

eID SERVICE
POCKET GUIDE
— 2011



CONTENTS

05	SECTION 1 IDENTITY MANAGEMENT IN THE 21 ST CENTURY
11	SECTION 2 THE NEW GERMAN ID CARD – FACTS AND FEATURES
17	SECTION 3 THE TECHNOLOGY IN DETAIL
27	SECTION 4 IDENTITY MANAGEMENT AT WORK – APPLICATION EXAMPLES
31	SECTION 5 OUTLOOK: eGOVERNMENT WITHOUT BORDERS
36	QUESTIONS AND ANSWERS
41	GLOSSARY

SECTION ___ 1

IDENTITY MANAGEMENT IN THE 21ST CENTURY

She didn't see it coming. A simple trick was all it took. With a fictitious e-mail address that contained the victim's name and date of birth, the criminals had been ordering expensive goods from mail order companies for months.

Numerous dunning letters landed in the letterbox of the woman whose identity had been stolen, a journalist with the weekly newspaper "Die Zeit". It took weeks and the help of a specialist lawyer to get to the bottom of the mistake at credit agencies and public authorities. "Kafka couldn't have described it any better," explains the author in her article on identity theft.¹ Today, she is no longer willing to disclose her date of birth and occupation in social networks.

This example shows that nobody in Germany is immune to this new form of fraud that has made its way into our lives through the Internet. Every year, more than 11 million US citizens fall prey to similar crimes. The US International Trade Authority estimates that the damage caused in the US alone totals 52 billion dollars each year. In Germany too, criminals are increasingly trying to capture other people's identities on the Net.

Up to now, citizens in Germany have refused to allow this to interfere with their fun in the online world: 72 percent of German adults

use the Internet and 42 percent shop online. According to market research company GfK, eCommerce sales in Germany in 2009 totalled an unprecedented 15.5 billion euro. A good 70 percent of citizens, however, are increasingly concerned about transactions on the Net and fear that their identities could also be misused.²

WHAT EXACTLY IS IDENTITY THEFT?

Specialist literature comes up with different definitions for the term identity theft. It usually means "gaining unauthorised possession of an identity": A perpetrator gains possession of another person's identity, i.e. of certain data through which the victim can be clearly linked to a certain context. In this case, criminals combine, for instance, the name and credit card data, name and address or even the name and date of birth.³ This theft is often followed by fraud in order to obtain a financial gain or to ruin the victim's reputation. Around one third of all identity theft still takes place today in the real, physical world where fraudsters use the data of a stolen ID card, for instance, to place orders for themselves. In two thirds of cases, however, the data used by fraudsters for criminal attacks is already being obtained on the Internet – a situation that is often made easy when citizens all too freely disclose their data. The police estimate that victims of online identity theft need to invest an average of around 400 working hours in order to eliminate the damage caused and to prevent further misuse.⁴

UNCERTAINTIES FOR USERS AND PROVIDERS

Irrespective of whether a person wants to open a bank account at a local bank or via the Internet, proof of identity must be furnished as required by the Money Laundering Act and the German Tax Code. Either an ID card can be presented at the bank or the Postident method can be used. Anybody ordering from a web shop must disclose their identity. The same applies when booking a trip, transferring money online or accessing an eGovernment service. But other service providers, such as social networks and forums, require that their customers disclose personal data and hence their identity on the Internet. All of this data is frequently not really necessary for a transaction.

For people using online transactions with government agencies, data protection, data security and reliable systems are very important. With a view to these eGovernment services, however, only a third of users claim that their data protection is good or very good.

Many criticise media inconsistencies in numerous eGovernment services. Although an application form can be downloaded and completed online, many found it annoying that the form then has to be returned by post to the agency. Users today also need a vast number of user names, changing passwords and PINs in order to protect themselves against fraudsters on the Net. Travel bookings and especially online banking hence become tiresome processes where identities and authorisation are verified in an extremely complex manner. Anybody wishing to conclude legally valid contracts from the comfort of their own home needs an electronic signature card and the required hardware and software. The scope of the German Act on Digital Signature that provides the legal framework for electronic signatures is proof of just how complex this matter is. For many people, these procedures are simply too demanding. They soon become lost in the data jungle and in an effort to keep things simple use the names of relatives or other easy to guess passwords, thus making life easy for online fraudsters.

On the other hand, when it comes to eCommerce, suppliers often lack security especially since systems that provide reliable ID verification are often very expensive. In addition to the matter of price, integrating systems like these is very time-consuming and difficult. No web shop operator knows for certain whether the young man who has just ordered an adult film is in fact of a legal age. Although the Interstate Treaty on the Protection of Minors requires that providers verify the age of their customers, it is not possible to verify without doubt whether the copy of the ID document submitted actually belongs to the person placing the order.

IDENTITY AS A FOUNDATION

What is identity? What is it about identity that makes a person unique? Such issues, which in earlier times were left to philosophers to discuss, are now top of the agenda in the age of the Internet. Per definition, identity is the set of characteristics by which one individual can be distinguished from another. Identity should not be confused with the roles a person has in day-to-day life – as an employee, a judge or a doctor, for instance, as a father or as a user with a chosen fantasy name on the Net.

Unlike these flexible roles, identity is the foundation of individualism. It is the basis upon which citizens can exercise rights and

fulfil obligations in both their public and professional lives. Identity is needed in order to apply for tax numbers, health and social insurance benefits, to travel to other countries and to work at international companies. The more mobile a person is and the more global business processes are, the more urgently security measures are needed to protect this identity.

There are various ways in which to check an identity, i.e. to verify a person. Individuals can identify themselves either through knowledge, i.e. by stating a code, a password or a PIN. Or they can authenticate themselves through possession of an object, for instance, a card that is assigned to the individual at random and for a certain amount of time. The third possibility is authentication through biometric data – physical features that can be neither passed on, forgotten nor lost.

FROM CONVENTIONAL ID DOCUMENTS TO STATE-OF-THE-ART ID CARDS

Conventional ID documents have reached their limits today. It is impossible on the Net to check identity through the physical presentation of the document. It is not sufficient to request a copy of the ID document or to simply trust that the security features in traditional ID documents are forge-proof. In a global, mobile and virtual environment, a completely different method must be used to verify whether a person is in fact who he or she claims to be.

Technologies that guarantee secure identities without physical verification will hence become the key technologies for modern society. All the more so, since the Internet is developing further and new trends are cropping up: cloud computing, for instance, allows users to access external memory space via the Internet – which is only safe when it is ensured that nobody with a false identity can gain access. The huge success of smartphones is also promoting even greater networking and hence the greater need for more secure identities. Today, 11 percent of Germans already use this kind of device. Estimates state that by 2012, more than 22 percent⁵ will access information world-wide using their smartphones.

This is also changing user lifestyles at a rapid pace. Always online is considered to be normal. Almost 70 percent of people state that they are on the Internet every day and almost never switch

off their mobile phones.⁶ This is why it is so important to make people more careful about disclosing their personal information. Having control over one's data and not disclosing more than necessary – that's a top priority, especially since it will never be possible to achieve complete data and network security on the World Wide Web. Whilst most users are aware of this, they increasingly find it difficult to adequately protect themselves against attacks by online fraudsters. Only 37 percent, for instance, use hard-to-hack passwords and change these regularly.⁷

FIGURE 1: SECURE ELECTRONIC IDENTITY

ANALOGUE WORLD	DIGITAL WORLD
<ul style="list-style-type: none"> - Border traffic - Police checks - Public agency traffic - Business processes 	<div style="border: 1px solid black; padding: 5px; display: inline-block; margin-bottom: 10px;">eidentity</div> <ul style="list-style-type: none"> - eGovernment - Business processes/eBusiness
<p>Requirements: A trustworthy issuing authority</p> <p>Traditional ID card</p> <ul style="list-style-type: none"> - Trusting that security features are forge-proof - Degree of recognition of the document 	<p>Future eID card</p> <ul style="list-style-type: none"> - Trust in the verification authority - Secure data transmission and processes - Protection of personal data - Technical infrastructure
<p>- Limited data control All personal data is optically read from the document</p>	<p>+ Full data control Only data approved by the citizen can be read</p>

GERMANY AS A PIONEER

Politics, science and companies in the high-security sector must join forces to take up this challenge and to provide citizens with identity management solutions that are easy to use. 20 percent of the population is already on the Net and this highlights the huge market potential that secure electronic identities have to offer. The continued growth of eCommerce as well as the development of eGovernment will depend heavily on how easily and securely identities can be verified on the Internet. The global market for ID systems has already grown rapidly in recent years. Market research institute Pira International forecasts that sales with such cards will increase from 1.4 billion euro in 2009 to around 3.1 billion euro in 2014. This represents annual growth of around 17 percent. In recent years, numerous different solutions have been launched on the market in Europe alone. The European

Network and Information Security Agency (ENISA) plans to harmonise today's ten different ID concepts within the scope of a multinational eCard strategy.

