Security requirements for future ID documents

Physical security requirements for next generation identity documents

by Dr Roland Gutmann

Modern identity documents have to meet various technical requirements in order to be considered secure and fully functional. In addition, they should enable a fast and reliable match between documents and their owners. The security requirements aside, modern documents need complex graphical background designs, ideally reflecting the national identity and lifestyle of the issuing country. There are various approaches to achieving an effective solution for states and supranational organisations. As many citizens of industrialised states are frequent travellers, their documents are used in a large number of countries, so document security should be considered an international topic. In this article, Dr Roland Gutmann shares his forward-looking definition of highly secure identity documents.

The production of secure identity documents is a very complex topic since various distinct aspects have to be considered. Before production can start, a process has to be created covering data capture, data transmission (in case of centralised personalisation) and the delivery of the document to its owner after production. When the production of a security document is planned, the production environment, the specified security level, customer requests or concerns, the durability of the document and the individual security features have to be considered. And lastly, the control, the verification and the identity match between the document and its owner have to be dealt with.

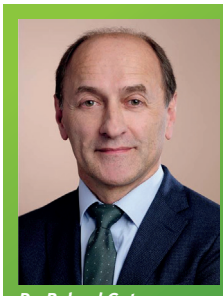
Security requirements for document production facilities

Production facilities for identity documents have to meet various security requirements. These include: a secure and CCTV-monitored building, employee access/exit control, and two or more security levels for the administration and the production area with entrance control and reporting of all incoming and outgoing data, materials and products. Documentation of the material flow, including the registration of waste material and the destruction of invalid documents, is an additional requirement. Furthermore, all partners, subcontractors and customers have to sign a non-disclosure agreement. Finally, a highly secure data network with limited and registered access which is controlled by certification and/or customer audits is strongly recommended. For more details, please consult the security production recommendations of ICAO.[1]

Security requirements for documents

The security requirements for the identity document itself are of highest importance, because these documents, once released, will be scrutinised for their potential to be re-engineered, manipulated or otherwise tampered with. Hence, it is of the utmost importance that identity documents are able to withstand attacks such as the change of personal details, the separation and re-use of individual security elements or the design and production of a counterfeit document. A recommended approach for customers would be to insist on a background design with a high resolution, the use of non-CMYK colours, security printing and a combination of different printing techniques in order to prevent forgery and counterfeiting. A highly secure card set-up should also protect the background design and the personalised data and different personalisation methods and data redundancy will further enhance the protection. Non-surface personalisation technologies such as laser engraving or an ink penetration into the substrate layer allow the data to be integrated in the printed security layer. Data and background overlaying security printing[2] and the encapsulation of the card with a transparent overlay with a graphical structured surface also offer essential protection.

The following paragraphs will cover this highly sophisticated approach in more detail and provide several examples which will give the reader more insight into the creation of secure ID documents. As not all aspects can be discussed here in detail, data handling, including data acquisition, encryption, transmission and the electronic recording on the RFID chips are not covered in this article.



Dr. Roland Gutmann *started as a Research Project Manager at the Swiss Material Research Institute EMPA, after his PhD in Physics at the ETH-Zürich in 1993. As of 1996, he joined the R&D group at the German Government Printing Office, Bundesdruckerei GmbH in Berlin, developing new features and verification systems for ID documents, bank notes and stamps, and defining and specifying new documents like the German eID-card, the electronical residence permit and the German ePassport. Parallel to the development activities Dr. Roland Gutmann became an active member of different national and international standardisation groups in 2004, for ID documents and driving licences. In 2015, he was appointed as Vice President at the lamination plate producer VTT, Germany.*

Figure 1:
European residence permit with laser engraved 3D image, additionally protected with a holographic overlay at the top right corner of the image.

Design requirements

The design of a security document is quite a challenge, because it has to cover general security requirements, specification issues, production aspects and customer expectations regarding a design that reflects the nationality of the final holder. Without considering the security aspects, the background design has to be developed with professional prepress software which makes re-engineering the document design with standard software and hardware difficult. Choosing non-CMYK colours impedes potential scanning and printing attacks. Multiple guilloche structures using faint, interlacing patterns or lines of symbols and faint colour gradients (rainbow printing) are very difficult to reproduce. The design is subject to the available security printing technology as well as the security feature and design elements specifically requested by the customer (e.g. MLI/CLI, window element, national symbols or flags and the MRZ-zone).

