eID CARD
POCKET GUIDE
___2012
<table>
<thead>
<tr>
<th>05</th>
<th>SECTION 1</th>
<th>INTRODUCTION</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>All about the eID card: Facts and functions</td>
<td>Why we need modern eID cards – and what’s so special about them</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>07</th>
<th>SECTION 2</th>
<th>AREAS OF APPLICATION</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>AT A GLANCE</td>
<td>Which cards are actually being used – and what are the requirements for these cards</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>12</th>
<th>SECTION 3</th>
<th>FEATURES OF SECURE DOCUMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Which security features can be integrated into ID cards – and what’s important in this context</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>35</th>
<th>SECTION 4</th>
<th>THE CHIP AS THE STRONGBOX OF THE eID CARD</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>What’s special about the embedded chip – and how it can be integrated into high-security ID systems</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>40</th>
<th>SECTION 5</th>
<th>FROM THE DRAWING BOARD TO VERIFICATION</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>How an eID card is created and handled – and how Bundesdruckerei accompanies this process</td>
</tr>
</tbody>
</table>

| 45 | GLOSSARY | |
|----|----------|
INTRODUCTION

eID cards – opening the door to tomorrow’s world

Today, it’s a business appointment in Berlin, tomorrow, a holiday in the sun. Always online, at work or on the go, always jumping back and forth between the analogue and digital world. For many people today, this kind of lifestyle is perfectly normal. That’s why it is so important that ID documents keep pace with these trends and be designed for a world that is becoming ever-more complex. Documents are needed that allow us to prove who we are on the net or identify ourselves in road checks, that grant us access to security zones or which serve as ID in dealings with public authorities. These documents must be both forge-proof and user-friendly, not just for the holder but also for public authorities or private companies.

How can a person’s identity be determined today, both quickly and without any trace of doubt, and at the same time protected? How can we guarantee now, during times of extensive mobility, that only trustworthy and authorised parties can access personal data – and how can anonymity be reconciled with security on the net?

Bundesdruckerei has responded to these questions with products for modern identity management that are in high demand the world over. ID cards in standardised ID1 format especially are opening up new perspectives. These cards are equipped with both tried-and-tested and innovative optical security features, protecting the card core itself, i.e. the polycarbonate body, and the optically personalised data against forgery.
An integrated high-security chip also enhances card security because the personal data, such as the holder's photo, is not only optically visible but is also stored in electronic form on the card itself. The chip also enables a host of functions, such as the qualified electronic signature (QES) which the holder can use to sign contracts on the net in a manner recognised by law. At the same time, the communication channels are so well encrypted that misuse can be ruled out. The eID functions of the card are opening up new possibilities for eBusiness and eGovernment. They have the potential to open doors in both the virtual world and in the real world while meeting with the highest security standards. What is clear is that the future belongs to the handy multi-functional cards “made in Berlin”. The experts at Bundesdruckerei will be pleased to help you find just the right solution to meet your needs. They can show you what you need to consider, which combinations are possible and they will be pleased to support you from the drawing board to verification. To find out more, simply go to the next page.

Plastic cards are widely used nowadays. ID1 format especially is very popular. This standard size measuring 85.60 millimetres times 53.98 millimetres (3 3/8” × 2 1/8") was laid down in the ISO/IEC standard 7810 by the International Organization for Standardization (ISO).

This means that the sides of the ID1 card are in the golden ratio (1.618:1). The cards are made of different plastic materials, such as polycarbonate (PC), polyethylene terephthalate (PET) or polyvinyl chloride (PVC), they are less than a millimetre thick and have rounded corners. Fitted with memory or processor chips, they are used all over the world as bank or cash cards, telephone cards or health insurance cards. They are also being increasingly used by governments for national ID documents.

SECTION ___ 1
ALL ABOUT THE eID CARD: FACTS AND FUNCTIONS

The development and production of innovative eID cards belong to Bundesdruckerei’s core areas of expertise. These cards can be fitted with a host of functions and meet with high security standards.
The biggest advantages of these cards are their handy format, the large range of security features possible and, above all, that they can be used for several functions as required. The cards can be used as photo ID for official checks and are often additionally fitted with a security chip. They can be designed as eID cards that guarantee secure ID on the Internet; and a signature function can also be integrated in order to digitally sign documents or to enable legally binding business transactions on the net. The card functions can be combined and expanded, and the technology can be tailored precisely to fit the environment where the card is to be used.

ID AND TRAVEL FUNCTION: SECURE MOBILITY ON NATIONAL AND INTERNATIONAL LEVEL

This flexibility is very important because ID cards with an official ID function have to meet with very high requirements today. Awareness of security issues has grown significantly. Many countries want official ID documents that meet with the highest standards in terms of forgery protection based on state-of-the-art technology. At the same time, both citizens and control officers want ID cards to be easy to use – so that only the data actually needed is checked. eID cards made of polycarbonate (PC) meet with these requirements to the highest extent possible. This material makes the cards robust, a particularly important aspect in light of the frequently long validity periods of official ID documents. Their security features can be ideally adapted to the respective application field and forgeries are near to impossible thanks to diverse protection mechanisms. With the right kind of verification devices, the cards can be easily checked and databases can also be accessed when permitted by data protection regulations. This makes it much easier to identify fraud compared to conventional ID documents. Electronic ID cards in ID1 format are hence the ideal solution for national ID documents. More and more countries are also using them for driving licences, another official ID document. In this case, the card not only documents that the holder is authorised to drive a vehicle, but also serves as proof of ID. That’s why it is so important to protect the card with innovative security features and biometric data against misuse.

In light of this, European countries wishing to grant their citizens smooth, secure mobility mostly rely on eID documents that meet with recognised standards (refer to Section 2). The leading organisation here is the International Civil Aviation Organization (ICAO), a United Nations agency. Today’s ICAO-compliant travel documents feature a machine-readable zone which shows the information printed on the document a second time in standardised form as well as a biometric photo of the holder. In order to make the document even more secure, many countries additionally integrate a contactless chip containing the encrypted data. ICAO has been recommending this since the late 1990s. The chip is embedded in several layers of plastic. Any attempt to manipulate it immediately makes the electronic ID function unusable.

eID FUNCTION: IDENTITY MANAGEMENT ON THE NET

Mobility today is no longer restricted to the analogue world. This is the second major challenge facing ID cards today. In the digital world, people can act under any number of different pseudonyms and secure identities become a threatened asset. Conventional ID documents have clearly reached their limits here. It is impossible to physically present an ID card directly on the net and this makes it very difficult to verify the identity of the other party. Photocopies of
ID cards are not safe enough because they can be easily manipulated. It hence comes as no surprise that fraudsters today commit only one third of identity theft crimes in the physical, analogue world, for instance, ordering goods using the data of a stolen ID card. Two thirds of these crimes already take place on the net. Many Internet users unintentionally make life easy for thieves because they all too easily disclose their personal data in social networks. Almost everyone knows that personal data on the net is hardly ever protected – and we accept this, albeit with some misgivings.

This is where ID cards, like the new German ID card produced by Bundesdruckerei, come into their own. Thanks to their eID function, card holders can identify themselves on the net without the fear of unauthorised parties accessing their data. All you need is your ID card, a reader, preferably class II or III, as well as a PIN – and you yourself decide precisely which data you wish to disclose. A complex ID management system with authorisation certificates ensures that this data arrives at the correct, trustworthy transaction partner. The so-called eID Service offered by Bundesdruckerei is a central element of this system in Germany. It allows private companies and public agencies in possession of the required authorisation certificates to read out the personal data stored on the chip of the ID card. In this way, both partners to a transaction can rest assured that their virtual partner is in fact who he or she claims to be. Unlike with conventional ID cards, you do not have to trust solely on the reliability of the security features and familiarity with the document. Additional security is warranted by a complex, technical infrastructure and a supervisory body, like Bundesdruckerei’s eID Service which is described in detail in the company’s eID Service pocket guide.