Compared to other countries, Germany is one of the pioneers in the development of ID systems and cards. Germany's government was quick to pave the way here with its eGovernment 2.0 programme which it adopted in 2006. Since 1 November 2010, citizens of the Federal Republic of Germany have one of the world's most advanced ID documents available to them. Just how this card can be used is subject to the provisions of the German ID Card Act. The new ID card is more than just photo ID. With its online ID function and the qualified electronic signature (QES), it helps to achieve a completely new level of quality in communication and transaction security on the Internet. With very little effort, citizens can now protect themselves against identity theft.

What makes this ID card so unique is that it is part of a complex and highly secure system. Apart from the ID card itself, the central components of this system are the so-called AusweisApp software, the authorisation certificates and the security protocols and especially the eID Service. This service allows private companies and public agencies which possess the required authorisation certificates to read out the personal data stored on the chip of the ID card. Pursuant to German data protection regulations, which are very strict compared to other countries, only companies which meet with high requirements are authorised to offer an eID Service. With its accredited D-TRUST trust center, Bundesdruckerei provides such a high-performance service that is rooted in extensive experience in the management of electronic identities. Instead of having to invest heavily in order to set up their own infrastructures, providers can now use this eID Service to open the door to greater security for their customers on the World Wide Web.

SECTION ___2

THE NEW GERMAN ID CARD – FACTS AND FEATURES

The new German ID card was the centre of much attention even before it was introduced on 1 November 2010. Experts had been quick to point out that the new ID card could serve as a central element of secure identity management on the Internet.

In June 2010, Germany's Federal Ministry of the Interior (BMI) was awarded the European Identity Award for the new ID document at the European Identity Conference 2010. The Kuppinger Cole analysts thus honoured the "innovative and well thought-out concept that addresses concerns about data security in an exemplary fashion". This triggered the curiosity of many an innovation enthusiast who on 1 November applied straight away for the new ID document in credit-card format.

The Federal Ministry of the Interior laid down the specifications of the new ID card. Bundesdruckerei is responsible for production and for the technical infrastructure in which the ID card is embedded. The company produces the documents and equips the around

5,500 passport and ID card offices with hardware and software components (for instance, update terminals and fingerprint scanners).

NEW APPLICATIONS

Citizens can use the new ID card for all the same purposes as its predecessor, however, the new card is much more versatile. The online ID function and the qualified electronic signature (QES) are two new applications which make online transactions more convenient and secure. Citizens themselves decide if and when they wish to use these functions. The new ID card is the first widely used, standardised ID document with which citizens can identify themselves on the Internet. At the same time, the new card allows users to retain control over their data at all times.

As a handy document in credit-card format, the new ID card can still be used as so-called photo ID, for instance, in police checks. Its ID1 format is the same format used for many standardised smart cards and is similar in size to the European driving licence card. Measuring just 86.50mm by 53.98mm, the compact ID card fits snugly into any wallet.

The card bears its own specially designed logo on the back, featuring two opposing semicircles to indicate that citizens can use the card in both the real world and the virtual world. At the same time, the circles are designed to symbolise the authentication that is mandatory for both parties in online transactions. Both the ID card holder and the service provider or public agency must clearly identify themselves so that an online transaction can take place.

Just like its predecessor, the new ID card with its optical, tactile and holographic features, as well as the security protocols used, is among the most secure documents world-wide. Fine, interlaced patterns, so-called guilloches, along with microlettering, special colour effects and tactile surface structures, make the ID card impossible to forge.

THE SECURITY CHIP AS THE HEART OF THE CARD

With a six-digit access number on the front and a data field on the back for postcode and artist's pseudonym/religious order name, the new ID card also contains more information than its predecessor.

when placing orders that require that the customer is a certain age, the precise date of birth does not have to be disclosed. The AusweisApp software sends a simple “yes” or “no” reply to the question as to whether the age criteria are fulfilled or not.

The so-called AusweisApp software is a special driver software that is needed in order to use the online ID function. This software and an approved card reader must be installed on the computer before communication with the ID card is possible. Furthermore, business partners on the Internet must explicitly offer identification with electronic proof of identity and first identify themselves as authorised online partners. Such authorisation is only granted to companies that are willing to provide precise details of their services, their place of business, their data protection rules and the reason for the potential data requests. These companies, however, are only permitted to access precise, previously defined data categories. This means that citizens know who they are doing business with and the service provider can also rest assured that the data received is in fact correct. This fulfils the principle of mutual authentication which is one of the core elements of secure online transactions.

LEGALLY BINDING SIGNATURE

The qualified electronic signature (QES) enables legally binding contracts, powers of attorney or applications to be signed online. The QES is legally equivalent to the personal, hand-written signature. Unlike the online ID function (eID) with which users can quasi present themselves (“that’s me”), the QES is used to declare that the user agrees to a certain circumstance (“I agree to this”).

In order to use this function, the online ID function must be activated and the user requires an individual eID PIN along with an additional signature PIN. The user can obtain this and the necessary signature certificate from an accredited certification service provider (CSP), such as D-TRUST, Bundesdruckerei’s trust center. While a basic reading device is suitable for using the online ID function, an advanced reader is required in conjunction with the QES. During the signing process, the user places his or her new ID card on the device and enters the signature PIN.

CLEAR IDENTIFICATION

The sovereign ID functions are solely relevant for dealings with government authorities and agencies. Nobody apart from the police, border and customs control authorities, the tax authorities of the federal states of Germany and the registration authorities can access these functions. These authorities, however, cannot read out this data without the holder’s knowledge. A corresponding authorisation certificate is also needed here which is issued by the CSP. The ID card holder must also be present in person and show the document so that the data can be read out. Only then can a staff member using a special reading device capture the access number printed on the card. This method is used, for instance, during ID checks at borders or when a change in address is entered at registration offices.

There are several options available to service providers who wish to offer their customers the online ID function or the QES. Basically speaking, they can develop the corresponding hardware and software themselves and hence control for themselves the entire communication with the customers’ AusweisApp software and the related administration processes. They are required, however, to comply with the applicable technical guidelines.⁸

For most online providers, however, this would mean investing heavily in personnel and material. That’s why many providers opt for the so-called eID Service provided by accredited CSPs like D-TRUST, Bundesdruckerei’s trust center. The CSPs have considerable experience in the management of digital identities and provide a powerful infrastructure for this purpose. The service provider does not have to set up his own eID server in order to enable his customers to use the online ID function or the QES. Instead, the eID Service handles the entire communication with the ID card chip and ensures that both the authorisation certificates and the revocation lists are always up to date. This saves service providers from having to invest heavily in the necessary systems or having to operate such systems. At the same time, transactions with customers are ideally secured. The eID Service can be integrated quickly into the service provider’s IT system architecture so that the online shop can enjoy the benefits of the new ID card applications with a minimum of effort and cost.

SECTION 3 THE TECHNOLOGY IN DETAIL

The new German ID card is part of a complex, high-security eID system architecture. Apart from the ID card itself, the main elements of this system are the reading device, the AusweisApp software and the so-called authorisation certificates. The eID Service links these components and enables citizens and service providers to communicate with each other and complete business transactions on the basis of the online ID function. In other words, it provides the participating parties with the space where they meet.

Put simply, the dialogue between the participants is as follows:

1. A citizen wishes, for instance, to buy a product from an online shop and wants to identify himself to the service provider using his online ID function. To do so, he sends a request to the service provider.

2. In order to clearly authenticate the buyer's identity, the request is passed on to the eID Service.

3. The eID Service first authenticates the service provider and then passes on the service provider's authorisation certificate to the user (see below). Now, and only now does the eID Service access the data stored on the chip which has been approved for disclosure to the service provider.

