Electronic Identity Cards for User Authentication—Promise and Practice

Andreas Poller, Ulrich Waldmann, Sven Vowé, and Sven Türpe |
Fraunhofer Institute for Secure Information Technology

Electronic identity (eID) cards promise to supply a nationwide user authentication mechanism. The core technology seems ready for mass deployment, but application issues might hamper eID adoption.

Long before the Internet became a commodity, many governments had public authentication schemes in place, distributing identity cards to citizens. Governments trust their cards, and so do businesses that require reliable authentication of persons. Even in countries without national ID card schemes, similar documents, such as driver's licenses, serve the same purpose.

Will government-issued electronic identity (eID) documents achieve the same success? Many European governments think so and have deployed eID schemes. The most recent and apparently most advanced eID deployment is the German eID card *neuer Personalausweis*. Advertised as citizens' "most important card," it promises a universal, secure authentication scheme for government and private-sector applications. Besides the obvious question of how useful national schemes can be on the Internet, will such eID schemes improve online authentication?

An Authentication Scheme for Everyone

On 1 November 2010, the German government began distributing a contactless smart card (see Figure 1) with three distinct electronic functions, each with its own protected dataset:

- The mandatory ePass function, reserved for government use, stores a digital representation of the cardholder's identity similar to electronic passports.
- The eID function for general applications stores an identity record that authorized services can access with cardholder permission. Citizens choose whether they want this function activated.
- The optional eSign function lets cardholders store a single private key and certificate for qualified electronic signatures. Private-sector trust centers issue the certificates.

Separate PINs protect the eID and eSign functions. Table 1 gives an overview of the functions and data records. Here, we focus on the eID function, which public- and private-sector services can use online.

Applications for eID

Proponents of eID envision a world in which identity cards replace usernames and passwords, support business processes online and offline, and allow services to be provided online that currently require the citizen's presence or paperwork. They hope that someday we'll use a single eID scheme to shop online, open bank accounts, check in to hotels, rent cars, and file taxes.

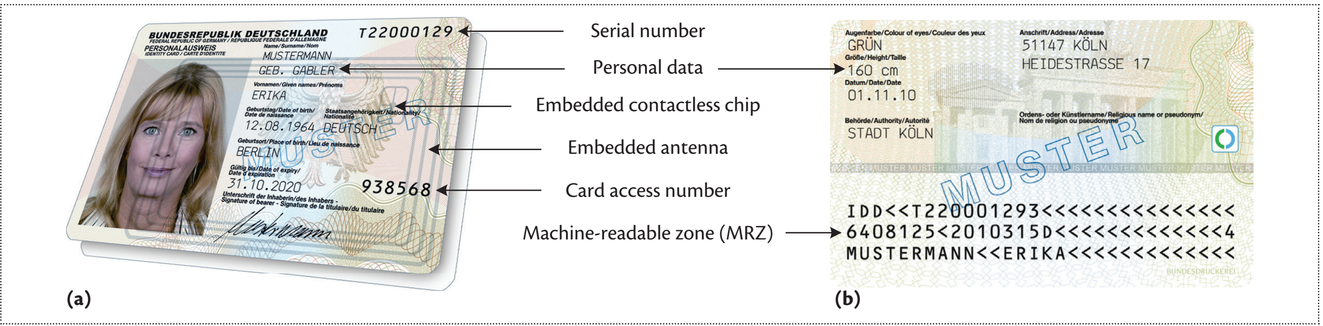

Figure 1. The new German electronic ID (eID) card: (a) front and (b) back. The card carries human-readable data on its surface and a contactless chip inside, combining the functions of a conventional ID document and a digital authentication token. (Source: Bundesministerium des Innern; used with permission.)

Table 1. The eID card's electronic functions and data.

Function	Purpose	PACE (Password Authenticated Connection Establishment) password	Data	Uses
ePass (mandatory)	Authorized offline inspection systems read the data	Card access number (CAN) or machine-readable zone (MRZ)	Face image; two fingerprint images (optional); MRZ data	Offline biometric identity verification; reserved for government access
eID (activation optional)	Online applications read the data or access functions as authorized	eID PIN	Family and given names; artistic name and doctoral degree; date and place of birth; address and community ID; expiration date	Identification; age verification; community ID verification; restricted identification (pseudonym); revocation query
	Offline inspection systems read the data and update the address and community ID	CAN or MRZ		
eSign (certificate optional)	A certification authority installs the signature certificate online	eID PIN	Signature key; X.509 certificate	Electronic-signature creation
	Citizens make electronic signatures with the eSign PIN	CAN		

Piggybacking on widely deployed ID cards' authentication schemes will supposedly help achieve this goal. When the rollout is complete after 10 years, so goes the reasoning, the established infrastructure will be attractive to both citizens and service providers.