Electronic ID cards are opening up a huge range of possibilities, not just for card holders, but also for government and the private sector. Users no longer have to remember dozens of user names and passwords in order to identify themselves to online services. Instead of filling in time-consuming forms for public authorities or private providers, the eID function allows users to directly enter the personal data needed for many eGovernment and eBusiness services. This saves time since users no longer have to travel to the public agency or post office and also prevents incorrect entries. The eID function makes it easier, for instance, to open an online account which in most countries requires presentation of official ID, or for users to identify themselves when applying for government services. Depending on the concept in place, the eID function provided on state-of-the-art ID cards allows citizens to consciously decide which data to disclose. For instance, eID cards permit users ordering online to specifically transmit only the information actually required for the transaction. This means, for instance, that although online shops can ascertain whether a potential customer is above the age restriction for ordering alcohol, they do not know exactly how old they are. Bundesdruckerei has already successfully implemented this data-thrifty solution for the new German ID card. Users who do not want to disclose their identity to all other users of a forum or network can use the pseudonym function of the ID card if the service provider permits this kind of access.

DIGITAL SIGNATURES FOR SIGNING CONTRACTS IN A LEGALLY BINDING MANNER

While the eID function allows users to identify themselves on the net, the electronic signature function goes one step further. Holders of eID cards with this function can digitally sign contracts on the net in a legally binding manner. In Germany, for instance, electronic office ID cards can be equipped with a signature function so that employees can digitally sign bids in public invitations to tender. The so-called qualified electronic signature (QES) of the new German ID card is a particularly secure form of signature and is regarded by German law to be equal to the handwritten signature. It is required for contracts which must be laid down in writing, for instance, in the case of rental or insurance contracts. A number of public providers in the Federal Republic of Germany provide citizens with short-term ad-hoc certificates so that they can sign documents on the net. This means that qualified electronic signatures are no longer only possible with special signature cards but can now be used by private individuals in possession of an ID document with this function activated. This makes concluding contracts on the Internet more attractive for many users. The European Union welcomes such developments and aims to soon establish the electronic signature as the standard worldwide. According to the European Commission, electronic invoicing is to be the main form of invoicing in the member states by 2020. If this is to happen, the EU member states will have to increasingly rely on multi-functional eID cards in order to make online transactions easier and more secure for citizens, private companies and public authorities.
SECTION 2
AREAS OF APPLICATION AT A GLANCE

Whether national ID documents, office ID cards or driving licences, eID cards are being used in a host of different areas. What’s important here is to consider the requirements of the respective area from the very outset.

The ID market is growing. The expectations of individual countries are also growing when it comes to ID document functionality. This in turn means that new security methods are needed in order to prevent manipulation and misuse. At the same time, new solutions are being developed in the fields of IT, nanoscience, bioscience and neuroscience to make ID documents meet with tomorrow’s highest security demands. These solutions include new materials and security features just as much as innovative chips that guarantee greater memory capacity and processing power. According to the Global National eID Industry Report conducted by consultancy company Acuity, half of the ID cards issued around the globe are still conventional documents. That’s why experts forecast that the market for ID documents will grow by 17 percent annually in the near future.

The requirements for such cards are laid down on international level by experts, for instance, from the International Civil Aviation Organization (ICAO), the European Union and the International Organization for Standardization. ICAO, a special United Nations agency, defines basic guidelines for national ID documents. This agency was established in 1944 by 190 member states in order to support international civil aviation through multi-lateral regulations and to help create greater security. In the same year and as part of the Chicago Convention, ICAO was granted the mandate to define standards and specifications for travel documents. Bundesdruckerei is represented in various ICAO committees and can contribute its expertise in document production towards the development of new standards.

WHICH ORGANISATION IS RESPONSIBLE FOR WHAT?

Committees and their subordinate working groups involved in the development of document standards:

> International Civil Aviation Organization (ICAO), Montreal
A specialised agency to promote the safe and orderly development of civil aviation that sets standards for international travel documents.
Section 2

> **Technical Advisory Group on Machine Readable Travel Documents (TAG/MRTD)**

Drafts and adopts specifications for machine readable travel documents which are published by ICAO in document 9303 [6]. This group’s members include representatives of the Airports Council International (ACI), International Air Transport Association (IATA), the International Criminal Police Organization (INTERPOL) and ISO.

> **New Technologies Working Group (NTWG)**

Checks on behalf of the TAG/MRTD which new technologies are suitable for use with ID documents.

> **Air Transport Committee (ATC)**

Helps ICAO to boost security for air transport.

> **Comité Européen de Normalisation (CEN), Brussels**

European equivalent of ISO.

> **CEN/Technical Committee (TC) 224**

Develops pan-EU standards for ID and signature cards as well as the connected systems and applications.

> **International Organization for Standardization (ISO), Geneva**

The world’s largest developer and publisher of standards. ISO is a network of the national standards institutes of 162 countries. The organisation sees itself as a bridge between the public and private sectors and implements in concrete technical standards the requirements laid down by organisations such as ICAO.

> **ISO Working Group 8 (WG8)**

Develops standards for contactless smart cards.

> **International Electrotechnical Commission (IEC), Geneva**

The world’s leading developer and publisher of standards specifically for electrical engineering.

> **ISO/IEC Joint Technical Committee (JTC) 1**

Joint ISO and IEC committee that develops standards for IT.

> **Standardization Committee (SC) 17**

This committee works for the ISO/IEC JTC 1 committee on standardising electronic ID cards.

> **European Union organisations**

These organisations determine the requirements to be met by the ID documents of the member states of the European Union.

> **Brussels Interoperability Group (BIG), Brussels**

Technical working group of the European Commission working to establish the interoperability of European ID documents.

**TRAVEL DOCUMENTS**

As previously explained in section 1, international travel documents today are designed as more than just photo ID, they are often already equipped with an integrated chip. According to ICAO specifications, they contain a machine readable zone (MRZ). The related specifications are laid down in ICAO document 9303. The current version of this standard comprises three parts: passports (Part 1), visas (Part 2) and other official travel documents (Part 3) and includes the following requirements:

> **Machine readability (9303, Part 3, Volume 1 – Guideline for ICAO-compliant ID1 MRTDs)**

The machine readable zone of ICAO-compliant ID cards usually contains two to three lines with information. They are printed in a standard format and with standard OCR-B characters that were developed in the late 1960s specifically to facilitate machine reading. The name, date of birth and other data of the document holder are stated here. Check digits allow the officer to check that the data has been correctly read using optical verification devices. Border control officers and other authorised agencies capture the data of the machine readable zone using optical readers, like the ones supplied by Bundesdruckerei, and send the data directly to an IT system. This makes document verification more efficient and prevents the officer checking the document from accidentally entering incorrect data into the system. In order for the document to be deemed to be machine readable as contemplated by ICAO, the required photo of the holder must...
also be of a specific size and arranged in a certain way. ICAO demands that all member states should replace conventional passports with their state-of-the-art, machine-readable counterparts by 2015.

