On the Acceptance of Privacy-Preserving Authentication Technology: The Curious Case of National Identity Cards

Marian Harbach[1], Sascha Fahl[1], Matthias Rieger[2], and Matthew Smith[1]

[1] Distributed Computing & Security Group, Leibniz Universität Hannover, Germany
{harbach,fahl,smith}@dcsec.uni-hannover.de
[2] Institute of Sociology, Leibniz Universität Hannover, Germany
mrieger@ish.uni-hannover.de

Abstract. Many attempts have been made to replace the ubiquitous username-and-password authentication scheme in order to improve user security, privacy and usability. However, none of the proposed methods have gained wide-spread user acceptance. In this paper, we examine the users' perceptions and concerns on using several alternative authentication methods on the Internet. We investigate the adoption of the new German national identity card, as it is the first eID-enabled card with dedicated features to enable privacy-preserving online authentication. Even though its large-scale roll-out was backed by a national government, adoption rates and acceptance are still low. We present results of three focus groups as well as interviews with service providers, showing that preserving privacy is just one of several factors relevant to the acceptance of novel authentication technologies by users as well as service providers.

Keywords: Privacy-Preserving Authentication, Usable Security, National Identity Cards, eID, Technology Acceptance, Social Factors.

1 Introduction

Username-and-password remains the prevalent mechanism for every-day online authentication. While services and usage patterns evolve, this authentication mechanism has been largely unchanged throughout the history of Information Technology. Of Alexa's top 100 websites[1], most sites offer additional features behind a username-and-password-based login or require a login to access the site at all. Users have learned to accept this form of authentication [12] and use creative schemes to tailor the system to their needs [20]. They use separate pseudonyms for different services and choose password strength according to several criteria [8,10,12] to maintain appropriate levels of privacy and security.

[1] cf. http://www.alexa.com/topsites/global

E. De Cristofaro and M. Wright (Eds.): PETS 2013, LNCS 7981, pp. 245–264, 2013.

Several papers (e. g. Bonneau [2], Dhamija et al. [7], Jakobsson and Dusseault [14], as well as Perito et al. [23]) and incidents[2] have shown problems with the current practice and numerous alternative online authentication schemes have been proposed to overcome these [6,3]. However, none of these schemes has found wide-spread adoption yet. In an extensive survey of proposals for improving online authentication, including password managers, graphical, cognitive, phone-based or biometric schemes, as well as paper and hardware tokens, Bonneau et al. [3] found that none of the 35 mechanisms under investigation came close to the benefits username-and-password currently offers to users. While security was generally better with the alternatives, deployability was always worse and with many usability also suffered. While hardware tokens such as smartcards could provide strong security, these mechanisms have high deployment costs for both users as well as providers and additionally require the user to carry an object around.

A trend of the past years could, however, be able to alleviate these major downsides of physical tokens. Many countries are currently in the process of rolling out or have already rolled out national identity cards with a means to access identity information electronically (electronic identity, eID). Acuity Market Intelligence projects that 85 % of identity credentials issued annually will be electronically readable by 2015 and four out of five countries will be issuing eID-capable identity cards[3]. This implies that, soon enough, a considerable portion of Internet users will be carrying a token, capable of electronic authentication, that has already been paid for.

While the USA have not yet announced plans to introduce eID documents, 24 of the 27 countries in the European Union have already deployed or plan to deploy eID cards[4]. The European Commission is actively supporting digital identities and aims to adapt legislation to increase adoption[5]. Since national eID cards are compulsory in many states, they have the potential to gain broad acceptance as an electronic means of identification. Additionally, these cards are often habitually carried by their owners and hence, similar to mobile phones, are more or less ubiquitously available. Currently, available solutions in countries such as Estonia or Belgium aim at proving real identities for public services/eGovernment as well as eCommerce and eBanking applications. This focus has however limited their applicability as a general online authentication mechanism.

In this paper, we analyze the most recently introduced eID scheme: the nPA (*Neuer Personalausweis*, new personal identity card) launched by the German government in November 2010. This official document is the first to include privacy-preserving features beyond proving one's true identity electronically.

[2] http://www.h-online.com/security/news/item/Password-leaks-bigger-than-first-thought-1614516.html, http://arstechnica.com/security/2012/08/passwords-under-assault/

[3] http://www.acuity-mi.com/GNeID_Report.php

[4] http://www.epractice.eu/en/community/eureid/view_resources/Factsheet-on-the-electronic-Identity-at-pan-European-level—May-2012

[5] http://www.euractiv.com/infosociety/brussels-wants-identities-eu-cit-news-512833

While the nPA can reliably verify that a person lives in a certain city or is of certain age without disclosing the actual address or age, it can also generate a provider-specific pseudonym directly on the card. It is therefore the first national ID card technically capable of substituting username and password without any threat to the user's privacy. With the nPA, the user can choose to login without disclosing identifying information or with dependable proof of his true identity.

In this paper, we aim to analyze which factors inhibit the acceptance of the nPA in order to support the development of future Internet authentication alternatives. The core contributions of this paper are as follows:

- We investigate the users' perceptions in using a new system for everyday online authentication and identify motivations for, as well as barriers to adoption.
- We present technical and social factors that influence the acceptance of alternative authentication mechanisms in general and how privacy-preserving features compare to these other factors.
- We shed light on the needs and perceptions of businesses offering such an alternative authentication mechanism for their online services.
- We provide recommendations that can support the deployment of future large-scale authentication systems.

To the best of the authors' knowledge, this paper is the first to discuss the role of national ID cards in the search for a username-and-password alternative. While we do not suggest that the nPA is the best possible solution, we believe that smartcards issued by national governments can provide a viable basis for more security and good usability in online authentication. Germany's efforts to maximize privacy in their eID scheme is an important step towards enabling wide-spread use.

