Walter Fumy, Manfred Paeschke (Eds.)

Handbook of eID Security

Concepts

Practical Experiences

Technologies

PUBLICIS

Fumy/Paeschke (Eds.)
Handbook of eID Security

Handbook of eID Security

Concepts,
Practical Experiences,
Technologies

by Walter Fumy and
Manfred Paeschke

PUBLICIS

Bibliographic information published by the Deutsche Nationalbibliothek

The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie;
detailed bibliographic data are available in the Internet at http://dnb.d-nb.de.

Authors, editors and publisher have taken great care with all texts and illustrations in this book. Nevertheless, errors can never be completely avoided. The publisher, the editors and authors accept no liability, regardless of legal basis. Designations used in this book may be trademarks whose use by third parties for their own purposes could violate the rights of the owners.

www.publicis.de/books

Publishing editor:
Gerhard Seitfudem, Publicis Publishing, Erlangen
gerhard.seitfudem@publicis.de

ISBN 978-3-89578-379-1

Publisher: Publicis Publishing, Erlangen

Printed in Germany

Foreword

IT security today is faced with a complex array of challenges. Our society wishes and is also forced to use the opportunities of the digital world and is at the same time under the obligation to identify and minimise existing risks – especially with a view to the increasing threat of online crime. The principle of electronic identity (eID) is an important approach in this context because a unique and secure identification in the virtual world is a precondition for greater security in electronic everyday life.

New figures and research make clear how important progress in protecting electronic identities is. While until recently phishing attacks were primarily aimed at banking information of users, criminals are now increasingly focusing on complete digital identities. This is the result of a study on identity theft on the Internet which was commissioned by the Federal Ministry of the Interior and the Federal Office for Information Security. This concerns, for instance, data submitted by users in social networks or while shopping online. The study expects unforeseeable forms of identity theft and misuse to develop in the future, due to ever new technologies and platforms, which continuously allow new attack scenarios.

In 2009 already, the Federal Criminal Police Office recorded a total of 6,800 cases of digital identity theft, although the real figure may well be much higher. Cyber attacks on personal data have hence long since reached a new level of quality and quantity, and experts expect this form of crime to increase further in the future. Public administrations, the business community and citizens are increasingly integrated into digital networks and thereby offer criminals new inroads. Both technical solutions and education of Internet users are required in order to counteract this.

Against this background, the security of the electronic identity must be regarded as a government task. A possibility to prove one's identity on the Internet beyond any doubt must be created, not least in the interest of internal security. An unequivocal proof of identity is the only way to ensure secure eGovernment and eCommerce.

In Germany, the concept of electronic identity will be implemented with the new ID card, starting in November 2010. It will break new ground in identity management and enable crucial infrastructures for electronic business and administration processes. Citizens can use the integrated eID function in order to clearly identify themselves to public authorities and eCommerce suppliers. At the same time, they are also in the position to verify the identity of their virtual counterpart. The new ID card hence provides new opportunities for businesses and enables the shifting of public services into the Internet via eGovernment applications. This also benefits public authorities, which can achieve a higher level of automation and work more effectively. Furthermore, we also reduce the risk of data misuse and identity theft. The new ID card in credit-card size – including the solutions and high security standards which were created for it – is hence an important technical response to the challenges of IT security.

An essential feature of the implementation process is to minimise risks at an early stage and to create a high level of application security. The technical challenges of electronic identities are connected to data security. This includes the protection of the data on the chip as well as the guarantee of secure transmission paths for Internet users. The new ID card is based on the use of advanced cryptographic methods such as the PACE protocol, as well as "AusweisApp" as a newly developed application software. They offer a high security standard for the communication between citizens and authorities or businesses and make sure that the data cannot be accessed by third parties.

Since cybercrime does not stop at national borders, compatibility of the electronic identity solutions developed in Europe is crucial: STORK (Secure Identity Across Borders Linked) is the name of a pilot project of the European Commission which bundles European eID activities and in which the Federal Office for Information Security was involved from the very beginning. Cross-border co-operation not only affords protection against crime – it is also a prerequisite for cross-border eGovernment services for EU citizens as demanded, not least, by the EU's Services Directive. We are intensively working on integrating our powerful system concept for the new German ID card as a trailblazing element into a pan-European solution.

eID solutions today are technically mature and enable a high standard of data security. However, their success must be measured by their acceptance: more security on the Internet will always depend on the large-scale adoption of solutions. Furthermore, eID can only be a part of the solution for improving IT security. Despite all high quality standards which are available, citizens have to accept their personal responsibility for themselves. It hence remains an important task to continuously educate Internet users on new dangers from cyberspace and about the correct use, also of eID solutions. Only when state-of-the-art technology and educated users come together will the secure use of the opportunities of the digital world be possible.

