Electronic Identity Cards for User Authentication – Promise and Practice

Andreas Poller* Ulrich Waldmann† Sven Vowé‡
Sven Türpe§
Fraunhofer Institute for Secure Information Technology (SIT)
Rheinstraße 75, 64295 Darmstadt, Germany

Abstract

Electronic identity (eID) cards promise to supply a universal, nation-wide mechanism for user authentication. Most European countries have started to deploy eID for government and private sector applications. Are government-issued electronic ID cards the proper way to authenticate users of online services? We use the German eID project as a showcase to discuss eID from an application perspective. The new German ID card has interesting design features: it is contactless, it aims to protect people's privacy to the extent possible, and it supports cryptographically strong mutual authentication between users and services. Privacy features include support for pseudonymous authentication and per-service controlled access to individual data items. The article discusses key concepts, the eID infrastructure, observed and expected problems, and open questions. The core technology seems ready for prime time and government projects deploy it to the masses. But application issues may hamper eID adoption for online applications.

Index Terms: K.6.5 [Management of Computing and Information Systems]: Security and Protection—authentication; K.4.1 [Computers and Society]: Public Policy Issues—privacy; K.4.4 [Computers and Society]: Electronic Commerce—security; K.6.m [Management of Computing and Information Systems]: Miscellaneous—security

Keywords: eID, user authentication, electronic identity card, identity management, smart card, privacy, Germany

*andreas.poller (at) sit.fraunhofer.de
†ulrich.waldmann (at) sit.fraunhofer.de
‡sven.vowe (at) sit.fraunhofer.de
§sven.tuerpe (at) sit.fraunhofer.de

1 Introduction

Long before the Internet became a commodity, many governments had public authentication schemes in place, handing out identity cards to citizens. Governments trust their cards, and so do businesses where they need reliable authentication of persons and identity documents are available. Even in countries without national ID card schemes, similar documents, such as driving licenses, are used in everyday life to the same end. Will this success story repeat on if governments issue electronic identity documents? Many European governments think so and deploy eID schemes. The most recent and apparently most advanced eID deployment is the German electronic ID card *neuer Personalausweis*. Advertised to citizens as their "most important card", the new electronic ID card promises to provide a universal, secure authentication scheme for government and private-sector applications, a scheme with privacy benefits. Apart from the obvious question, how useful national schemes can be on the Internet, are such electronic identity schemes the way to go to improve online authentication? Our article describes the concepts of the new German electronic identity card, and uses this implementation as a showcase to discuss application issues.

1.1 An Authentication Scheme for Everyone

Rolling out to citizens since November 1st, 2010 is a contactless smart card (Figure 1) with three distinct electronic functions, each with its own protected data set:

- The mandatory ePass function, reserved for government use, stores a digital representation of the card holder's identity in a similar way as in electronic passports.
- The eID function for general applications stores an identity record that authorized services can access if the card holder permits it. Citizens choose whether they want this function activated or not.
- The optional eSign function allows the card holder to store a single private key and certificate for qualified electronic signatures. Private sector trust centers issue the certificates.

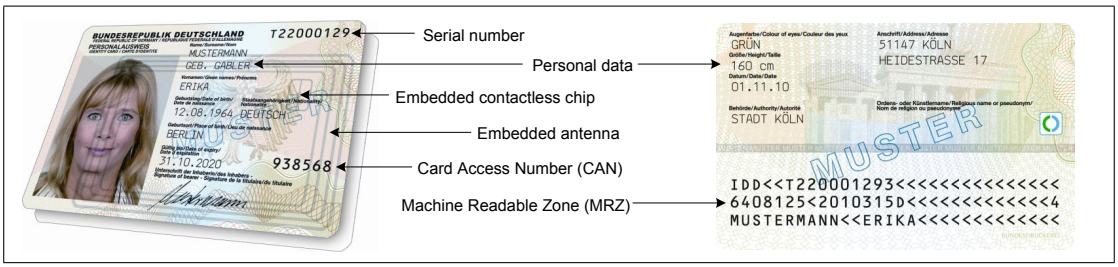

Figure 1: Front and back side of the new German ID card (source: Bundesministerium des Innern)

The eID and the eSign function are each protected by their own personal identification number (PIN). Table 1 gives an overview of the functions and data records. We focus here on the eID function, which is open for public and private sector services to use online.