2 Related Work

There is a long line of research on technology acceptance in general from the area of Information Science and Business. A recent model for security technology acceptance of Herath et al. [13] explicitly addresses IT security services. They combine the well-known and widely discussed Technology Acceptance Model (TAM) of Davis et al. for general technology acceptance [5] with Liang et al.'s Technology Threat Avoidance Theory (TTAT, [19]), which relates avoiding security threats to coping behavior and Protection Motivation Theory.

In Herath et al.'s model, a user's motivation to adopt a mechanism depends on three main factors: threat appraisal, internal coping mechanism appraisal and external coping mechanism appraisal. This means that the user needs to decide to what extent a threat applies to him or her, evaluate whether or not he or she can cope with this threat using existing – or internal – mechanisms, and whether or not another – or external – mechanism is suited to cope with this threat. In the model, the appraisal of external mechanisms mainly depends on the two main factors outlined in TAM: Ease of Use and Usefulness. Additionally, Herath et al. posit that concerns about the violation of privacy play an important role in this

process. In this work, we identify the components of this model in the real-world nPA deployment, propose additional factors relevant to Internet authentication systems and provide a detailed understanding of the users' underlying decisions.

The challenges for digital identity management have been discussed in general by Dhamija and Dusseault [7] and for eID in particular by Grote et al. [11]: While, according to both these works, the eID functionality of Germany's new ID card has flaws, the scale of the roll-out and the implicit trust in a government-issued document offers an opportunity to investigate the acceptance of a real world deployment above and beyond purely academic proposals.

Sun et al. [26] found that users need more privacy control, better integration and trust in the involved parties when using OpenID. Dey and Weis [6] presented an approach to add pseudonymity to OpenID federations and Perito et al. [23] demonstrated that it can be easy to link pseudonymous and public user profiles across services to gain additional information about users. These papers argue for the need of privacy in online authentication, which the German eID scheme is able to offer to a wide audience.

Other past work has also investigated user acceptance of authentication technology: Jones et al. described users' general perceptions of authentication mechanisms [15] and Weir et al. compared the usability of two-factor authentication for eBanking applications [28]. Both papers discuss interesting individual insights into users' decisions on authentication technology, but, in contrast to this paper, do not attempt to paint a more general picture.

Furthermore, the EU projects PRIME and PrimeLife addressed many facets of digital identity management. In particular, Wästlund et al. [27] analyzed several UI metaphors to communicate privacy-enhancing features in identity management to users. This paper complements this work by investigating the role of privacy-preserving features in the light of other acceptance factors in a real-world, large-scale roll-out of a new authentication system.

3 The German eID Scheme

The information accessible on the new German ID card includes first and surnames, title, address, date of birth and document type.[6] Additionally, the card can provide functionality for residence verification, age verification and pseudonymous identification without disclosing the actual information [9]. It is the first eID-enabled document in the EU to provide such functionality while including privacy and security as major design goals.

Margraf [21] lists the requirements adhered to during the design process of the new card, including encryption of all transmitted data, explicit user consent to all data transmission, authentication of the communication partner, transmission of necessary data only, inability to monitor the card holder's activities, revocation of lost cards, the ability to provide pseudonymous authentication, and

[6] Currently, the only document type is the ID card itself. However, if eID functionality was integrated into other types of official documents (e.g. driver's licenses), this field would indicate which type of document the user is authenticating with.

the infeasibility of identifying the user and the card through unique properties. These requirements are met using a number of technologies (Card-Verifiable Certificates, Extended Access Control) and organizational processes. The interested reader is referred to the technical specification [4]. In the following, we present the online authentication process using the nPA from a user's perspective and will also briefly outline the requirements for a service provider.

To authenticate to a service, the user needs three things: his ID card with the corresponding PIN, a certified card reader and a certified client software to run the necessary protocols. The card reader costs between 30 Euro for a basic reader without keypad and 160 Euro for a model with display and keypad. This is also one of the major disadvantages of the scheme that we will discuss below. A free reference implementation of the software, called the *AusweisApp*, is currently available from the Ministry of the Interior. Although the need to memorize a PIN may cause problems common to password schemes, users would only need to remember one PIN instead of a larger number of passwords. Users are also used to remembering PINs through the use of banking cards and mobile phones.

When the authentication process begins, the service provider requests authentication using an eID service run by a certified third party. The eID service initiates the cryptographic protocols and establishes a secure channel between the card and the service provider. The user is then presented with information on the service he is authenticating to by the AusweisApp and can also verify which of the information on his nPA will be shared. The user enters the personal PIN code and the client software securely delivers the desired information to the service provider.

In order to use eID functionality, a service provider needs to apply for an authorization certificate at the Federal Office for Authorization Certificates. The provider's need for identifying data will be evaluated by examining her business processes. Service providers get an authorization certificate if they can demonstrate a need for the requested information in compliance with privacy regulations. Only this certificate then enables a service to read exactly the approved data items from the ID card. Currently, 85 providers hold one or more authentication certificates. It is important to note that almost any service provider would be able to get a certificate to access the pseudonymous identification function, which does not disclose any personal information to the service provider but only allows to re-identify a returning user.

In November 2011, after one year, 8 million citizens already received an nPA[7]. Our interview partners from public offices (see below) estimated based on internal statistics that in September 2012 up to 15 million German citizens were in possession of a new eID-capable personal identity card. These sources also reported that only about 20 to 30 % of card holders have their eID capabilities activated, since eID can be deactivated upon request when the user picks up the card; we discuss this further below.

