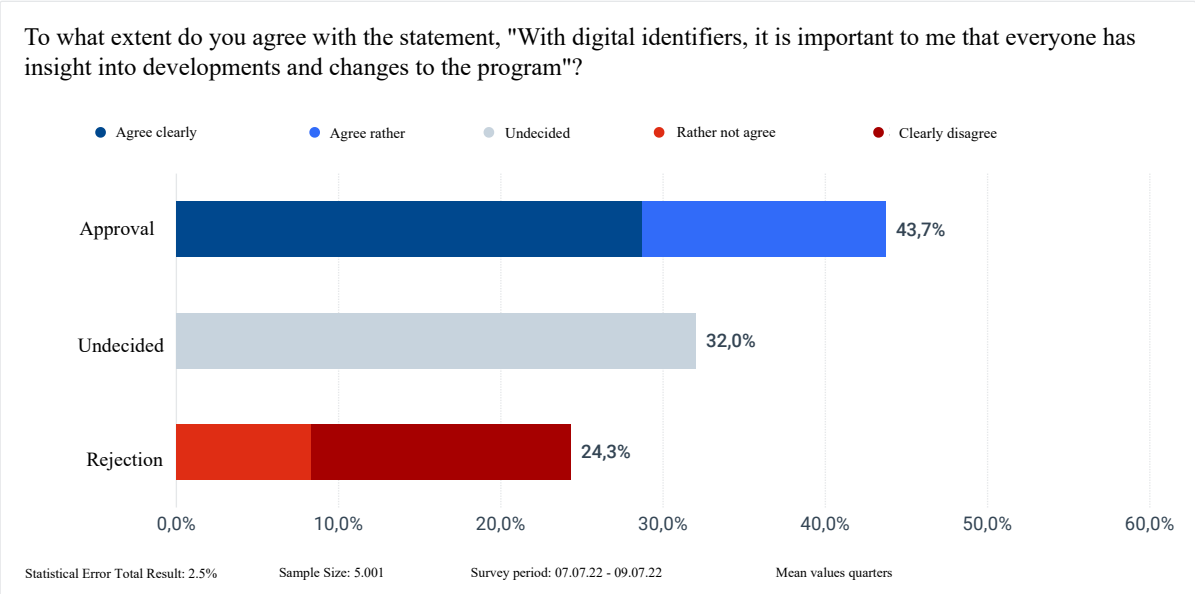
Graph 6 Preference on Responsible Unit for Data Security, Showcase Project Secure Digital Identities, 2022

Other than that, the failed ID Wallet project by the Chancellery that should have affected the end user's trust has not been changed. The reason for that mostly comes from citizens not being aware of the project to begin with. This aspect shows the difference of marketing success between two implementation projects. While the Covid-Warn-App solves an urgent problem that citizens constantly complain about: The tracing of infections and the deposition of the QR Code of the Covid Certificate. The ID Wallet project only assumed that there would be a need of saving a driver's license on the mobile phone. Before and after the ID wallet project of the Chancellery, not many end users have been complaining that they wanted to save their driver license on their phone (IPG3+IPG4, IPS1+ IPS2).



Graph 7 Trust in ID Wallets after the Chancellery Failed Launch, Showcase Project Secure Digital Identities, 2022

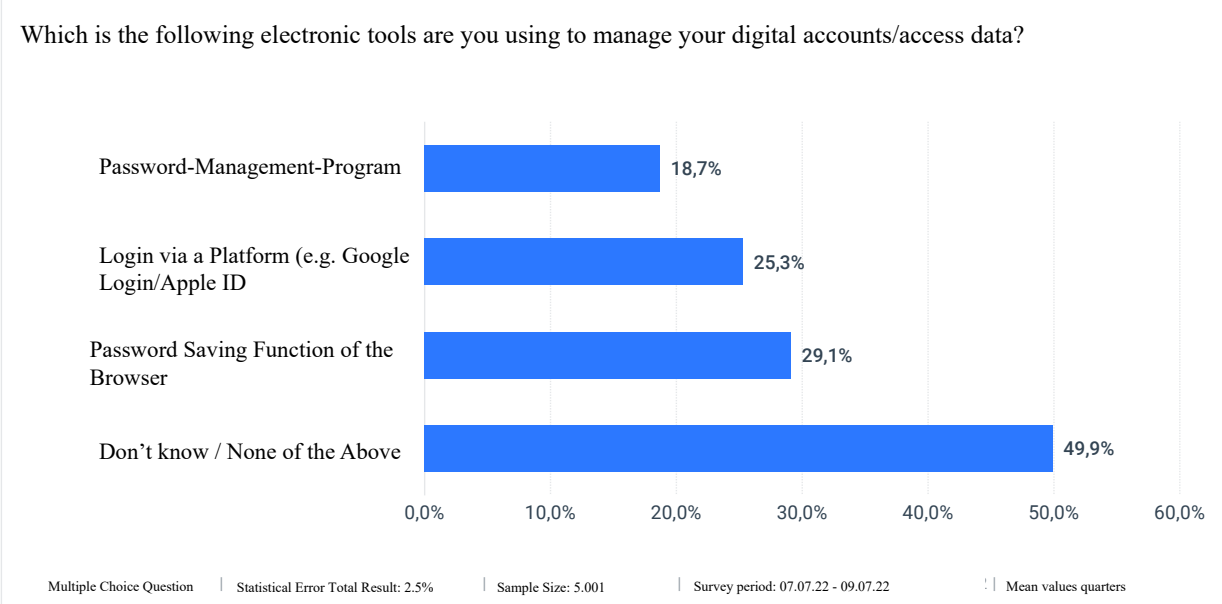
One question, that was chosen to be part of the survey is a question that hasn't been asked before. Through the question end users were asked whether they preferred an open-source project or not. Now, it is clearer that end users appreciate if they can follow developments and changes of a program. This output goes directly against the implementation strategies of the government level. So far, implementation projects were only made publicly known just before they were being launched (see Chapter 5). In contrast to that, transparency throughout the development of a technology is preferred.



Graph 8 Preference on Open Source in Implementation Project, Showcase Project Secure Digital Identities, 2022

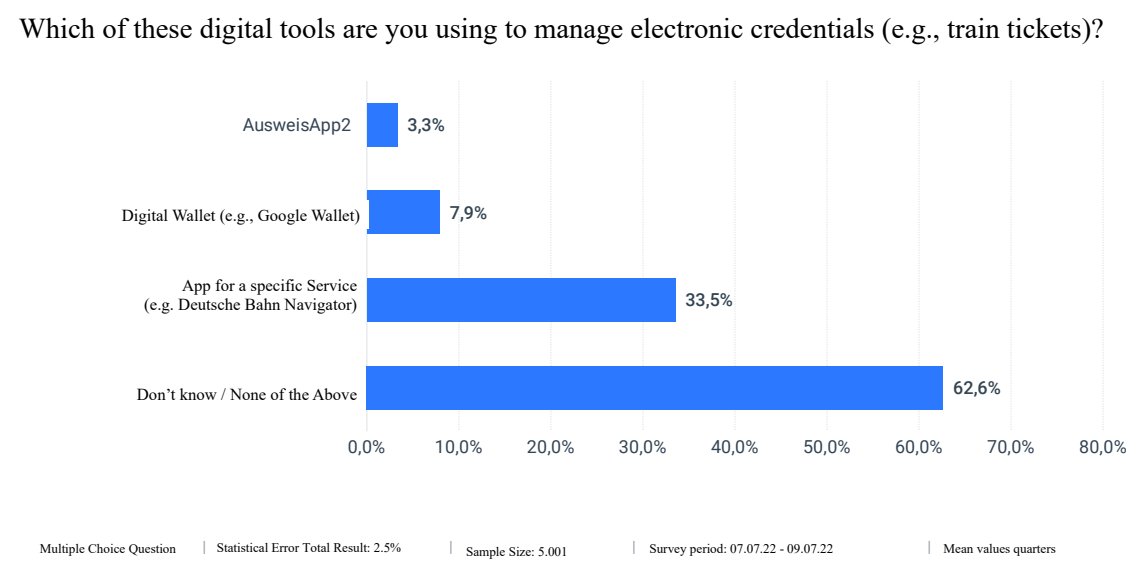
… leading to the use of eID use cases

When asking about the current use of electronic tools of managing digital accounts, the output also comes of no surprise. Approximately 50% don't manage their digital account at all or aren't aware of such tools. With not many use cases existing for which those tools would be needed, the diffusion of data management tools can't happen (Rogers et al., 2014).



Graph 9 Usage of Electronic Tools, Showcase Project Secure Digital Identities, 2022

When asking specifically about digital tools to manage credentials, the amount of end users that don't use one or aren't aware of the one's existing increases even more (63%). On the other side, Apps that are meant for specific purposes, like train ticket apps do have a good amount of awareness.



Graph 10 Usage of Digital Tools to manage credentials, Showcase Project Secure Digital Identities, 2022

As it was shown above, the nPA is still relatively unknown in many areas. One example of how the perception of the nPA was influenced is from back in 2010. The Chaos Computer Club proceeded a public hacking attack of the ePA. They believed they could prove the nPA was hackable. Though it was a simple tojan constellation that identified everything. But what remained? The identity card is not safe (IPG4).