Michael Hange
President, Federal Office for Information Security
(Bundesamt für Sicherheit in der Informationstechnik, BSI)

Contents

Part I: Concepts and Trends

Part II: Solutions and Practical Experiences

Part III: Technologies and Standards

Part I:
Concepts and Trends

1 Challenges in eID Security

Walter Fumy and Manfred Paeschke

In late October, on a gray and stormy day, I drove to the local post office of our small country town to withdraw some cash from my account. Dutifully, the clerk asked for ID. Horrified, I realized I had not brought along any proof of my identity. What now? Drive back home and get to the office extremely late? The clerk leaned back, thought about it, and said: "Well, I know who you are, I know where you live, and you have been here before – so, yes, I suppose I know you." Pleased with his own way of solving the problem, he completed the transaction.

Nowadays, with everyone carrying out their transactions online, I would have been out of luck. Now the situation is entirely different. When asked for your electronic ID, your only choice is to provide ID or cancel the transaction. eID solutions have widely replaced personal interaction within a community, and so security is more essential than ever. That's what this book is all about.

The past quarter of a century has seen human activities shifting away from physical, person-to-person contacts towards the anonymity of an electronic world. Globalization would be impossible without modern information technology, high-bandwidth, inexpensive communications and the accessibility of the World Wide Web. Cyberspace, the interdependent network of IT components that underpins a large part of our communications, has become a key component of many critical infrastructures.

We use the cyberspace to exchange information, buy and sell products and services as well as to facilitate many other online transactions across a wide range of sectors, both nationally and internationally. The transfer of processes from the physical to a digital world offers the potential of increasing efficiency and accuracy, reducing costs, and improving the end-user experience. Some of the critical issues raised by this development include its effects on security and privacy, these being of concern to individuals, enterprises, and governments alike.

While we accept the high value of anonymity for many online activities, in a large proportion of the interactions between citizens, businesses and administrations it is vital that the involved parties can safely trust that they are interacting with accurately identified entities. Identities play a central role in processes as diverse as online communication, placing an online order, registering a car, applying for a mortgage or claiming unemployment benefits.

Symptoms of an untrustworthy computing environment include spoofed websites, stolen passwords and compromised log-in accounts. One fundamental step in reducing online fraud and identity theft is to increase the level of trust associated with identities in cyberspace. An electronic identity consists of a set of attributes related to a specific entity, be it a person, an enterprise, or an object. The unique identity of one entity allows it to be distinguished from any other.

In order to reap the full benefits of our increasingly digitalized environment, an assured way of authenticating electronic identities (eIDs) that does not fall short in a pan-national, cross-border context is required. Furthermore, organizational and technical infrastructures are needed to specify, assign and administer appropriate identity attributes. These infrastructures are known as identity management systems.

In an ideal online environment, individuals, organizations, companies, services, and devices can trust one another because reliable sources establish, manage and authenticate their electronic identities. Moreover, in such an environment we would be able to utilize secure, efficient, easy-to-use, and interoperable eID solutions. Specific objectives for such an environment include:

- high-end security, making it virtually impossible for adversaries to carry out identity theft, to perform online fraud, or to compromise online transactions;
- increased privacy and trust for individuals who can rely on their eIDs and related data being adequately protected and who have complete control over their personal data;
- efficiency and convenience for citizens, who would need to manage fewer user accounts and passwords than they do today, as well as for the public and private sectors, both of which would benefit from a reduction in person-to-person and paper-based processes; and
- ease-of-use thanks to automated eID solutions whenever feasible, and technology that is easy to operate with minimal training.

1.1 Fighting Identity Fraud

Identity-related crime has been receiving more and more attention over the past few years, and a debate about the abuse of identity documents and data – known as identity fraud – is in full swing.

Document fraud, such as fraud with ID cards, passports, or other travel documents (such as visa), has always existed. Blank documents, in particular passports or visa documents, were stolen and later used illegally, identity documents were counterfeited, authentic identity documents were used by somebody other than the owner to whom the document was issued (“look-alike fraud”).

In the course of the last few years, the focus of discussion has shifted from document theft or fraud to identity-related theft and fraud. According to the 2010 Identity Fraud

Survey Report[1], almost five percent of the U.S. population are victims of identity theft each year, with about 13 % of identity fraud crimes being committed by someone the victim knew. The costs of these crimes extend far beyond direct financial losses and include many other expenses associated with re-establishing an attacked identity. A survey found that after an identity crime, victims spend an average of 21 hours reconstructing their identities (e.g. bank accounts, credit rating, personal reputation).

Identity-related crimes have spread significantly with the increasing use of cyberspace, where the process of verification and authentication is less transparent than in an offline environment. In addition, these new communication channels and technologies are misused to fraudulently obtain confidential information such as personal and identity-related data about individuals (e.g. via "phishing"). With this information, criminals attempt to gain access to bank accounts or conclude contracts in someone else's name.

The statistics cited above identify various causes of online fraud and identity theft. Out-of-date software, unsafe web browsing behaviour or lack of appropriate anti-virus protection can all lead to compromising of computer systems. Criminals and other adversaries often exploit poor identification, authentication and authorization practices for individuals, websites, eMail, as well as the infrastructure that the Internet utilizes.

Drastic reduction of the frequency of identity fraud is one of the prime challenges facing eID programs.