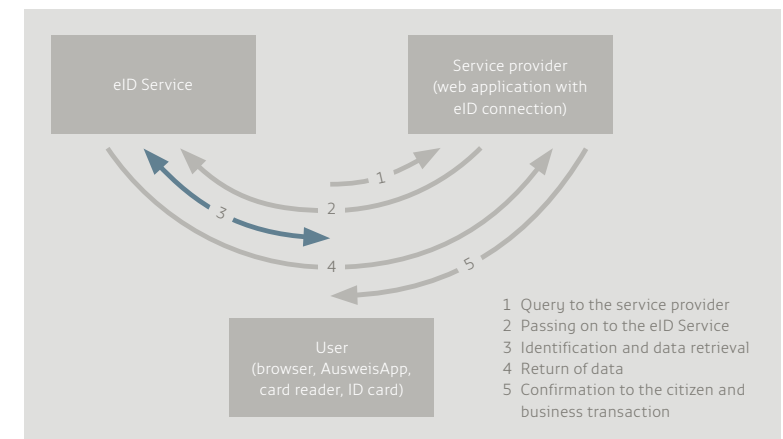
4. A mask on the citizen's PC shows the data selected for transmission. If necessary, the citizen can restrict this data. The eID Service then transmits the information selected to the service provider.

5. Finally, the service provider confirms the buyer's request and triggers the next steps, i. e. shipping of goods and issuing the invoice.

The eID Service hence enables mutual authentication of both parties on the Internet.

In order to make use of the comfort offered by the online ID function, citizens and service providers must create the necessary pre-conditions. They need, for instance, special hardware and software in order to be able to read out the data stored on the chip. On the other hand, they must prove their authorisation with the necessary certificates.

FIGURE 3: THE eID SERVICE



STARTER KIT FOR ID CARD HOLDERS

Citizens themselves decide whether they want to use the online ID function and QES. If so, the following steps must be taken in order to use the functions for transactions on the Internet:

- > **PIN:** The card holder must authorise each data transmission using their six-digit PIN. After applying for a new ID card, the citizen first receives a PIN letter from Bundesdruckerei before collecting the document. This letter contains the five-digit transport PIN, the unblocking number (PUK) and a disable password. The card holder should immediately replace the transport PIN with a secret number of their own.
- > **PUK (Personal Unblocking Key, also unblocking number):** The PUK is a ten-digit number that is known only to the ID card holder. It is made up of numbers only. If an incorrect ID card PIN is entered three times, the PIN will be disabled. This can be reversed by entering the PUK.
- > **Disable password:** The disable password is a word that is easy to remember (e. g. train). If the ID card is lost or stolen, the holder must have the ID card and its functions disabled using the disable password. The password in question is only known to the ID card holder and the issuing authority. Unlike the PIN and PUK, the user does not enter the disable password on the computer. Instead, the disable hotline staff or the ID card authorities ask for this password when necessary.
- > **Reader:** BSI-approved readers are commercially available. The citizen can recognise this by the circular green and blue logo of the new ID card.
- > **Certificate:** Citizens require a certificate in order to be able to use the QES of the ID card. This certificate can be obtained from a certification service provider (CSP), such as Bundesdruckerei.
- > **Signature PIN for the QES:** The ID card holder uses the signature PIN in order to electronically sign a document.
- > **Driver software:** The AusweisApp software makes it possible for the ID card and the computer to communicate with each other.

This software is available for Windows, Linux and Mac OS and can be downloaded for free at: www.ausweisapp.bund.de.

STARTER KIT FOR SERVICE PROVIDERS

Service providers must fulfil clearly defined requirements pursuant to Section 21 of the German ID Card Act and prove such compliance in writing. They also require the following in order to integrate the online ID function or the QES into their range of services.

- > **Authorisation:** The Issuing Office for Authorisation Certificates (VfB), a unit of the Federal Office of Administration, requires that the service provider make a voluntary declaration concerning data protection. The service provider must also demonstrate to what extent the data which is to be read out is required for the service provided. The authorisation granted by VfB is valid for a maximum period of three years.
- > **Authorisation certificates:** Once authorisation has been granted, the company can sign an individual service provision agreement with a CSP. D-TRUST, Bundesdruckerei's trust center, is one such a CSP. The authorisation certificates authenticate the service provider. They are valid for just a few days only and are automatically renewed on a regular basis. If there is any suspicion of data misuse, the certificates are no longer issued.
- > **eID Service:** This is provided by a high-security company with which the service provider can enter into an agreement. Using the authorisation certificate, Bundesdruckerei's eID Service makes it possible to read the data stored on the chip of the ID card.
- > **SAML 2.0 token:** SAML stands for Security Assertion Markup Language and is a standard for the secure exchange of authentication and authorisation information between domains. SAML assertions are statements which an eID Service provider uses as a basis for granting access to certain services. The SAML token contains information from the ID card and is made available to the service provider for its further use.
- > **Token certificates:** They permit the service provider to access the eID Service. The related private service provider key is known only to the service provider and the eID Service key

is known only to Bundesdruckerei. The SAML 2.0 tokens are signed with these keys and then encrypted for the recipient. This hence establishes a second individually secured connection within the SSL tunnel.

- > **SSL certificates:** SSL stands for Secure Sockets Layer and is a security protocol. This enables secure data transmissions on the Internet. Service providers require SSL certificates in order to encrypt communications with their website users. These certificates can be obtained from a CSP.

ADVANTAGES OF THE eID SERVICE

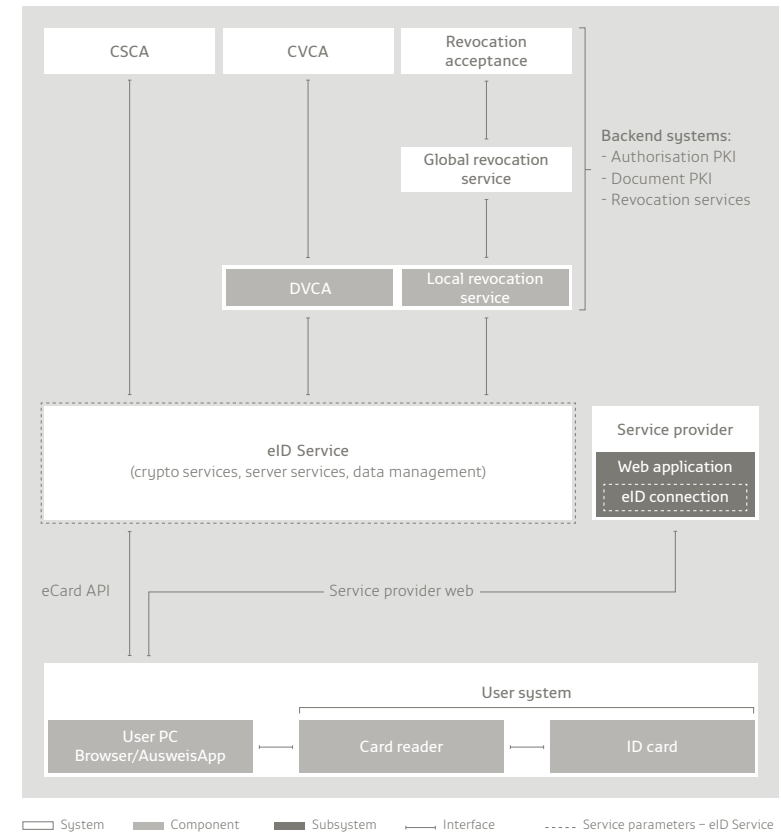
Equipped like this, service providers can enjoy all the benefits of the eID Service and gain a lead over competitors. Banks and insurance companies can clearly identify applicants and comply with the requirements of the Money Laundering Act. When opening an account or taking out insurance, the other partner to the contract can be legitimised on the PC, thus making it no longer necessary to appear in person. Electronic ID is attractive for both citizens and service providers. That's because it is media consistent and saves time and money. Some suppliers have age restrictions on their goods and are hence required to ask their customers' age. This is now easy with age verification provided by the eID Service.

The age verification application, as well as other applications, such as confirmation of place of residence or the pseudonym function are further interesting options which service providers can make available to potential users on their websites. The eID Service reads out the data required for the specific transaction.

A special server (the eID server) forms the heart of the eID Service. As a hardware and software component, the server enables communication between the card holder's PC and reader terminal and the service provider. It transmits and manages the authorisation certificates of the service provider, checks the authenticity of the chip in the ID card and reconciles revocation lists. The eID Service has two interfaces; an internal interface and an external interface. The internal interface complies with the BSI's eCard API Framework (TR-03112) and enables the exchange of information with the ID card. It includes cryptographic protocols, as well as PACE and EAC access control. The external interface

supplies the data stored on the chip of the ID card to the service provider via an internationally standardised token (SAML 2.0 Assertion).

FIGURE 4: SYSTEM OVERVIEW



TRIED-AND-TESTED SECURITY MECHANISMS

Various protocols and methods protect the personal data stored on the chip. They also check the authenticity of the new ID card and make it impossible to forge. Solutions that secure the contactless interface between the ID card and the reading device are very important in this context.