It's too early for an ecosystem of eID-enabled services to emerge and stabilize. Before the rollout, an application field test with early adopters indicated that four service types might see an immediate benefit from supporting eID:

- government services that require formal identification of citizens;
- services that must let citizens exercise their right to access personal information (institutions such as credit information agencies or pension funds might want to let citizens access their data online, but they must first identify the requester);
- companies required to record their clients' identities, such as banks or telecommunications operators (currently, contracting with such companies requires an offline step for identity verification); and
- operators of age-restricted services, such as cigarette vending machines or adult entertainment (currently, they use a variety of means for age verification, such as optical ID document scanners and age verification functions on debit cards).

Such applications could drive eID adoption at first, but the intended application scope is much wider. For example, online elections based on eID functions are under discussion but remain far from implementation.

Whether there will be a killer application on which service providers and users agree remains to be seen.

Authentication with Privacy Benefits

A public, all-purpose authentication scheme based on ID cards raises privacy concerns. Can it be abused to link users' data and actions throughout the Internet to their identity? Will eID force users to let every website know their birthday? Who can access their data, and how can users remain in control? Can they choose to be anonymous?

The German eID card translates privacy into a set of features. Services must authenticate themselves to citizens and their ID cards. Authorization certificates determine the extent to which a service can access eID data fields and functions. Citizens must consent to every access. On-card verification supports uses such as age verification while releasing minimum information. Restricted identification creates service-specific pseudonyms that are unlinkable across services.

The eID Function

The eID function makes a subset of the card's identity data (for example, name, academic title, birth date and place, and street address) accessible to authorized services. Biometric data (facial image and, optionally, fingerprints) is restricted to the ePass function and not accessible through the eID interface. The card serial number and the cardholder's handwritten signature printed on the surface aren't part of the eID dataset. With these exceptions, the eID function works with the same data that's printed on the card.

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

System Components

The German Federal Office for Information Security's technical guideline TR-03127 specifies the eID card system's architecture.[1] Four principal components participate in online authentication. A dedicated eID server handles authentication on the server side and returns the result to the service. eID servers might be operated by the service provider or a third party. They use an authorization certificate on the relying service's behalf.

On the client side, a card reader and a client software package provide interfaces to the user and 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 eID server, displays authorization certificates, and lets the user restrict access to eID data fields.

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

Cryptographic Protocols

Cryptographic protocols secure the channels between the card and the reader and between the card and the eID server. Between the card and the reader, the Password Authenticated Connection Establishment (PACE) protocol establishes a shared session key and verifies the password without transmitting it. All ID card functions use PACE, but with different passwords. The six-digit eID PIN is used during online authentication. Other functions use the card access number or the machine-readable zone (see Table 1).

Between the card and 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 a service's authorization certificate to the card in a challenge-response protocol. Chip authentication uses a chip authentication key built into the card to prove authenticity to the eID server. It also establishes a session key between the eID server and the card. The result is a trusted channel between the ID card and 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 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 German Federal Office for Information Security's technical guideline TR-03110 specifies the cryptography in detail.[2] As cryptographic primitives, the eID card uses

- AES-128 CBC (cipher block chaining) and CMAC (cipher-based message-authentication code) for messaging security;
- SHA-256 for hashing;
- elliptic-curve Diffie-Hellman for key establishment in PACE, chip authentication, and restricted identification; and