Table 1: Electronic functions and data of the ID card

Function	**Purpose**	**PACE Password**	**Data and *Functions***
ePass (mandatory)	Readout by authorized offline inspection systems	CAN or MRZ	- Face image - 2 fingerprint images (optional) - MRZ data
eID (activation optional)	Online applications read data or access functions as authorized	eID PIN	- Family name, given name - Artistic name, doctoral degree - Date and place of birth - Address and community ID - Date of expiry - *Age verification* - *Community ID verification* - *Restricted identification (pseudonym)* - *Revocation feature*
	Offline inspection systems read all data, update address and community ID	CAN or MRZ	
eSign (certificate optional)	Certification authority installs signature certificate online	eID PIN	- Signature key and X.509 certificate - *Create electronic signatures*
	Citizen makes electronic signatures with eSign PIN	CAN	

1.2 Applications for eID

Proponents of eID envision a world where the identity card replaces username and password, supports business processes online and offline, and allows services to be provided online that up to now require presence of the citizen or paperwork. They hope that some day we will use one single eID scheme to shop online, open bank accounts, check into hotels, rent cars, and file our tax declarations. Piggybacking the authentication scheme on widely deployed ID cards supposedly works towards this goal. When the rollout is complete after 10 years, so the reasoning, an infrastructure will be there that is attractive to use for both citizens and service providers.

It is too early yet for an ecosystem of eID-enabled services to emerge and stabilize. An application field test with early adopters, carried out before the start of the rollout, shows a tendency. The following types of services might see an immediate benefit from supporting eID:

- Government services that require formal identification of citizens.

- Services that must allow citizens to exercise their right to access personal information. Institutions like credit information agencies or pension funds may want to let citizens access their data online, but they have to identify the requestor.
- Companies that are required to record the identities of their clients, such as banks or telecommunications operators. Up to now, contracting with such companies requires an offline step for the sole purpose of identity verification.
- Operators of age-restricted services, such as cigarette vending machines or adult entertainment. Currently they use a wide variety of means for age verification.

Such applications could drive the adoption of eID in the beginning, but the supposed scope of application is much wider than that. Even proposals for online elections based on the eID functions are being discussed, but they remain far from implementation attempts yet. Whether there will be a killer application some day that service providers and users agree on remains to be seen.

1.3 Authentication with Privacy Benefits

As a downside, a universal authentication scheme based on ID cards raises privacy concerns. Can it be abused to link my data and actions throughout the Internet to my identity? Will eID force me to let every website know my birthday? Who can access my data at all and how can I remain in control? Can I be anonymous if I want to?

The German electronic ID card translates privacy into a set of features. Services need to authenticate themselves to the citizen and to the ID card. Authorization certificates determine the extent to which a service can access eID data fields and functions. The citizen has to consent to every access. On-card verification supports use cases like age verification while releasing a minimum amount of information. Restricted identification creates service-specific pseudonyms that are unlinkable across services.

2 The eID Function

2.1 Digital Identities

The eID function makes a subset of the identity data on the card accessible to authorized services:

- Names and academic title
- Date and place of birth
- Street address and municipality.

Biometric data (facial image, eye color, body height, and optionally fingerprints) are restricted to the ePass function and not accessible through the eID interface. The card serial number and the card holder's handwritten signature printed on the surface are

not part of the eID data set. With these exceptions, the eID function works with the same data that are printed on the surface of the card.

Besides direct data access, the eID function supports a privacy-preserving access mode for the date of birth and the registered place of residence. Instead of returning data from the eID record, the card responds only with *yes* or *no* to a verification request. This way a service can verify for instance the age of a citizen without learning the date of birth. In addition, the restricted identification feature allows the card to be used as a login token without revealing personal information.