The Federal Office for Information Security (BSI) has defined the following protocols and measures:

- > **PACE:** Password Authenticated Connection Establishment
Access control that protects against reading of the contactless chip
- > **EAC:** Extended Access Control
Extended access control that is made up of two sub-protocols, i. e. CA (Chip Authentication) and TA (Terminal Authentication)
- > **PA:** Passive Authentication
Checks the authenticity and integrity of the data on the chip
- > **RI:** Restricted Identification
Generation of chip-specific and user-specific pseudonyms
- > **PKI:** Public Key Infrastructure
Hierarchy of digital certificates: CSCA (Country Signing Certification Authority) and CVCA (Country Verifying Certification Authority)

Source: Federal Office for Information Security (BSI)
"Innovations for an eID architecture in Germany"

- > **PACE**
Password Authenticated Connection Establishment
PACE ensures that the contactless chip in the new German ID card cannot be read out unless the six-digit eID PIN is entered. This PIN is only known to the holder. PACE access control also ensures that data is encrypted for transmission to the reading device.
- > **EAC**
Extended Access Control
EAC contains different protocols. EAC comprises the Chip Authentication (CA) and Terminal Authentication (TA) sub-protocols. These are executed together with PACE and Passive Authentication (PA). CA establishes a secure connection to the chip and recognises cloned chips. TA protects the sensitive

data of the new ID card against unauthorised access. The chip then only releases certain data for reading if the reading device proves that it is authorised to access precisely this data.

- > **PA**
Passive Authentication
PA checks the authenticity and integrity of the data on the contactless chip. Only the ID card producer officially commissioned by the German Federal Ministry of the Interior (BMI), i. e. Bundesdruckerei, is authorised to save data on the chip of the new ID card. This data can be edited at registration offices using update terminals. During production, Bundesdruckerei digitally signs the data saved using the so-called document signing certificate. This, on the other hand, is signed with the Country Signing Certification Authority certificate (CSCA certificate) of the nation issuing the ID card. When the ID card is read, PA is used to verify the signature of the chip and trace it back to the CSCA certificate.

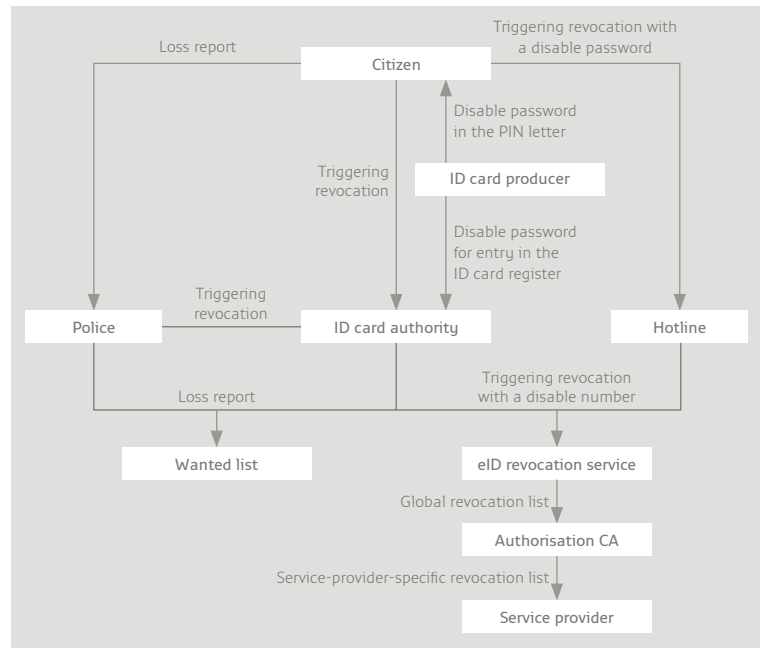
- > **RI**
Restricted Identification
RI automatically generates pseudonyms for an individual chip and a certain provider. This enables the service provider to recognise the chip based on the previously received pseudonym – without reading out the personal data. Different pseudonyms are generated for different service providers. It is hence not possible to compare pseudonyms from different service providers, for instance, and to exchange information about the user. This method serves the interests of data protection.

BMI has commissioned several studies to examine how secure the protocols used are. Within the scope of a study in which the security of the EAC protocol was analysed⁹, Technische Universität Darmstadt examined whether sensitive data remains confidential when the protocol is executed and whether authentic participants can successfully identify themselves to the partner. In their final report, the study managers noted: "The cryptographic methods ensure sufficient security in this respect". And Gelsenkirchen University of Applied Sciences, which specialises in Internet security, noted in the report on its study on the residual risks in conjunction with the use of AusweisApp software¹⁰ that: "Compared to conventional authentication with passwords, the eID function has a higher security level".

REVOCACTION MANAGEMENT

What happens, however, when an unauthorised individual uses an ID card which they have stolen or found? This is where the revocation management function of the electronic ID card comes into play. The ID card holder is obliged to inform the respective authority if the ID card is lost. This authority then orders the revocation list operator to revoke the ID card, it records the card in the ID card register and immediately reports the loss to the police pursuant to Section 11 (5) of the German ID Card Act. Once entered in the revocation list, the online ID function can no longer be used. This ensures that no services can be performed for the person currently in possession of the ID card. If the original ID card holder used the QES function, this must also be revoked by the CSP that issued the card holder with the signature certificate. The so-called global revocation list is managed by the German Federal Administration Office (BVA), regularly updated and made available to the CSPs.

FIGURE 5: REVOCATION MANAGEMENT – GENERAL OVERVIEW



Customary smart cards, such as cards for the qualified electronic signature, are usually revoked via a chip-specific public key. This is reconciled using a revocation list. This feature is a personal feature because it clearly identifies the chip and its holder. The data-protection friendly design of the electronic ID function does not permit this kind of mechanism.

With this in mind, revocation lists are generated on the basis of specific service providers. When sending electronic proof of identity, each ID card transmits a service-specific and card-specific revocation feature to the service provider. The service provider compares the revocation feature with his individual, service-provider-specific revocation list. It is the task of the CSPs to create for each service a service-provider-specific revocation list from a global revocation list.

This method makes it possible to effectively revoke ID cards without having to store personal data in a central register. It is also thanks to the functions of the eID Service and the support of the CSPs that the “new ID card” system not only protects a citizen’s personal data, but also protects citizens and service providers against economic loss caused by fraudulent use of ID documents.

SECTION ___4

IDENTITY MANAGEMENT AT WORK – APPLICATION EXAMPLES

As complex as the functionality of the eID Service may be, for citizens and service provider staff who are not entrusted with IT tasks, this complexity remains invisible in day-to-day use.

The technical processes that run in the background are fully automated. Thanks to both a method that is to a high degree self-explanatory and to intuitive user guidance, citizens and service providers can easily use the functions of the new ID card, both online and offline. Three examples will illustrate this in detail:

EXAMPLE 1

Identification of personal data:

Ms Mustermann opens an account

In order to open a bank account, customers are required to present official ID at the bank. In Germany, this is a mandatory requirement pursuant to the Money Laundering Act and the German Tax Code. Up to now, customers went to the local branch where a bank clerk recorded their personal data from the ID document and entered it

into the corresponding bank forms. The only alternative to going to the bank was to use the so-called Postident method where the customer had to go to the local post office rather than to the bank. With the online ID function, which more and more financial service providers are offering on their websites, this procedure is now much more convenient and customer-friendly.

A customer, who we will call Erika Mustermann, has already had her online ID function activated at her local registration office and has installed the AusweisApp software on her PC. She has also purchased a BSI-approved advanced reader and connected this to her PC. She visits the website of her future bank and checks there whether and for which transactions the bank offers identification with the electronic ID function. The certificate displayed shows Ms Mustermann that the bank has been authorised to use the new ID card for opening accounts. The bank is authorised to access the data categories of family name and first name, date and place of birth, address, as well as the verification of place of residence function, on condition that the citizen, in this case, Ms Mustermann consents to this.

Ms Mustermann now clicks the product offered by the bank and selects a special private account. Ms Mustermann is now requested on the screen to identify herself for a request to open an account using an ID document with the online ID function. To do this, Ms Mustermann places her ID card on the reading device so that the data on the integrated chip can be read. Even before the reading process begins, the eID server, as the intermediary between the user and the service provider, checks whether the bank has the authorisation certificate needed to request the data. A mask appears on Ms Mustermann's PC with the data requested by the service provider. Ms Mustermann de-selects the information which she does not want to disclose and by entering the PIN, she releases the data selected for transmission to the eID server. The data is read from the chip via connections that are secured with PACE and EAC and is securely transmitted to the service provider in an SAML 2.0 token. The process is now completed from the customer's perspective. Ms Mustermann removes her ID card from the reader. If necessary, she can select special options for her account in the bank's online request and sends these off to the bank with a click of the mouse. The bank can now process her request and rest assured that the identity of its potential customer is correct.