1.2 ID Document Security

For many centuries, paper was the material of choice for producing secure identity documents. Nowadays, specially-designed plastic cards allow the same security-printing quality as that achieved with paper and, in addition, are able to provide reliable protection for the integrated microprocessors used in the current generation of identity documents. The Finnish national ID card issued in 1998 was the first national eID document made of polycarbonate – today all national eID documents in Europe are made of this material.

In many countries, apart from a birth certificate and a passport, the classic ID card is the main state-issued identity document, a document originally introduced in Europe around and after the time of the industrial revolution, i.e., between 1870 and 1910. Since high counterfeiting and falsification resistance requirements are placed on ID documents, it has always been usual to apply the most up-to-date security technologies of each respective period to them.

With the introduction of eID documents, the role of the classical visible document is being extended to that of its digital representative in the Internet. Before the document

[1] Javelin Strategy & Research, February 2010

can assume this digital representative role, an electronic chip must be integrated into it. It is the need to integrate the chips safely that has led to the change from paper-based document materials to plastics. Initially, communications between the document and the electronic host system were implemented using direct electrical contacts, but in recent years contactless information transmission as defined in ISO/IEC 14443 is gaining in popularity. As the infrastructure for handling bank cards with contact pads is already in place in many countries, so-called dual-interface-based eID documents that have both a contact interface and a contactless interface are still being issued.

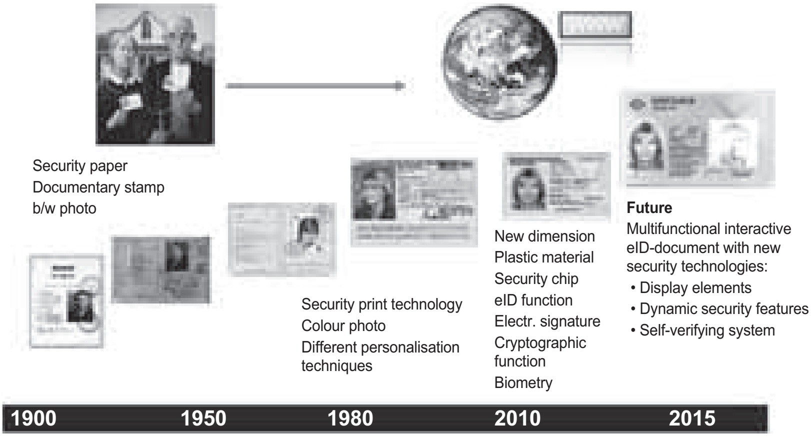


Figure 1.1 Evolution from purely visible documents to eID documents

The integration of microprocessors into ID documents has not diminished the extreme importance of the role of optical security techniques in the overall security architecture of an eID infrastructure. Over the last decades, the quality of conventional reproduction techniques (e.g. photocopiers, high-resolution photo cameras, image editing software, digital printers) has been improving steadily, which has necessitated continuous innovation of measures to combat counterfeiting. As one can see, the subject of optical security techniques covers an exceptionally wide range nowadays.

The core of modern security features are digital perforation, embossing, digital watermarking, digital printing, optically variable devices or diffractive structures which are the basis of many security elements, including holograms. These structures have a wealth of useful features, not the least of which is their ability to produce images that cannot be reproduced by photographic methods. While this is often due to their three-dimensional appearance, it can also be the result of various other chromatic effects. For a detailed discussion on security printing and optical security features, please refer to Chapter 13.

With the introduction of eID chips, optical security techniques have been complemented by cryptographic techniques. While security and privacy can be obtained in a variety of ways, cryptography is an essential tool to this end, particularly in the world of electronics. However, security is a process, rather than a static condition. In particular the field of cryptology is constantly progressing – attacks and attack tools will continue to become more sophisticated, as will cryptographic technologies and other security controls. Therefore recommendations for the use of cryptographic algorithms, keying material (e.g. key lengths) and other parameters need to be reviewed and updated on a regular basis. Chapter 14 provides an overview on the current state of the art.

In the future, technological progress is going to pose new challenges to eID documents at ever-shorter intervals. If eID documents are to meet these challenges by providing new functions, then they will not only be expected to meet state-of-the-art security technology requirements, but also requirements for user-friendliness and acceptance, for access to new business fields in the consumer market and commercial sectors, interaction with mobile devices as well as world-wide interoperability.

For eID documents to meet future technological challenges, new card-based technologies such as:

- security features that are dynamic and can be stimulated electrically,
- display technologies,
- secure data input elements and
- multimodal biometric match-on-card technologies

will have to be discussed. In this way, eID documents may become multi-functional and user-friendly digital representatives of their holders.

Consequently, the security industry needs to engage in continuous research and development aimed at designing new and innovative security features, addressing both the field of material-based security and of IT-based security including cryptographic primitives and cryptographic protocols.

1.3 Trust, Data Control and Usability

Trust and understanding are two basic preconditions that need to be fulfilled from the user's point of view, and both are closely linked to the organization and functioning of an identity management infrastructure. If potential users do not trust the system's security and do not understand its basic design and operating principles with the resulting assertions, the infrastructure is likely to remain unused or to be seen as an infringement on peoples' lives rather than as an enabler of new benefits.