FIGURE 3: MACHINE READABLE ZONE (ID1 CARD)

Biometric identification (9303, Part 3, Volume 2 – Guideline for ICAO-compliant eID cards / ID1 eMRTDs)
ICAO considers three types of biometric identification: facial recognition, which is already mandatory, as well as optional fingerprint and iris recognition. If such features of a person are stored on the chip of the ID card, the person’s identity can be confirmed each time they enter or leave a country. To do this, the border control officer compares the features either with the photo on the ID card or the data from the chip or with the information from a database. Cryptographic methods are used to ensure that the data on the chip is genuine, has not been manipulated and can only be read by authorised authorities.

Designing the security chip (9303, Part 3, Volume 2 – Guideline for ICAO-compliant eID cards / ID1 eMRTDs)
Only contactless integrated circuits are approved for international travel. ICAO has additionally defined a standardised data structure and certain security protocols to ensure that these circuits work reliably all over the world, are protected against unauthorised access and can be flexibly integrated into different IT structures. These requirements are explained in detail in section 4.

It is left to the individual states to decide whether or not to adopt these ICAO recommendations for their eID cards. It certainly makes sense, however, if electronic ID cards are to be used for international travel. In this case, national eID documents or electronic residence permits should also be designed in line with ICAO’s recommendations.

ELECTRONIC RESIDENCE PERMITS
Electronic residence permits, which up to now often came in the form of a sticker in a passport, can be easily issued as eID cards in ID1 format. Council Regulation (EC) 380/2008 specifies that in future all EU member states with the exception of Denmark will have to observe the same criteria when issuing residence permits to third-country nationals. This means that, beginning May 2012, the fingerprints of residence permit holders (over the age of six) must be stored on the chip of the document. In addition to this, Extended Access Control (EAC) is also mandatory. In Germany, the electronic residence permit, which is produced by Bundesdruckerei, was already introduced in 2011. This card, just like the new German ID card, is excellently protected against forgery and misuse thanks to a host of different security features. The document comes with an eID function and is also prepared for use of the qualified electronic signature.

DRIVING LICENCES IN ID1 FORMAT
More and more countries around the world are replacing their paper driving licences with more robust cards made of plastic. Electronic driving licences are already on the market in Australia, Canada, India, Japan, the US and other countries. ISO standard 18013, Part 1–4, already defines minimum requirements for the security and data structure of such cards. However, these requirements are not binding. It is left to the countries themselves to decide whether or not to adopt the standards.

The European Union, on the other hand, has issued binding guidelines for EU driving licences in Council Directive 2006/226/EC. A polycarbonate card with uniform security features is foreseen. Some of these features are mandatory, such as laser engraving and the omission of optical brighteners. Each country must additionally select three other security features from a list. It is also left to each country to decide whether or not a chip is to be integrated into the card to store additional data, for instance, in order to allow citizens to use the card to pay traffic fines. Beginning 2013, the EU driving licence card is to replace all the 110 types of driving licences in circulation up to now in the member states. Bundesdruckerei has been producing the German EU driving licence card since 1999. This card already meets with all EU requirements and complies with all current international security standards for electronic ID
documents. The EU driving licence means greater transparency for citizens, law enforcement officers and public authorities. Forgeries are easier to detect and card holders can rest assured that their licences will be recognised everywhere in the European Union.

**ELECTRONIC OFFICE ID CARD**

eID cards can help shape the changes taking place in the working world in a more secure and convenient manner. Now that many companies are determined to comply with security and quality standards, it must be possible to track processes, for instance, in logistics and production. Office ID cards with a security chip permit only authorised employees to enter certain rooms. Home-office employees can use their eID card to easily access the company’s virtual space in the same way as a colleague who has been temporarily deployed to a customer’s project office. This benefits employees, companies and the environment. Data security remains guaranteed without the necessity for permanent presence on site. Depending on how the card is configured, working hours can be recorded electronically, cash-free payments can be made in the canteen or documents can be signed electronically. Electronic office ID cards can come with a contactless chip, a contact chip or as a hybrid model. Bundesdruckerei helps companies and public authorities to adapt ID cards like these precisely to their specific needs.

**OTHER GOVERNMENT APPLICATIONS**

Since 2006, certain commercial vehicles in the EU must be fitted with a digital tachograph in order to clearly record that drivers observe the mandatory break times. Since the end of 2010, these cards have also been mandatory for many HGVs from other countries. Documents such as the electronic vehicle registration document or the electronic document of origin are also becoming more popular around the globe and ICAO is currently developing recommendations here.

**FUTURE-ORIENTATED eGOVERNMENT SOLUTIONS**

Greater proximity to citizens and transparency, less red tape and more efficient controls – these are the goals that are being pursued by a growing number of governments around the world. The European Union, for instance, is determined to exploit the potential offered by eID cards in order to achieve more efficient interaction between the private sector and the public administration. In 2011, more than half of the 27 EU member states were already planning national eID projects. Almost everywhere, conventional ID documents in ID2 format are to be replaced step by step by more robust multi-functional eID cards. There are, however, considerable differences when it comes to the individual card concepts. Many countries have their very own ideas with regard to security levels, data protection or the use of central databases. While multi-functional eID cards have become firmly established in countries such as Estonia, other countries still have a long way to go. There is a trend in Europe towards uniform card concepts that allow users to make use of eGovernment and eCommerce services, even across borders. The EU’s Secure identity across borders linked project, in short: STORK, aims to introduce an EU-wide platform. This platform is to allow citizens who have national eID cards to easily access online services in their neighbouring countries. The partners are working, for instance, on cross-border eLearning projects or on a service that allows citizens to simply change their address data no matter where they are in Europe.
Forgery resistance is the most important requirement that today’s ID documents have to live up to. In recent decades, new technologies have created numerous ways to effectively protect ID documents against unauthorised access and manipulation.

In addition to traditional, tried-and-tested security features, such as guilloches, high-tech solutions are increasingly being put to use. Optically variable and machine-readable elements are making ID cards increasingly difficult to forge. The many different features are broken down into substrate features, inks, types of printing, tactile and mechanical features as well as overlays and foils. Security features are integrated on all levels into multi-layer documents. In this way, they can supplement each other and boost the security of the card even further. The chips integrated into eID cards also provide electronic security features which are described in section 4.

Which security features are used depends on a number of different factors. A country using ID documents that comply with ICAO recommendations must consider different requirements than a country that wishes to issue ID cards to be used within its own borders. What’s decisive are the criteria which the ID card must fulfil: What is it to be used for? What kind of cost limits are foreseen? How much security is expected? How durable and robust should the document be? Are applications to be provided in co-operation with partners and do these applications have special technical requirements? Are the ID documents to be personalised in a centralised or decentralised process? Bundesdruckerei advises its customers on all these matters and helps them to find the ideal solution for the task at hand. This is one of the reasons why we have not included all possible security features in this publication. Document protection is a sensitive subject and Bundesdruckerei’s experts will be pleased to discuss particularly innovative solutions with you in person.

Greater complexity means greater security: the verification level
In order to be able to determine whether documents are genuine, border control officers, public agency staff and, in some cases, even business partners must be able to recognise and verify the security features of the document. The more complex the features, the higher the level of verification. Bundesdruckerei’s experts distinguish between three different levels.

> Checking the features of level 1 merely calls for familiarity with these features because they can be seen with the naked eye and no additional tools are required.

> Level 2 is broken down again into level 2a and 2b. The features of level 2a can be identified using simple tools, such as a magnifying glass, UV lamp or filter. When it comes to level 2b, the person checking must be skilled and have tools, such as an infrared camera, verification device or laser.

> Level 3 requires detailed knowledge of security features. These features can only be identified and verified using special laboratory equipment or sensors, such as a microscope, spectrometer or an x-ray device.