EXAMPLE 2

Online authentication using Restricted Identification: Ms Mustermann joins a social network under a pseudonym

One problem familiar to anyone who frequents online portals or social networks is that as a user you have to remember a vast number of passwords and user names in order to log on to these websites. The online ID function of the new ID card offers Ms Mustermann an option here to make life easy. With the help of the pseudonym function, she can easily log on to portals without having to disclose her personal data. What she has to do here depends on the service offered by the respective service provider who can determine to a certain degree how the method for logging on with the pseudonym function is to be designed. To illustrate this mechanism, the fictitious procedure described below will serve as an example.

Ms Mustermann wants to protect her identity in a social network. She first checks the certificate visible on the website of the social network to see if the service provider supports the online ID function and the use of the pseudonym function. If this is the case, she selects the “Register” option in the service provider’s menu. As soon as a corresponding prompt appears, she places her new ID card on the reading device. The eID server first checks whether the service provider has all the current certificates needed for the registration process. If this is the case, Ms Mustermann will be requested to enter her personal eID PIN. The reading device only reads out her data after she has entered this PIN.

In the mask on the PC, Ms Mustermann then de-selects all the categories except for the pseudonym function. Depending on the type of portal she wants to register for, Ms Mustermann can completely rule out the disclosure of her personal data. If the service provider accepts registration with a pseudonym only, Ms Mustermann enters the eID PIN to activate the “Pseudonym” category for transmission to the eID server. This ensures that this network can always recognise Ms Mustermann’s chip – without her having to disclose personal data for this purpose.

Since the eID server generated the pseudonym specifically for this special site, the social network is completely unable to compare this with other pseudonyms of the same user with other service providers. Ms Mustermann’s identity is hence protected as far as technically possible today. As long as she herself does not disclose

any details about herself which would reveal her identity, she remains anonymous for both the service provider and for other users. The next time Ms Mustermann logs on to the network, she simply repeats the steps described – the service provider’s authenticated terminal automatically recognises her again. This process not only simplifies procedures for the user, but also for the service provider. That’s because it is no longer necessary to reset forgotten passwords and user names and this reduces administrative work. Service providers can credibly claim that they guarantee the best possible data protection and that their services comply with the strictest security requirements.

EXAMPLE 3

Age verification for online shopping: Ms Mustermann orders wine on the Internet

It is very difficult for suppliers to check whether a user ordering alcoholic beverages, adult films or similar products on the Internet is old enough to do so. In most cases, they have to rely on the customer’s honesty. The online ID function of the new ID card makes secure age verification much easier for suppliers.

The online shop where Ms Mustermann is ordering wine has obtained an authorisation certificate from a certificate provider in order to verify the name, address and the legal age of his customers using the online ID function. Rather than disclosing the precise date of birth, the eID server in this case merely states whether or not the age specified has been reached.

Just like in the examples already cited, Ms Mustermann first selects what she wants to order; this time, a case of wine. As soon as a corresponding prompt appears, she places her new ID card on the reading device. The eID server first checks whether the supplier has all the certificates needed for the data to be transmitted. The data categories which the wine dealer wishes to request now appear in the mask on the screen. Ms Mustermann de-selects those categories which she does not want to transmit and enters her personal eID PIN. The data is then read out of the ID card via PACE and EAC-secured connections. The wine dealer receives the data from the eID Service in an SAML 2.0 token. Now, the dealer can rest assured that Ms Mustermann is old enough to purchase alcohol. As soon as the order has been completed, the dealer can ship the goods.

SECTION ___5

OUTLOOK: eGOVERNMENT WITHOUT BORDERS

Wouldn't it be convenient if people all over Europe could identify themselves with their national ID cards and make use of cross-border services? The participants of the EU STORK project are determined to make this vision come true.

STORK stands for Secure idenTity acrOss boRders linKed.¹¹ The aim of the project involving 17 European countries and 32 consortium partners is to establish an EU-wide platform within the framework of the European Union's ICT Policy Support Programme. This is to allow citizens to use their national electronic ID cards in other EU countries too.

At the end of 2010, twelve EU countries were already using electronic ID. Finland was the first country to introduce an electronic ID card in 1999. Belgium and Estonia followed suit in 2003.

The new German ID card that has been available since November 2010 is considered by experts to be the most advanced and secure eID card world-wide. By the end of 2011, citizens in an estimated 16 European countries will be able to furnish eID. However, not

all of these cards are based on the European standards issued by the International Civil Aviation Organization (ICAO) and/or the European Committee for Standardization (Comité Européen de Normalisation, CEN) which have been available since 2004. It is especially the pioneering countries of Finland, Belgium and Estonia (their eID cards were introduced before 2004) which have not used an international standard up to now.

The different card and system architectures in Europe up to now have prevented the cross-border use of national eIDs. Various pilot projects have been initiated by STORK in which citizens in different states can use their ID documents for eGovernment services in several European countries. In this project, the German Federal Office for Information Security represents the interests of the Federal Republic of Germany and wishes to enable citizens to use the new ID card for Internet offers throughout Europe. A total of 20 million euro is available for this EU project over a three-year period.

Six pilot projects have been open to the public since October 2010: "Cross-border authentication for electronic services", "Safer Chat", "Student Mobility", "Cross-border electronic delivery", "Change in address" and "Commission Services".

CROSS-BORDER AUTHENTICATION FOR ELECTRONIC SERVICES

The pilot project coordinated by the Federal Republic of Germany is testing how citizens can use their national electronic IDs for the online public services of other member states. In this context, the performance and user friendliness of the cross-border eID services are also being tested.

SAFER CHAT

Iceland's Ministry of Finance is coordinating the Safer Chat pilot project. The project aims to enable cross-border eLearning. School children are to work together with children of the same age from other countries. In an effort to improve Internet skills among children and young people, teachers are developing tasks for different age groups and defining safe chat rooms for young users. Special education packages are making these young target groups more aware of Internet security.

FIGURE 6: eID SOLUTIONS IN EUROPE

Country ¹ Year of introduction	eID	eGov	eSignature ³	Travel	eHealth	Others
Finland 1999	■	■	■	■		eBanking
Belgium 2003	■	■	■	■		
Estonia 2003	■	■	■	■		
Austria 2004	■	■	■		■	eTax and eBanking
Sweden 2005	■ ²	■	■	■		
Italy 2006	■	■	■		■	eTicketing
Spain 2006	■	■	■	■		
Portugal 2007	■	■	■	■	■	eTax
Serbia 2007	■	■				
Great Britain 2009/2010	■ ²			■		
France 2010	■	■	■	■		
Germany 2010	■ ²	■	■	■		
Czech Republic 2011	■	■		■		Others planned
Poland 2011	■	■		■	■	Social service and EHIC ⁴

1 ID cards are not required in all countries.
 2 Electronic variant is voluntary.
 3 QES is voluntary, exception Estonia.
 4 EHIC = European Health Insurance Card.

STUDENT MOBILITY

This application allows students to use their national electronic ID (ID card, digital certificates) to authenticate themselves and use the related academic services – for instance, they can apply to take part in the Erasmus Programme.¹² This project marks the first milestone in the analysis of future data exchange between universities in the different EU countries. This data exchange is needed in order to credit university points which students have acquired in other countries. Jaume I university in Castelló de la Plana is steering this sub-project on behalf of the Conference of Rectors of Spanish Universities.

CROSS-BORDER ELECTRONIC DELIVERY

In this pilot project, citizens can use their national electronic IDs in order to make use of portals from other EU countries for electronic delivery (eDelivery). Furthermore, public administrations will be able to send documents directly to citizens in other countries via the eDelivery portal of the respective country. This project is being coordinated by Technische Universität Graz.

CHANGE IN ADDRESS

This pilot project will enable foreign citizens to change their address using their national electronic ID and to inform all the relevant offices of such change in address. The procedures that apply in the individual member states do not have to be changed here because the platform developed by STORK is interoperable, i. e. it can be used for different types of cards and country-specific infrastructures. Two scenarios are currently foreseen: the request and the updating of an address. This project is being managed by Agência para a Modernização Administrativa in Portugal.

COMMISSION SERVICES

The European Commission Authentication Service (ECAS) allows employees of the EU Commission to log on for a host of applications. The Commission Services pilot project links STORK and ECAS. This allows employees in the member states to use their national eIDs in order to make use of the electronic services provided by the European Commission. EACS, for instance, provides authentication services for communication between member states (the Internal Market Information System, IMI) and for the participant portal for the European research programmes. Nine member states are taking part in this pilot project that is being coordinated by Technische Universität Graz: Austria, Belgium, Estonia, Germany, Iceland, Italy, Portugal, Slovenia and Spain.