2.2 System Components

The technical guideline TR-03127 [1] specifies the architecture of the electronic identity card system. Four principal components participate in the online authentication process. A dedicated *eID server* handles authentication on the server side and returns the result to the service. The eID server may be operated by the service provider or a third party. It uses an *authorization certificate* on behalf of the relying service.

On the client side, a *card reader* and a *client software* package provide interfaces to the user and to the ID card. Basic card readers leave all control and user interaction to the software. Advanced readers have their own PIN entry keypad, protecting the PIN against malware attacks. The client software mediates the protected communication between the card and the eID server, displays authorization certificates, and allows the user to restrict access to eID data fields.

The chip on the *ID card* verifies the user's PIN and the authorization certificate of the eID server and releases information as authorized. The card is an end point of cryptographic protocols.

2.3 Cryptographic Protocols

Cryptographic protocols secure the channels between the card and the reader, and between the card and the eID server. Between the card reader and the card, the Password Authenticated Connection Establishment (PACE) protocol establishes a shared session key and verifies a password in the process. All functions of the ID card use PACE, but with different passwords. The 6-digit eID PIN is used during online authentication. Other functions use the card access number or the machine-readable zone password as shown in Table 1.

Between the card and the eID server, the Extended Access Control (EAC) protocol provides mutual authentication and creates a session key. EAC comprises terminal authentication and chip authentication. Terminal authentication presents the authorization certificate of a service to the card in a challenge-response protocol.

Chip authentication uses a chip authentication key built into the card to prove authenticity of the card to the eID server. Chip authentication also establishes a session key between the eID server and the card. The result is a trusted channel between the ID card and the eID server. An access control policy in the card is bound to this channel, and the channel implicitly authenticates data sent through it.

Restricted Identification (RI) cryptographically creates unlinkable card- and service-specific identifiers. Using a unique chip identifier and a service identifier, restricted identification calculates a static pseudonym for user authentication.

The technical guideline TR-03110 [2] by the German Federal Office for Information Security (BSI) specifies the cryptography in detail. As cryptographic primitives the ID card uses AES-128 CBC and CMAC for messaging security; SHA-256 for hashing; elliptic curve Diffie-Hellman for key establishment in PACE, chip authentication and restricted identification; and ECDSA for authorization certificates and signatures. The specification facilitates later transition to other algorithms or longer keys. ID cards indicate through object identifiers the cipher suites supported.

2.4 eID Authentication Process

To authenticate a user with eID, an online service triggers the client software through a browser plugin and hands over to the eID server to execute the process depicted in Figure 2:

1. **Authentication request:** The service requests eID data of the user from its associated eID server.
2. **Display of authorization:** The eID client receives and displays information about the service and its authorization certificate.
3. **PIN entry and PACE:** After reviewing the service information and optionally, further restricting the authorization, the user enters her eID PIN to express consent. This PIN is used locally to execute the PACE protocol.
4. **Extended Access Control:** Mediated by the client, the eID server and the ID card authenticate each other and establish a trusted channel.
5. **Use of eID function:** The eID server reads the subset of eID data according to the effective authorization.
6. **Authentication response:** The eID server forwards the received eID data to the service provider.

After this process, control returns to the service, which uses the authentication result for its purposes.

2.5 Security and Privacy Properties

For the citizen, the cryptographic protocols ensure that the ID card releases data (1) only with the card holder's consent, (2) to an authenticated and authorized service, (3) within the limits of authorization, and (4) through a channel protected against eavesdropping and tampering. Endpoints of the secure channel are the ID card chip and the eID server. The card chip itself authenticates the eID server and verifies its authorization