[7] `http://www.personalausweisportal.de/SharedDocs/Pressemitteilungen/DE/2011/Jahrestag.html`

4 Problem Statement

In this paper, we provide a new perspective on the question of improving online authentication and replacing username-and-password. In this line of research, the interplay of social and technological factors is often neglected. We believe this is a critical oversight which is hampering the search for new and better authentication systems. In this work, we offer new insights by examining the users' perceptions of a large-scale and secure scheme that they already have access to but are reluctant to put into use. By investigating the acceptance of a mechanism that is currently being deployed at a national scale, we have a unique opportunity to analyze what keeps users from adopting an alternative means of online authentication after a dependable, privacy-preserving and secure infrastructure was created by the government and to reveal the social as well as technological factors of their non-acceptance.

For the new German ID card and its eID functionality, Poller et al. [24] postulate one main obstacle for adoption: an imbalanced cost-benefit ratio for both businesses and end-users causing a chicken-and-egg problem. Without useful and relevant services, users shy away from investing both time and money into a new technology. Yet, without a significant user base, service providers do not implement and invest in a new technology that would only replace existing mechanisms, which currently fit their needs well. In the model of Herath et al., this means that users decide that their internal mechanism (i. e., the existing username-and-password practice) is suited to cope with the given situation, which negatively affects the appraisal of a new external mechanism.

Beyond this problem, we find that there are further factors that influence the appraisal of an external authentication mechanism, including governmental involvement, social factors and comfort or a feeling of control. In our study, we address the following questions from a user's perspective and also present the providers' views of a novel authentication technology:

1. Which technical and social factors influence authentication behavior?
2. Which deficiencies do users see in their current authentication practice?
3. How do users perceive alternative authentication mechanisms?
4. Why do users not adopt the available eID mechanism?
5. How does the official nature of the identity card influence their perceptions?
6. Which types of services can benefit from using eID?
7. Which measures might increase eID adoption?

5 The User Perspective

eID adoption has been very slow in Germany from the first day of its introduction. While many people have received a new identity card, only few services offer eID authentication. Due to the users' lack of practical experience, we chose to conduct focus groups to explore the perceptions of eID technology from the user perspective.

5.1 Method

Focus Groups are a variation of a group interview that "collects data through group interaction" [22]. Focus groups have been repeatedly used to "study perceptions, thoughts, and emotions" [1,18]. Even though the use of focus groups for HCI research has been subject to discussion [25], they can extract information where other qualitative tools fail [22]. We chose this method to collect a number of factors that might influence participants' perceptions of a rather unknown topic. Since eID mechanisms are not part of common knowledge or commonly used yet, a traditional interview might have intimidated participants. Krueger and Casey [16] suggest that interviewing participants in a homogeneous group can elicit more open and honest responses, since participants realize that others also do not know so much. Additionally, discussion and interaction between participants can raise points that would otherwise not have been addressed.

We stress that our focus groups yield purely qualitative results from which we aim to extract a set of possible factors, perceptions and influences. While group dynamics may have biased the views of individual participants, we believe that we present a superset of issues that influence the acceptance of authentication technology. Furthermore, due to the nature of focus groups, we do not analyze individual views or draw quantitative results from this analysis and will therefore not report counts for the issues raised [16]. Investigating the relative importance of each of the discovered factors will be subject to future work.

We invited 971 students from a university mailing list using a screening survey that collected demographics, technical experience and Westin's Privacy Index [17]. The invitation advertised a "group discussion on daily usage behavior on the Internet" that would last 90 to 120 minutes and offered 20 € of compensation. Students of computer science, information technology and electrical engineering did not receive the invitation in order to prevent anyone from disrupting the groups by being perceived as experts. This is an important consideration for focus groups, especially when discussing a topic where most people would readily defer to experts, since a single individual with extended knowledge can diminish the variety of responses and make participants reluctant to offer own explanations [16]. We received 76 complete responses to our screening survey. According to indicated time preferences, we randomly selected 4 groups of eight people and sent out invitations for the first three. We ran three of the four planned groups before we reached saturation (i. e. there were no more new aspects discussed in the third group).

Of the 24 people invited to the three groups, 18 attended. A demographic overview can be found in Table 1. According to their Westin index, none of our participants belonged to the privacy unconcerned category, which includes individuals that do not feel that their privacy is threatened by current practice and that the benefits of disclosing data outweighs the potential dangers. Most belonged to the pragmatist category, that would "weigh the potential pros and cons of sharing information" [17]. The remaining eight participants belonged to the so-called Privacy Fundamentalists, who are most protective of their privacy. We accept the lack of unconcerned participants for our study, considering

Table 1. Overview of demographics for focus group participants. Technical Experience is rated on a scale from (1) "I often get help from others" to (5) "I often help others". The Privacy column shows the counts for the three categories of the Westin Index: Privacy Fundamentalists/Pragmatists/Unconcerned

Group	# N (female)	Age (sd)	Tech. Exp. (sd)	Privacy
1	6 (4)	23.5 (1.4)	3.0 (1.1)	2/4/0
2	7 (3)	24.1 (4.9)	3.6 (1.3)	2/5/0
3	5 (1)	23.0 (3.2)	3.2 (0.8)	4/1/0
Overall	18 (8)	23.6 (3.4)	3.3 (1.1)	8/10/0

that privacy pragmatists and fundamentalists represent those groups that would express most concerns on using eID.

During the focus groups, one moderator and one assistant were present. The moderator actively engaged with the participants while the assistant monitored recording and took notes. We tried to create a comfortable atmosphere, using a small conference room and unobtrusive recording equipment. The moderator used informal language and first names during the entire process and encouraged direct exchanges between the participants. Name tents with first names were placed on the table to increase direct interaction.

During discussion, the moderator interfered as little as possible: he steered the conversation towards the topics of interest and encouraged participation from less active subjects. We prepared a questioning route, that gradually lead participants from their current behavior and use of authentication mechanisms towards their attitudes and perceptions of eID technology in the new German ID card. In the debriefing session, participants unanimously reported that they perceived the group as a non-threatening and interesting experience. Some participants indicated that they wished that they could participate in such groups on a regular basis to learn more about their own online security.