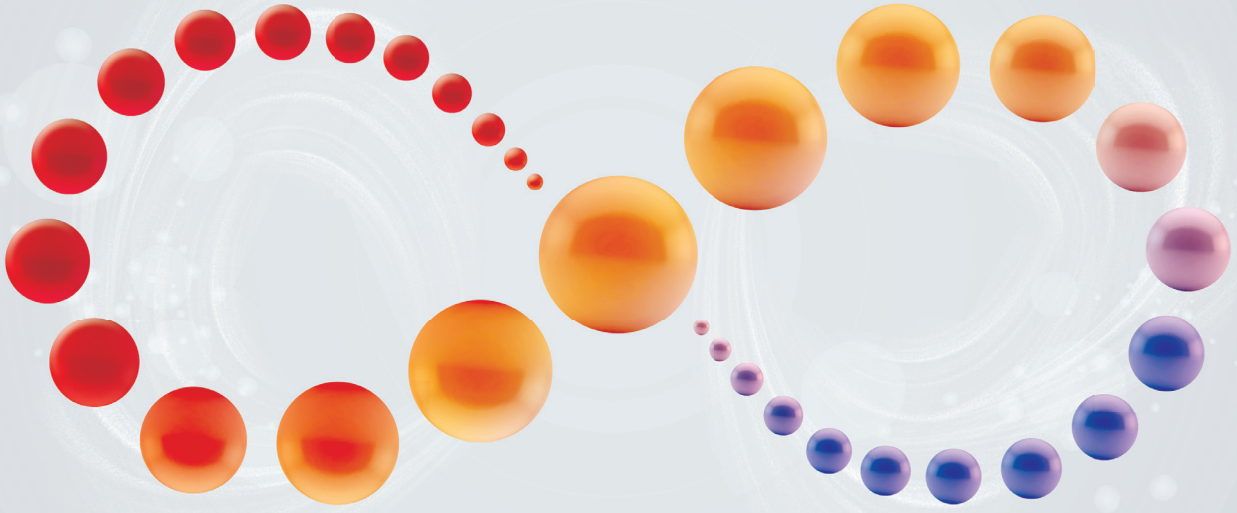
Card body set-up

For most customers the card body construction is not a point of discussion and it is generally an internal development or production issue. Readers interested in this topic will therefore hardly find any detailed recommendations, standards or specifications. It is usually the list of security features which determines the choice of material. The card body material is important when it comes to enabling security features and protection against manipulation. This topic is quite complex, and some of the most important requirements are:

- UV dull card material
  Traditionally, security documents are made of UV dull materials. This improves visibility of various UV elements, including very faint ones which are printed or added as stripes or planchettes.
- Background printing on different layers
  This means that the data side consists of more than one printed layer. The personal data and the photo of the document owner could each be printed in their own layer. It is ideal to enclose the personal data between two printed layers. The top layer could then be a UV print which is invisible in daylight.
- Tamper-evident card body
  A tamper-resistant and/or tamper-evident card body includes a transparent overlay on both the front and the back of the card. The personal data of the holder would be in one of the inner layers protected by a graphical structured surface (see examples). The prevention of various card materials, standard adhesives, ink coverage below an acceptable limit, as well as the protection of the personalised data on the front and back and the use of complex security elements integrated during the printing, lamination and personalisation process, such as CLI/MLI, play an important role in making the card tamper-resistant

NEW

NAME
FORMAT
TARGETS
LOCATION



-THE LEADING TRUST-BASED TECHNOLOGIES EVENT-

29 Nov. › **01** Dec.
Palais des Festivals
Cannes France
2016

www.trustech-event.com / #Trustech2016

an event by
comexposium
The place to be

TRUSTECH
PAY | IDENTIFY | CONNECT & SECURE
Incorporating CARTES
SECURE CONNEXIONS

Figure 2: (Top left)
European driving licence with laser engraved data, hologram patch, MLI, 1-line MRZ and a personalised window element (green patch on the right hand side of the card).

Figure 3: (Top right)
German e-ID card with an internal, tamper-proof inkjet colour photo and laser engraved personal data.

and/or tamper-evident (see Figure 1). The card body could be further protected by applying or integrating UV fibres, planchettes or holographic threads in one of the core foils or layers.