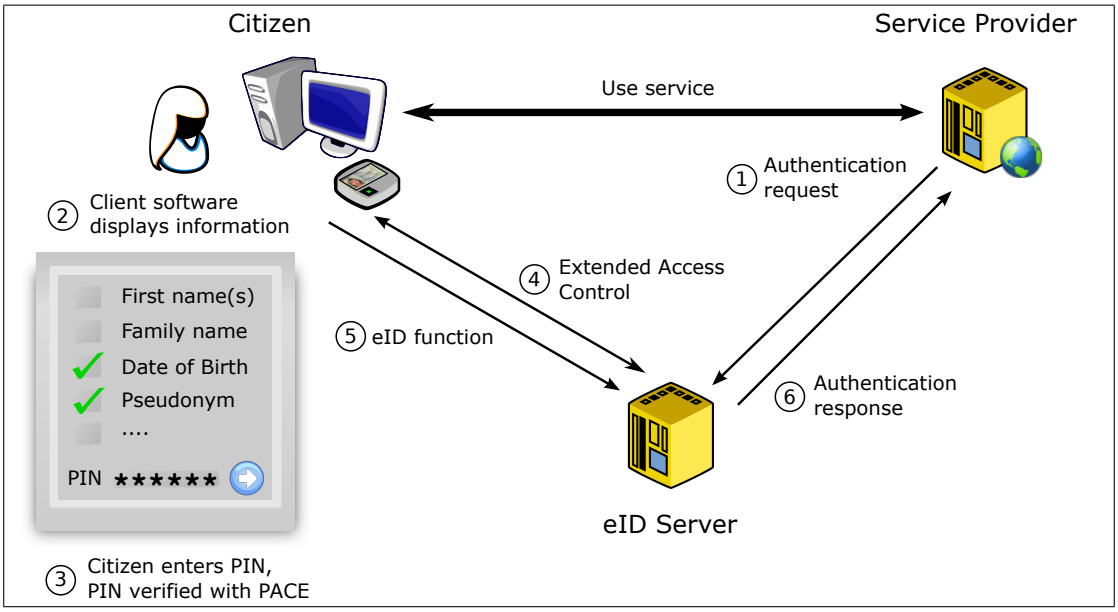

Figure 2: Online authentication process

using lightweight certificates [3]. If, as recommended, an advanced card reader with a keypad is used, the eID PIN is protected against malicious software on the user's computer.

For the service provider, chip authentication ensures that the data received originate from a genuine and valid ID card issued by the government. A revocation mechanism allows service providers to recognize ID cards that were reported lost, for details cf. TR-03127 [1].

Two design features in the details enhance the citizens' privacy: chip authentication keys are not unique, and eID data remain unsigned. If each ID card were equipped with a unique chip authentication key, a service provider might gain a unique identifier as a side effect of the protocols. Therefore a batch of cards share the same secret chip authentication key, making them indistinguishable at the protocol level. To prevent service providers from proving to others that an eID record is authentic, there is no trusted party in the system that would sign eID data. Only the context of an EAC protocol run and the secure channel thus established assure the eID server of the authenticity of eID data. Outside this context, there is no way to verify the origin of eID data.

2.6 Roles and Responsibilities

The government and the private sector share the implementation and operation of the eID system as shown in Figure 3. Local administrative agencies register citizens and issue ID cards to them. Federal administrative agencies authorize service providers and oversee the certification of equipment. Federal agencies also manage the revocation of lost ID cards.

The private sector supplies equipment and operates eID servers and infrastructure services. The industry produces the ID cards on behalf of the local agencies, and supplies the end user equipment. Citizens need a certified card reader and a client application. A government-funded reference implementation of the client software, called *AusweisApp*, is available free of charge for Windows, Linux, and Mac OS. Alternative implementations of the client software may appear on the market in the future. Service providers may operate their own eID servers or contract with an eID service provider. Private-sector companies also operate the certification authorities responsible for the technical part of service authorization.