Another example is at the process of picking up the ePA. End users are mostly consulted something like this: "We have a new thing, but I'm not sure how it works, and I wouldn't know what to use it for ". Employees at the registration office are not tasked with promoting anything in particular. The ePA, on the other hand, is a product, and a product does not begin to diffuse process by the government level stating, "I drafted a law, it has to run now," (IPG3).

To summarize, the effects of acceptance factors on the end user level don't have a traceable influence on the diffusion of the eID scheme in Germany. Since so far there hasn't yet been an urgent problem that was solved with the eID scheme, there naturally hasn't been an uptake in usage. ID solutions remain a topic for a niche of users that are focused on anything digital.

6.4 Mutual Influences of Acceptance and Success Factors

Some variables cannot be looked at in a siloed way, they mutually influence the acceptance and diffusion of the eID scheme in Germany. The following Chapter will go through such mutual influence factors.

Awareness and Know-How Transfer

As it was shown above, the awareness and know-how transfer has not yet been professionalized in the diffusion of the eID scheme. Therefore, there is a knowledge gap detectable on all three levels. That gap mutually influences the acceptance of the overall eID scheme, as trust and perceived usability can only be achieved through a common ground to start with. As this is not the case, that gap leads to actively deciding against the diffusion/usage of the eID scheme as shown in the Chapters of acceptance factors on all three levels.

As the eID scheme does not play such a decisive role for the everyday life of the people. The disruption of a market is therefore not given by just offering the solution. The eID scheme needs to hit a nerve in society. As mentioned before, the introduction of the Corona-Warn-App was exactly something like that. There were talks about connecting the eID function with the app, but it was quickly ruled out again. It would have had a great chance as the nPA could have been connected to an emotional topic such as the Covid pandemic (IPG3). When looking at key success factors, the image and visibility are not given.

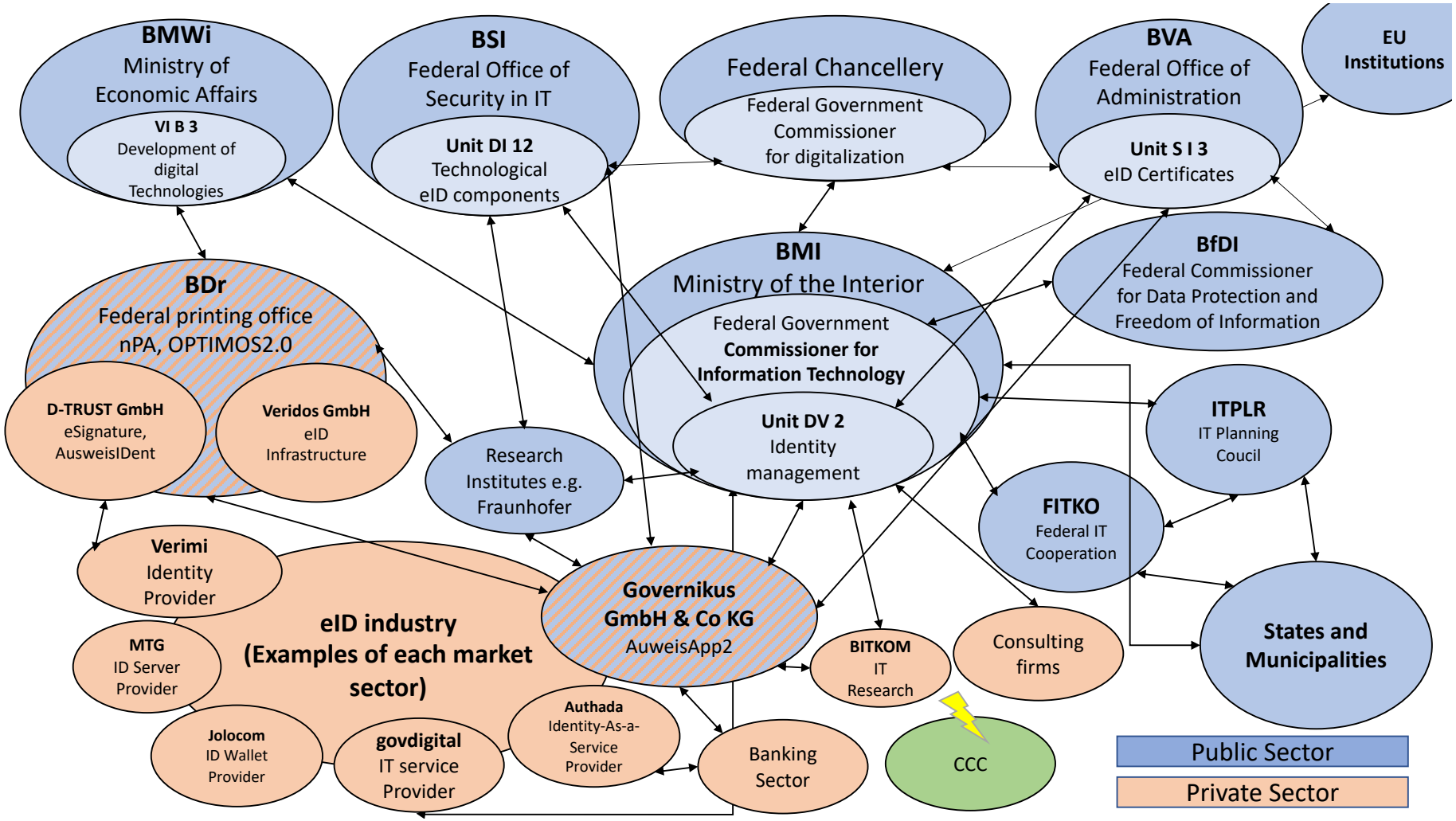


Figure 9 Actor Constellation as of 2022

The Actor Network

The figure above shows the complexity of the actor network. Please note that the entirety of the network is not guaranteed at this was created based on attained knowledge by research and data collection. Nonetheless, the figure nicely shows Germany's dominance of public agencies. The BSI played a role in both the emergence and collapse of Germany's eID development. Only after obtaining BSI security certification can an IT project be considered secure (IPG3). Their efforts have made the German electronic passport the safest in the world, but they have hindered the country's progress as an e-service provider (IPG4). Many stakeholders, including Governikus, BMI, BSI, and Fraunhofer Usability Standards, have an impact on the continuous development of the AuweisApp2 and other eID projects. Consulting firms have a long history in Germany as professional counsellors to government officials. Because linked ministries are responsible for overall accountability, they frequently plan in four-year legislative cycles. In the context of key success factors, the lack of trust between partners, the challenges and expenses associated with drafting and maintaining contractual agreements, and investment costs are given (Ivy, 2010; Jensen & Jaatun, 2013). One player of the network plays a specific role when it comes to trust and is presented underneath.

One group that has an influence on all three stakeholder groups but cannot be counted as being part of any of them is the interest group Chaos Computer Club. They are a group of hackers, calling themselves hacktivists, and manage an extremely successful online campaign fighting for cyber security in all areas of the internet. Since eID's are part of it, they have been actively analysing attempts to deal with electronic identification since the ePA. As their social media (Twitter especially) strategy is to be provocative but still constructive, they tend to get the biggest audience – hence influencing all three levels of stakeholders (IPG3+4; IPS1). Evidence for such an influence is the press citations of the invitee of the CCC of the public hearing on electronic identification on July 4th, 2022. The member of the CCC was cited most prominently and reached the furthest audience, as being the loudest critique of the current diffusion approached of the German eID scheme (Budras, 2022).

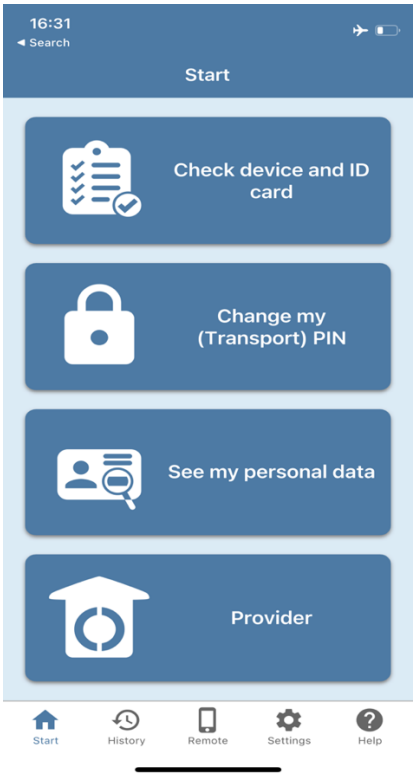
Lack of Interoperability of Existing Solutions

A direct consequence of the fragmentation of the regulations is lack of interoperability and recognition of digital identities among the different service providers. The German eID system is based on the extended access control standard (eAC), whereas other eIDAS notified eID schemes are based on X.509 certificate-infrastructures (BSI, 2017; Skierka, 2021b). While the national market might be interesting for some service providers, most of them expressed uncertainty to be a major barrier to enter the market at all (IPS4-6). Especially since the novelization of eIDAS it is clear that the aim is to offer European solutions, making the interoperability issue a much bigger one than before. Additionally, the technological developments are much faster than the adjustments on technical standards by the BSI, which

means that private sector service providers have created ID solutions that do not meet the security standards of the public sector, also hindering interoperability amongst solutions (e.g.: Jolocom and their Blockchain ID Wallet[33] vs. the AusweisApp2 and SmarteID).