5.2 Results

The three sessions each lasted between 96 and 115 minutes. The audio recordings were transcribed and statements subsequently assigned to the general questions introduced above. To present the results, we report statements from all three sessions grouped by these questions. Participants are referred to as P1 to P18.

Current Authentication Behavior. We began the discussion by asking for the participants' general habits on the Internet, before focusing on their authentication practice. Most participants stated that they use two to ten passwords, assigned to "service categories". The categories having the strongest passwords were often linked to attributes such as "important", "serious" or "official".

Online banking was treated with particular care by participants: they use unique and longer passwords that they generally do not write down. Participants also reported that they may actively hide security tokens used for online banking, because, in their opinion, usernames and passwords are easily obtainable by

attackers. Generally, participants reported that the consequences that might arise from a compromised account affects how they choose their passwords.

Next, we asked for password management behaviors. Those who had few passwords mostly kept them in memory, while those with a larger number often used a paper-based list. Mixing passwords and usernames or using password patterns while changing individual components was also mentioned: "I have five to six passwords, two to three usernames and I mix those and then I have to remember that. Very easy. It's good for your memory [and] good for your security" (P9).

Participants also used password managers and also synced them between devices. Interestingly, many participants did not know of password managers before the discussion. P16 indicated that he has a password manager which is secured by a fingerprint reader on his laptop, but doesn't use it because he does not care enough about security.

Deficiencies of Current Authentication Practices. When queried how secure participants feel with their current practices, participants generally said that they were confident with their schemes and that they did not see immediate problems. They offered several justifications: friends and family manage their passwords in a similar fashion and have not had problems thus far; it is too frustrating to forget a password; too many passwords get confusing or hard to manage; and fewer passwords help to keep authentication fast and effortless. P6 said: "It's not that I have to think about my password, instead it simply comes without thinking [...] I type it and then I am already logged in."

Yet, a few deficiencies of current practice came up as well. Participants mentioned that password recovery fails if the registered email address is no longer accessible. P17 reported that she does not feel safe anymore, even though she increased her password strength after being hacked. In later stages of the discussion, a number of participants seemed to realize that they might not be as safe as they thought. P3 said: "you get used to it, it works well, it's easy and you stick with it. Maybe until you have a bad experience." And P10 first stated: "I think [I'm safe]. Because, someone would tell me [if I wasn't]". However, at a later point, she said "I don't feel safe anymore with my two passwords". We suspect that some participants needed external motivation to think about their online security and did not do so before participating in the focus group. But, at the same time, some participants also offered that "when I get back home, I will be too lazy [to change anything]" (P18).

Perceptions of Alternative Authentication Mechanisms. We went on to ask about alternative authentication mechanisms, including using password managers and Facebook's OAuth (described by the moderator as the "Login with Facebook"-Button).

Password managers were perceived to be too complicated. This mirrors the fact that few participants had used or known about a password manager before. Participants also mentioned that saved passwords implied lost control: They stated that if someone had access to the password database, that person could get into all the services contained in the database, for example by "hacking" or using the computer when the password database is unlocked. P2 said: "I don't

use it, because this way I still have, no matter whether or not it's actually true, the feeling that I am still in control, when I really log in and that it is not an automated process." On the other hand, other participants said that they value the comfort offered by password managers higher than avoiding possible threats.

Participants also criticized being dependent on a password manager. They were afraid that they may not be able to access accounts from other locations or that they may forget the master password and therefore loose access to all accounts. Additionally, participants felt that a cloud-sync feature is unsafe because passwords are transmitted over the Internet. They also added that passwords can be compromised when the password list is on a smartphone that gets lost.

Using Facebook's OAuth had participants afraid that their information is shared with Facebook, because they felt that "they already have enough access to many things" (P11). Participants also said that another mechanism is unnecessary since passwords work fine. They also doubted the mechanism's security, because they don't understand what happens behind the scenes. A loss of control was also mentioned, since Facebook might lock users out or go out of business.

Overall, participants expressed a general reluctance to adopt new services or technologies on the Internet, due to a feeling of insecurity and negative reports in the news. They showed no interest or motivation to gain an understanding of a new mechanism. P1 said that she would rather not use something "simply because then I can have a bit more security for myself". Others believed that they stick with their mechanisms because this is what they are used to and that they might be using other mechanisms, such as password managers, if they had been using them "from the beginning". Participants stated that they would wait for a mechanism to gain popularity, especially with their friends or family, before switching. They were also not ready to relinquish any comfort or mobility offered by their current practice.

Barriers to eID Adoption. After discussing these more or less well known password alternatives, the moderator introduced the eID functionality of the nPA and stated that this technology might be able to comfortably fulfill their authentication needs. They were told that given the necessary hardware and adoption by service providers, one would simply need to hold the ID card to a reader and enter a PIN to be securely authenticated and that it was even possible to achieve this without disclosing any personal data using the pseudonymous identity functionality. Additionally, the moderator stated that this would generally be more secure than using passwords, that the system is backed by the federal government and that service providers need to demonstrate a need for every piece of personal information before being granted access to this information on a cryptographic level. In order to keep the introduction short, the moderator used simple terms and examples. Participants had a chance to ask questions in order to gain a basic understanding of the technology. Comparing different ways of describing eID functionality was not a goal of this study, as we intended to assess the participants' perceptions of this new technology.

After answering all questions, the moderator elicited participants' attitudes towards this means of authentication. Participants saw the potential of this

mechanism, even though most of them had not previously heard of all possible use cases. In each group, there was at least one person that had already received the new ID card. However, especially the pseudonymous identification functionality was not known to any of the participants.

When thinking about using their nPA for authentication, participants struggled to judge the mechanism because they did not know anyone using it, even though 10 to 15 million of German citizens have already received the nPA. Therefore, participants offered: "one would need to wait and find out whether or not it makes things easier and quicker" (P13). The following issues were raised during the discussions.