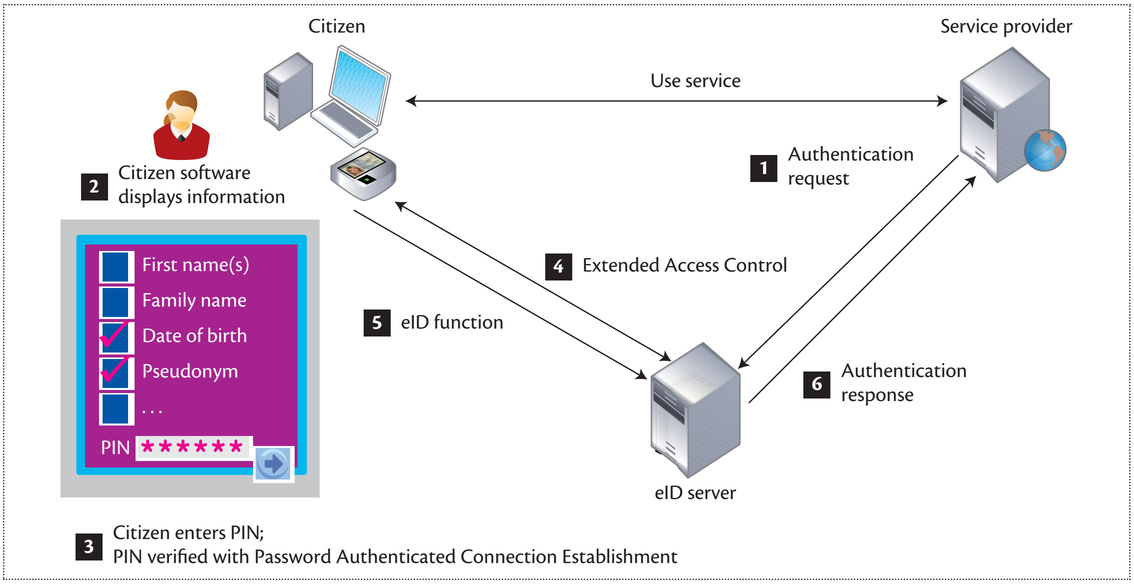

Figure 2. Online authentication. The eID server interacts with the client software, user, and eID card. The relying service initiates the process and receives identity data in response if authentication was successful.

- ECDSA (Elliptic Curve Digital Signature Algorithm) for authorization certificates and signatures.

The specification facilitates later transition to other algorithms or longer keys. Through object identifiers, eID cards indicate the supported cipher suites.

eID Authentication

To authenticate users with eID, an online service triggers the client software through a browser plug-in, then the eID server executes the authentication process (see Figure 2):

1. *Authentication request*. The service requests users' eID data from the 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, users enter their eID PIN to express consent. This PIN is used locally to execute the PACE protocol.
4. *EAC*. Mediated by the client, the eID server and ID card authenticate each other and establish a trusted channel.
5. *Use of the 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, the service resumes control and uses the authentication results for its purposes.

Security and Privacy Properties

For citizens, the cryptographic protocols ensure that the eID card releases data

- only with the cardholder's consent,
- to an authenticated and authorized service,
- within the limits of authorization, and
- through a channel protected against eavesdropping and tampering.

The eID card chip and eID server are the secure channel's endpoints. The card chip authenticates the eID server and verifies its authorization using lightweight certificates.[3] If, as recommended, citizens use an advanced card reader with a keypad, the eID PIN is protected against malicious software on their computers.

For service providers, chip authentication ensures that the data received originates from a genuine and valid government-issued eID card. A revocation mechanism lets service providers recognize cards that were reported lost.[1]

Two design features enhance citizens' privacy. First, chip authentication keys aren't unique. If each eID card had a unique chip authentication key, a service provider might gain a unique identifier as a side effect of the protocols. So, a batch of cards shares the same secret chip authentication key, making them indistinguishable at the protocol level.