Lack of User-Friendliness of the Solution

The nPA meets the highest IT security standards in a global comparison (Skierka, 2021a). However, until today its use has been unsatisfying for all three stakeholder levels: government, service providers, and end users. As it was illustrated during Chapter 5, the eID could only be read with a card reader. The lack of ease of use was also caused by very high security standards set by the BSI as well as a neglect of user experience measures (Margraf, 2014; Margraf et al., 2019). Therefore, this factor has a mutual effect on all three levels for the system acceptance and diffusion of the eID scheme. The current Smart-eID project has so far repeated exactly the same fault of the preparation phase in 2010. The belief of the consortium partners that they understand usability needs of end users is far from reality. In the meantime, there are more usability studies regarding the ePA, but the actual implementation is lacking. The anchor that connects the nPA and the end user is the AusweisApp2 and remains exclusively the ID card app - but this app remains largely unknown and is anything but user-friendly, as already shown in Chapter 6.3.2 and in the example picture underneath of the opening screen of the AA2.



Screenshot 1 Opening Screen of AusweisApp2 that the End User is greeted with

[33] Jolocom is building solutions based on decentralized identity management and blockchain https://jolocom.io/de/

Lack of Applications

As of today, 142 service providers have been authorized to enter the ID infrastructure and implement ID use cases. According to a 2020 study by the Boston Consulting Group and Nortal, 131 applications integrate the online ID function of the ePA, 86 of which are services of individual municipalities or states, which are only accessible to a few citizens. In total, therefore, only 45 services can be used with the nPA across Germany, of which only 28 are services from private-sector providers. As described in the Chapter 6.2.2, the application process in order to get the authorization to enter the ID infrastructure and offer the eID function of the nPA time-consuming and therefore costs resources that not every possible interested service provider can come up with. The result of the combination of the lack of attractiveness of the solution for both users and service providers was a negative network effect. Without ID use cases, there is no use and without use there is not ID use cases – a decade old conundrum that still needs to be solved.

Lack of Innovative Mindset in the Public Sector

As long as someone in government says that a solution must be 100 percent secure or I will not buy or invest in it, you must stick to your guns and say it does not align with innovation. Someone always takes a risk when they innovate. The government cannot be inventive as long as it is unable to think in this manner. Amazon is the service benchmark, not eGovernment.

This attitude can be traced back to the Napoleonic era. Administrative reforms were implemented at the time; it is a 200-year-old culture that is incredibly difficult to modify. Now the administration must realize that the consumer is king and will determine the next administration's success or failure (IPS2). When looking at key success factor of Chapter 3.4, insufficient funding and political support are not given, since the innovative mindset doesn’t exist.

Lack of Financial Subvention by the Government

Unless actors are part of a funded research initiative, such as the Secure Identities Showcase, there is currently no government subsidy. To overcome the first financial barrier, the government might subsidize certificates. In other words, the Bundesdruckerei contracts with the BMI, and the BMI pays for the certificates. That reduces the prices for people who wish to use it. It will not operate in the field of eID services because there are multiple providers. And if the government says, "We'll do it on our own," the market will be destroyed. Since they would ultimately choose the Bundesdruckerei because it can be commissioned without a tender. Other organizations that currently provide ID-as-a-service as an integration function would then exit. IPG3 2022

Lack of Communication and Marketing

The biggest mistake that was made in Germany with nPA is that they've created a functional medium but haven't advertised it. Marketing is a critical concern. As mentioned earlier, marketing funds were cut in 2010. As it all can be explained, it is politically unreasonable. According to the polls presented in Chapter 6.3, German citizens are unaware of the capabilities of the ID card. Furthermore, persons working in administrations must be convinced of the nPA in order to produce a multiplier effect.

The IT department, on the other hand, is always required to collaborate with all departments, states, and ministries. Their system struggles with these cross-cutting challenges and will never reach this speed. As a result, we are infinitely slow, and the state loses significant traction as a result. IPS1

Lack of Risk Appetite

The ePA project is driven by legal and security specialists because to Germany's disproportionate reliance on technical progress and the fear of being unable to manage the multitude of impacts in all administrative, social, and economic spheres. The German e-ID was designed inside a system of exceptional security for exchanges and personal data, subject to complicated legal limits, with a focus on zero-fault and zero-risk (Thales, 2020). While the nPA is now the safest electronic identification technology in the world, other aforementioned key success factors have had to await their moment until today.

Data security itself is set much higher in the heads of all stakeholder groups than it actually is in the law. People tend to complain about the lack of diffusion due to data protection issues, but there is always prove that it is not as strict in the law. Data protection is sometimes used as a shield if people don't want to change anything (IPG3).

Lack of Coordination

As it was shown during the presentation of the results and the German case itself, it can't work if five separate ministries of different political interest streams come together and try to solve the eID issue of non-diffusion. And it will not function as long as the power battle between these several ministries is won by one as it is also proven as a key success factor (Van Cauter, 2016). All the concessions made by placing the digital in the name of one ministry and telling the next ministry that they may continue influencing the eID scheme for a certain aspect is counterproductive.

The chancellor's office also believes to be on top of everything and form a new steering committee (IPG3). When one looks backs back it becomes evident, that the government doesn't learn from past mistakes or even successes. While some public employees would wish to build on already existing findings, the issue is that there is no institutional learning process happening. There is no system in place that says, "This project went wrong; let's approach the other initiatives differently." (IPG4).

The Bundestag, as the parliament, might theoretically impose the necessary pressure. The parliament is trapped in the legislative process itself though and has little interest in confronting its own faults. This is especially obvious since the worst adjustments to technical projects are made by Minister Presidents who claim that something must be included due to constituency interests (IPS1). This lack of coordination mutually influences all three levels, as it actively blocks a successful diffusion the German eID scheme. As mentioned in Chapter 3.2, governance that identity ecosystems must be collaborative for them to be advantageous for all stakeholders. So far this is not given.

Germany is a Laggard Country

In Germany, neither user acceptance nor usage of eID solutions are widespread. Until now, the country has focused on a public-sector electronic identification solution (e.g., digital identity cards), which has mostly been used for public services (Arkwright, 2022). In contrast to the pioneers as they are presented by Rogers et al. (2014), private providers, such as Verimi or Yes, lack the critical mass to become the dominant answer to the lack of eID acceptance in Germany. As a result, the possible client base is limited, and the evolution toward the supremacy of a state-owned or private solution is questionable (Arkwright, 2022).

One factor that only mutually influences two levels, the government and service provider level is:

Fragmentation of Regulatory Requirements

When looking at the legal context, both national and European regulations have an impact on government and service provider stakeholder levels and mutually affect their behaviour on implementing the ID infrastructure and establishing eID use cases (Skierka, forthcoming) .

Depending on the sector that the specific stakeholder is working in there are different interpretations on how to handle the collection of identity data, the requirements for establishing identity, or the proofs that are permitted apart from identification documents.[34] On the other side, the technical guidelines that need to be followed in order to access the ID infrastructure also differ depending on the sector. The most common technical guideline comes from the BSI

[34] e.g., for sector-specific regulations are: OZG, GWG, TKG, SGB V

though, which has by far the strictest requirements and minimum security level (vs. Financial Agency or Infrastructure Agency) (Skierka, forthcoming).
In practice that means that the government and the service provider level mutually effect each other's acceptance by not adjusting the regulations fast enough or implementing a more efficient ID infrastructure while service providers need have to deal with fragmentation of the regulations which directly hinders the implementation process of ID use cases.

To adequately understand the legal context, the European regulation is also looked at. Just like the national one, it is fragmented. Even though the eIDAS Regulation offers a framework for EU-wide mutual recognition of electronic identity systems, only notified eID system can recognize each other. Additionally, standards for security and interoperability layer are only applicable to public sector identities and the private sector so far excluded.
In terms of the theoretical framework this means that service providers coming from the private sector are so far exempt from an easy entrance to a European ID ecosystem and its market potential. Additionally, digitalization (and automatically eID) maturity levels across Europe differ significantly as it can be seen in the EU Benchmark reports each year (European Commission, 2021). A consequence of the maturity of each market is also mutually effecting the use of ID use cases as it can be seen at the output of the Survey in Chapter 6.3.2 (Skierka, forthcoming).

In summary, according to Rogers' criteria for the diffusion of innovations, the nPA has limitations, mainly in visibility, the relative advantage it delivers, and its complexity. The benefits of electronic identification with the nPA are not obvious or can only be presented in specialized circles rather than to the general public due to a lack of applications or high-quality use cases. The total complexity of its use or integration into applications remains high.

7 Conclusions

As this thesis has shown, there is no issue of identifying why the diffusion of the eID scheme in Germany has not yet happened. The challenge is rather for practitioners to choose a course and follow it until the eID scheme is successfully diffused. Until now, the benefits of digitization in the public sector have not been fully realized. Bridging the gap between the three explored stakeholder groups is of central importance in order to out the current conundrum of creating positive network effects. In the following conclusion the leading research question(s) are answered, limitations of the presented research, and prospective possibilities for future research are presented.