No added value/no motivation: Participants did not know of any relevant services offering authentication with the nPA, hence they saw no obvious advantages. Additionally, there was no motivation to adopt the new mechanism:"Honestly, I can't be bothered to look into [eID-based authentication], because I am happy with the way it is" (P10). Participants also didn't know of any services that cannot be used without the nPA.

Complexity: Participants stated that they would need a person they trust to tell them what it does and to convince them that it works. Those participants do not think that they can make that judgement by themselves. Participants also stated that they found the mechanism to be complicated. Participants said they would trust in expert reviews in computer magazines or similar reporting as well as positive experiences of family members, friends, or colleagues.

Control: Participants mentioned a fear that the system might behave in an unexpected way and that the user cannot react in a timely fashion: "[...] I'd rather have everything in my own hands" (P11), "I might forget to do something, to uncheck a box [...] I'm afraid of my own negligence" (P18). Participants also stated that they cannot be sure which information is actually transmitted.

Comfort: Participants suggested that fetching the card before being able to authenticate might be harder than relying on a password manager or one's memory. Participants were ready to make the extra effort if they saw an improvement for their security or if they do not have to remember passwords anymore. Additionally, the current need to have a dedicated card reader was also repeatedly mentioned as a barrier to adoption. Participants generally valued the comfort of using smartphones, tablets and laptops anywhere very highly and objected to the idea of reducing that comfort for purely security-related reasons.

Insufficient information: Participants who already had received the new ID card reported that the person at the public service office was not able or willing to convince them of the advantages of using eID functionality with their nPA. However, this is a crucial moment for the acceptance of this technology, since users are asked if they want to deactivate the functionality when the card is picked up.

Cost: Participants stated that the card readers are too expensive and offer too little added value to justify that cost at the moment.

Influence of the Official Nature of the Identity Card. Participants found that a national ID card is one of the most important documents one has and it is perceived to be "a very personal document" that might not be suitable for "playing around on the Internet" (P4). They also stated the possible contradiction between being pseudonymously authenticated while using an ID card with their photo on it. Participants said, that the card is already important enough and by using it for online authentication as well, potential trouble increases when the card is lost. They also stated that they would be reluctant to use an official identity card for every-day purposes, because, in the worst case, "the government is the one that is able to storm into your house at 5 a.m. with machine guns" (P8).

On the other hand, participants also stated that the official nature actually makes the system more trustworthy for them. One reason given as an explanation referred to the immediate uproar in the media, when a government project has problems. Participants also felt that companies, such as Google or Facebook, can get away more easily with morally doubtful practices. On the whole, participants attributed less motivation for gathering personal information to the government than to companies.

Potential eID Use. When participants where queried for which services they would more readily use eID-based authentication, they stated that they would use their ID cards on services with "an official character". This includes eGovernment services, eBanking and (health) insurance companies. Participants felt that the institutions behind these services are "more tightly bound by legal regulations" (P4) or more personal, because users know where they reside or because they have had a face-to-face encounter with someone from these institutions before. Additionally, participants would be willing to use eID with services "that already have most of [their] information anyway" (P18), such as eCommerce sites. Less "official" or less important services, such as Facebook or Skype, caused more reluctance, since these can already be used more or less anonymously if desired: "For everything that concerns my personal life and that is fun or offers entertainment, [...] I don't find [authenticating with my ID card] very useful" (P14). Participants mentioned that if they were using eID with their nPA for some services regularly, they would probably use it for all of their services.

The possibility to increase security through stronger authentication and identity assurance was acknowledged by participants. They stated that using your ID card would enable them to prove "that it is really me" (P14). However, the discussion on the utility of eID technology for different services showed that many participants, including those who had already received an nPA, had not fully understood the concepts behind eID authentication. The nPA's eID functionality was mostly reduced to how ID cards are currently used and especially the privacy-preserving pseudonymous identification functionality was quickly forgotten during the discussion. When the moderator reminded participants of that possibility and reintroduced the concept, participants would often not see an immediate advantage in the light of other issues (see above).

Measures to Make eID More Attractive. Towards the end of each session, the moderator asked for suggestions to improve the acceptance of eID features in the new identity card. Participants offered that "if, at some point, almost everyone used [eID-based authentication], then this might mean that it works [...] that it comes with a certain level of security" (P3). Participants said that testing the process and getting hands-on experience might help them to appreciate it. Participants also wished for proper and understandable information on this topic as well as having a competent person to talk to about the implications of using eID features. As noted above, participants that already had an eID-enabled card did not receive any guidance on the features and benefits of their new identity card, even after explicitly asking questions at a public service office. Participants added that banks generally explain the security measures for online banking at length and that they would appreciate such a practice for eID functionality as well.

Generally, an increased public presence and more active marketing were mentioned as possibilities to increase public awareness. Furthermore, participants postulated that services that offer benefits through using eID might make the system worthwhile. Participants felt a need for information that was not satisfied by current practice and said they would expect television, newspaper and magazine reports about a beneficial technology. They also proposed dedicated informational events, that offer opportunities to ask questions and discuss possible uses with peers.

Additional Issues. During the discussions, participants expressed that they treat the Internet as a generally insecure medium and that they therefore, for example, do not use online banking at all. Among other comments, P5 believed that password managers "surely could be hacked by someone". P9 said: "I don't believe that there will ever be perfect security on the Internet. Whether you use [an alternative mechanism] or continue using passwords [...] there are vulnerabilities everywhere." Another participant believed that there will be a way to circumvent any security system at some point in time.

We suspect that participants were not ready to invest in additional security for their Internet conduct because they don't see that this will have personal benefits in the end. Also, they might not see that security consists of several independent parts and that increasing security for one of those parts might make them safer. They do not differentiate between security risks occurring because of, for example, authentication mechanisms, lax privacy policies or missing transport security. It appears that, in several cases, this is all simply attributed to the generally unsafe Internet.