End users should be willing to confide in an eID system. To this end, specific standards of security and privacy protection need to be defined and systematically evaluated. To ensure user trust, these standards must be communicated to the user community in a transparent and understandable manner.

In addition, user trust strongly relates to data control. In any eID scheme, end users should be entitled to maximum control over their own personal data. This implies that it must be left up to the data owner to grant access to her or his personal data to a service provider – either voluntarily or, in the case of justified necessity, e.g. national security issues, or emergency health care, compulsorily. However, most of today's online environment is not user-centric; individuals tend to have little control over their own personal information.

The citizen's options for utilizing a single digital identity across multiple applications are currently very limited. People are faced with the increasing complexity and inconvenience associated with managing the large number of user accounts, passwords and other identity credentials required to make use of online services provided by different organizations. The collection of identity-related information across multiple providers and accounts, together with the sharing of personal information through the growth of social networks increases the possibility of data being compromised. For example, personal data used to recover lost passwords (e.g. the name of your favorite pet, your mother's maiden name, etc.) is often publicly available.

In order to take the proportionality principle of data protection and privacy regulations into account, it is essential that users have sufficient control and awareness of what personal data a service provider will be able to access. Data control principles may also imply active involvement in issuing, extending, restricting and withdrawing credentials and in the management of personal data (including accessing and updating personal data) in order to ensure that this data remains as accurate as possible.

1.4 Interoperability

Another essential pillar of an eID infrastructure is interoperability. Interoperability facilitates the portability of identities and enables service providers to accept a variety of credential and identification media types. In an eID infrastructure, governments are not necessarily the only identity providers. Instead, interoperability could allow a variety of public and private-sector identity providers to participate in the system.

In many countries, initiatives are underway to introduce electronic identities for public services (cf. Chapter 8). In order to achieve eID interoperability, eID infrastructures need to:

- allow administrations to mutually trust each other's identification and authentication methods and to accept these methods on the basis that they were considered acceptable by the administration of origin (federation in a policy sense);
- provide for various security levels for eID services, so that the authentication requirements for a service can be tailored to the security needs of that service (multi-level authentication);
- permit a context-sensitive approach, whereby the context may be determined by the application framework or the conceptual framework within which the eIDs are used; and

- allow for participation of the private sector, whereby administrations choose to rely on private sector partners (e.g. financial institutions) for the provision of eID management services. In addition, the encouragement of the development of private sector applications that give leverage to public eID infrastructures may be necessary in order to ensure sufficient return on investment.

For a detailed discussion of interoperability aspects, please refer to Chapter 12.

1.5 Role of Personal Devices

The market for personal and mobile devices is exploding. The world's current 6.8 billion inhabitants are already using roughly 4.6 billion mobile phones, in contrast to the 1.7 billion Internet users (which includes those accessing the Internet via mobile phones), 1.6 billion television sets and 3.9 billion radio receivers. The infrastructure for operating mobile telephones is the best-developed infrastructure in the world. Particularly in the developing countries mobile phones play a more important role than radios, for instance.

New devices such as smart phones or tablet computers will continue to change the market at a breathtaking pace. These new device developments will promote mobile Internet usage by introducing new applications and business models, and the importance of eID security will increase in step with the developments. However, the main task of eID security will always be to guarantee security and privacy in Internet transactions, both in stationary devices and in mobile devices with limited resources. This means that these devices have to be integrated into the security infrastructure. Technologies such as contactless secure information transmission between eID documents and mobile devices are being implemented. In this context, near field communication (NFC) techniques are going to play a special role. Another approach might be to integrate eID functions directly into the mobile devices.

Nevertheless, mobile ID management and the use of eIDs place higher requirements on security than those already necessitated by hitherto-known attack scenarios. In this case, the challenges are posed by:

- identity theft,
- eavesdropping,
- spyware,
- surveillance,
- phishing,
- collection and storage of private information beyond the stated purpose,
- failure to recognize context,
- inadequate (for processing stronger authentication algorithms) device resources,

- intrusive authentication and
- lack of user awareness;

whereby this list is by no means exhaustive.

1.6 Privacy Protection

Privacy protection and voluntary participation are additional fundamental pillars of an eID infrastructure. eID solutions should protect anonymous entities by keeping their identity a secret and sharing only the information necessary to complete a transaction. For example it should be possible for an individual to provide relevant age information (e.g. over eighteen, over sixty) without having to disclose her or his birth date, name, address or other identification data. At the other end of the spectrum, eID solutions need to support transactions that require the maximum possible assurance of a participant's identity. The eID infrastructure has to provide the most robust access control techniques in order to minimize the risk of exploitation of information by unauthorized access. Finally, participation in an eID infrastructure should be voluntary for both individuals and organizations.