Refer to the table “Security feature functions and levels at a glance” on page 33.
SUBSTRATES

The substrate of the eID card is usually made of polycarbonate that is almost unbreakable, heat-resistant and abrasion-proof. The new German ID card, the EU driving licence or the electronic office ID card supplied by Bundesdruckerei, for instance, are made of polycarbonate. So-called semi-finished products are integrated into the substrate during production.

FIGURE 4: POLYCARBONATE

Fluorescent fibres are one example of this. These multi-colour, plastic fibres are randomly distributed between the individual polycarbonate foils when the foils are compiled. They are approx. 0.3 millimetres long and are visible to the naked eye or under UV light. Fluorescent fibres are mostly used in paper-based documents and sometimes in ID cards too. In the case of the Romanian EU residence permit, the fibres are spread evenly across the entire surface of the card. These fibres are only visible under UV light and appear in fluorescent green and red.

FIGURE 5: FLUORESCENT FIBRES

The same can be said for the security thread. Made of metal or plastic, this thread can be applied to the outside or inside of the card. Security threads can be coloured, fluorescent, printed with microlettering, holographic and machine-readable. The security thread of the new German ID card, for instance, runs horizontally on the back of the card and is personalised with the document number and the card holder’s name. The security thread, just like fluorescent fibres, protects the card against copying and counterfeiting. It is almost impossible for forgers to copy it or to obtain similar quality material.

FIGURE 6: SECURITY THREAD

INKS

Special inks create characteristic effects and make ID cards very difficult to forge. Inks can be distinguished on the basis of the level of their verification.

Level-1 effect inks

Level-1 effect inks are optically variable, iridescent and thermochromic inks. Optically variable inks (OVI) contain special

FIGURE 7: OVI
pigments that have a specific structure. This changes the colour depending on the viewing angle or lighting. In the title line of the new German ID card, the words “Bundesrepublik Deutschland” are printed using OVI. If the card is tilted, the colour of the lettering changes from green to blue. Other examples include the Slovakian ID card where the colour of Slovakia’s country code changes from magenta to gold or the Icelandic driving licence where the blue map of Iceland changes to red when the card is tilted.

Iridescent inks contain tiny mica flakes that act as mirrors and reflect the incident light in different ways depending on the viewing angle. The inks have a pearl-like shimmer.

**FIGURE 8: IRIDESCENT INK**

Thermochromic inks change when they are heated, for instance, by holding them in your hands. Once the ink has reached a certain temperature, it becomes transparent and the underlying information becomes visible or another colour appears. This effect is reversible and can be repeated any number of times. All level-1 inks protect the card against reproduction and are visible to the naked eye or using simple means.

**Level-2 and level-3 effect inks: Inks for an even higher verification level**

Level-2 effect inks are even more difficult to check. This requires tools, such as infrared or UV light. Level-2 effect inks include, for instance, UV-fluorescent, bi-fluorescent, up-conversion, UV-absorber, UV-phosphorescent, IR-effect, photochromic, metameric and magnetic inks. UV-fluorescent inks contain pigments that are visible under a UV lamp. The UV-fluorescent ink can be visible or invisible. On the front of the German ID card, the German eagle and the continuous wording “Bundesrepublik Deutschland” are applied as UV prints just like the country name on the Slovakian driving licence.

**FIGURE 9: THERMOCHROMIC INK**

**Bi-fluorescent inks** need at least two different UV light sources to change their colour, for instance, under a UV-A and UV-C lamp.

**FIGURE 10: UV-FLUORESCENT INK**

**FIGURE 11: BI-FLUORESCENT INK**
IR-effect inks need IR light to show different characteristics. They either specifically absorb the infrared light and this causes their colours to appear, or they are IR-transparent and hence have no colour. This kind of ink is ideal for protecting personalised data against manipulation.

**FIGURE 12: IR-EFFECT INK**

![IR-EFFECT INK Specimen](image)

**Level-3 effect inks** make it difficult to counterfeit an ID card. These inks can only be read with forensic tools. The fluorescent **Innosec® Colour CX** ink developed by Bundesdruckerei enables the light emitted to be specifically distributed, thus creating a unique profile in the spectrum. Innosec® Colour CX hence offers many different and, above all, customised coding variants.

**FIGURE 13: INNOSEC® COLOUR CX**

![INNOSEC® COLOUR CX](image)

**TYPES OF PRINTING**

Different types of printing create unique patterns and screens that protect eID cards against copying. **Guilloches**, an invention dating back to the 17th century, are used today in all modern cards made of plastic. The ornamental pattern comprises artfully intertwined fine lines. Guilloches are visible to the naked eye. If the lines are printed using fluorescent inks, they then become visible under UV light. Guilloches are used, for instance, to depict the German eagle on the front of the new German ID card and the Brandenburg Gate on the back. As in this case, guilloches can have several colours.

**FIGURE 14: GUILLOCHES**

![GUILLOCHE Specimen](image)

In so-called **rainbow printing**, the printer uses two or more inks that flow into each other. This merging of colours can be seen with the naked eye and, when combined with UV-visible inks, offers a high degree of protection against copying or counterfeiting.

**FIGURE 15: RAINBOW PRINTING**

![RAINBOW PRINTING Specimen](image)
Anti-copy patterns are hidden information that is embedded in background printing and which is invisible to the naked eye. During copying, they cause the so-called interference pattern to appear which clearly differs from the original.

**FIGURE 16: ANTI-COPY PATTERN**

Line screens create an image in the background. If an attempt is made to copy, the lines run into each other and create interfering elements.

**FIGURE 17: LINE SCREEN**

Microlettering is another widely used type of printing. It is used on the Icelandic and Slovakian driving licences to show the country name. Microlettering can be printed as positive or negative text and comprises tiny letters, numbers, motifs or symbols that are between 0.15 and 0.30 millimetres high. A magnifying glass is needed to read microlettering. This type of printing is difficult to copy and makes forging ID documents difficult.

Another means of protection against counterfeiting is the see-through register: Parts of the entire motif are printed in this case on the front and back of the document in such a way that the viewer cannot see the motif in its entirety until the document is held against the light.

**FIGURE 19: SEE-THROUGH REGISTER**

**FIGURE 20: EMBossing AND DEBOssing**

Tactile and mechanical features

In this case, lasers or dies apply images and text that can then be felt on the plastic card. Bundesdruckerei's experts distinguish between embossing (raised) and debossing (recessed) and penetrating features. Embossing and debossing on the surface of ID
cards are easy to feel and can also be combined. The German ID card features security embossing that comprises microlettering and a map of Germany on the back of the card. This creates a relief-type, tactile surface.

**Tactile laser engraving.** like the card number on the Romanian EU residence permit, is applied to the card using a laser. This engraving is raised on the card surface and can hence be clearly felt. Both features protect the document against copying and forgery.

The so-called penetrating features include **image perforation.** In this case, the laser burns small holes into the document that form images, symbols or logos. Image perforations are both visible and tactile and provide protection against copying and forgery.

**FOILS AND OVERLAYS**

In addition to the security features that are applied on or into the plastic card itself, so-called foils and overlays additionally protect the personal data visible on the documents. Foils and overlays can be applied to all or just part of the card and can also be integrated into the card. The integrated hologram is located, as the name suggests, inside the card body and protects the photo of the document holder. For instance, both the Slovakian ID card and driving licence have integrated holograms. They feature a kinematic structure and can contain machine-verifiable elements.