Information in Public Service Offices. Because participants stated that they were not able to obtain enough information from public service offices, we visited three of these and acted as if we were unsure of whether or not to switch to an eID-enabled ID card. During our visits, we had similar experiences as our participants: clerks were not able to answer our questions or, in one case, even refused to, saying that she was the wrong person to talk to. Yet, she was also not able to name a person to contact on this issue either. We were always referred to

a brochure with a phone number inside. We tried calling that number and finally got qualified answers to the questions a layperson might have. This premium rate phone service of the Federal Ministry of the Interior can cost up to 0.42 Euro per minute.

Summary. Overall, the focus groups identified a number of problems for the acceptance of new authentication mechanisms in general and eID-based authentication in particular. The factors identified by our investigation also indicate that there are barriers to adoption beyond the chicken-and-egg-problem suggested by Poller et al. [24]. The results of the focus groups allow a more detailed understanding of the external mechanism appraisal factors presented by Herath et al. [13]: Complexity at a technical or process level and a reluctance to find out more can lead to a perceived loss of control, a lack of understanding and hence decreased motivation for adoption. Participants repeatedly stated that they do not understand technology and have no interest in it either. Hence, in order to promote privacy-preserving authentication technology to users, several other factors need to be considered before privacy benefits are appreciated. For example, our participants valued comfort and mobility highly and were not ready to relinquish any in order to gain security or privacy.

6 The Business Perspective

The focus groups confirmed the problem of a lack of relevant services that either offer an added value or demonstrate how the nPA can make daily life easier. For trans-national companies, such as Amazon, Facebook, or Google, there is obviously little reason to adopt a technology that is currently limited to a small portion of their customer base. Yet, if many governments were to agree on a global eID standard, identity cards could be used throughout the Internet. Today, there still are several national businesses that could benefit from eID technology. Banks, insurance companies and eCommerce providers would have a means to reliably establish a customer's true identity and almost any service that has a login functionality could offer an optional eID-based authentication to appear innovative or increase customer comfort, security and privacy.

According to the list of authorized services[8], 85 public offices, companies and other businesses have been certified to access eID functionality on the nPA, of which 45 actually publicly offer eID authentication in their online processes[9]. Eight of these are not related to eGovernment applications, banks or insurance companies, which traditionally need reliable identity validation. Of these eight, only two do not request any personal information and rely on the pseudonymous functionality. The remaining 40 service providers with authorization certificates would be able to offer and use eID services but chose not to. Of those, only three sought privacy-preserving functionality, such as anonymous age verification, while the rest requested the authorization certificate to reliably establish users' true identities.

[8] `http://gsb.download.bva.bund.de/VfB/npavfb.pdf` – last access: 20.09.2012
[9] `http://www.ccepa.de/onlineanwendungen` – last access: 20.09.2012

This indicates that, from the business perspective, a large number of service providers see eID features as a means to establish customer identities or to fulfill legal requirements. Using eID features of the nPA as a general means of authentication, especially in its pseudonymous form, is only adopted by two service providers after two years of being available. To find out more about the service provider's reluctance, we sent requests for phone interviews to selected companies.

6.1 Method

In August 2012, we sent emails to 51 service providers on the list of authorized services, leaving out infrastructure providers that mainly obtained authorization for operational or testing purposes. Additionally, we cherry-picked 26 well-known Internet services that reside in Germany and have a primarily German audience, but have not requested or received an authorization certificate yet. We asked for an interview partner that could comment on the use of eID technology in their online services. 15 providers responded, including four companies that did not appear on the authorized services list. Of the 15 respondents, two were banks, two were insurance providers, one offered free-to-play online games, one was a consulting firm that offered brochures behind a login, one a mobile phone network operator, one offered cloud-based end-user security solutions and the remaining seven were either local administrations or communal service providers for local administrations. It is important to note that eight respondents had participated in an official application testing call, run by the Ministry of the Interior prior to the nPA roll-out.

The semi-structured interviews were conducted over the phone, lasted an average of 24 minutes ($sd = 11.1$ min, ranging from 7 to 51 minutes), and were recorded with the interviewees' consent. Again, we were interested in extracting a set of factors that play a role in their decision making process and will explore the quantitative relationships in future work. The central statements of each interview were extracted into an analysis sheet by the interviewer during a subsequent replay of the recording.

6.2 Results

Our results confirm that there is little motivation for adopting eID features through non-governmental providers. Two insurance companies stated that they provide nPA-based authentication for marketing purposes and to appear customer-friendly. The two banks we spoke to stated that the functionality currently offered by the nPA does not suffice to replace the systems currently in use to authorize bank transactions, due to the lack of a qualified electronic signature (QES). While the nPA is prepared to support QES, QES certificates have not been pre-installed on the cards by the government and could also not be purchased by customers at the time of the interviews. Furthermore, strict regulations for financial transactions and bank processes require identification that cannot be provided by the nPA. German banks have also been issuing smartcards

for home/online banking since 1998. The two interviewees representing banks referred to the acceptance of those smartcards and stated that, while providing considerably stronger security features, these cards were never widely adopted. When presented with an (almost) free alternative having lower security, private bank customers usually opt for the lower cost, according to the interviewees' statements.

Public administrations generally saw eGovernment as a necessary tool for the future, to streamline administrative processes and to offer convenient services for citizens. Since the new ID card was introduced with eGovernment as a central focus, its features are suitable for these applications. Yet our interview partners indicated that, even for eGovernment, several regulatory hurdles still need to be addressed in order to be able to provide more processes online, that currently still require citizens to visit offices in person. While two of the responding administrations were in the process of actively promoting the benefits of eID technology and the nPA, others were waiting for more adoption in the public or stronger internal demand before committing to the technology.