Fear of government control over databases and private-sector usage has been raised as one objection to eID infrastructures. It is important to understand that, in general, it is not the eID technology itself that provides the potential to compromise privacy, but rather the processes employed by governments and organizations that issue eIDs and conduct business transactions with eIDs. Therefore governments and organizations need to implement forceful privacy protection policies for the issuance of eID cards and to enforce strict privacy protection practices for all systems and processes related with eID transactions.

eID documents and eID cards are produced with very strong inherent security protection (refer to Section III of this book for a detailed discussion) and users can be confident that their personal information is safely stored in them. Moreover, private data are typically separated from public data so that unauthorized requestors cannot access them. In addition, eID holders should be required to authenticate themselves to the document to permit any export of sensitive data. Adopting and enforcing best practices for privacy protection and then educating citizens about the benefits of eID solutions and the measures being taken to protect eID holders' privacy are key actions that governments should take to promote eID technologies.

As far as biometrics are concerned, many eID documents only contain an electronic version of a facial image, just as traditional ID cards or passports carry a photograph. eID documents which contain fingerprint or iris pattern data in addition are provided with another layer of privacy protection, severely restricting the entities who are allowed to access the biometric data (cf. Chapters 7 and 16). Furthermore, most countries have privacy laws that restrict the dissemination of biometric information to other organizations.

1.7 How to Read this Book – a Recommendation

This book aims to offer a unique collection of contributions addressing a comprehensive range of security aspects in the field of eID solutions, while also presenting state-of-the-art concepts and current trends.

It is organized into three parts:

- Part I "Concepts and Trends" introduces basic eID concepts such as pseudonymity and anonymity (Chapter 3), documentless identities (Chapter 4) and covers key trends in the areas of public-sector and private-sector eID security (Chapters 5 and 6).
- Part II "Solutions and Practical Experiences" complements Part I by providing in-depth information on eID solutions in selected contexts and by sharing practical experience in the implementation of such solutions. Topics covered include ICAO compliant Machine Readable Travel Documents (MRTDs, see Chapter 7), European eID solutions (Chapter 8), the national approaches of Belgium (Chapter 9), Italy (Chapter 10), and Germany (Chapter 11) and conclude with a detailed discussion of interoperability aspects (Chapter 12).
- For those interested in specifics, Part III "Technologies and Standards" provides a detailed discussion of relevant technologies and standards. Areas covered include classical document security (Chapter 13), basic cryptographic techniques (Chapter 14), security protocols for eID solutions (Chapter 15), biometric techniques (Chapter 16), security features of eID chips (Chapter 17), and display technologies for eID documents (Chapter 18).

Acknowledgements

Apart from the individual authors, a number of people have helped to make this book possible. In particular, the editors would like to thank Gerhard Seitfudem from Publicis for his excellent guidance and support throughout the project. Most importantly, we are indebted to Ulrich Hamann for his vision and encouragement.

And of course we wish to thank you, our readers. We welcome your comments and suggestions, and hope to update the book periodically. If there are topics you would like us to cover or errors you think we should correct, please let us know. Compliments are welcome too, of course. Please send your feedback to publishing-distribution@publicis.de.

2 More Freedom – more Security

Ulrich Hamann

Mobile Internet and cloud computing are revolutionising how we live and communicate. They offer users the highest degree of freedom and flexibility. At the same time, they are posing new challenges for the security industry as secure identity is set to become the key issue of tomorrow.

Imagine that a man, let's call him Ebling, changes his mobile phone provider and is given a new number. Just a short time later, he realises that his new telephone number is in fact an old one, returned by a so-called Ralf who seems to be leading a fairly interesting, you could even say, spectacular life. Men and women are calling Ebling about bizarre matters. They think he's Ralf, especially since he sounds very similar. At the beginning, Ebling tries to rectify the mistake, but he becomes increasingly fascinated with Ralf's life – and decides to assume Ralf's identity, at least while on the phone. He slips into Ralf's role: as a colleague, advisor and lover. The phone calls in which Ebling pretends to be Ralf range from entertaining to scary. Gradually, the new bogus identity begins to change rather boring Ebling. Ralf becomes a part of him, Ebling not only pretends to be Ralf, he even takes on new character traits. With just a little bit of fantasy, you can imagine how this game could become very, very serious. Who's who? The lines become blurred. This is roughly how Daniel Kehlmann's novel *Ruhm* [Fame] begins.[1] But the issue is not limited to the world of novels. In reality, mistaken identities can also lead to enormous intangible and monetary losses for people, companies and governments. In the globally networked world, they pose a huge security risk.