**FIGURE 23: CLI**

**FIGURE 24: INTEGRATED HOLOGRAM**

**Changeable** or **Multiple Laser Images (CLI/MLI)** are special forms of tactile and mechanical elements. Cylindrical lenses are applied to the surface of the ID card. A laser engraves different information at different angles into these lenses. Photos, logos or also personal data are shown, depending on the viewing angle. This security feature makes it possible to provide particularly good protection for the card holder’s personal data, thus effectively preventing copying or manipulation.
The so-called volume hologram with its kinematic structures is another security feature that is used to protect plastic-based documents. The special characteristic of this hologram that is applied to the surface of the document is its optical appearance. The holographic information is written directly into the volume of the holographic material so that this information only becomes visible when viewed at a specific angle. Unlike less complex holograms, the volume hologram does not show any rainbow effect, instead it only appears in one colour. Volume holograms feature an excellent brilliance and are very difficult to forge. German ID documents, such as the ID card, the driving licence and the passport, are all protected by this special type of hologram.

FIGURE 25: VOLUME HOLOGRAM

A PERFECT BLEND OF DESIGN AND SECURITY

Many of the aforementioned security features can be combined with each other in order to boost the security of an ID document. Both the document’s security features and design must meet with ICAO’s requirements. What’s important here is to achieve a perfect blend between security requirements and design. On the one hand, ID documents are like the calling cards of an issuing country or company. On the other hand, new national and international regulations call for the ongoing enhancement of security features for ID documents that could change the appearance of these cards. Bundesdruckerei is an expert when it comes to advising customers on the ideal combination of features and on custom document design.

SECURITY FEATURE FUNCTIONS AND LEVELS AT A GLANCE

<table>
<thead>
<tr>
<th>Security feature</th>
<th>Brief description</th>
<th>Area of application</th>
<th>Protection against</th>
<th>Verification level</th>
<th>Verification method</th>
<th>ICAO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Substrate</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fluorescent fibres</td>
<td>Security fibres that are mixed into the substrate</td>
<td>Paper, Plastic</td>
<td>Copying, Counterfeiting</td>
<td>Level 1</td>
<td>Level 2</td>
<td>Visual, UV lamp</td>
</tr>
<tr>
<td>Security thread</td>
<td>Made of metal or plastic, is applied onto or into the substrate, large range</td>
<td>Paper, Plastic</td>
<td>Copying, Counterfeiting</td>
<td>Level 1</td>
<td>Level 2</td>
<td>Visual, UV lamp, Machine sensor</td>
</tr>
<tr>
<td>Inks</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Optically variable inks (OVI)</td>
<td>Contain pigments which change colour depending on the viewing angle</td>
<td>Paper, Plastic</td>
<td>Copying</td>
<td>Level 1</td>
<td>Visual</td>
<td>ICAO optional</td>
</tr>
<tr>
<td>Indescent inks</td>
<td>Contain transparent pigments made of tiny mica flakes; they have a pear-like shimmer</td>
<td>Paper, Plastic</td>
<td>Copying</td>
<td>Level 1</td>
<td>Visual</td>
<td>ICAO optional</td>
</tr>
<tr>
<td>Thermo-chromic inks</td>
<td>Colourants respond to changes in temperature</td>
<td>Paper, Plastic</td>
<td>Copying</td>
<td>Level 1</td>
<td>Visual, by a change in temperature</td>
<td>ICAO</td>
</tr>
<tr>
<td>UV-fluorescent inks</td>
<td>Inks emit a visible spectrum under UV light</td>
<td>Paper, Plastic</td>
<td>Copying</td>
<td>Level 2</td>
<td>UV lamp, VISOTEC Expert 300/600</td>
<td>ICAO</td>
</tr>
<tr>
<td>Bi-fluorescent inks</td>
<td>Change to a different colour under two different UV sources</td>
<td>Paper, Plastic</td>
<td>Copying</td>
<td>Level 2</td>
<td>UV lamp with different wavelengths</td>
<td>ICAO optional</td>
</tr>
<tr>
<td>IR-effect inks</td>
<td>Different characteristics appear under IR light</td>
<td>Paper, Plastic</td>
<td>Copying</td>
<td>Level 2</td>
<td>IR source + IR camera, VISOTEC Expert 300/600</td>
<td>ICAO</td>
</tr>
<tr>
<td>Innosec® Colour CX</td>
<td>Spectral distribution of light creates specific characteristics</td>
<td>Paper, Plastic</td>
<td>Copying, Counterfeiting</td>
<td>Level 2</td>
<td>Level 3</td>
<td>UV lamp, Spectrometer</td>
</tr>
<tr>
<td>Types of printing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Guilloches</td>
<td>Ornamental patterns made of artfully intertwined lines</td>
<td>Paper, Plastic</td>
<td>Copying, Forgery</td>
<td>Level 1</td>
<td>Level 2</td>
<td>Visual, Magnifying glass</td>
</tr>
<tr>
<td>Rainbow printing</td>
<td>Inking method where two or more colours flow into each other</td>
<td>Paper, Plastic</td>
<td>Copying</td>
<td>Level 1</td>
<td>Level 2</td>
<td>Visual, UV lamp</td>
</tr>
</tbody>
</table>
### Security feature

<table>
<thead>
<tr>
<th>Feature</th>
<th>Brief description</th>
<th>Area of application</th>
<th>Protection against</th>
<th>Verification level</th>
<th>Verification method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anti-copy pattern</td>
<td>Elements integrated into background printing create an interference pattern when an attempt is made to copy the document</td>
<td>Paper, Plastic</td>
<td>Copying</td>
<td>Level 1</td>
<td>Visual</td>
</tr>
<tr>
<td>Line screen</td>
<td>Creates an image in the background</td>
<td>Paper, Plastic</td>
<td>Copying</td>
<td>Level 2</td>
<td>Visual</td>
</tr>
<tr>
<td>Micro-lettering</td>
<td>Comprises tiny numbers, letters, motifs and symbols</td>
<td>Paper, Plastic</td>
<td>Copying, Forgery</td>
<td>Level 2</td>
<td>Visual</td>
</tr>
<tr>
<td>See-through register</td>
<td>Individual images on both sides that create a single image when held against the light</td>
<td>Paper, Plastic</td>
<td>Copying, Counterfeiting</td>
<td>Level 1</td>
<td>Visual</td>
</tr>
</tbody>
</table>

### Tactile and mechanical features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Brief description</th>
<th>Area of application</th>
<th>Protection against</th>
<th>Verification level</th>
<th>Verification method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Embossing/debossing</td>
<td>Tactile embossing</td>
<td>Plastic</td>
<td>Copying, Forgery</td>
<td>Level 1</td>
<td>Visual</td>
</tr>
<tr>
<td>Tactile laser engraving</td>
<td>Creates raised images and text using a laser</td>
<td>Plastic</td>
<td>Copying, Forgery</td>
<td>Level 1</td>
<td>Visual</td>
</tr>
<tr>
<td>MLI/CLI</td>
<td>Laser images that change when the viewing angle changes</td>
<td>Plastic</td>
<td>Copying, Forgery</td>
<td>Level 1</td>
<td>Visual</td>
</tr>
</tbody>
</table>

### Foils and overlays

<table>
<thead>
<tr>
<th>Feature</th>
<th>Brief description</th>
<th>Area of application</th>
<th>Protection against</th>
<th>Verification level</th>
<th>Verification method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrated hologram</td>
<td>Hologram made on metallised or demetallised foils, embedded in the card body (rainbow effect)</td>
<td>Plastic</td>
<td>Copying, Forgery</td>
<td>Level 1</td>
<td>Visual</td>
</tr>
<tr>
<td>Volume hologram</td>
<td>Holographic film applied to the surface containing information which is incorporated in the film material; in one colour or several colours</td>
<td>Plastic</td>
<td>Copying, Forgery, Counterfeiting</td>
<td>Level 1, Level 2</td>
<td>Visual, Machine-based</td>
</tr>
</tbody>
</table>

### Section 4

**THE CHIP AS THE STRONGBOX OF THE eID CARD**

Taking up only a tiny amount of space, the chip contains everything an eID document needs. In other words, the chip is the communication centre of the card. To provide outstanding protection against unauthorised reading of the data, the chip is integrated into high-security ID systems.