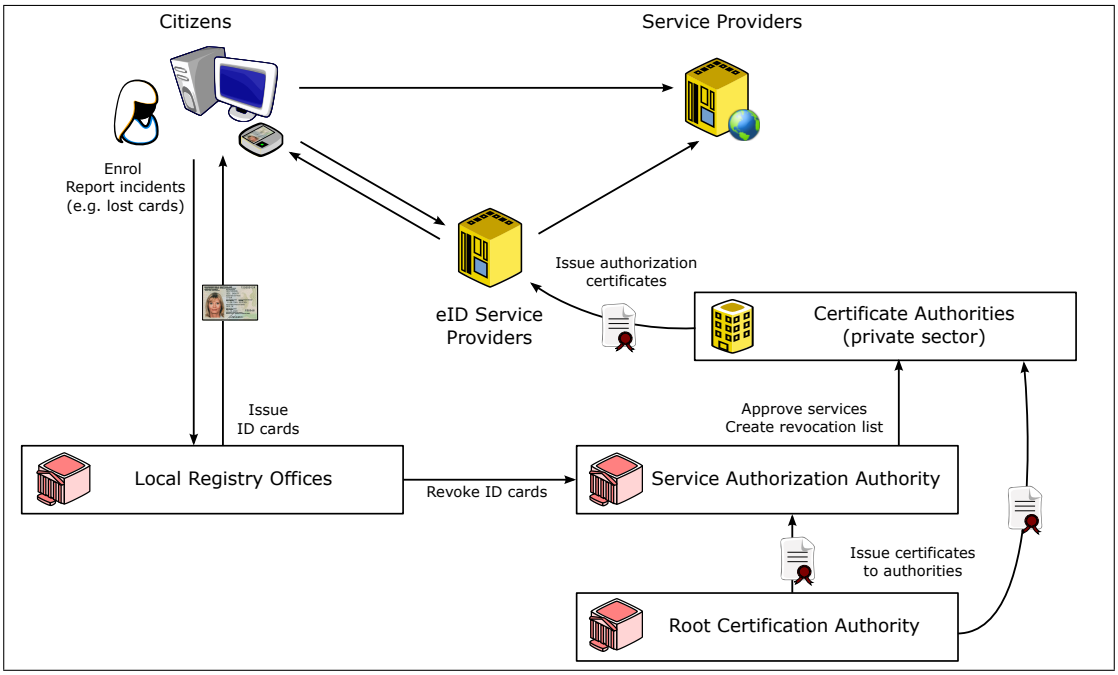

Figure 3: Roles and responsibilities for the new eID Card

2.7 Service Authorization

The authorization of a service to access eID data fields or data verification functions is managed in three steps. First, the service provider requests approval from the Federal Office of Administration (BVA). The BVA approves a service if it has a legitimate interest to use eID data as requested and the provider complies with all pertinent regulations. The approval can remain valid for up to 3 years.

In a second step, the service provider contracts with a technical certification authority. These certification authorities issue cryptographic authorization certificates to service providers for their respective eID servers. Authorization certificates for online services are short-lived, typically valid for only two days, to simplify client-side validity checks. Authorization certificates just expire quickly if approval expires or is revoked. The

certification authorities also provide eID servers with ID card revocation lists based on notifications from the Federal Office of Administration.

The third step occurs when an authorized eID server on behalf of an approved service requests access to the card. The user is presented with the authorization certificate and has the option to deselect data fields from the service authorization. The client software also presents to the user the approved privacy policy of the service. The authorization certificate includes a hash of the policy.

3 Design Rationale

The eID system design arise from a number of objectives, requirements, and design decisions:

User benefits eID authentication is supposed to make online authentication easier while allocating more control and responsibility to the citizen. The ID card is meant as a citizen identification scheme for the Internet, and should reduce the users' troubles with managing user account names, passwords and other credentials. The user-controlled release of selected eID data fields to a service is to curtail the uncontrolled collection of identity-related information across service providers and accounts.

Service provider benefits Government-issued ID cards provide reliable authentication and high quality data records. They can be used not only for general authentication but also to fulfill legal identification requirements. A service supporting eID receives identity information without typos, confirmed by the government as genuine and belonging to a real person. Through eID, existing services get more trustworthy authentication, and new services become feasible.

Authentication only The eID function does not secure transactions, it provides authentication only. However, the card allows trust centers to install a key and certificate for electronic signatures. The eID function can be used to obtain a certificate online.

Data reduction and data economy The entire eID system is designed according to the need-to-know principle under the control of the government. Service providers will be authorized to access data fields and functions only to the extent they can demonstrate a need for.