The application scenarios mentioned above are opening up new possibilities for citizens and government agencies. “The pilot projects will demonstrate to citizens and public administrations that interoperability of electronic identities is achievable in eGovernment services. They will highlight the added value which citizens

receive when they can assert their identities electronically in a protected, secure and private environment,” says Professor Antonio Lioy from Politecnico di Torino in Italy and STORK Co-Chair.¹³ The eID network would save public money, reduce time for both government and citizens, lessen the risk of misuse or fraud and create a wealth of opportunities. “It is one more step towards a borderless EU marketplace.” At the same time, this development will make it more and more normal for citizens to use the eID function of their ID card - even in the private sector. This will create market opportunities for online service providers who integrate the electronic ID function into their service at an early point in time.

QUESTIONS AND ANSWERS

The eID Service is a new technology. How can a service provider be certain that the service will in fact do what it promises?

Bundesdruckerei has already successfully conducted a comprehensive test and made its eID Service available to more than 40 companies and institutions.

Where can a service provider find out more about the eID Service?

The service provider can reach Bundesdruckerei’s experts by calling +49 30 2598-0 or sending an e-mail to info@bundesdruckerei.de. For general information about the eID Service, go to: www.bundesdruckerei.de or www.personalausweisportal.de

Which IT components does a service provider need if he wants to integrate the online ID function (eID function) into his service?

The service provider exchanges data with Bundesdruckerei using web service communication. In addition to an interface description, the service provider also receives an implementation example.

Which preconditions must a company or an agency (service provider) fulfil in order to be authorised to use the online ID function in its service?

Applications for authorisation must be submitted to the Issuing Office for Authorisation Certificates (VfB), a unit of the Federal Office of Administration, which issues the letter of authorisation.

The service provider's application must include various documents and information, such as proof of the extent to which the service provider wishes to read out data for the purpose of his service. The letter of authorisation issued by VfB is valid for a maximum period of three years.

Which authorisation certificates does a service provider need in order to integrate the online ID function into his service?

As soon as the Issuing Office for Authorisation Certificates has granted authorisation, the public agency or company can enter into an individual provision agreement with an authorisation CA (BerCA). D-TRUST, Bundesdruckerei's trust center, is one such authorisation CA. The authorisation certificates identify the service provider to the ID card holder. These certificates are valid for a few days only and are automatically renewed on a regular basis.

Which advantages does the eID Service have to offer compared to a server operated by a service provider?

If a service provider wishes to operate his own server, it must first fulfil the strict requirements laid down in technical guideline BSI TR-03127, "Architecture electronic Identity Card and electronic Residence Permit" of the Federal Office for Information Security. This, however, would mean considerable personnel and material expenditure. That's why many providers opt for the so-called eID Service provided by accredited certification service providers (CSPs) like D-TRUST, Bundesdruckerei's trust center. The advantages at a glance:

- > CSPs have considerable experience in the management of digital identities
- > CSPs provide powerful infrastructures
- > The eID Service takes care of the entire communication with the ID card chip
- > Authorisation certificates and revocation lists are always up to date
- > Optimum security for transactions
- > The eID Service can be easily integrated into the service provider's IT system architecture
- > Using the eID Service is a cost-efficient and resource-saving option when compared to setting up a separate server

Which services do eID Service providers perform for government agencies and private companies which accept the new German ID card as an online authentication document?

The eID Service provider reads the data which has been released for the service provider from the ID card. This release is dependent on the regulations of the Issuing Office for Authorisation Certificates (VfB), the requirements of the service provider and, of course, on the holder of the ID card who must authorise each data transmission with his or her eID PIN.

How much does this cost the service provider?

The cost of connecting an eID Service can vary depending on the specific requirements of the customer and the legacy IT infrastructure. The service provider can contact Bundesdruckerei for a customised quotation.

What happens when data fraud is suspected?

Data misuse is when the service provider uses his authorisation certificate for transactions which he did not name when applying for authorisation or when the service provider passes customer data on to third parties. The Issuing Office for Authorisation Certificates can revoke authorisation if data misuse is suspected. The technical authorisation certificates of the CSP are only valid for two days and would not be renewed in such a case.

What happens if the user refuses to release the data categories requested by the service provider?

In this case, the data is neither read nor transmitted because the holder of the new ID card must consent to the transmission and confirm this with his or her PIN. The service provider is generally authorised by the Issuing Office for Authorisation Certificates to request certain data. If the ID card holder does not want to transmit this data in full, the service provider decides whether or not to continue with the transaction.

How can service providers find a suitable eID Service provider?

The eID Service providers currently available in Germany can be found at www.personalausweisportal.de.

For which industries does Bundesdruckerei offer its eID Service?

Generally speaking, companies from all industries wishing to enhance their Internet service with the online ID function can use Bundesdruckerei's eID Service.

What are the advantages of integrating the online ID function (and hence a connection to an eID Service) compared to using a password and PIN for online services?

The online ID function offers enormous benefits for both customers and service providers:

- > The customer only has to remember one password; this makes the online service much more convenient
- > Lower costs for resetting passwords and the related posting of password letters
- > Phishing and trojan attacks are more difficult; this means greater security for the customer portal operator
- > The service provider's customer data is also better protected
- > The service provider automatically fulfils the Commission's requirements regarding youth media protection by state institutes
- > The requirements of the Money Laundering Act are also complied with

Can service providers test the eID Service before using it?

Yes, this is possible during various phases of the project. If a service provider is interested in connecting to an eID Service, Bundesdruckerei recommends that the service first be used in a test environment. In this case, the data exchange channel between the service provider and Bundesdruckerei is already mapped. Pre-defined messages and error codes are sent so that the service provider can prepare fully before going live. The following scenarios, for instance, are played through: The ID card holder enters the wrong PIN or fails to release the data. ID cards are not used in the test environment. This takes place during a test in the so-called reference environment. A test run in the reference environment corresponds almost fully to real implementation and is recommended, for instance, for demonstrating the eID Service within the company. It is generally possible to go live with the eID Service once the trial in the test environment has been completed.

Data protection is very important to service providers. How can data protection and data security be guaranteed when the online ID function is used?

The new ID card offers maximum protection for a citizen's data. It protects against identity theft and with its security protocols and mechanism, it prevents unauthorised parties from reading, copying or manipulating information. Before data is transmitted, the ID card checks whether the requesting service or the requesting agency is authorised to request the information. Unnoticed reading of the data is not possible. Furthermore, all information and transmissions are protected by internationally recognised and established technical means (encryption and signature).

The citizen's personal information is also safe on the Internet: Only the person in possession of the ID card and the six-digit PIN can release the information for transmission. Data is exchanged between the ID card holder and the service provider only.

The technical security level of the entire system that protects the data of the new German ID card against unauthorised access is very high. The chip also meets with the highest security standards. Just like with other applications, such as eBanking or Internet shopping, the precise level of security depends on the user's computer environment.

GLOSSARY

A

Act on Digital Signature

A law governing the framework conditions for electronic signatures, in German briefly referred to as SigG or SigG 2001, from 16 May 2001; defines rules for using >electronic signatures.

Advanced electronic signature

An >electronic signature which pursuant to Section 2 of the German >Act on Digital Signature is

- a) exclusively assigned to the >signature key holder,
- b) enables the identification of the signature key holder,
- c) is generated with means which the signature key holder can keep under his/her sole control, and
- d) is linked to the data to which it refers in such a manner that any later modification of the data cannot go unnoticed.

Age verification

A feature within the >online ID function of the new German ID card. This feature makes it possible to check whether the holder of the document has reached a certain age. In the interest of data thriftiness, the holder's precise date of birth is not transmitted.

AusweisApp

This special driver software must be installed on the citizen's PC in order to use the >online ID function. The software enables the reader and the ID card to communicate with each other. Service providers who wish to provide their customers with access to AusweisApp, should refer to the <https://www.ausweisapp.bund.de/pweb/index> official portal. Marketing of this software through other providers or websites is not permitted.

Authentication (of an Internet user)

Checking and confirming the identity of Internet users who have previously authenticated themselves. When the online function is used, this is guaranteed by the >eID server through possession, the ID card and knowledge of the PIN. The principle of authentication for both parties by an independent, third party, i.e. a >CSP, is one of the core elements of secure online transactions.