For hundreds of years philosophers, such as Plato, John Locke, René Descartes, Immanuel Kant and Albert Camus, have deliberated on the existential question about the self and identity. Whilst a book like this may not be the proper setting for philosophical discourse, a quintessence can be drawn from the history of philosophy: the fact that, in a globalised society, identity is the basis of a person's individuality. It is also the basis for the perception of rights and obligations. We need it to apply for tax numbers, health and social insurance services, to travel to other countries and to work for international companies. State-of-the-art information technologies are increasingly transforming the way in which we communicate both at home and at work. Discussions are held in online forums where users can register with any name they choose. It's not easy to guess who PinkPanther78 might be. Business transactions are also shifting increasingly to the

[1] Daniel Kehlmann. *Ruhm*. Rowohlt, 2009

Internet: people shop online, they book summer holidays on the net, take out life insurance with a click of the mouse and manage their shares portfolios in much the same way. This all brings greater freedom but also places special demands on the security systems that are supposed to protect our personal identity. There is a number of different trends in IT and telecommunications that in the years to come will accelerate further the developments outlined above and thus strengthen the focus on the issue of "secure identity". These trends include cloud computing and the mobile Internet identified by the IT industry association BITKOM.[1]

Cloud computing enables users to access external memory capacity, computing resources and single applications via the Internet. Companies have a keen interest in this because it allows them to outsource part of their IT and to thus cut costs. This also makes them more flexible, for instance, when reorganising or merging with another company. It goes without saying that this "new working world" means new challenges for security experts. Just like the mobile Internet, it provides people with unrestricted and unlimited access to information, services and products. Intelligent devices, such as Google Nexus One and Apple's iPhone and iPad, combine mobile phone and Internet technology. They can bring even the most reluctant online user to dream of total networking. These devices allow us to communicate from anywhere in the world with friends and business partners, and to read, process and manage documents. About 11 percent of the Germans today own a smartphone, and this figure is already set to rise to more than 22 percent by 2012.[2] Across Europe, 71 million people use their mobile phones to go online for an average of one hour per day.

The new applications popular among smartphone fans are even "expanding" reality. So-called augmented reality apps display additional information on the touchscreen depending on the user's current position. Examples of the latest applications include interactive city guides which can lead the user to the next city sight or bar (like, for instance, the "Le Bar Guide" app from Belgian brewer Stella Artois) or explain stellar constellations – viewed from the user's current position ("Pocket Universe" from Craic Design). Augmented reality apps are also useful in the world of business. There is already an app available to show work nomads where they can find the next WiFi hotspot (WorkSnug, developed by Richard Leyland). With their mobile office under their arm, they can stop off at a park or café. This app works in international cities like London, New York, San Francisco and Barcelona – and since April 2010 in Berlin, too. A host of other interesting fields of application are set to follow. In complex structures or when performing maintenance work, augmented reality apps could help firemen to quickly find their way in a building or a team of architects to work together on a 3D model.

[1] Survey conducted in 2010 by the German Association for Information, Technology, Telecommunications and New Media (BITKOM)

[2] GO SMART 2012: Always in Touch, survey on Smartphone use 2010. Issued by Google, Otto Group, TNS Infratest and Trendbüro

2.1 The Mobile Internet is Transforming Lifestyles

Hans Vestberg, CEO of Sony Ericsson, believes that in five years' time there will be around three billion mobile broadband users. By 2020, an unbelievable 50 billion devices will be connected to the World Wide Web. The number of mobile PCs will also increase six-fold whilst the volume of data exchanged on the Internet will grow fifty-fold. It is particularly the so-called digital natives, i.e. those who are in fact growing up with the new interactive technologies, who are not only "always on", i.e. able to access the Internet, but who are also "always in touch". In other words, they are permanently on the Internet and hence in contact with friends and the community.

The mobile Internet is fostering not just new forms of communication but also a new way of life. And this is impacting on values in society. This development led to the formation of a new political party in Germany in September 2006: Piratenpartei Deutschland [Germany's Pirate Party]. Their agenda is as follows: The Digital Revolution, which affects all areas of life, is increasingly threatening people's dignity and freedom. The Party has committed itself to defending this dignity and freedom. But it is not just the supporters of the Pirate Party who hold dear the *freedom* which the Internet offers. For the majority of online users, freedom is the greatest asset. Scientists at Trendbüro Hamburg reached this conclusion after analysing 150,000 digitally published user opinions taken from blogs, forums and communities. They compiled their findings in a study titled "Value Index".[1] Users weighed freedom up against one other important value: *security*. The community is ambivalent when it comes to this issue. Whilst government security policies tend to be regarded in a negative light and seen more as a form of control, users are willing to sacrifice data security on the Internet in order to remain flexible and act freely. In this context, the authors of the Value Index used the term "relative security". "Users are in no way under the illusion that complete data or network security is possible on the Internet. What's more important is to achieve relative security, i.e. to be one step ahead of the threat."

2.2 Secure Identity in the Digital World

This is a challenge that must be taken up by politics, science and the private sector. Systems and products must be developed here to secure identity, always staying one step ahead of potential threats. Prior to the launch of the World Wide Web, identities were checked in a local, physical setting – either at borders, during police checks, at public authorities or when closing business deals. In the analogue world, the party doing the checking had to rely on the protection against forgery offered by the security features of traditional ID documents. The holder of the document was not able to determine which of the personal data in the document was to be disclosed because all the data was visible on the document. In today's digital world, this type of ID verification would be com-

[1] Value Index 2009, issued by Prof. Peter Wippermann, Maria Angerer, Trendbüro – Consultancy for Social Change

pletely insufficient. What is needed now is secure electronic proof of identity. With the new electronic ID cards (eID cards), citizens have full control over their data. The only personal data which the checking party can read is the data actually released by the card holder.