No centralized databases The underlying public key infrastructure and the production of the cards are the only centralized components of the eID infrastructure. No centralized databases of personal information are kept. Data needed for card production are deleted afterwards.

Privacy enhancements To make data reduction effective, the ID card supports pseudonyms and on-card data verification.

Adversarial assumptions The design also considers the less obvious threats to privacy, such as the possible abuse of protocols, keys, or other technical features for privacy invasion. The protocols and the key management are designed such that they avoid to provide hooks for abuse.

Keeping the user in control For all eID applications it is mandatory that the user enters her PIN to grant access to any data or function. The user may restrict the set of data fields released to a service.

4 Promise vs. Practice

Will eID in the long run become the technology of choice for online authentication? It may, but only if it evolves to overcome a number of issues. The requirements and design decisions have some downsides.

4.1 Smart Cards Force Tradeoffs

Ideally, one would like to achieve privacy properties through cryptographic mechanisms like blind signatures and zero-knowledge protocols. Technologies such as Microsoft's U-Prove [4] or IBM's Identity Mixer [5] demonstrate this approach. However, current smart card technology available for the mass-market is not yet powerful enough for the computations that these mechanisms require.

To achieve privacy without the computational overhead, the designers of the German ID card chose the workaround that we outlined in the system description above. Sharing a private chip authentication key within a batch of cards [6] makes these cards indistinguishable on the protocol level, and eID data remain unsigned, requiring the context of a protocol execution to prove their authenticity. Consequently, the security of eID authentication relies on tamper-resistance of the smart card chips.

While enhancing privacy, this feature makes the eID function more vulnerable. Should an attacker some day manage to extract the chip authentication key from any ID card, this attacker would be able to forge arbitrary identities. There would be no way for eID servers to recognize spoofed cards. Revoking the compromised chip authentication key would solve the security problem, but render all affected cards useless for eID purposes, requiring their replacement.

The specification may permit a technical workaround for this scenario. The ID card supports a second chip authentication mode with unique keys, intended for privileged offline terminals. This mode, if used consistently for all applications online or offline, would allow the revocation of individual cards at the cost of degrading privacy.

4.2 Complex Changes in the Risk Landscape

Introducing eID has two opposite consequences, the balance of which is not clear yet. On the one hand, eID provides a stronger authentication mechanism and therefore more security. On the other hand, eID facilitates the deployment of new online services that up

to now were only available offline due to security concerns or impracticality. Protecting these services requires more than an authentication mechanism.

An example is the information service of the German Federal Pension Fund, an early adopter of eID. Periodically, the fund informs citizens about their paid insurance contributions and the estimated pension by letter or, in the future, online. These data are obviously sensitive as they give deep insight into employment histories (former employers, salaries, employment periods, etc.). An attacker getting access to these data could easily misuse them, resulting in serious damage.

How well such data are protected is a matter of application security. If not accompanied by appropriate further security measures, eID might therefore increase the overall vulnerability and risk.

4.3 Limits of Applicability

Some of the design decisions have a profound impact on the feasibility of eID use:

- The ID card is primarily an authentication token with a high security and privacy level. Even card holders themselves, lacking authorization certificates, cannot read data from their own cards.
- Except for a single certificate for electronic signatures, the ID card cannot contain any additional applications or data. This limits applications to those functions built into the card, regardless of the actual requirements.

During the field test, all requests for changes to the specifications, like the incorporation of additional data into the eID channel, were rejected. For example, banks asked for means to authorize transactions through the eID function for secure online banking. The optional electronic signature function of the ID card can replace their current security mechanisms only if citizens universally accept it. In another case, a manufacturer of cigarette vending machines requested access to age verification without the user entering a PIN. In both cases, lack of support for their requirements had these companies reconsider their eID plans.

4.4 Obstacles to Adoption

The German eID system as a new technology competes with established mechanisms. Adoption may be hampered on the part of the service providers as well as of the citizens as users.