7.1 Answer to the Research Question(s)

This thesis intended to explore the factors that are influencing the diffusion of the eID scheme in Germany. The research questions, which is: *Which impact do contextual and acceptance factors (X-Variable) of the government, service providers, and end users have on the diffusion (implementation and use) (Y-Variable) of the eID scheme in Germany since its rollout in 2010?* can therefore be answered as such:

Contextual Factors:

The **legal context** has a high impact on the government and service provider levels. While the government level creates the legal context and implements it, the service provider level needs to comply to any upcoming adjustments. When looking at the end user level, there is detectable data that reveals any measurable indicators on how the legal context influences that group.

The **institutional context** has an equally high impact on all three stakeholder levels. As the actor constellation has shown for the government and service provider levels, there are existing interdependencies that highly impact the diffusion of the eID scheme. When looking at the end user level, trust and the relationship with the respective institution highly influence the following usage of a prospective ID use case.

The **market context** has a high impact on the service provider level. As the service providers need to integrate the eID scheme, invest their resources, and think about how they want to solve the benefit-usage tension field, they are constantly on the outlook for current market developments. On the other hand, the market only has semi-strong influences on the government and end user levels. As it was detected, the German Government s has so far not been necessarily concerned with the market as they are more concerned with their public sector digitalization, which is much different from the market outside the public sector. The end users on the other side have not yet been confronted with the eID scheme itself and can therefore neither complain about nor learn about its potential. The little encounters that they might have with the nPA in a market basis have not led to any detectable change in the overall usage.

The **socio-cultural context** has a high influence on all three levels as different cultural approaches towards innovation and making use of digitalization are constantly confronted with each other on all levels. While the government level is concerned with offering the most secure eID solution, they are limiting the innovative possibilities of the service providers. That conflict directly influences the overall acceptance of the end users as they are confronted with inconsistent and non-transparent eID solutions that they are supposed to accept every other legislative period.

The **technological context** could be proven to be high on government and service provider level. Especially the contradicting practice of writing down legal requirements and regulatory bills vs. the pace of technological developments is contributing heavily toward the non-diffusion of the German eID scheme. When looking at the end user level, the data at hand has not given enough insight for knowing in what way the technological context influences that group.

Acceptance Factors:

The **ease of use** was proven to have a high impact on service provider level. Only with a positively perceived ease of use, the motivation will be high enough for a critical mass of service providers to invest in integrating the ePA. So far only a small number has been doing so, not because of the perceives ease of use though. It has a semi-strong impact on the government level. Even though the public servants also need to decide to market the ePA, the public sector is mainly concerned with managing the ID infrastructure. It has a low impact or even none, since there are no use cases for the mass end user group. As soon as there are more use cases, the impact will change.

Usefulness has a high impact on service providers and end users. Only if the profitability (therefore usefulness for the business of service providers) and usability for daily practices is given, the acceptance will rise. Since so far, these two aren't given, the impact is high on the non-acceptance/refusal to use the German eID scheme. The government level on the other side is only partly affected by the usefulness, as they have already established a working ID solution. In their sense, the project has been implemented successfully.

The aspect of **trust** has a high impact on all three levels. All three levels need to be able to trust each other. As this aspect doesn't just come from high security standards, but also building trust relationships with each other, the current trust levels have not yet reached their full potential.

The first sub-question was: *which factors mutually affect all stakeholder groups in the diffusion of the eID innovation in Germany?*

As briefly presented during the answer to the main question, the socio-cultural and market context as well as trust are the leading factors that mutually influence the overall system acceptance of the German eID scheme.

> The second sub-question is: *how do the stakeholder groups affect each other in the diffusion process?*

The research has shown that by following their current practices, they actively limit potential, innovativeness, market share, and an overall successful diffusion of the German eID scheme. Only in history, during the formation of the eSignature Act and the integration of NFC, have the stakeholder groups shown positive influences on each other. Other than that, Germany remains as a laggard country.

> The last sub-question is: *which stakeholder group has the highest impact on the diffusion of the eID innovation in Germany?*

Not just content-wise, but also evidence-wise the Government stakeholder group influences the diffusion of the eID scheme the strongest and has the highest impact on how it can proceed in the future. As the framework setter of not just regulations but also standards, the former of committees, and the biggest investing force in big innovation project, the government level can shape the diffusion like no other.

7.2 Limitations

A major limitation of single case studies is the generalizability. Finding from this case will most probably not be applicable anywhere else. Nonetheless the case itself has brought insights that remain of scientific relevance. Another limitation is the potential subjectivity and bias of the researcher as they are part of the research project on secure digital identities and the survey that was used for this thesis was conducted during the project. Influences from other members of the research project should not be ignored.

On the other hand, being a member of the research project has offered a unique access point to data that would otherwise not have been as extensive as it is now. The data that came out of the survey that is used is hard to contextualize. The answers at hand could give out data on all elements of the theoretical framework. Limited time is another limiting factor of this thesis, as more time could be invested into contextualizing the end user answers for instance.

The researcher also doesn’t have in-depth knowledge of underlying technologies of the eID scheme, which limits the understanding of certain technological developments during the eID project. The last detected limitation is that there are more levels than just the three that were analysed during this thesis. Focusing on more levels is out of the scope of this thesis though and a great prospective for future research.

7.3 Future Research

A first possibility to research the topic further is to move onto a much more in-depth analysis on the technological level. This is a major shortcoming of this thesis and would be very interesting to look into. As it was already discussed in the limitations, it became clear that there are more than just the three levels used as an analytical basis in the theoretical framework. Future research could aim at completing the levels that have an influence on the overall system acceptance of the German eID scheme.

As this research is a X -> Y design, only that stream was analysed. Future research can proceed to go through the other way and analyse Y -> X and find out how diffusion causes acceptance.

Another interesting stream for future research is to attempt to find an alternative approach to the current top-down structure in the eID scheme, in which the government level sets all boundaries, and the service providers and end users have to follow them.

References

Aichholzer, G., & Strauß, S. (2009). *Understanding a complex innovation process: identity management in Austrian e-government*. https://doi.org/10.1145/1556176.1556218

Alkhalifah, A., & D'Ambra, J. (2012). Factors effecting user adoption of identity management systems: An empirical study. *Proceedings - Pacific Asia Conference on Information Systems, PACIS 2012*.

Alkhalifah, A., & D'Ambra, J. (2013). The Role of Trust in the Initial Adoption of Identity Management Systems. In (pp. 25-39). Boston, MA: Springer US. https://doi.org/10.1007/978-1-4614-7540-8_2

Allen, C. (2016, April 25 2016). *The Path to Self-Sovereign-Identity*. Retrieved 25.06.2022 from http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

Arkwright. (2022). *DIGITAL IDENTITIES IN EUROPE*. https://assets.website-files.com/61509dd26eb1ae688f25b0d8/62b59f24387174848f6657ec_ARKWRIGHT-REPORT-EIDs-IN-EUROPE-062022.pdf

Benbasat, I., Gefen, D., & Pavlou, P. A. (2008). Special Issue: Trust in Online Environments. *Journal of Management Information Systems*, *24*(4), 5-11. https://doi.org/10.2753/MIS0742-1222240400

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77-101. https://doi.org/10.1191/1478088706qp063oa

Brugger, J., Fraefel, M., & Riedl, R. (2015). Raising Acceptance of Cross-Border eID Federation by Value Alignment.

BSI. (2017). *Technische Richtlinie TR-03128 Diensteanbieter für die eID-Funktion*. Bonn Retrieved from https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03128/BSI_TR-03128_Teil1.pdf?__blob=publicationFile&v=1

Budras, C. (2022). Viel Geld für nichts: Experten kritisieren Digitalpolitik. *Frankfurter Allgemeine Zeitung (FAZ)*. https://www.faz.net/aktuell/wirtschaft/digitaler-personalausweis-kritik-an-digitalpolitik-des-bundes-18149276.html

Bundesregierung. (2021). *Ökosystem Digitale Identitäten*. https://www.bundesregierung.de/breg-de/suche/oekosystem-digitale-identitaet-1960124

CCC. (2021). *Stellungnahme zum elektronischen Identitätsnachweis und zur Zentralisierung der Biometriedaten*. https://www.ccc.de/de/updates/2021/gemeinsame-stellungnahme-zum-eid-gesetz-entwurf

Commission, E., Directorate-General for Communications Networks, C., & Technology. (2021). *eGovernment benchmark 2021 : entering a new digital government era : country factsheets*. Publications Office. https://doi.org/doi/10.2759/485079

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, *13*(3), 319-340. https://doi.org/10.2307/249008

Fensel, D., Bruijn, J., Domi, J., Lausen, H., Polleres, A., Roman, D., & Stollberg, M. (2007). *Enabling Semantic Web Services: The Web Service Modeling Ontology* (1. Aufl. ed.). Berlin, Heidelberg: Springer-Verlag. https://doi.org/10.1007/978-3-540-34520-6

Harbach, M., Fahl, S., Rieger, M., & Smith, M. (2013). On the Acceptance of Privacy-Preserving Authentication Technology: The Curious Case of National Identity Cards. In (pp. 245-264). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-39077-7_13

Homburg, V., & Dijkshoorn, A. (2013). Persuasive Pressures in the Adoption of E-Government.