It is the chip that transforms the eID card into a multi-functional document. It provides all the electronic functions and can also contain in digital form all of the information printed on the ID card. Biometric data can also be stored on the chip. This data creates an even stronger link between the holder and the card. According to ICAO, biometric data actually must be stored on chips in travel documents. The photo of the holder is captured according to specific quality criteria. The fingerprints can also be saved in the document. The respective data records are cryptographically secured and stored on the chip of the card. During a check, the fingerprint stored on the chip is then compared with the holder’s live print. If permitted by a country’s data protection laws, biometric data can also be stored in central databases, making automated, reliable comparisons possible.
CHIPS AVAILABLE
The type of memory medium selected depends on the requirements for the eID card. The card can be fitted with a contact chip or with a contactless chip. Combinations are also possible, for instance, using a hybrid model with both a contact and a contactless chip, or a dual interface solution with two interfaces on one chip. If the travel document is to meet with ICAO requirements, a contactless memory medium is mandatory. These chips have a much longer service life and are more difficult to manipulate or damage. They also have no separate source of energy, instead they draw their power from the electromagnetic field of the reading device.

The top-most priority for eID documents is protection against unauthorised access to the chip and its sensitive data. That’s why the eID document is integrated into a so-called public key infrastructure, a system that can issue, distribute and verify digital certificates. Only holders of valid government authorisation can read fingerprint data, for instance, stored on the chip. The certificates thus secure communication between the chip and various terminal devices, such as PCs, readers or update terminals. There are various types of PKI structures possible: National ID documents require integration into government PKI structures; eID cards that are used as online ID and for transactions between business partners are integrated into their own PKI structure. Companies and public authorities that use eID cards as office ID also require their own special PKI. Bundesdruckerei’s experts are familiar with the respective requirements and can offer their partners valuable support when it comes to implementing these structures.

SECURITY MECHANISMS OF A CHIP
ACCORDING TO ICAO
In order ensure the best possible protection for chips and that they work in different IT systems, ICAO has defined various standard procedures and security features. Many of these are also recommended for eID cards even if they do not serve as international travel documents.

> The data stored on the chip of official travel documents that can be used all over the world must follow a standardised logical data structure (LDS) containing a series of mandatory and optional data elements. Data group DG1 is mandatory. This is a digital version of the printed machine readable zone containing the holder’s biographical data, the document number and the expiry date. Data group DG2 is also mandatory and contains the digital facial image that is optimised for automated facial recognition. All other data elements are optional.

> In order to protect the chip against unauthorised access, ICAO recommends Basic Access Control (BAC), an access protocol used for passports by almost all countries. BAC protects especially against eavesdropping and so-called skimming which involves secretly reading out data from memory media using hidden readers. To combat this, BAC uses a complex cryptographic method to generate a key from the data of the machine readable zone (MRZ). In the case of the new German ID card, the Password Authenticated Connection Establishment (PACE) method is used. This ensures that the contactless chip is not released for reading until the CAN number recorded on the ID card has been entered. ICAO intends to establish this method on an international scale under the name Supplemental Access Control (SAC) in order to make BAC even more secure.

> The two mandatory data groups must support the Passive Authentication (PA) security mechanism. This basically contains a digital signature of the hash values of the data groups stored on the chip. The document signer, usually the ID card producer, generates the signature during chip personalisation. The card producer’s document signer certificate can be stored as a further option.

> A two-level public key infrastructure is needed for Passive Authentication. The certificates of the top level of the PKI hierarchy, as defined by ICAO, are issued by the national root authority, the so-called Country Signing Certification Authority (CSCA). In Germany, this is the Federal Office for Information Security (BSI). CSCA certificates are self-signed. They are sent through diplomatic channels to other countries and to ICAO so that with their help a check can be carried out to ascertain whether or not the digital signature of different eID documents is genuine. Authorised bodies can acquire CS certificates via ICAO’s public key directory (PKD). Using revocation lists, they can check whether certain certificates have been revoked and hence listed as invalid.
Section 4

> So-called Extended Access Control (EAC) is needed in order to protect particularly sensitive biometric data, such as the fingerprint stored on the chip. Up to now, EAC is only mandatory in the countries of the European Union. With this security protocol, the chip must first authenticate itself to the reader. This procedure is referred to as chip authentication (CA) and indirectly protects against attempts to clone the contents of the chip. In the next step, the reading device authenticates itself to the chip using an authorisation certificate (terminal authentication, TA). Only now can the reader access the fingerprint data stored on the chip.

THE eID FUNCTION OF THE CHIP:
ADDED VALUE FOR CITIZENS, PUBLIC AUTHORITIES AND BUSINESS

Whether ICAO-compliant or not, one of the most important features of eID cards is the freedom to assign functions to the chip that go beyond its official use. Take Germany’s new ID card, for instance. This card is now even more attractive because it can be used as online ID, making transactions between card holders, public authorities and private companies much easier. To facilitate this, many different functions can be added to the previously mentioned security mechanisms. The new German ID card, for example, supports restricted identification. This function allows pseudonyms to be generated automatically for the individual chip and for the respective transaction partner.

A key requirement for the eID function is that the chip must be integrated into its own high-security eID system architecture. This should not be seen as a replacement for the government PKI, but as an additional, separate system. In the case of the new German ID card, the cornerstones of this system are the ID card itself, the reader which card holders can use to read the data on their cards and to release data for online transactions, special driver software for the user PC and the so-called authorisation certificates for service providers. The eID service links these components and enables citizens and service providers to communicate with each other and complete business transactions via the online ID function. On an international level, this kind of service is subject to very different requirements. Its functionality, however, is always based on the same principles. There are generally two models available to online service providers. On the one hand, they can develop the hardware and software for the eID service themselves and independently control the administration processes for communication with the chip of the eID card. Since this involves considerable time and money, many providers choose to co-operate with specialists like Bundesdruckerei. These specialists provide the required infrastructure so that the online service provider and its partners can make use of the advantages of the eID function in a convenient and affordable manner. Details of how the eID service works can be found in Bundesdruckerei’s eID Service pocket guide.
SECTION__5
FROM THE DRAWING BOARD TO VERIFICATION

There are many steps that have to be performed before an eID card can be delivered to the holder. Bundesdruckerei supports its customers throughout the entire process. From data capture to document verification, the company serves customers with know-how and innovative solutions.

As explained in the previous section, eID cards are integrated into highly complex ID systems. The enrolment and administration of personal data are just as much part of this as are the production and issuing of the documents themselves. In order to ensure secure identities, the entire process chain must be effectively protected against manipulation and misuse. As a high-security company, Bundesdruckerei is in an excellent position to do this. The company has many years of experience in designing and integrating digital network structures. Since 2007, Bundesdruckerei has been successfully operating the world’s largest sovereign public key infrastructure. The company also helps its customers to draw up a requirements profile for a new eID card and use this as a basis to develop the entire process chain for matching ID systems. The focus here is always on the customer’s specific demands. Tailored solutions for private companies wishing to use electronic office ID cards are just as much part of our portfolio as is the introduction of complex, national eID documents in countries that issue large numbers of ID documents.