Service Provider Perspective Supporting eID imposes costs on the service provider. An initial investment is required for technical integration and for the service approval process. Recurrent costs ensue, such as fees to the certification authority and to the eID service provider. For eID to be economically feasible, the savings from eID—including saved opportunity cost—must at least make up for the costs.

A large user base makes it more likely that eID pays off for the service provider. However, since eID remains optional for the citizen, there is no automatism to create this user base. Citizens have to be convinced to use eID.

Even with many users, cost savings through eID may remain limited. Service providers will still have to manage user accounts, regardless of the authentication scheme. It may even become more difficult for service providers to handle exceptions: while they can reset forgotten passwords at their discretion, coping with lost ID cards requires a fallback authentication mechanism. Otherwise, users are locked out of a service until replacement arrives.

Another possible issue lies in service approval and authorization. While the formal criteria are laid down, it is uncertain yet how the approval practice will work out in the long run. The dilemma of service approval is that it has to be restrictive to be useful, but permissive to encourage adoption.

User Perspective Citizens are free to opt in or out of eID at any time. If they opt in, they have to make investments as well. While possession of an ID document is mandatory in Germany, citizens can fulfill this obligation by obtaining either a passport or an ID card. When obtaining a new ID card, citizens can choose whether they want the eID function to be disabled or enabled. This decision incurs no cost or saving. If they change their mind later, they can activate or deactivate eID for a small fee in citizen registration offices. A recent survey by Unisys [7] estimated that about 20% of the German population consider using the eID authentication mechanism.

To use the eID function online, a citizen needs a certified card reader. Prices range from 25 EUR for basic readers without a PIN entry keypad to 160 EUR for a multi-purpose reader with display and keypad that supports other smart card applications as well. The range of eID-enabled services deployed so far hardly justifies this investment for the average citizen.

The eID function imposes responsibilities upon the card holder: not to surrender possession of the card at any time, to report loss of the card immediately, not to disclose the PIN, and to use suitable equipment and software [1].

How responsibilities and the choice of equipment will affect liability remains to be seen, there have not been pertinent lawsuits yet. A legal expert opinion commissioned by the German government concluded that citizens could successfully dispute eID authentication under some conditions. Particularly, using a basic card reader makes abuse assertions plausible as it exposes the eID PIN to malware attacks.

A Chicken-and-egg Problem The network effect is obvious. For eID to become useful and justify the investment of a participant, it has to be widely deployed and supported. Service providers need a sufficient user base, and users need a sufficient number of everyday services. The present situation can be summarized as a chicken-and-egg problem, service providers and citizens waiting for each other to make the first step.

To get deployment started, the German government supported service providers and citizens. An application field test prior to the rollout of the ID card helped service

providers to implement and test eID support early. For the citizens, the government sponsored the distribution of 1.5 million basic readers free of charge.

5 The International Perspective

The German eID infrastructure is a national solution, but the Internet extends beyond the domestic market. To make eID the online authentication scheme of choice, service providers worldwide have to support it. International support becomes feasible only if national eID schemes are standardized and interoperable.

Standardization efforts are underway in Europe. Roughly half of the European Union member states, as well as Norway and Switzerland, have already introduced electronic ID cards. More states plan the introduction in the near future [8]. A European Citizen Card (ECC) specification [9] is emerging. It defines card profiles based on identification, authentication and signature services of European signature cards [3]. The research project STORK [10] works towards a European interoperability platform. Beyond Europe, the International Civil Aviation Organization (ICAO) has adopted some of the technologies used for eID, namely the PACE protocol [11], for travel documents.

Despite these efforts, we are far from having a universal eID scheme for the Internet. Different approaches will continue to compete, not the least due to cultural differences. A recent OECD report [12] compares international eID strategies. In Europe, the governments have a strong role in designing, deploying and operating eID schemes. In contrast, the U.S. National Strategy for Trusted Identities in Cyberspace [13] emphasizes the role of the private sector and consumer choice.