Hood, C. (2011). *The blame game: spin, bureaucracy, and self-preservation in government*. Princeton : Princeton university.

Kahlo, C. (2022). Stellungnahme zu Fragen im Rahmen des Auschusses zu Digitalen Identitäten im deutschen Bundestag. In.

Khatchatourov, A., Laurent, M., & Levallois-Barth, C. (2015). Privacy in Digital Identity Systems: Models, Assessment, and User Adoption. In (pp. 273-290). Springer International Publishing. https://doi.org/10.1007/978-3-319-22479-4_21

Klischewski, R., & Ukena, S. (2010). E-Government Goes Semantic Web: How Administrations Can Transform Their Information Processes. In (pp. 99-125). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-03507-4_5

KPMG. (2022). Marktstudie eID. https://www.bitkom.org/sites/main/files/2022-06/08.06.22_Marktstudie_eIDAS_Summit.pdf

Kubicek, H., & Hagen, M. (2000). One-Stop-Government in Europe: Results of 11 national surveys.

Kubicek, H., & Noack, T. (2010). The path dependency of national electronic identities. *Identity in the Information Society*, *3*. https://doi.org/10.1007/s12394-010-0050-2

Kuhlmann, S., & Wollmann, H. (2019). *Introduction to Comparative Public Administration: Administrative Systems and Reforms in Europe*. Edward Elgar Publishing. https://books.google.de/books?id=Qp36uwEACAAJ

Lawler. (2013). *Chaos Computer Club says it's beaten Apple's Touch ID fingerprint reader*. Retrieved 23.06.2022 from https://www.engadget.com/2013-09-22-chaos-computer-club-apple-touch-id-fake-fingerprint.html

Lips, S., Bharosa, N., & Draheim, D. (2021). eIDAS Implementation Challenges: The Case of Estonia and the Netherlands. In (Vol. 1349, pp. 75-89). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-67238-6_6

Mahula, S., Tan, E., & Crompvoets, J. (2021). With blockchain or not? Opportunities and challenges of self-sovereign identity implementation in public administration: Lessons from the Belgian case.

Margraf, M. (2014). Der elektronische Identitätsnachweis : Einsatzmöglichkeiten des neuen Personalausweises im privat-wirtschaftlichen Umfeld. In. https://doi.org/10.15771/RFID_2014_22

Margraf, M., Ohlendorf, T., & Studier, W. (2019). Digitale Identitäten auf dem Smartphone. *Datenschutz und Datensicherheit - DuD*, *43*, 17-22. https://doi.org/10.1007/s11623-019-1054-1

Monitor, e. (2021). *Initiative D21*.

Nortal. (2020a). *Identifikatoren als Grundlage eines leistungsfähigen eID-Ökosystems*.

Nortal. (2020b). *Zehn Jahre Personalausweis:*

Wie Deutschland ein erfolgreiches eID-Ökosystem aufbauen kann. http://a73hcfvauxwyowr1jbvt5656-wpengine.netdna-ssl.com/wp-content/uploads/2020/11/Report-eAuthentifizierung-und-eSignatur_vff_20201105.pdf

Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (Onlinezugangsgesetz - OZG), (2017). https://www.gesetze-im-internet.de/ozg/OZG.pdf

Pickel, G., & Pickel, S. (2009). Qualitative Interviews als Verfahren des Ländervergleichs. In S. Pickel, D. Jahn, H.-J. Lauth, & G. Pickel (Eds.), *Methoden der vergleichenden Politik- und Sozialwissenschaft. Neue Entwicklungen und Anwendungen.* (Vol. 1). VS Verlag für Sozialwissenschaften / GWV Fachverlage GmbH Wiesbaden.

Podgorelec, B., Alber, L., & Zefferer, T. (2022). *What is a (Digital) Identity Wallet? A Systematic Literature Review*. https://doi.org/10.1109/COMPSAC54236.2022.00131

Poller, A., Waldmann, U., Vowe, S., & Turpe, S. (2012). Electronic Identity Cards for User Authentication-Promise and Practice. *IEEE security & privacy*, *10*(1), 46-54. https://doi.org/10.1109/MSP.2011.148

pwc. (2021). *Der Online-Ausweis auf dem Smartphone und die digitale Brieftasche*.

Koalitionsvertrag 2021 – 2025 zwischen der Sozialdemokratischen Partei Deutschlands (SPD), BÜNDNIS 90 / DIE GRÜNEN und den Freien Demokraten (FDP), (2021).

Rogers, E. M. (1995). *Diffusion of innovations* (4th ed.). New York (N.Y.) : Free Press.

Rogers, E. M., Singhal, A., & Quinlan, M. M. (2014). Diffusion of innovations. In *An integrated approach to communication theory and research* (pp. 432-448). Routledge.

Saunders, M. N. K., Lewis, P., & Thornhill, A. (2019). *Research methods for business students Mark N.K. Saunders, Philip Lewis, Adrian Thornhill* (8th edition. ed.). Harlow : Pearson.

Schulze, L. (2022). *Arbeitsverträge: Zurück ins Analoge*. Tagesspiegel Background. Retrieved 22. Juli from https://background.tagesspiegel.de/digitalisierung/arbeitsvertraege-zurueck-ins-analoge

Seltsikas, P., & O'Keefe, R. M. (2010). Expectations and outcomes in electronic identity management: the role of trust and public value. *European journal of information systems*, *19*(1), 93-103. https://doi.org/10.1057/ejis.2009.51

Skierka, I. (2021a). Governing the digital ID – How Germany and the EU plan to reclaim our digital sovereignty. Retrieved 29.07.2022, from

Skierka, I. (2021b). *Nationale Ökosysteme für digitale Identitäten*. ESMT Berlin.

Skierka, I. (forthcoming). Digitale Identitäten. In F. N. Tanja Klenk, Göttrik Wew (Ed.), *Handbuch Digitalisierung in Staat und Verwaltung* (2 ed.). Springer VS.

Söderström, F. (2016). Introducing public sector eIDs : The power of actors' translations and institutional barriers.

Stepanaia, i., & Jerman, B. (2018). Exploring European Digital Single Market: user adoption and preferences for eID services. *International Journal of Electronic Governance*, *10*, 1. https://doi.org/10.1504/IJEG.2018.10015741

Subrahmanyam, K., & Šmahel, D. (2011). Constructing Identity Online: Identity Exploration and Self-Presentation. In (pp. 59-80). Springer New York. https://doi.org/10.1007/978-1-4419-6278-2_4

Thales, G. (2020). *Overview of the German identity card project and lessons learned (2020 update)*. https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/eid-in-germany

Tsap, V., Lips, S., & Draheim, D. (2020). Analyzing eID Public Acceptance and User Preferences for Current Authentication Options in Estonia. In (pp. 159-173). Springer International Publishing. https://doi.org/10.1007/978-3-030-58957-8_12

Valtna-Dvořák, A., Lips, S., Tsap, V., Ottis, R., Priisalu, J., & Draheim, D. (2021). Vulnerability of State-Provided Electronic Identification: The Case of ROCA

in Estonia. In (Vol. 12926, pp. 73-85). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-86611-2_6

Van Cauter, L. (2016). *Government-to-government information system failure in Flanders: an in-depth study* KU Leuven]. Leuven.

Venkatesh, V., Brown, S. A., & Bala, H. (2013). Bridging the Qualitative-Quantitative Divide: Guidelines for Conducting Mixed Methods Research in Information Systems. *MIS Quarterly*, *37*(1), 21-54. http://www.jstor.org/stable/43825936

Vries, H., Tummers, L., & Bekkers, V. (2018). The diffusion and adoption of public sector innovations: a meta-synthesis of the literature. *Perspectives on public management and governance*, *1*(3), 159-176. https://doi.org/10.1093/ppmgov/gvy001

Williams, M. D., Rana, N. P., Dwivedi, Y. K., & Williams, J. (2012). Theories and Theoretical Models for Examining the Adoption of E-Government Services. *E-service journal*, *8*(2), 26-56. https://doi.org/10.2979/eservicej.8.2.26

Yin, R. K. (2018). *Case study research and applications: design and methods* (6th edition ed.). Thousand Oaks : Sage.

Zefferer, T., & Teufl, P. (2015). Leveraging the Adoption of Mobile eID and e-Signature Solutions in Europe. In (Vol. 9265, pp. 86-100). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-22389-6_7

Appendix

A List and Details of Interviews

Interviewee Code	Organization	Dates	Duration
IPG1	Ministry of Economics (BMWK)	December 2019	1h5min
IPG2	Federal Office for Information Security	January 2020	1h25min
IPG3	Federal Ministry of Administration	First Interview February 2020 Second Interview May 2022	First: 1h53min Second: 1h51min
IPG4	Fraunhofer Institute for Applied Integrated Security (AISEC)	First Interview February 2020 Second Interview: June 2022	First: 53min Second: 1h26min
IPS1	ESMT Berlin in 2020 GovDigital in 2022	First interview: December 2019 Second Interview: May 2022	First: 1h31min Second: 56min
IPS2	Governikus	First interview: February 2020 Second Interview: May 2022	First: 1h26min Second: 1h31min
IPS3	Nortal AG	May 2022	1h23min
IPS4	Authada	April 2022	1h
IPS5	MTG	April 2022	1h
IPS6	mvneco	May 2022	1h

Table 2 Length, Date, and Name of Organization of Interviewees

B Interview Guide – English Translation and German Original

English Translation of Interview Guide

Greeting

- Introduction of the interviewer
- Student of the PIONEER MSc, write MA.