Authentication

Proof of one's own identity, for instance, through knowledge (e.g. input of a code), possession (presentation of an ID card) or biometric features. Holders of the new ID card can authenticate themselves physically by presenting the new ID card. On the Internet, the data stored on the >security chip of the new ID card can be read.

Authorisation

Permission for service providers to integrate the online ID function or the >qualified electronic signature (QES) into their services. This is granted by the >Issuing Office for Authorisation Certificates (VfB), a unit of the Federal Office of Administration. This requires a voluntary self-declaration regarding data protection and proof that the data which the service provider wishes to read is in fact required for his service. The authorisation granted by VfB is valid for a maximum of three years and must be reapplied for. If requested, an eID Service provider can act fully on behalf of the applicant and support the applicant during the application process.

Authorisation certificate

This certificate is issued to service providers who sign an individual provision agreement with a >CSP. These certificates authenticate the service provider and enable him to access the previously defined data categories. The certificates are only valid for a few days and are regularly renewed unless data misuse is suspected.

B

BerCA (Authorisation Certification Authority)

The Authorisation Certification Authority (BerCA) is operated by the >CSP and technically implements the issuing of the authorisation certificate.

BMI

Germany's Federal Ministry of the Interior

BSI

>German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik)

C

CA

>Certification Authority

Certification Authority (CA)

The certification authority that issues digital certificates; this is another term used for certification service providers (CSPs) and >trust centers.

Certification Service Provider (CSP)

Also referred to as: Certification Authority (CA); a service provider who is registered with the Federal Network Agency according to the >Act on Digital Signature, in the version dated 17 July 2009, and is entitled to issue qualified certificates or qualified time-stamps. Only accredited CSPs are authorised to issue >authorisation certificates for service providers. The list of CSPs in Germany is available at: <http://www.nrca-ds.de/ZDAListe.htm>.

CSCA certificate

Country Signing Certification Authority certificate that contains the country code of the issuing agency. This forms part of the >PKI and is hence a key element of the numerous security mechanisms in electronic ID documents.

CSP

>Certification Service Provider

CVCA eID

Country Verifying Certification Authority eID; a certification authority at >BSI. It issues the necessary certificates for >CSPs like >D-TRUST, for instance. These certificates, in turn, allow CSPs to issue authorisation certificates to authorised service providers and operators of visualisation and update terminals (refer to the BSI website).

D

Disable password

An easy-to-remember password (e. g. train) that a citizen needs in order to disable a lost or stolen ID card. The password in question is known only to the ID card holder and the issuing registration office. Unlike the PIN and PUK, the user does not enter the disable password on the computer. Instead, the disable hotline staff or the ID card authorities ask for the password when necessary.

D-TRUST

The accredited >CSP operates in Bundesdruckerei's high-security building and offers customers in industry and public administrations tried-and-tested, interoperable signature products, certification services and electronic notary services.

E

EAC

Extended Access Control for the data stored on the chip of the new ID card in which different protocols are bundled. These protocols include, for instance, Chip Authentication (CA), which establishes a secure connection to the chip and recognises cloned chips, and Terminal Authentication (TA), which protects the sensitive data of the new ID card against unauthorised access. Both protocols are executed together with >PACE and >PA.

eGovernment 2.0

A strategy adopted by the government in 2006 to modernise IT structures in Germany's administration. The introduction of the new ID card and the development of electronic ID concepts are among the core elements of this strategy. The implementation of this strategy is being overlooked by >BMI.

eID

Electronic identity

eID PIN

A self-selected six digit secret number which the user must use each time in order to authorise the transmission of data from his/her new ID card to an >eID server. No other data category, except

for information as to whether the ID card is valid or not, can be transmitted without the PIN. The transport PIN in the PIN letter sent by Bundesdruckerei, which all holders of a new ID card receive at the beginning, must be replaced by a personal PIN that is only known to the user in order to use the online ID function. Only now are online transactions possible.

eID server

A hardware and software infrastructure that enables communication between citizens and service providers on the basis of the online ID function. Service providers can either set up their own eID server, as long as they observe the technical guidelines of BSI, or they can use the eID server of an >eID Service.

eID Service

Takes care of the entire communication with the ID card chip and ensures optimum security for transactions. This means, for instance, that it checks that the >authorisation certificates are valid and keeps >revocation lists with invalid ID cards up to date.

Electronic signature

Also called digital signature; refers to electronic data that is attached or connected to a message. The electronic signature guarantees the authenticity and integrity of the message. It ensures that the sender is in fact who he/she claims to be and that the message was not changed during transmission from the sender to the recipient.

ENISA

The European Network and Information Security Agency. This agency advises EU committees and member states and is committed to harmonising the different ID concepts within the European Union.

ePassport

The electronic passport was introduced in Germany in 2005. The digital passport photo is stored as a biometric feature on the security chip integrated into the first-generation ePassport. In the second-generation ePassport, which has been available since 2007, the chip additionally contains two fingerprints of the passport holder.

Unlike the new ID card, fingerprints have been required by law since 1 November 2007 and are no longer optional when applying for a new ePassport. This means that the ePassport offers the highest degree

of protection against forgery. Old passports, however, will remain valid. An ePassport is, for instance, a requirement for entering certain countries, such as the US.

Three different types of passports have been in circulation since 2005. Passports without a chip, first-generation electronic passports, which only contain the passport photo on the chip, and the second-generation electronic passport in which the passport photo and two fingerprints are stored on the chip.

External interface

This is part of the eID server. During transactions using the new ID card, it supplies the data stored on the chip to the service provider via the internationally standardised token (SAML 2.0 Assertion).

G

German Federal Office for Information Security (BSI)

National security authority, a subordinate unit of >BMI, responsible for matters of security in the information society. BSI is responsible, for instance, for the approval of reading devices with which the chip of the new ID card can be read and for the accreditation of the >CSPs.

German ID Card Act

A law ratified in 2009 in the German Bundestag which lays down the legal framework for the new ID card and electronic ID. It covers, for instance, new legislation in conjunction with changes in passport law, the registration framework law, the signature ordinance and the money laundering act, and can be downloaded at http://www.personalausweisportal.de/SharedDocs/Downloads/DE/pauswg.pdf?__blob=publicationFile.

I

ID1

The world's most widely used format for ID cards, standardised by the International Organization for Standardization (ISO) under ISO 7815. These cards measure 85.60x53.98x0.76 mm. The format is used, for instance, for driving licences, bank cards, credit cards and debit cards – and has been used for the new ID card since November 2010.

Identity theft

A crime where an unauthorised party uses the identity of another person in order to damage their reputation, for instance, or to conduct business in their name. This happens when the data stolen by a criminal can be used to clearly identify the victim in a specific context. If an unauthorised person comes into possession of a citizen's personal data, such as name, credit card data, address and date of birth, they could use this data for criminal purposes.

Identity management

Technical term to describe the professional handling of identities. This includes, for instance, the secure management of identities and the process with which individuals, groups or organisations are identified and, if necessary, authenticated.

ID systems

This refers to the interaction between high-security technologies (hardware and software) that effectively protect sensitive data in ID documents against unauthorised access and manage the exchange of data between authorised users.

Internal interface

An element of the eID server that allows information to be exchanged with the new ID card. The internal interface complies with BSI's eCard API Framework (TR-03112) and, in addition to several cryptographic protocols, also includes >PACE and >EAC access control.

Issuing Office for Authorisation Certificates (VfB)

A unit of the Federal Office of Administration that controls the issuing of authorisation certificates, operates the >revocation list service and takes care of >revocation management. Service providers must meet with clearly defined requirements pursuant to Section 21 of the >German ID Card Act and must prove this in writing to the Issuing Office for Authorisation Certificates. They must also submit a voluntary self-declaration regarding data protection in order to receive >authorisation to request ID card data. The authorisation issued by the Issuing Office for Authorisation Certificates is valid for a maximum period of three years. It is a mandatory requirement so that the service provider can make and enter into an individual provision agreement with a >CSP and can acquire technical >authorisation certificates.

O

Online ID function

The electronic ID function of the new German ID card allows citizens for the first time ever to identify themselves with ID on the Internet. Using their six-digit >eID PIN, the ID card holder alone decides which information is to be disclosed during each individual transaction. In order to use the online ID function, the document holder must have the function activated, the >AusweisApp software installed on their PC and be at least 16 years of age. Furthermore, the business partner on the Internet must explicitly offer electronic proof of identity and identify themselves as an authorised online partner.

P

PA

>Passive Authentication

PACE

Password Authenticated Connection Establishment; a security protocol that protects the contactless >security chip in the new ID card against unauthorised access. Thanks to PACE, the chip can only be read after the holder has entered the six-digit >eID PIN. PACE also encrypts the data that is transmitted to the reading device.