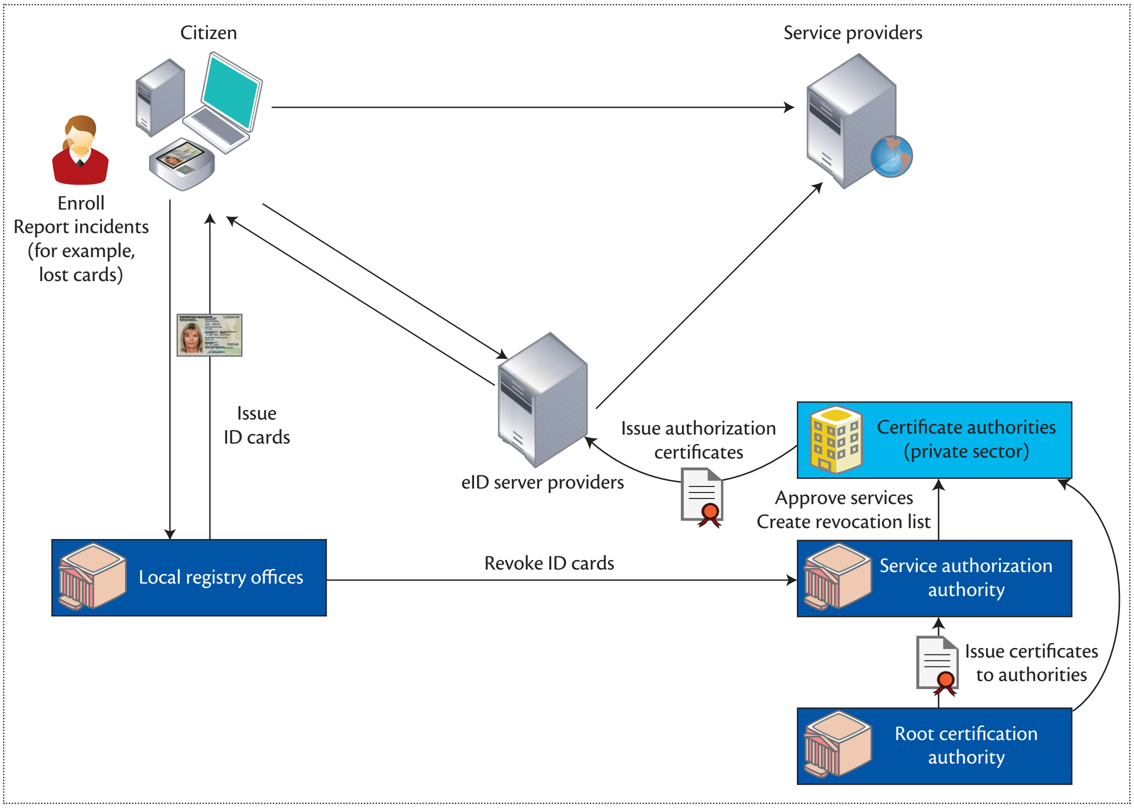

Figure 3. Roles and responsibilities for the eID card. The government and the private sector share eID system implementation and operation.

Second, eID data remains unsigned. To prevent service providers from proving to others that an eID record is authentic, there's 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 ensure the eID server of the eID data's authenticity. Outside this context, there's no way to verify the eID data's origin.

Roles and Responsibilities

The government and private sector share eID system implementation and operation (see Figure 3). Local administrative agencies register citizens and issue ID cards. Federal administrative agencies authorize service providers, oversee equipment certification, and 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 freely available for Windows and Linux (and is pending for Mac OS). Alternative implementations of the client software might eventually appear on the market. Service providers might 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.

Service Authorization

Service authorization to access eID data fields or data verification functions involves three steps. First, service providers request approval from the Federal Office of Administration (BVA), which 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 three years.

Second, service providers contract with technical certification authorities, which 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 expire quickly if approval expires or is revoked. The certification authorities also provide eID servers with ID card revocation lists on the basis of BVA notifications.

Finally, authorized eID servers request access to the card on behalf of approved service requests. Users receive an authorization certificate and can deselect data fields from the service authorization. The client software also presents users the service's approved privacy policy. The authorization certificate includes a hash of the policy.

Design Rationale

The eID system's design arose from the following objectives, requirements, and design decisions.

User benefits. eID authentication is supposed to make online authentication easier while giving citizens more control and responsibility. The ID card is meant as a citizen identification scheme for the Internet and should reduce users' troubles with managing user account names, passwords, and other credentials. The user-controlled release of selected eID data fields to services curtails 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. Services supporting eID receive 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 doesn't secure transactions; it provides only authentication. However, the card lets trust centers 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 government's control. Service providers will be authorized to access data fields and functions only to the extent they can demonstrate a need for them.

No centralized databases. The underlying public-key infrastructure and card production are the eID infrastructure's only centralized components. No centralized databases of personal information exist. Data needed for card production is deleted afterward.

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

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

Keeping the user in control. For all online eID applications, users must enter their eID PIN to grant access to any data or function. They can restrict the set of data fields released to a service.

Promise versus Practice

Will eID become the technology of choice for online authentication in the long run? It might, but only if it overcomes several issues. The requirements and design decisions have some downsides.

Smart Cards Force Tradeoffs

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

To achieve privacy without the computational overhead, the German ID card designers chose the workaround we outlined in the system description. Sharing a private chip authentication key among a batch of cards makes them indistinguishable on the protocol level, and the eID data remains unsigned, requiring the context of a protocol execution to prove its authenticity. So, eID authentication security relies on the smart-card chips' tamper resistance.

Although this feature enhances privacy, it makes the eID function more vulnerable. Should attackers manage to extract an eID card's chip authentication key, they could forge arbitrary identities. eID servers wouldn't 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.[6]

The specification might 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 degraded privacy.