6 Conclusion

In the general case, it seems unlikely that electronic ID cards will soon replace other online authentication mechanisms. In three contexts, however, eID is becoming a viable alternative to established mechanisms. First, eID supports formal authentication where the law requires it, and may be the only mechanism to do so. Electronic ID cards may therefore become an enabler for new online applications—they simplify procedures that service providers are required to implement. We expect that eID will blossom in these contexts, but not generally replace other authentication schemes. In other words, electronic ID provides online what its predecessor and carrier, the traditional ID card, provided offline: support for government applications and for applications regulated by the government. Second, the ID card supports authentication without prior establishment of a relationship. If a service provider is authorized, people can use their card right away, without having to go through a registration process. This makes eID attractive for applications that are being used infrequently but require strong authentication. Third, they support strong authentication and attribute verification for ambient applications, such as age verification at vending machines or at the entrance to age-restricted premises.

One open question is how using an official ID card to login might affect user behavior elsewhere in a service. Will they feel more or less secure? Will they trust the service

more or less? Will people refrain from some behaviors that they would expose if they hadn't shown their ID card at the beginning of their session?

A related question is how the wrapping as an ID card might interfere, despite the privacy features, with the users' perception of certain services. Will people trust the eID scheme enough to use it with services that they may deem sensitive, such as adult entertainment sites? Features like pseudonymous authentication or access control become visible only through software, and thus may remain much less obvious than the physical act of placing an ID card with my photo on a card reader.

Finally, the most fundamental question is how much security formal authentication through eID schemes really yields. The security problems that online service providers are trying to solve may be subtly different from the problem that an eID scheme promises to solve. Some services for instance require authorization rather than authentication, making sure that an entitled party has approved of a particular transaction.

An interesting observation to ponder is the clash of different conceptions of privacy. On the one hand, the core technology goes to great lengths to protect the data on the ID card itself from unauthorized access—data that one might find on the Internet for a considerable portion of the population. On the other hand, the eID infrastructure specifically supports applications that make sensitive data accessible online or in which businesses are required to record certain data, whether they want it or not. Will eID make us more or less secure in the end?

References

[1] *BSI TR-03127 Architecture electronic Identity Card and electronic Resident Permit*, Bundesamt für Sicherheit in der Informationstechnik, March 2011, version 1.13.

[2] *BSI TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI)*, Bundesamt für Sicherheit in der Informationstechnik, October 2010, version 2.05.

[3] *CEN prEN 14890 Application Interface for Smart Cards Used as Secure Signature Creation Devices*, European Committee for Standardization, 2011, draft version.

[4] S. A. Brands, *Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy*. Cambridge, MA, USA: MIT Press, 2000.

[5] J. Camenisch and B. Pfitzmann, "Federated identity management," in *Security, Privacy, and Trust in Modern Data Management*, ser. Data-Centric Systems and Applications, M. Petković and W. Jonker, Eds. Springer Berlin Heidelberg, 2007, pp. 213–238.

[6] H. Plötz, "Technik des neuen ePA," Presentation, 26th Chaos Communication Congress, Dec 2009. [Online]. Available: http://events.ccc.de/congress/2009/Fahrplan/events/3510.en.html

[7] "Unisys security index – Germany," February 2011. [Online]. Available: http://www.unisyssecurityindex.com/usi/germany/reports

[8] W. Fumy and M. Paeschke, Eds., *Handbook of eID Security*. Erlangen: Publicis Publishing, 2011.

[9] *CEN prTS 15480 Identification card systems - European Citizen Card (ECC)*, European Committee for Standardization, 2011, draft version.

[10] "STORK project," Project website. [Online]. Available: https://www.eid-stork.eu/

[11] *Machine Readable Travel Documents - Supplemental Access Control for Machine Readable Travel Documents*, International Civil Aviation Organization, November 2010, version 1.01.

[12] OECD, "National strategies and policies for digital identity management in OECD countries," OECD Publishing, OECD Digital Economy Papers 177, March 2011. [Online]. Available: http://www.oecd-ilibrary.org/content/workingpaper/5kgdzvn5rfs2-en

[13] The White House, "National strategy for trusted identities in cyberspace," April 2011. [Online]. Available: http://www.nstic.us/strategy.html