CAPTURING AND ENROLLING DATA

The convenient solutions supplied by Bundesdruckerei already begin with the capture of the card holder’s personal data, i.e., so-called enrolment. These solutions allow the complex processes to be handled in a simple and secure manner. The ID enrolment platform, for instance, contains several modules that can be combined and individually adapted to the customer’s specific needs. In addition to a hardware infrastructure with PCs and servers, these solutions also include readers for fast reading of data on previously issued eID cards, special cameras that are used to take facial images according to standardised criteria, as well as signature pads to capture signatures electronically and various kinds of scanners. They capture fingerprints, for example, as compressed images or scan forms. Once the data has been captured, special software checks its quality and then forwards it. Bundesdruckerei protects all of these steps with a reliable and secure PKI. The data captured is digitally signed and encrypted. Only persons and devices integrated into the system can access and process the data. This ensures that only genuine, authentic data is used in the next steps of the process. Bundesdruckerei’s electronic enrolment can be easily integrated into legacy IT landscapes. It meets with the highest data security requirements as recommended by ICAO. For the introduction of the new German ID card, Bundesdruckerei installed this kind of infrastructure at all of Germany’s 5,500 passport and ID card offices.

PROCESSING AND TRANSMITTING INFORMATION

In the second step of the process chain, administration, the data captured is processed and administered. In this case, central or decentralised database solutions can be used, depending on both legislation in the country in question and customer specifications. Even during transmission, the data is digitally encoded. Both text and optical information like photos are converted to bits and bytes and then encrypted. Users trying to access this data must first digitally authenticate themselves and furnish valid authorisation certificates. The administration of such certificates is performed.
by certification service providers like D-TRUST, Bundesdruckerei’s accredited trust center. D-TRUST sets up tailored trust centers for customers all over the world and adapts its certificate services to the specific needs of each customer. Additional special card and application management systems, including matching software, are offered for electronic ID documents which, for instance, enable digital signatures.

DEVELOPING AND PRODUCING DOCUMENTS

Bundesdruckerei uses state-of-the-art systems and the know-how of seasoned experts in its eID card production. This allows the company to offer customers a combination of various high-tech processes and to develop solutions tailored specifically to customer needs. Bundesdruckerei’s research department is working continuously on new production processes and is developing methods to integrate innovative security features into eID cards. All of the materials used meet with the highest quality requirements. Thanks to many years of experience in producing ID documents, Bundesdruckerei is in a position to shape production processes very efficiently. All of its production facilities have been audited and have received security accreditation according to the strictest international guidelines. But the company also expects the same high level of professionalism from its suppliers. Bundesdruckerei only works with suppliers who can demonstrate and guarantee quality.

CREATING AND ISSUING UNIQUENESS

An ID document becomes unique as soon as the applicant’s personal data is added. Bundesdruckerei operates one of the world’s largest special facilities for this. The company offers tailor-made solutions for personalisation to match the eID card concept. Customers can choose between individual components or complete personalisation systems. All solutions can be set up either as a central or decentralised system. When a central system is chosen, the data is managed by a single, high-security production site. It applies the personal data optically to the document, for instance, using laser personalisation machines, and at the same time writes the biographical or biometric data onto the chip. If the customer chooses the decentralised variant, optical and electric personalisation of the documents is then carried out at several of the customer’s regional offices which issue the ID documents directly. Irrespective of the method selected, Bundesdruckerei supplies advanced systems along with the required blank documents. Colour photo personalisation, for instance, is also used for the new German ID card. In this case, personalisation is carried out during production of the card body using a highly innovative inkjet printing process. The personal data is also laser engraved onto the card and can be partially felt on the card. For forgers, it is extremely difficult and almost impossible to copy this combination of different personalisation methods.

The personalisation solutions can be easily adapted to new types of documents. All of the software packages offered by Bundesdruckerei for this purpose meet with international standards. Bundesdruckerei also supplies reader and update terminals that enable the issuing offices to verify and edit the documents.

CHECKING AND VERIFYING DOCUMENTS

Public authorities and private companies need reliable devices and systems if they are to be able to check documents in a quick and reliable manner. This is where Bundesdruckerei provides national agencies with solutions such as the VISOCORE® Border Control Platform. The services in this package can be selected as individual modules and can be adapted, modified, activated and deactivated. In addition to ID checks by border control officers at national borders or airports, the modules also enable mobile checks, for instance, on trains. Fully automated processes can also be implemented where travellers can have their ID documents checked at self-service terminals. Depending on the specific requirements, the devices can be integrated into complex network systems that control access to central databases, for instance, for visas. Based on its many years of experience with official document systems, Bundesdruckerei has also developed solutions designed to meet the needs of the private sector. They allow bank staff, airline boarding staff or mobile phone company employees to check a customer’s ID quickly and easily.

eID MANAGEMENT – A TOPIC FOR TOMORROW

The eID service offered by Bundesdruckerei marks the next step here. This service enables the secure verification of digital identities and thus opens up a host of possibilities for innovative multi-functional cards. D-TRUST, Bundesdruckerei’s accredited
SOLUTIONS FOR TOMORROW’S WORLD

Bundesdruckerei enables public agencies and private companies around the globe to benefit from the new possibilities offered by state-of-the-art ID documents. To do this, the company is continuously broadening its know-how. Solutions are being developed by the company’s own innovation department and in co-operation with renowned partners to reliably protect and quickly confirm a person’s identity without any doubt whatsoever. These solutions warrant during times of comprehensive mobility that only authorised parties can access personal data. In this way, they ensure that anonymity and security are reconciled in the analogue and digital world: a decisive precondition if government, business and society are to be able to exploit the full potential of the digital revolution.

certification service provider, helps countries and companies all over the world to set up the structures needed for secure eID management. This centres around the implementation of special eID servers that send and manage authorisation certificates, check whether the chip in the user’s ID card is genuine and compare revocation lists. In this way, eID cards can be effectively revoked without having to store personal data in a central register. The eID service thus protects sensitive user data and safeguards all system users against economic damage caused by fraud with ID documents. The complex IT structure required to master this task remains invisible to both the user and the service provider. More information on this topic can be found in the Trust Center and eID Service pocket guides.

GLOSSARY

A

Authentication
a) Checking and confirming the identity of a person who is physically present or of an Internet user who has previously authenticated themselves.
b) Proof of one’s own identity, for instance, through knowledge (e.g. input of a > PIN), possession (presentation of an ID document) or > biometric features, such as > fingerprints.

Authorisation certificate
Must be shown in order to read the chip of an > eID card; enables access to previously defined data categories.

B

Basic Access Control (BAC)
Access protection for the data stored on > eID cards. BAC ensures that the data stored on the chip can only be read out by an authorised > reading device following successful > authentication.

Biometrics / biometric feature
The measurement of quantitative human features, making automated recognition possible. Important biometric features include, for instance, a > fingerprint, > iris recognition, the face or a person’s signature.
Certification Authority (CA)
A certification authority that issues digital certificates; this is another term used for certification service providers (CSP) and trust centers.

Certification Service Provider (CSP)
Also referred to as: Certification Authority (CA); a service provider authorised to issue qualified certificates or qualified time stamps. In Germany, only accredited CSPs are authorised to issue authorisation certificates, for instance, for Internet service providers who wish to allow their customers to use the online ID function on their websites.

Check digit
Simplest form of a checksum that is calculated from a host of digits using special methods. Makes it possible to recognise errors made when digits are entered manually; examples include ID card numbers, ISBN numbers or EAN codes.