Explanation of the purpose

- In this thesis I will focus on the factors that affect the diffusion of the creation of the eID scheme in Germany. My work compares the decision and policy behavior for the introduction and enforcement of an eID in Germany among several stakeholder groups. An analysis of the decision behavior about the effects of the possibilities of the ID card version shall provide information from the introduction of the new ID card in 2010, which decisions and views of the nPA have promoted the enforcement and establishment of the eID and which have inhibited it. This analysis will also identify core actors that have influenced the development of eID since 2010.
- To trace the trajectory of eID, I use the phase-based concept of path dependencies, among others. The interview will be guided by a temporal path.
- In the following, I will refer to eID as the online identification functions of the new identity card

Specification of the interview process:

- Audio recorded
- Introduction of the interviewee
- Narrative Interview, questions serve as guidance, but the interview will be more open and follow the natural process of the conversation
- Briefly present career history

- Present role and responsibilities in the ministry
- Explain where insights exist and where technical focus lies

Preparation phase 2002 to 2010

1. were there any decisions you would have made differently from today's perspective?
2. to what extent did political pressure/agenda play a role in your day-to-day work?
3. the BSI was also held accountable. How did you perceive the cooperation between BSI and BMI during your work?
4. After 2005, the ruling coalition and consequently the political agenda changed. How did the change from an SPD leadership to a CDU leadership affect the work on eID?
5. The digital passports were introduced relatively smoothly. How do you explain the difficulties of introducing the ID card as opposed to the passport?
6. From the end of 2008 until the introduction of the new ID card in 2010, pilots and application tests were conducted by the BMI and BSI in cooperation with consulting firms and the public administration for its use. Would you say that this approach was effective?
    a. Should the user perspective that plays a central role in the OZG today have been included at that time?
    b. To what extent do you perceive the differences between the program for digitizing administrative offerings at that time and the OZG program today?
    c. How do you explain the lengthy establishment of the eID, which has not yet achieved widespread use?
7. Another key player is the federal commissioner for data protection and freedom of information. How do you assess the influence of the BfDI on the introduction and establishment of the eID function of the new ID card?

Start of the enforcement of the eID of the ID card as of November 2010

After years of conception, Germany introduced the new identity card including the online ID function in 2010. Politicians and academics agreed that the usage figures of the online function would increase exponentially from the date of introduction. One year later, 8.5 million cards were in circulation, one third of these cards had an activated online ID function, and 600,000 readers for authentication were sold. At first glance, these numbers seem mixed. However, the low level of activation of the online ID function is particularly interesting.

1. what can you say in principle about the decision-making processes and integration of applications when introducing the eID of the new identity card?
2. in your opinion, which decisions were particularly conducive to establishing a secure eID in society?
3. which decisions should have been taken differently, given today's knowledge?
4. What is your basic assessment of the path Germany has taken with regard to the design of the voluntary activation of the online ID function?
5. In your opinion, should voluntary measures such as the online ID function and the infrastructural design of possible online services have been implemented differently?
6. How would you rate the provision of knowledge about online ID functions prior to the introduction of the new ID card in November 2010?
7. What would you identify as the drivers of the steps taken at an early stage to legislate digital identity?
    i. What factors do you think have exacerbated inhibited use of the online ID card function?

Establishment of an eID management system

As early as 2011, the ID card app for connecting the smartphone and the ID card via NFC chip was programmed by Fraunhofer FOKUS. At that time, the antennas of the end devices were not

strong enough for this type of use. Easy nPA software developed by INIT AG was presented, and new versions of the ID cards were already being discussed. From the government side, however, only an excessive number of administrative services were digitized with which the new ID card could be used.

1. How did you perceive the first period after the introduction of the eID?
2. in your estimation, which decisions were particularly progressive and particularly promoted projects such as easy nPA and the first version of the AusweisApp?
3. to what extent has it changed the landscape of actors since 2010?
4. would you say that the lack of disclosure capabilities in municipalities has been a major factor in the low use of the online ID card function?
5. How did you perceive the education about the new ID cards in the public administration?

D. eGovernment Initiative and eGovernment Act 2013.

In 2013, the BMI launched the eGovernment Initiative to promote more application possibilities for DE-Mail, online ID card functions, and easier access to the use of the new ID card. In addition, the eGovernment Act, Act to Promote Electronic Administration and to Amend Other Regulations was passed on July 25, 2013, which was intended to oblige federal authorities to enable the use of electronic proof of identity from January 1, 2015, and to provide the necessary infrastructure for this on the part of the authorities.

1. what impact did the eGovernment initiative have on the further process of establishing eID?
2. how did you cooperate with the departments mainly involved with regard to the establishment of the eID?
    i. BMI?
    ii. BSI?
    iii. Federal printing office?

3. to what extent has the eGovernment Act affected the establishment of the application options for the new ID card?

E. eIDAS and ID Card AUSWEISAPP2 2014

The eIDAS Regulation 2014 established that ID cards from EU member states are entitled to use services Europe-wide. The AusweisApp2 should significantly simplify the use of administrative services.

1. How do you evaluate the introduction of the AusweisApp2?
    a. Has the work with secure identities changed since the introduction of the AusweisApp2?
2. how do you assess the impact of the eIDAS regulation on decision-making behavior with regard to new projects related to eID?
3. how did you perceive the introduction of the AuweisApp2?

F. Hurdle reduction since 2017-2020.

Since 2017, the online ID function has been automatically activated for newly issued ID cards. Since November 1, 2019, it has been possible to provide an address abroad in order to receive administrative services from there. Since then, initiatives have been launched to keep up with the rapid development of the digital environment, such as the OPTIMOS 2.0 project.

1. How did you perceive the BMI's approach to eID as an outsider then? What has changed since you left?
2. How do you assess the decision-making behavior of the BMI with regard to the removal of hurdles to the use of the online functions of the new ID card?
3. Which hurdles to the use of the online ID card function do you consider particularly important to be removed?

4. How do you assess the usage figures for online authentication with a mobile identity as opposed to the nPA?
5. What lessons do you draw from the last ten years of establishing a culture of use of the online ID function?
6. how do you explain the lengthy establishment of the eID, which has not yet achieved widespread use?

G. Megatrends and major projects 2020-present

Since the start of the pandemic in 2020, the need for a viable eID function has been made clear. To keep up with this social pressure, projects have been launched in several arenas in combination with new techniques and trend solutions. I am talking here about the BMWK's Secure Digital Identities showcase project as well as the Chancellery's ID Wallet project and a general trend towards SSI. Especially the latest technology principles like SSI have met with vehement headwind from IT security experts.

1. how have you perceived the time since 2020?
2. do you expect a shift in the usability of eID with new technologies like ID Wallet and SmartID?
3. how open are you to the German eID market?
4. What would you like to see in a functioning eID ecosystem?
5. To what extent do you trust the current nPA solutions and plans?
6. How easy is it to use and integrate the nPA?
7. How useful has the nPA become since 2010?

Interview Guideline – German Original

Gesprächsleitfaden 1

0. Begrüßung
   - Vorstellung des Interviewers
     - Studentin des PIONEER MSc, schreibe MA

- Erläuterung des Anliegens

  - In der Arbeit widme ich mich Entscheidungsprozessen, die zu Erschaffung der eID Ökosystems geführt haben, welche die heutige Nutzung des neuen Personalausweises ermöglichen soll. Meine Arbeit vergleicht das Entscheidungs- und auch Policy Verhalten zur Einführung und Durchsetzung einer eID in Deutschland unter mehreren Stakeholdergruppen. Eine Analyse des Entscheidungsverhaltens in Hinsicht auf die Auswirkungen der Möglichkeiten der Ausweisversion soll ab der Einführung des neuen Personalausweises 2010 Aufschlüsse bringen, welche Entscheidungen und Ansichten des nPA die Durchsetzung und Etablierung der eID gefördert und welche sie gehemmt haben. Im Rahmen dieser Analyse sollen auch Kernakteure ermittelt werden, welche die Entwicklung der eID seit 2010 beeinflusst haben.
  - Um den Werdegang der eID nachvollziehen zu können, bediene ich mich unter anderem am phasenbasierten Konzept der Pfadabhängigkeiten. Das Interview wird sich an einem zeitlichen Pfad orientieren.
  - Im Folgenden werde ich eID als die Online-Ausweisfunktionen des neuen Personalausweises bezeichnen

- Tontechnische Aufzeichnung
- Vorstellung des Interviewten
  Narratives Interview:
  - Kurz Werdegang darstellen
  - Rolle und Verantwortlichkeiten im Ministerium darstellen
  - Erläutern, wo Einblicke bestehen und wo fachlicher Fokus liegt