Many of the respondents stated that they saw problems for user acceptance due to expensive or bulky card readers, lengthy and complicated user authentication procedures as well as an insufficient UI in the current version of the eID software. They also saw a need for killer applications, that demonstrate the benefits and a relevance for day-to-day use. Those who offered eID-based authentication treated this mechanism as an optional offer, that a user can but does not need to use. Obtaining an authorization to use eID features did not cause any problems. As a side note, some respondents also gave accounts of trying to increase authentication security by dictating stronger password requirements. These restrictions soon needed to be reverted since customers started to complain.

The general idea of eID technology, being able to prove actual identities in the digital realm, was welcomed by all respondents. Many stated that they expect many day-to-day processes and interactions to take place on the Internet in the future and that there is a need for effective identity management. Some respondents also acknowledged that the government can effectively roll out such an infrastructure and that users will trust in such a system eventually. Others, however, were skeptical whether or not a fear of surveillance will keep users from trusting the eID features in a personal identity card, considering computer surveillance and telecommunications data retention laws being controversially discussed.

6.3 Summary

Interviews with service providers showed that card features enabling providers to offer additional functionality online are either not available yet (e. g. QES) or do not meet current legal norms. Companies see little need to replace existing mechanisms beyond legal requirements to establish a customer's true identity in some cases. This is especially true since providers indicated that their customers are happy with the current practice as well. The provider interviews also

confirmed the chicken-and-egg problem. Without useful and relevant services, users will not adopt a new authentication mechanism, and without user adoption, service providers will not invest in the mechanism. For the future however, service providers indicated a need for reliable digital identity management.

7 Discussion

In our study, we found that our participants struggled to fully appreciate the benefits of the nPA's privacy-preserving features. In addition to the findings of Wästlund et al. [27], we also found that several other factors play an important role for the users' acceptance and can actually overlay the perception of privacy-preserving features. Overall, our results show that, in order to deploy novel authentication systems on a large-scale, effort particularly needs to be invested into service, marketing and guidance for users. This is true for both existing as well as for new systems. Surprisingly, after spending a very large amount of money on deploying an eID scheme, these factors were neglected by the German government and consequently the beneficial technical properties, such as the privacy-preserving nature of the card's authentication facilities, did not receive public attention.

Getting users' to accept new authentication technology is also an important precursor for adoption by businesses: the interviews showed that many companies are ready to adopt new technology in order to satisfy the customers' demands. Yet, legal hurdles and insufficient technical features can also keep providers from adopting authentication technology. Similar to the users, enhancing their customers' privacy was not a central concern when evaluating a new authentication mechanism.

In terms of Herath et al.'s acceptance model for security technology, our results show that under the given circumstances, users do not see a problem with their current authentication method (internal mechanism appraisal). Even though the new mechanism does offer beneficial properties (external mechanism appraisal) with respect to ease of use (e. g. no more need to remember passwords), usefulness (e. g. no need to remember many passwords), and privacy, other factors tip the scales in favor of the existing mechanism. Users indicated that perceived relevance, complexity and control of the mechanism as well as cost, comfort and trust in the system play an important role when judging a novel authentication technology.

7.1 Recommendations

The roll-out of the German nPA demonstrated effects of news coverage on acceptance factors in the first few weeks after a large-scale roll-out: During the introduction of the nPA, one of the first reports in the media covered how the system is vulnerable to an attack. During the focus groups, this attack vector always came up as an argument for the vulnerability of the scheme and eventually had to be clarified by the moderator, since it was only a minor issue arising due

to the use of cheap card readers. To avoid this negative influence on the users' perceptions, the entire digital ecosystem of a novel authentication mechanism needs to be considered during its design.

Our results also discovered social influences for the adoption of novel authentication mechanisms: Our participants stated that they would wait until there are immediate benefits, a more wide-spread trend towards the new technology and adoption by trusted third parties, such as friends, families or experts. This goes beyond a personal appraisal of an external mechanism in Herath et al.'s model and shows that users rely on several sources to inform their decisions. Concerning the use of an eID-based online authentication solution, trust can be bipolar due to the involvement of the government. While a share of users trusts the mechanism more, others have less trust for the same reason. Future efforts should keep users' perceptions of an infrastructure or identity provider in mind.

On the technical side, novel authentication technology needs to create an effortless integration into daily workflows. While current eID systems require card readers to function, our results suggest that this additional piece of hardware is a stumbling block. Users repeatedly mentioned that the need to buy a card reader or to carry one around would keep them from adopting eID technology for daily use. We hence believe that future authentication systems need to leverage smartphone and NFC technology in order to satisfy these needs. Additionally, the complex and therefore opaque nature of the technology and processes underlying the nPA's eID functionality raised the users' concerns and is in conflict with their need for control.

Another important consequence of our findings is to establish user awareness: It is necessary to make users realize the problems of the authentication systems they currently use and to stress the security benefits of a new mechanism. While security experts know the shortcomings of passwords and benefits of novel privacy-preserving technologies, our results indicate that many users feel quite safe with their current practice of using a handful of memorized passwords. Users also showed little differentiation in terms of risks to their security on the Internet. Without knowing how certain practices can improve their security, the users will show less motivation to adopt them. Adding educational material about previous systems and current problems to information campaigns and instructing staff to provide better support is thus a simple action that can be taken to improve adoption.

8 Conclusion

In this paper, we examined users' perceptions and concerns on using alternative authentication methods on the Internet. As a concrete example, we studied why the German nPA is receiving little adoption as a privacy-preserving authentication technology, even though the technical capabilities are excellent. The takeaway of this paper is that "simply" ensuring that enough users get a smartcard through a national roll-out is not enough to kick-start adoption. Non-technical factors, such as the availability of information and reviews as well as services

with everyday relevance, are necessary prerequisites for the adoption of authentication mechanisms. On a technical level, our results suggest that non-intrusive technology is a central factor when designing a new authentication system. We also argue that it is necessary to find a balance between technical complexity and transparency, in order to satisfy the users' need for control. A final result of the user studies shows that users need to be made more aware of immediate problems with their current practice, since unlike "functional" technology there is a lack of intrinsic motivation to adopt new authentication technology.