Passive Authentication (PA)

Checks whether the data on the contactless chip of the new ID card is genuine and has not been manipulated. This is only the case when the data has been signed with Bundesdruckerei's digital document signing certificate. Bundesdruckerei is the only company officially authorised by >BMI to save data on the chip of the new German ID card. The document signing certificate itself is also marked by another certificate, i.e. the >CSCA certificate. While the new ID card is being read, the software uses PA to check the signature of the chip and traces this back to the CSCA certificate.

PIN

A Personal Identification Number or secret number which a person uses in order to identify themselves to a machine.

PKI

Public Key Infrastructure; this refers to a system that can issue, distribute and check digital certificates. At the heart of the PKI structure is a software that operates the >Certification Authority (CA).

Pseudonym function

This feature of the new ID card makes it possible to log on to an online portal, for instance, without entering personal data. If the service provider supports the online ID function and accepts the use of the pseudonym function, the eID server generates a pseudonym specifically for the respective online service. This pseudonym cannot be compared with other pseudonyms of the same user.

PUK

A Personal Unblocking Key is a number that the citizen receives together with the PIN letter from Bundesdruckerei and which should be stored safely. This is used to unblock the online ID function if the wrong eID PIN is accidentally entered three times in succession. A PUK can be used up to ten times.

Q

Qualified electronic signature (QES)

A special form of the >advanced electronic signature which, pursuant to the >Act on Digital Signature, a) is based on a qualified certificate that was valid at the time the signature was generated and b) is generated by a secure signature generation device. The written form pursuant to Section 126 of the German Civil Code (BGB) is required for some declarations of intent (e.g. loan agreements). This means that pursuant to Section 126 BGB, a QES is required when data is exchanged electronically. Moreover, various laws, while not referring to the legal written form, explicitly require a qualified electronic signature (sometimes with provider accreditation or long-term availability for authentication) for signing electronic documents.

In order to use the QES, citizens need an advanced reader as well as a >signature certificate and a >signature PIN, both of which are available from a >CSP. The QES is legally equivalent to the personal, hand-written signature.

R

Reader

For citizens and authorised public offices, this is the basic equipment needed to read data from the new German ID card. Whilst standard and advanced readers have their own PIN pad for entering the PIN, users with a basic reader must use their PC keyboard or a screen keyboard. Card holders who wish to use the >QES need an advanced reader with its own display in order to enter the required >signature PIN. BSI recommends that users use accredited card readers only. Accredited card readers bear the same green and blue logo that can be seen on the new ID card.

Restricted Identification (RI)

A security protocol for generating chip-specific and user-specific pseudonyms.

Revocation hotline

A telephone number that citizens must use to report the loss of their new ID card. Citizens must state their family name, first name, date of birth and >disable password if the >online ID function has been activated. The ID card office in charge must also be notified because the revocation hotline does not automatically exchange information with the ID card authorities.

Revocation list

A list of ID cards that have been disabled due to loss or theft. This list is managed by the >Issuing Office for Authorisation Certificates.

Revocation management

The process of revoking an electronic ID document, for instance, the new German ID card.

Revocation service

Disables the electronic ID function of the new ID card in order to prevent misuse after the card has been lost or stolen. This service is operated by the >Issuing Office for Authorisation Certificates. The central tasks of the revocation service also include the central management and storage of a revocation list with the revocation keys of the ID cards lost with an activated >online ID function, the provision of interfaces with the ID card producer, with the hotline

and with the ID card offices, as well as the passing on of revocation lists to the certification services.

RI

>Restricted Identification

S

SAML 2.0 token

Stands for Security Assertion Markup Language 2.0 token; a standard for the secure exchange of authentication and authorisation information between domains. SAML assertions are statements which an eID Service provider uses as a basis for granting access to certain services. The SAML token contains information from the ID card and is made available to the service provider for further use.

Security chip

Contactless readable computer chip that is integrated into the new German ID card. The following information is stored on this chip in digital form: the data of the machine-readable zone (printed on the back of the card), family name and nee, first name(s), doctoral degree, date and place of birth, photo, address, nationality, serial number as well as the religious order name or artist's pseudonym. The ID card holder can also request to have the data from two fingerprints additionally stored on the chip as well as the certificate information for using a >qualified electronic signature (QES).

Security protocol

Defined scheme of data sequences for communication between a chip and a reading device. Security protocols, such as >EAC or >PACE, ensure data protection, protection against forgery and the authenticity of the data in the new ID card.

SigG

>Act on Digital Signature

Signature certificate

An electronic certificate that a citizen needs in order to use the qualified electronic signature. This is available from a >CSP.

Signature key

Pursuant to Section 2 of the >Act on Digital Signature, unique electronic data, such as private cryptographic keys that are used to create an electronic signature.

Signature PIN

A secret number issued by the >CSP which the ID card holder needs in order to electronically sign a document.

Sovereign ID function

This function makes it possible to identify oneself to government authorised bodies. Access to this data is only granted to the police, border control and customs authorities, the tax authorities in the federal states of Germany, and the registration authorities. In order to read the data, they also need special >authorisation certificates which are issued by the >CSPs. Moreover, the ID card holder must also be present in person while the data is being read.

SSL certificate

Encrypts communication between service providers and users of their websites. These certificates can be obtained from a >CSP.

SSL encryption

Secure Sockets Layer; this security protocol enables secure data transmissions on the Internet.

STORK

Secure idenTity acrOss boRders linKed; an EU project that aims to introduce an EU wide platform to achieve interoperability for electronic identities. This platform is to enable citizens to use their national eIDs for eGovernment services in several European countries. For more information, go to: <https://www.eid-stork.eu/>.

T

The new German ID card

The new ID card in >ID1 format for citizens in the Federal Republic of Germany; available since November 2010. The new German ID card contains a >security chip and not only serves as photo ID but can also be used by citizens as electronic ID on the Internet.

Token certificate

Permits the service provider to access the eID Service.

Trust center

Accredited certification service provider (> CSP).

V

Verification of place of residence

A function within the online ID function of the new German ID card; confirms or denies a place of residence query by a service provider. In the interest of data thriftiness, the citizen's full address is not transmitted.

VfB

> Issuing Office for Authorisation Certificates

FOOTNOTES

- 01 ____ Refer to: <http://www.zeit.de/digital/datenschutz/2010-01/identitaetsdiebstahl-selbsterfahrung>.
- 02 ____ Security monitor by IT service provider Unisys, refer to: http://www.unisys.de/about__unisys/presse/10102701.htm.
- 03 ____ Refer to: BSI study "Identitätsdiebstahl und Identitätsmissbrauch im Internet – Rechtliche und technische Aspekte" (Identity theft and identity misuse on the Internet – legal and technical aspects).
- 04 ____ Refer to: <http://www.zeit.de/digital/datenschutz/2010-01/identitaetsdiebstahl-selbsterfahrung>.
- 05 ____ GO SMART 2012: Always in Touch, study on smartphone use 2012, published by Google, Otto Group, TNS Infratest and Trendbüro.
- 06 ____ Representative Forsa survey conducted on behalf of BITKOM in November 2010, refer to: http://www.bitkom.org/65912_65908.aspx.
- 07 ____ Security monitor of IT service provider Unisys, refer to: http://www.unisys.de/about__unisys/presse/10102701.htm.
- 08 ____ Technical guideline by the Federal Office for Information Security (BSI): BSI TR-03127 "Architektur elektronischer Personalausweis und elektronischer Aufenthaltstitel" (Architecture electronic Identity Card and electronic Residence Permit) contains an overview of all the technical specifications.
- 09 ____ Technische Universität Darmstadt, Project 826, Study: "Sicherheitsanalyse des EAC-Protokolls", 11 October 2010.
- 10 ____ Institute for Internet Security at Gelsenkirchen University of Applied Sciences, intermediate report: "Restrisiken beim Einsatz der AusweisApp auf dem Bürger-PC zur Online-Authentisierung mit Penetration-Test", October 2010.
- 11 ____ <https://www.eid-stork.eu/>.
- 12 ____ The Erasmus Programme was launched on 15 June 1987 by Council Decision 87/327/EEC. The aim of this programme is to promote co-operation between universities within the EU and other European countries and to improve student and university teacher mobility.
- 13 ____ STORK press release dated 25 October 2010 and the German Federal Office for Information Security (BSI).

Bundesdruckerei GmbH
Corporate Communications
Oranienstraße 91
10969 Berlin
www.bundesdruckerei.de

August 2011

© 2011 Bundesdruckerei GmbH