2. Vorbereitungsphase 2002 bis 2010

1. Gab es Entscheidungen, die Sie aus heutiger Sicht anders gefällt hätten?
2. Inwiefern spielte politischer Druck/Agenda in Ihrem Arbeitsalltag eine Rolle?
3. Das BSI wurde auch in die Verantwortung genommen. Wie haben Sie während Ihrer Tätigkeit die Kooperation zwischen BSI und BMI wahrgenommen?
4. Nach 2005 wechselte die regierende Koalition und demnach die politische Agenda. Wie hat sich der Wechsel von einer SPD-Leitung zu einer CDU-Leitung auf das Arbeiten an der eID ausgewirkt?
5. Die Digitalen Pässe wurden problemlos eingeführt. Wie erklären Sie sich die Schwierigkeiten der Einführung des Personalausweises im Gegensatz zum Reisepass?
6. Seit Ende 2008 bis zur Einführung des neuen Personalausweises 2010 wurden Piloten und Anwendungstests vom BMI und BSI in Kooperation mit Beratungsfirmen und der öffentlichen Verwaltung für dessen Anwendung durchgeführt. Würden Sie sagen, dass diese Vorgehensweise effektiv war?
   b. Hätte man damals die Nutzerperspektive, die beim OZG heute eine zentrale Rolle spielt, mit einbinden müssen?
   c. Inwiefern nehmen Sie die Unterschiede des damaligen Programmes zur Digitalisierung der Verwaltungsangebote und des heutigen OZG Programmes wahr?
   d. Wie erklären Sie sich die langwierige Etablierung der eID, die bis heute keine flächendeckende Anwendung erreicht hat?

7. Ein anderer Schlüsselakteur ist der Bundesbeauftragte für Datenschutz und die Informationsfreiheit. Wie schätzen Sie den Einfluss des BfDI auf die Einführung und Etablierung der eID Funktion des neuen Personalausweises ein?

3. Beginn der Durchsetzung der eID des Personalausweises ab November 2010

Deutschland hat nach jahrelanger Konzeptionsphase 2010 den neuen Personalausweis samt Online-Ausweisfunktion eingeführt. Politik und Wissenschaft waren sich einig, dass die Nutzungszahlen der Online-Funktion ab dem Einführungszeitpunkt exponentiell steigen würden. Ein Jahr später waren 8,5 Millionen Exemplare im Umlauf, ein Drittel dieser Ausweise hatten eine Aktivierte Online-Ausweisfunktion und 600.000 Lesegeräte zur Authentifizierung wurden verkauft. Diese Zahlen wirken bei erster Betrachtung durchwachsen. Besonders interessant ist jedoch die geringe Aktivierung der Online-Ausweisfunktion.

1. Was können Sie grundsätzlich über die Entscheidungsprozesse und Einbindung von Anwendungen bei der Einführung der eID des neuen Personalausweises sagen? ´
2. Welche Entscheidungen waren Ihrer Ansicht nach besonders fördernd, um eine sichere eID in der Gesellschaft zu etablieren?
3. Welche Entscheidungen hätten mit heutigem Wissen anders getroffen werden sollen?
4. Wie bewerten Sie grundsätzlich den eingeschlagenen Weg Deutschlands hinsichtlich der Ausgestaltung der freiwilligen Aktivierung der Online-Ausweisfunktion?
5. Hätten Ihrer Meinung nach Freiwilligkeiten, wie die Online-Ausweisfunktion und infrastrukturelle Ausgestaltungen der möglichen Online-Dienste anders umgesetzt werden müssen?
6. Wie bewerten Sie die Wissensvermittlung zu Online-Ausweisfunktionen vor der Einführung des neuen Personalausweises im November 2010 ein?
7. Was würden Sie als Treiber der frühzeitig ergriffenen Schritte einer legislativen Ausgestaltung der digitalen Identität benennen?

b. Welche Faktoren haben Ihrer Meinung nach, die gehemmte Nutzung der Online-Ausweisfunktion verstärkt?

4. Etablierung eines eID Managements Systems

Bereits 2011 wurden die AusweisApp zur Verbindung des Smartphones und des Personalausweises via NFC-Chip vom Fraunhofer FOKUS programmiert. Damals waren die Antennen der Endgeräte zu dieser Art von Nutzung nicht stark genug. Eine von der INIT AG entwickelte Software easy nPA wurde vorgestellt, neue Versionen der Ausweise waren bereits im Gespräch. Aus der Behördlichen Seite wurde jedoch nur eine überhaubare Anzahl von Verwaltungsleistungen digitalisiert, mit welchen der neue Personalausweis eingesetzt werden konnte.

1. Wie haben Sie die erste Zeit nach der Einführung der eID wahrgenommen?

2. Welche Entscheidungen waren Ihrer Einschätzung nach besonders progressivorientiert und haben Projekte, wie easy nPA und die erste Version der AusweisApp besonders gefördert?
3. Inwiefern hat sie die Akteurs Landschaft seit 2010 geändert?
4. Würden Sie sagen, dass die mangelnde Auskunftsfähigkeit in den Kommunen maßgeblich die geringe Nutzung der Online-Ausweisfunktion beeinflusst hat?

5. Wie haben Sie die Aufklärung über die neuen Personalausweise in der öffentlichen Verwaltung wahrgenommen?

5. eGovenment Initiative und eGovenment Gesetz 2013

2013 startete das BMI die eGovenment Initiative, um mehr Anwendungsmöglichkeiten für DE-Mail, Online-Ausweisfunktionen und einen leichteren Zugang zur Nutzung des neuen Personalausweises zu fördern. Außerdem wurde das E-Government -Gesetz, Gesetz zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften am 25. Juli 2013 verabschiedet, welches die Bundesbehörden verpflichten sollte die Nutzung des elektronischen Identitätsnachweises ab dem 1. Januar 2015 zu ermöglichen und dafür die auf Seiten der Behörden notwendige Infrastruktur bereitzustellen.

1. Welche Auswirkungen hatte die eGovenment Initiative auf den weiteren Prozess der Etablierung der eID?
2. Wie war Sie die Zusammenarbeit mit den hauptsächlich beteiligten Ressorts in Hinsicht auf die Etablierung der eID?

   b. BMI?
   c. BSI?
   d. Bundesdruckerei?
3. Inwiefern hat sich das eGovenment Gesetz auf die Etablierung der Anwendungsmöglichkeiten des neuen Personalausweises ausgewirkt?

6. eIDAS und AusweisApp2 2014

Mit der eIDAS Verordnung 2014 wurde festgelegt, dass Ausweise aus EU-Mitgliedstaaten berechtigt sind Dienstleistungen Europaweit zu nutzen. Die AusweisApp2 sollte die Inanspruchnahme von Verwaltungsdienstleistungen signifikant vereinfachen.

1. Wie bewerten Sie die Einführung der AusweisApp2?
   b. Hat sich seit der Einführung der AusweisApp2 die Arbeit mit sicheren Identitäten verändert?
2. Wie schätzen Sie den Einfluss der eIDAS Verordnung auf das Entscheidungsverhalten in Hinsicht auf neue Projekte, die mit der eID zu tun hatten, ein?
3. Wie haben Sie die Einführung der AuweisApp2 wahrgenommen?

7. Hürdenabbau seit 2017-2020

Seit 2017 ist die Online-Ausweisfunktion bei neuausgestellten Personalausweisen automatisch aktiviert. Seit 1. November 2019 ist es möglich eine Adresse im Ausland anzugeben, um von dort Verwaltungsdienstleistungen in Anspruch zu nehmen. Seitdem sind Initiativen, die mit der rasanten Entwicklung der digitalen Umgebung, wie das OPTIMOS 2.0 Projekt, ins Leben gerufen worden.

2. Wie haben Sie die Arbeitsweise zur eID des BMI als dann Außenstehender wahrgenommen? Was hat sich verändert, seit Sie gegangen wurden?
3. Wie schätzen Sie das Entscheidungsverhalten des BMI in Hinsicht auf den Hürdenabbau zur Nutzung der Online-Funktionen des neuen Personalausweises ein?
4. Welche Hürden zur Nutzung der Online-Ausweisfunktion sehen Sie als besonders wichtig an, abgebaut zu werden?
5. Wie schätzen Sie die Nutzungszahlen der online Authentifizierung mit einer mobilen Identität im Gegensatz zum nPA ein?

6. Welche Lehren ziehen Sie aus den letzten zehn Jahren der Etablierung einer Nutzungskultur der Online-Auseisfunktion?
7. Wie erklären Sie sich die langwierige Etablierung der eID, die bis heute keine flächendeckende Anwendung erreicht hat?

8. Megatrends und Großprojekte 2020-heute

Seit Pandemiebeginn in 2020 wurde die Nötigkeit einer praktikablem eID Funktion verdeutlicht. Um diesem gesellschaftlichen Druck hinterherzukommen, wurden in mehreren Arenen Projekte in Kombination mit neuen Techniken und Trend-Lösungen ins Leben gerufen. Ich spreche hier von dem Schaufensterprojekt Sichere digitale Identitäten des BMWK's sowie dem ID-Wallet Projekt des Kanzleramts und einem generellen Trend in Richtung SSI. Gerade neueste Technologieprinzipien wie SSI sind auf vehementen Gegenwind von IT-SicherheitsexpertInnen gestoßen.