References

1. Agosto, D.E., Abbas, J., Naughton, R.: Relationships and Social Rules: Teens' Social Network and Other ICT Selection Practices. JASIST 63(6), 1108–1124 (2012)
2. Bonneau, J.: The Science of Guessing: Analyzing an Anonymized Corpus of 70 Million Passwords. In: 2012 IEEE Symposium on Security and Privacy, pp. 538–552 (2012)
3. Bonneau, J., Herley, C., van Oorschot, P.C., Stajano, F.: The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. In: 2012 IEEE Symposium on Security and Privacy, pp. 553–567 (2012)
4. Bundesamt für Sicherheit in der Informationstechnik. Technical Guideline TR-03127 (2011)
5. Davis, F.D., Bagozzi, R.P., Warshaw, P.R.: User Acceptance of Computer Technology: A Comparison of Two Theoretical Models. Management Science 35(8), 982–1003 (1989)
6. Dey, A., Weis, S.: PseudoID: Enhancing Privacy in Federated Login (2010), `http://www.pseudoid.net`
7. Dhamija, R., Dusseault, L.: The Seven Flaws of Identity Management: Usability and Security Challenges. IEEE Security & Privacy Magazine 6, 24–29 (2008)
8. Florencio, D., Herley, C.: A Large-Scale Study of Web Password Habits. In: Proceedings of the 16th International Conference on World Wide Web. ACM (2007)
9. Fromm, J., Hoepner, P.: The New German eID Card. In: Fumy, W., Paeschke, M. (eds.) Handbook of eID Security: Concepts, Practical Experiences, Technologies, ch. 11, pp. 154–166. Publicis (2011)
10. Gaw, S., Felten, E.W.: Password Management Strategies for Online Accounts. In: Proceedings of the Second Symposium on Usable Privacy and Security. ACM (2006)
11. Grote, J.H., Keizer, D., Kenzler, D., Kenzler, P., Meinel, C., Schnjakin, M., Zoth, L.: Vom Client Zur App. Technical report, Hasso Plattner Institute (2010)
12. Hayashi, E., Hong, J.: A Diary Study of Password Usage in Daily Life. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM (2011)
13. Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J., Rao, H.R.: Security Services as Coping Mechanisms: An Investigation Into User Intention to Adopt an Email Authentication Service. Info Systems J. (2012)
14. Jakobsson, M., Chow, R., Molina, J.: Authentication - Are We Doing Well Enough? IEEE Security &Privacy Magazine 10(1), 19–21 (2012)
15. Jones, L.A., Antón, A.I., Earp, J.B.: Towards Understanding User Perceptions of Authentication Technologies. In: Proceedings of the ACM Workshop on Privacy in Electronic Society. ACM (2007)

16. Krueger, R.A., Casey, M.A.: Focus Groups: A Practical Guide for Applied Research, 4th edn. Sage Publications (2009)
17. Kumaraguru, P., Cranor, L.F.: Privacy indexes: A Survey of Westin's Studies. Technical Report CMU-ISRI-5-138, Carnegie Mellon University (2005)
18. Kurniawan, S., Mahmud, M., Nugroho, Y.: A Study of the Use of Mobile Phones by Older Persons. In: CHI Extended Abstracts on Human Factors in Computing Systems. ACM (2006)
19. Liang, H., Xue, Y.: Avoidance of Information Technology Threats: A Theoretical Perspective. MIS Quarterly 33(1), 71–90 (2009)
20. Malone, D., Maher, K.: Investigating the Distribution of Password Choices. In: Proceedings of the 21st International Conference on World Wide Web. ACM (2012)
21. Margraf, M.: The New German ID Card. In: Pohlmann, N., Reimer, H., Schneider, W. (eds.) ISSE 2010: Securing Electronic Business Processes (2011)
22. Morgan, D.L.: Focus Groups as Qualitative Research. Sage Publications (1996)
23. Perito, D., Castelluccia, C., Kaafar, M.A., Manils, P.: How Unique and Traceable Are Usernames? In: Fischer-Hübner, S., Hopper, N. (eds.) PETS 2011. LNCS, vol. 6794, pp. 1–17. Springer, Heidelberg (2011)
24. Poller, A., Waldmann, U., Vowé, S.: Electronic Identity Cards for User Authentication – Promise and Practice. IEEE Security & Privacy Magazine 10(1), 46–54 (2012)
25. Rosenbaum, S., Cockton, G., Coyne, K., Muller, M., Rauch, T.: Focus Groups in HCI: Wealth of Information or Waste of Resources? In: CHI Extended Abstracts on Human Factors in Computing Systems. ACM (2002)
26. Sun, S.-T., Pospisil, E., Muslukhov, I., Dindar, N., Hawkey, K., Beznosov, K.: What Makes Users Refuse Web Single Sign-On? An Empirical Investigation of OpenID. In: Proceedings of the Seventh Symposium on Usable Privacy and Security. ACM (2011)
27. Wästlund, E., Angulo, J., Fischer-Hübner, S.: Evoking Comprehensive Mental Models of Anonymous Credentials. In: Camenisch, J., Kesdogan, D. (eds.) iNetSec 2011. LNCS, vol. 7039, pp. 1–14. Springer, Heidelberg (2012)
28. Weir, C.S., Douglas, G., Carruthers, M., Jack, M.: User Perceptions of Security, Convenience and Usability for Ebanking Authentication Tokens. Computers & Security 28(1-2), 47–62 (2009)