Complex Changes in the Risk Landscape

Introducing eID has two opposite consequences, the balance of which isn't clear yet. On one hand, eID provides a stronger authentication mechanism and therefore more security. On the other, it facilitates the deployment of new online services that previously were available only offline owing to security concerns or impracticality. Protecting these services requires more than an authentication mechanism.

An example is the German Federal Pension Fund's information service, an early eID adopter. Periodically, the fund informs citizens about their paid insurance contributions and the estimated pension by letter (or, in the future, online). This data is obviously sensitive, giving deep insight into employment histories (former employers, salaries, employment periods, and so forth). Attackers who access this data could easily misuse it, causing serious damage.

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

Limits of Applicability

Some design decisions profoundly affect the feasibility of eID use. The ID card is primarily an authentication token with high security and privacy levels. Even cardholders, lacking authorization certificates, can't read data from their own cards. In addition, except for a single certificate for electronic signatures, the ID card can't contain 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 specification changes, such as incorporation of additional data into the eID channel, were rejected. For example, banks asked for a means to authorize transactions through the eID function for secure online banking. The ID card's optional electronic-signature function can replace current security mechanisms only if citizens universally accept it. In another case, a cigarette-vending-machine manufacturer requested access to age verification without requiring the eID PIN. In both cases, lack of support for these companies' requirements led them to reconsider their eID plans.

Obstacles to Adoption

As a new technology, the German eID system competes with established mechanisms. Adoption might be hampered for both service providers and users.

The service provider's perspective. Supporting eID imposes costs on service providers. Technical integration and the service approval process require an initial investment. Recurring costs ensue, such as certification authority and eID service provider fees. For eID to be economically feasible, the savings it provides must at least make up for the costs.

A large user base will make it more likely that eID pays off for service providers. However, because eID remains optional for citizens, there's no automatism to create this user base. Citizens must be convinced to use eID.

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

Another possible issue lies in service approval and authorization. Although the formal criteria are established, it's uncertain how the approval practice will work out in the long run. Service approval must be restrictive to be useful but permissive to encourage adoption.

The user's perspective. Citizens are free to opt in or out of eID at any time. If they opt in, they must make investments as well. Although 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 to enable the online eID function. This decision incurs no cost or savings. If they change their mind later, they can activate or deactivate eID for a small fee. A recent Unisys survey estimated that approximately 20 percent of the German population are considering using eID authentication.[7]

As we mentioned before, to use eID online, citizens need a certified card reader. Prices range from €25 for basic readers without a PIN entry keypad to €160 for a multipurpose reader with a display and keypad that also supports other smart-card applications. The range of eID-enabled services deployed so far hardly justifies this investment for the average citizen.

The eID function imposes responsibilities on cardholders. They mustn't surrender possession of the card at any time or disclose their PIN, and they must use suitable equipment and software and report a card's loss immediately.[1]

How responsibilities and equipment will affect liability remains to be seen; there haven't been pertinent lawsuits yet. A legal expert opinion commissioned by the German government concluded that citizens could successfully dispute eID authentication under some conditions.[8] In particular, using a basic card reader makes abuse assertions plausible because 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 participants' investment, it must 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 each waiting for the other to make the first step.

To begin deployment, the German government supported service providers and citizens. The application field test helped service providers implement and test eID support early. For citizens, the government sponsored the distribution of 1.5 million basic readers free of charge.

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 the EU member countries, as well as Norway and Switzerland, have introduced eID cards. More countries plan the introduction in the near future.[9] A European Citizen Card specification is emerging;[10] it defines card profiles on the basis of identification, authentication, and signature services of European signature cards.[3] The research project Stork works toward a European interoperability platform (www.eid-stork.eu). Beyond Europe, the International Civil Aviation Organization has adopted the PACE protocol for travel documents.[11]

Despite these efforts, we're far from a universal eID Internet scheme. Different approaches will continue to compete, not the least due to cultural differences. A recent Organization for Economic Co-operation and Development report compared international eID strategies.[12] In Europe, governments have a strong role in designing, deploying, and operating eID schemes. In contrast, the US National Strategy for Trusted Identities in Cyberspace emphasizes the role of the private sector and consumer choice.[13]

Where eID Might Be Viable

It seems unlikely that eID cards will soon replace other online authentication mechanisms. However, eID is becoming a viable alternative to established mechanisms in three contexts.

First, eID might be the only mechanism to support formal authentication where the law requires it. eID cards might therefore enable new online applications—they simplify procedures that service providers are required to implement. We expect that eID will blossom in these contexts but generally won't replace other authentication schemes. In other words, eID provides online what its predecessor and carrier—the traditional ID card—provided offline: support for government and government-regulated applications.