1. Wie haben Sie die Zeit seit 2020 wahrgenommen?

2. Versprechen Sie sich einen shift der Nutzbarkeit der eID mit neuen Techniken wie ID-Wallet und SmartID?

3. Wie offen nehmen Sie den deutschen eID Markt auf?

4. Welche Wünsche hätten Sie für ein funktionierendes eID Ökosystem?

5. Inwiefern vertrauen Sie den derzeitigen nPA Lösungen und Vorhaben?

6. Wie leicht ist es den nPA zu nutzen bzw. zu integrieren?

7. Wie nützlich ist der nPA seit 2010 geworden?

C Questionnaire for Survey

Hilfsmittel zur Verwaltung von Identitätsdaten

1.

Frage	**Welche dieser digitalen Identifizierungsmittel sind Ihnen bekannt?**	66 Zeichen

Antwortoptionen	*Individuell*	
	FALSCH	
	1. Online-Ausweisfunktion des Personalausweises	44 Zeichen
	2. AusweisApp2 (Digitale Nutzung des Ausweises)	44 Zeichen
	3. Smart-eID (Ausweis auf dem Handy)	33 Zeichen
	4. ID Wallet (App zur Nachweis-Speicherung)	40 Zeichen
	5. Apple ID / Google-Konto	23 Zeichen
	6. Postident (Verfahren durch die Deutsche Post)	45 Zeichen
	7. VideoIdent (Verfahren per Videoanruf)	37 Zeichen
	8. AutoIdent (mit künstlicher Intelligenz)	39 Zeichen

** Ausschließende Antwort

Antworttyp	Mehrfachauswahl (unbegrenzt)
Anmerkungen	–
Grundgesamtheit	Bundesdeutsche ab 18 Jahren
Stichprobengröße	5.000

Frage	**Welche dieser elektronischen Hilfsmittel nutzen Sie zur Verwaltung Ihrer digitalen Nutzerkennungen / Zugangsdaten?**	114 Zeichen
Antwortoptionen	*Individuell*	
	FALSE	
	1. Passwort-Manager-Programm	25 Zeichen
	2. Login über einen Dienst (z.B. Google-Konto)	43 Zeichen
	3. Passwort-Speicherfunktion im Browser	36 Zeichen
	4. Weiß nicht / Keines der Genannten**	35 Zeichen

Ausschließende Antwort

Antworttyp	Mehrfachauswahl (unbegrenzt)
Anmerkungen	—
Grundgesamtheit	Bundesdeutsche ab 18 Jahren
Stichprobengröße	5.000

Frage	**Welche digitalen Hilfsmittel nutzen Sie, um elektronische Bescheinigungen (z.B. Zugtickets) zu verwalten?**	105 Zeichen
Antwortoptionen	*Individuell*	
	FALSE	
	1. AusweisApp2	11 Zeichen
	2. Digitale Brieftasche (z.B. Google Wallet)	41 Zeichen
	3. Zweckbezogene App (z.B. DB Navigator)	37 Zeichen
	4. Weiß nicht / Keine der Genannten**	34 Zeichen

Ausschließende Antwort

Antworttyp	Mehrfachauswahl (unbegrenzt)
Anmerkungen	—
Grundgesamtheit	Bundesdeutsche ab 18 Jahren
Stichprobengröße	5.000

Vertrauen in unterschiedliche Verwalter von Identitäten

4.

Frage	**Wer sollte Ihrer Meinung nach digitale Identifizierungsmittel für Bürgerinnen und Bürger technisch verwalten und speichern dürfen?**	129 Zeichen
Antwortoptionen	*Individuell*	
	FALSE	
	1. Nur der Staat	13 Zeichen

	2. Der Staat mit ausgewählten Partnerunternehmen	45 Zeichen
	3. Der Staat und deutsche / EU-Unternehmen	39 Zeichen
	4. Der Staat und internationale Unternehmen	40 Zeichen
	5. Nur deutsche / EU-Unternehmen	29 Zeichen
	6. Nur internationale Unternehmen	30 Zeichen
	7. Sollte für jeden erlaubt sein	30 Zeichen
	8. Weiß nicht / Niemand	Zeichen

Antworttyp	Einfache Auswahl
Anmerkungen	—
Grundgesamtheit	Bundesdeutsche ab 18 Jahren
Stichprobengröße	5.000

Frage	**Welcher Aspekt wäre am wichtigsten, um Sie von der Nutzung eines digitalen Identifizierungsmittels (z.B. Smartphone-App) zu überzeugen?**	135 Zeichen

Antwortoptionen	*Individuell*	
	FALSE	
	1. Sicherheit der Daten vor Identitätsdiebstahl	44 Zeichen
	2. Verfügbarkeit der Dokumente auch ohne Netz	42 Zeichen
	3. Nutzerfreundlichkeit / Bedienbarkeit der App	44 Zeichen
	4. Vertrauenswürdiger Anbieter	27 Zeichen
	5. Etwas anderes	13 Zeichen
	6. Weiß nicht	eichen

Antworttyp	Einfache Auswahl
Anmerkungen	—
Grundgesamtheit	Bundesdeutsche ab 18 Jahren
Stichprobengröße	5.000

Wallet

Frage	**Können Sie sich vorstellen, Ausweise und Karten digital auf dem Smartphone zu speichern („Wallet" / digitale Brieftasche), um sie so vorzeigen und verwalten zu können?**	167 Zeichen

Antwortoptionen	*Ja (...) Nein*	
	1. Ja, auf jeden Fall	18 Zeichen
	2. Eher ja	7 Zeichen
	3. Unentschieden	13 Zeichen
	4. Eher nein	9 Zeichen
	5. Nein, auf keinen Fall	eichen

Antworttyp	Einfache Auswahl
Anmerkungen	—
Grundgesamtheit	Bundesdeutsche ab 18 Jahren
Stichprobengröße	5.000

Frage	**Die Bundesregierung hat die „ID-Wallet" App zur Überarbeitung nach Veröffentlichung wieder aus App-Stores entfernt. Wie hat dies Ihr Vertrauen in digitale Brieftaschen („Wallets") beeinflusst?**	192 Zeichen

Antwortoptionen	*Individuell*	
	FALSE	
	1. Habe nun mehr Vertrauen in Wallets	34 Zeichen
	2. Habe nun weniger Vertrauen in Wallets	37 Zeichen
	3. Habe nun gar kein Vertrauen in Wallets mehr	43 Zeichen
	4. Hat mein Vertrauen nicht beeinflusst	36 Zeichen
	5. Weiß nicht / Wusste nichts davon	eichen

Antworttyp	Einfache Auswahl
Anmerkungen	—
Grundgesamtheit	Bundesdeutsche ab 18 Jahren
Stichprobengröße	5.000

Authentifizierungsmethoden

Frage	**Angenommen Sie hätten eine digitale Brieftasche mit persönlichen Daten auf einem Smartphone, wie würden Sie sich beim Öffnen der App am liebsten identifizieren?**	161 Zeichen

Antwortoptionen	*Individuell*	
	FALSE	
	1. Eingabe eines Passworts	23 Zeichen
	2. Nutzung des Fingerabdrucks	26 Zeichen

	3. Nutzung von Gesichtserkennung	29 Zeichen
	4. Anders	6 Zeichen
	5. Weiß nicht	eichen

Antworttyp Einfache Auswahl
Anmerkungen —
Grundgesamtheit Bundesdeutsche ab 18 Jahren
Stichprobengröße 5.000

Frage	**Inwieweit stimmen Sie der Aussage zu: „Bei digitalen Identifizierungsmitteln ist es mir wichtig, dass jeder Einsicht in Entwicklungen und Veränderungen des Programms hat"?**	171 Zeichen

Antwortoptionen	*Stimme eindeutig zu (...) Stimme eindeutig nicht zu*	
	1. Stimme eindeutig zu	19 Zeichen
	2. Stimme eher zu	14 Zeichen
	3. Unentschieden	13 Zeichen
	4. Stimme eher nicht zu	20 Zeichen
	5. Stimme eindeutig nicht zu	

Antworttyp Einfache Auswahl
Anmerkungen —
Grundgesamtheit Bundesdeutsche ab 18 Jahren
Stichprobengröße 5.000

Frage	**Angenommen Sie würden eine digitale Brieftasche („Wallet") nutzen, um persönliche Daten (z.B. Personalausweis) zu speichern, wo würden Sie diese verwenden können?**	162 Zeichen

Antwortoptionen	*Individuell*	
	1. Nur innerhalb Deutschlands	26 Zeichen
	2. In Deutschland und wenn nötig in der EU	39 Zeichen
	3. Standardmäßig in der gesamten EU	32 Zeichen
	4. Weiß nicht	10 Zeichen

Antworttyp Einfache Auswahl
Anmerkungen —
Grundgesamtheit Bundesdeutsche ab 18 Jahren
Stichprobengröße 5.000