The key preconditions for secure electronic proof of identity are doubt-free data capture methods, reliability authentication and authorisation methods, as well as secure hardware and software. It must also be possible, of course, to use eID documents as proof of identity and to check their authenticity in both the real and virtual world. The *new German ID card*,[1] which is available to citizens since November 2010, fulfils these criteria. The personal data, a digital image and, when explicitly requested by the user, two fingerprints, are stored on a chip on the eID card which is the size of a credit card. The combination of digital image and fingerprints makes the new ID card particularly difficult to forge and protects it against misuse. What's important here is that the biometric data [see box below] can only be accessed by government authorities, such as the police

No-Mistake Identification with Biometric Data

There are basically three ways to authenticate a person, i.e. to check their identity: knowledge, possession or being. An artificially generated code, a PIN or a password, for instance, requires knowledge. A card in the possession of an individual is assigned to that individual merely for a certain amount of time and at random. Features of being, on the other hand – like physical features or behaviour – are direct and usually permanently linked to a person. They cannot be deliberately or involuntarily separated from that person. Biometrics uses physical characteristics to clearly identify individuals. These characteristics include, for instance, fingerprints, facial features or the details of the iris. Biometrics is hence the science of counting and (physically) measuring living beings. In contrast to possession and knowledge, biometrics has considerable advantages to offer when it comes to authenticating individuals. The user is identified on the basis of his individuality. Unlike passwords, PINs or access cards, a person can't pass on, forget or lose his or her biometric features. They cannot be stolen by others. What is necessary is for the physical features to be correctly attributed to an individual. Then the data saved can be directly compared with the person physically present and thus clearly identified.

A host of application scenarios are already being applied in practice today:[1] In pilot projects, biometric methods are securing access to high security areas, tele-workplaces, border crossings and sensitive patient data. But personal data needs very special protection. Apart from identification on the basis of face, fingerprint and iris data, the next generation of biometric methods enables 3D facial recognition, gesticulation and voice analyses, behavioural analysis as well as multi-biometrics, i.e. recognition of several of the above features. The eID cards of the future will come with integrated colour displays which will, for instance, be able to play back video sequences. Another possibility is that machines will be fitted with biometric sensors and be able to provide authenticated users with additional information.

BITKOM, Biometrics – reference projects, 2nd edition, 2009

[1] For detailed information about the new ID card, go to: www.personalausweisportal.de

or border control officers. This data is protected by Extended Access Control (EAC), a special security protocol [see Chapter 15].

The new ID card will be the “alter ego” of its holder on the net and will make business transactions and dealing with public authorities much more convenient and secure. That is because the online ID function of the new ID card means significant benefits for citizens, public authorities or service providers, such as banks. To use the ID card, the citizen and provider of an online service have to mutually authenticate each other. This means that the citizen can rest assured that the party checking the data is in fact authorised to read the citizen's data. Alternative ID methods, such as the time-consuming Postident method or online banking that rely on PINs and TANs could soon be a thing of the past. Incorrect address data or forgotten passwords would become a faded memory. Media inconsistencies would no longer exist and processes would be faster. By integrating electronic identity, online service providers would gain a lead over competitors. Thanks to greater convenience for the user, for instance, fewer people would abort the process of opening an account online. At the same time, transactions are more secure because phishing, i.e., attempts to obtain data and passwords from Internet users using fake Internet addresses, would no longer be possible. And finally, the new document also makes age verification possible. Additional functions, such as the qualified electronic signature, mean that contracts can be signed and finalised online.

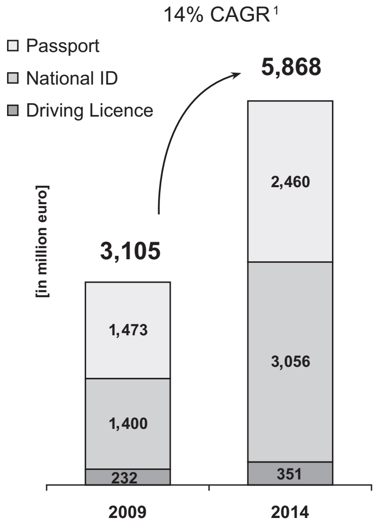
2.3 Standards are the Key to Widespread Use

Since there can be no absolute security in the digital world either, trust in the business partner determines whether or not an online transaction takes place. A reliable eID service provider is what's needed in order to create trust. This will usually be a so-called trust center that reliably steers processes in the background and meets with the highest security requirements. The trust center checks the citizen's digital ID features for the online service provider and the authorisation of the online service provider for the citizen. As a trustworthy, third-party authority, it confirms the identity of the business partners. However, this does mean that both parties – citizen and online service provider – must have the required reading devices or certificates, respectively. This is the only way to ensure secure data reading and transmission. Reading devices for home use are already available on the market. They are, however, only one part of a solution favoured by the industry. This is because the citizen has to actively obtain and install the device. And this device can only be used at one place – i.e., at home. A much more interesting and convenient option is the use of mobile phones with Near Field Communication (NFC) technology as reading devices. This is all the more interesting when we consider the previously mentioned development towards mobile Internet.