Second, eID supports authentication without prior establishment of a relationship. People can use their cards immediately with authorized service providers, without registering. This makes eID attractive for applications used infrequently but requiring strong authentication.

Third, eID supports 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 log in might affect user behavior with the service. Will users feel more or less secure? Will they trust the service more or less? Will they 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 using a government ID card to access commercial services might interfere with users' perception of those services, despite the privacy features. Will people trust eID enough to use it with services they might deem sensitive, such as adult-entertainment sites? Features such as pseudonymous authentication or access control become visible only through software, and thus might remain much less obvious than the physical act of placing an ID card with a 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 might differ subtly from the problem an eID scheme promises to solve. For instance, some services require authorization rather than authentication, ensuring that an entitled party has approved of a particular transaction.

An interesting point is the clash of different conceptions of privacy. On one hand, the core technology goes to great lengths to protect ID card data from unauthorized access—data that might exist on the Internet for a considerable portion of the population. On the other, 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. *Architecture Electronic Identity Card and Electronic Resident Permit*, ver. 1.13, tech. report TR-03127, German Federal Office for Information Security, Mar. 2011.
2. *Advanced Security Mechanisms for Machine Readable Travel Documents—Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI)*, ver. 2.05, tech. report TR-03110, German Federal Office for Information Security, Oct. 2010.
3. *Application Interface for Smart Cards Used as Secure Signature Creation Devices*, draft version, tech. report CEN prEN 14890, European Committee for Standardization, 2011.
4. S.A. Brands, *Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy*, MIT Press, 2000.
5. J. Camenisch and B. Pfitzmann, "Federated Identity Management," *Security, Privacy, and Trust in Modern Data Management*, M. Petkovic and W. Jonker, eds., Springer, 2007, pp. 213–238.
6. H. Plötz, "Technik des Neuen ePA," presentation at the 26th Chaos Communication Congress, Dec. 2009; http://events.ccc.de/congress/2009/Fahrplan/events/3510.en.html.
7. "Unisys Security Index—Germany," Unisys, Feb. 2011; www.unisyssecurityindex.com/usi/germany/reports.
8. G. Borges, "Rechtsfragen der Haftung im Zusammenhang mit dem elektronischen Identitätsnachweis," Ruhr-Universität Bochum, Nov. 2010; www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/Sicherheit/PaesseAusweise/studie2_npa.pdf?__blob=publicationFile.
9. *Handbook of eID Security*, W. Fumy and M. Paeschke, eds., Publicis, 2011.
10. *Identification Card Systems—European Citizen Card (ECC)*, draft version, tech. report CEN prTS 15480, European Committee for Standardization, 2011.
11. *Machine Readable Travel Documents—Supplemental Access Control for Machine Readable Travel Documents*, ver. 1.01, tech. report ISO/IEC JTC1 SC17 WG3/TF5, Int'l Civil Aviation Org., 11 Nov. 2010.
12. "National Strategies and Policies for Digital Identity Management in OECD Countries," Org. for Economic Co-operation and Development, Mar. 2011; www.oecd-ilibrary.org/content/workingpaper/5kgdzvn5rfs2-en.
13. "National Strategy for Trusted Identities in Cyberspace," the White House, Apr. 2011; www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf.

Andreas Poller works in the Fraunhofer Institute for Secure Information Technology's Security Test Lab. His research focuses on privacy protection, especially in Web 2.0 applications. Poller has a Diplom in applied computer science from the Chemnitz University of Technology. Contact him at andreas.poller@sit.fraunhofer.de.

Ulrich Waldmann works in the Fraunhofer Institute for Secure Information Technology's Cloud Computing, Identity & Privacy Department. His fields of work include smart cards, eID, and biometrics. Waldmann has a Diplom in computer science from Technische Universität Darmstadt. Contact him at ulrich.waldmann@sit.fraunhofer.de.

Sven Vowé works in the Fraunhofer Institute for Secure Information Technology's Cloud Computing, Identity & Privacy Department. His research interests include cloud computing security and privacy and network protocol security. Vowé has a Diplom in computer science from Technische Universität Darmstadt. Contact him at sven.vowe@sit.fraunhofer.de.

Sven Türpe works in the Fraunhofer Institute for Secure Information Technology's Security Test Lab. His research interests include application security, security evaluation and testing, and threat analysis. Türpe has a Diplom in computer science from Universität Leipzig. Contact him at sven.tuerpe@sit.fraunhofer.de.