Chip Authentication (CA)
A process where the chip must authenticate itself to the reading device; makes it possible to detect cloned chips.

Contact chip
A security chip with a visible interface; can only be read when it comes into direct contact with the reading device.

Contactless chip
A security chip without a visible interface; can be read without the need for mechanical contact with the reading device.

Country Signing Certification Authority Certificate (CSCA certificate)
Part of the PKI and an essential security element in electronic ID documents; contains the country code of the issuing authority.

Cryptography
A collective term that refers to methods for encrypting and decrypting information. This prevents unauthorised parties from accessing, changing or manipulating data.

D
D-TRUST
An accredited CSP operated in Bundesdruckerei’s high-security banknote printing building; offers private companies and public authorities tried-and-tested, interoperable signature products, certification services and electronic notary services.

Digital certificate
A digital data record that confirms certain features of a person or object and whose authenticity and integrity can be verified using cryptographic methods.

Dual interface card
An >eID card with two interfaces – a contact interface and a contactless interface. Unlike a >hybrid card, both interfaces can be accessed via a single chip.

E
eID
Electronic identity

eID card
A smart card that can be equipped with a host of functions, such as an electronic signature. Can also be designed as ID for both the real world and the virtual world, can serve as a driving licence or as an office ID card to enable access to security areas.

eID PIN
A self-selected PIN which the user must use each time in order to authorise the transmission of data from his/her >eID card to an >eID server.

eID server
A hardware and software infrastructure that enables communication between citizens and service providers on the basis of the online ID function.
**eID service**
Manages the entire communication with the eID card chip and ensures optimum security for transactions.

**eID system architecture**
A separate, high-security structure that exists in addition to the public key infrastructure into which the chip of an eID card is integrated. The cornerstones are the ID card itself, the > reading devices, special driver software for the user’s PC and > authorisation certificates for the service provider. The > eID service links these modules.

**Electronic documents of origin**
Documents which exporting companies need in order to prove the origin of goods. In many countries, these documents can now be applied for online using an > electronic signature.

**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 additionally confirms that the message has not been changed during transmission from the sender to the recipient.

**Enrolment**
Capturing the personal data required for eID documents. Bundesdruckerei, for example, offers special hardware solutions for this, such as > reading devices, special cameras, signature pads and various types of scanners.

**Extended Access Control (EAC)**
Extended Access Control for the data stored on the chip of > eID cards in which different protocols are bundled. These include, for instance, the > Chip Authentication protocols.

**Facial recognition**
A biometric identification method in which the face of the person to be checked is compared with one or more photos previously stored.

**Fingerprint recognition**
A biometric identification method where a fingerprint scanner first scans the fingerprint and then the image or a > template of the fingerprint is stored on the > eID card.

**German Federal Office for Information Security (BSI)**
National security authority, a subordinate unit of the Federal Ministry of the Interior (BMI), responsible for matters of security in the information society. BSI is responsible, for instance, for the approval of > reading devices that can read the chip of the new German ID card and for the accreditation of > certification service providers in Germany.

**Hybrid card**
An > eID card with both a > contactless and > contact chip. Unlike the > dual-interface card, two chips are integrated into the card body.

**ID1**
The world’s most widely used format for ID cards, standardised by the > International Organization for Standardization (ISO) under ISO 7815. ID1 cards are made of plastic and measure 85.60 x 53.98 x 0.76mm. The format is used, for instance, for national ID documents, driving licences as well as bank, credit and debit cards.

**ID2**
ID2 format measures 105 x 74mm; this corresponds to DIN A7. It was used, for example, for the old German ID card and is still used on an international level for residence permits in the form of visas.
ID document
A document that identifies and authenticates an individual; contains information that enables the authenticity of the document to be checked and proves the identity of its holder. ID documents are exclusively issued by public authorities.

ID system
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.

International Civil Aviation Organization (ICAO)
A United Nations agency; founded in 1944 by 190 countries in order to support international civil aviation through multi-lateral rules and to help create greater security; has also drawn up ICAO document 9303 which contains specifications for machine readable travel documents. Bundesdruckerei is the only company from the printing industry represented in ICAO. An overview of other important committees and organisations can be found on pages 13 to 15.

International Organization for Standardization (ISO)
A network of national standards institutes; draws up standards for all areas apart from electrics, electronics and telecommunications.

Iris recognition
A biometric identification method where a live photo is taken of the iris of the person to be checked and then compared with the reference image previously stored.

Laser personalisation machine
Machines which >eID card producers like Bundesdruckerei can use to apply personal data optically to the document and at the same time write >biometric or biographical data onto the chip.

Logical Data Structure (LDS)
Standardised logical data structure that defines a series of mandatory and optional data elements for the data that is stored on the chips of international travel documents.

Machine Readable Travel Document (MRTD)
Machine readable ID document with a format specified by >ICAO and featuring a >machine readable zone.

Machine Readable Zone (MRZ)
Visible part of an ID document that can be captured using optical character recognition. The MRZ of ICAO-compliant >eID cards usually contains the following information in standardised form: name, date of birth and other data of the document holder, as well as check digits.

Passive Authentication (PA)
Checks the authenticity and integrity of the data on the contactless chip of an >eID card. The data must be signed with the card producer's digital document signer certificate.

Password Authenticated Connection Establishment (PACE)
A >security protocol that protects the contactless security chip in an >eID card against unauthorised access. ICAO refers to this protocol as Supplemental Access Control (SAC).

Personal Identification Number (PIN)
A personal identification number that is known only to the lawful owner; used by an individual in order to >authenticate themselves to a machine.

Public Key Infrastructure (PKI)
Refers to a system that can issue, distribute and validate digital certificates.

Qualified Electronic Signature (QES)
An electronic signature which is based on a qualified certificate that was valid at the time the signature was created and is generated by a secure signature creation device. In Germany, the QES is legally equivalent to the personal, hand-written signature.
Reading device
Is needed in order to read data from ID documents; the reading device must authenticate itself with an > authorisation certificate in order to gain access to the document chip.

Secure Identity Across Borders Linked (STORK)
An EU project that aims to establish an EU-wide platform for the interoperability of electronic IDs.

Security chip
A readable, contactless computer chip that is integrated into > eID cards and is protected against unauthorised access by various > security protocols.

Security features
Various methods and high-tech solutions designed to ensure that ID documents are forge-proof. These are broken down into substrate features, inks, types of printing, tactile and mechanical features as well as overlays and foils. A detailed overview of the security features that can be used in eID documents can be found on page 22 and following.

Security protocol
Defined scheme of data sequences for communication between a chip and a > reading device. Security protocols, such as > Extended Access Control or > Password Authenticated Connection Establishment, ensure data protection, protection against forgery and the authenticity of the data on the chip of an > eID card.

Signature certificate
An electronic certificate that a citizen needs in order to use the > qualified electronic signature.

Supplemental Access Control (SAC)
Refer to > Password Authenticated Connection Establishment

Tachograph card
An eID card that is used as a digital tachograph, for instance, in long distance transport. It contains the driver’s ID and can document activities, such as compliance with mandatory breaks.

Template
A file containing only the most important information for identifying a previously captured > biometric feature and hence requires much less memory.

Trust center
An accredited > certification service provider (CSP).
FOOTNOTES

01 http://ec.europa.eu/internal_market/payments/e invoicing/index_de.htm
02 Refer to The Global National eID Industry Report – Acuity Market Intelligence (2011), page 15
03 Refer to the study titled The Future of Personal Identification to 2016 by the Printing Industry Research Association (PIRA) from 2009.
eID CARD
POCKET GUIDE
___2012