Although NFC-enabled phones are already available on the market, NFC and ISO/IEC 14443, an international standard series for contactless smartcards, will have to be compatible if these phones are to be a success. This is the goal being pursued by the NFC Forum founded back in 2004. Bundesdruckerei is involved in this forum along with founders NXP Semiconductors (formerly Philips), Sony and Nokia, as well as other companies. This is because NFC is a key precondition for eID cards and their functionality to be used on the mobile Internet as well. At the same time, experts expect that the growing number of eID card holders will also significantly boost demand for NFC-enabled smartphones. eID will thus also stir up the market for mobile phones.

2.4 Electronic Identities are an Economic Factor

On the whole, secure electronic identities are of growing importance for the economy. 72 percent of German adults use the Internet.[1] 42 percent shop online[2] and eCommerce sales in 2009 totalled €15.5 billion.[3] 38 percent of people conduct bank business with a click of the mouse.[4] Worldwide, there are already around 1.6 billion online users,[5] which is about 20 percent of the world's population. That's a huge market potential. According to Pira International, a market research institute, global sales with national ID cards will increase from 1.4 billion in 2009 to around 3.1 billion in 2014 (cf. Figures 2.1 and 2.2). This corresponds to annual growth of approximately 17 percent.[6]



Source: Pira 2009
1 Compound Annual Growth Rate

Figure 2.1
Growth of eDocuments worldwide

[1] Forschungsgruppe Wahlen, second quarter 2010
[2] Eurostat 2009
[3] GfK 2010
[4] Eurostat 2009
[5] Centre for Science, Society and Citizenship Rome
[6] Pira International 2009

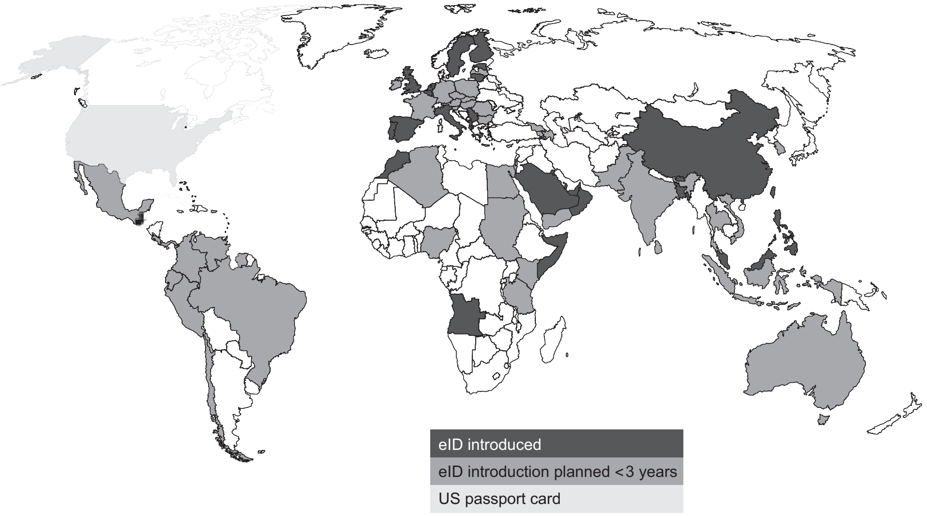


Figure 2.2 Introduction of eIDs all over the world

It is no wonder, therefore, that the security industry is booming. There are 220 companies in the security industry in Berlin-Brandenburg alone.[1] They provide around 24,500 jobs, generating sales of €2.43 billion.[2] The region hence has the potential to become Europe's leading centre for secure identity. In light of this, it makes sense to combine individual areas of competence and to form strong networks. This not only helps to promote innovation and gain a lead over international competition, it also creates greater public awareness of the enormous relevance of tomorrow's "secure identity" as an issue of tomorrow. The worlds of business, science and politics must align their efforts with these goals. Bundesdruckerei's secure ID strategy is tailored to these goals and based on three pillars.

Research and product development form the first pillar of the company's strategy. Since 2007, Bundesdruckerei has been collaborating with various Fraunhofer institutes. The partners have successively established four so-called Security Labs in Berlin and Potsdam. Another is set to open in 2010. The different projects underway are primarily geared towards developing new security features for electronic ID cards, protecting ID documents better against forgery and making online transactions secure, reliable and user-friendly. Bundesdruckerei is also actively involved in the regional innovation cluster of Fraunhofer-Gesellschaft. This innovation cluster is a network of different Fraunhofer institutes, universities and industrial partners that aims to combine forces for defined research tasks. The different research activities have led, for instance, to the 3D Face project in which future ID documents will feature a video sequence of the ID card

[1] Includes security technology, IT security and security services.

[2] Senate Department for Economics, Technology and Women's Issues, study titled "Security Industry in Berlin and Brandenburg", 2008