- Window element

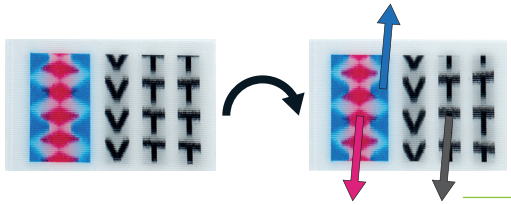
A strong security feature is the transparent window element which nowadays is often found in high-tech identity documents, passport cards and driving licences. This feature has been used in polymer banknotes for over a decade and since a few years window elements have also become more popular in complex, multilayer and ISO-conform polycarbonate ID-1/3 cards.[3] Whereas in a polymer banknote the window element simply needs an unprinted area on both sides, a window element in a laminated card is more complicated as the card consists of graphical, RFID-functional and pre- or post-laminated personalised layers. A window can be incorporated into a card by partially printing the surface or by punching or cutting an opening in opaque card bodies which is then filled with transparent elements. There are also technologies available to integrate security elements into the window that are visible in daylight or under UV light. In addition, the window element can also be individualised or even personalised using a suitable card body set-up (see Figure 2). Finally, adding a graphical (see Figure 3) or optical diffractive surface structure (see Figure 4) makes counterfeiting or tampering with this feature very difficult. If the requested card set-up is translucent, there is also the possibility to generate a front-to-back adjusted element with see-through elements and reflective elements which together form a complete symbol or image. The individual elements can either be created using a printing process with a sheet-turning module or by registering the background printing on the front with the printing on the back of the card.

Card production

Individual production steps such as printing, lamination and personalisation also offer various possibilities for increasing the card body security of ID-1/3 cards. However, post-lamination refinement processes such as the application of top coating foils with optical effects can be difficult as the properties of foils are different from those of the card body material and glues. This also applies to the use of any material other than the card body with a size between 1 mm² and 300 mm² in or on inner layers. Customer requests are more likely to be accepted if a single card body material (100% pure) is chosen. RFID inlays for PIC cards and/or contact chip modules for IC cards are no topic of discussion, because there exists no alternative.

Figure 4:
Window element combined with a nanostructured surface embossing integrated during the lamination process.

Figure 5:
Lens-structured CMI® (Convers Moving Image).



Printing process
Starting with the printing of the background layer, non-CMYK inks are mandatory as explained in the design chapter. Any printing equipment used should not be commercially available and it is strongly recommended that at least one printing technology (for example off-set, letterpress, flexo-, or silkscreen) is used. To enable a strong enough bond between printed and non-printed foils, the ink coverage should be limited to 30-40% of the surface. If a higher ink coverage is necessary for elements such as national symbols or flags, the size of these elements should be reduced to enable the layers to bond. In terms of printable security features, there are various first, second and third level optical and non-optical (for example magnetic) features available. At the top of the list there are several types of UV pigments, printed in ink which is either visible or invisible in daylight. In both cases the pigments are just added to the base ink. Further optical inks worth mentioning are IR effect (including anti-stokes) based pigments, optical effect pigments such as Iriodin and OVI/OVF, and thermochromic pigments, all added to standard security ink systems. Finally, there are also pigments for non-optical effects which are used in magnetic, metallic or conductive inks.

Lamination
After the printing of the front and back designs the sheets of the complete card set-up will be joined and laminated. The lamination process is responsible for a coalescing connection between the individual layers which prevents the separation of individual elements or foils without a reduction of the print quality or visible damage to the card body. If a graphically structured lamination plate is used, state-of-the-art surface elements such as MLI/CLI lenses, guilloche patterns with micro-lettering, areas with different surface textures (glossy/matt) and latent images can be integrated during the lamination process (see Figures 5 and 6).

Innovative lamination technologies combine the graphical background printing of the card design with the surface structure of the laminated cards (see Figures 5 and 7). In addition, new lamination plate production processes allow the in-situ creation of sub-nm structures or specially formed 3D shapes for multiple latent images, 3D photographs (see Figure 1) or even optical diffractive elements known as holograms (see Figures 4 and 6) on identity card surfaces. All this is possible without the use of foils or additives such as glues, which are often needed when adding holographic patches or complete top coatings with optical diffractive structures.

Personalisation
The final step in the card production process is the integration of personal data and a photo of the document owner. The personalisation of identity cards should be carried out in a secure production environment, preferably at the same location where the blank cards are produced, in order to prevent the loss or theft of blank cards on their way to a decentralised personalisation facility.

They should be personalised using highly specialised technologies such as laser engraving. Laser engraving enables a card set-up dependent integration of the data inside the laminated card body. Additional security features such as tactile elements, micro-letters, viewing angle dependent information (MLI), 3D and ghost images can also be personalised in a secure way. Technologies based on a surface personalisation should be avoided, because the data can be changed or replaced quite easily, even if protected by so-called 'protective overlays.'

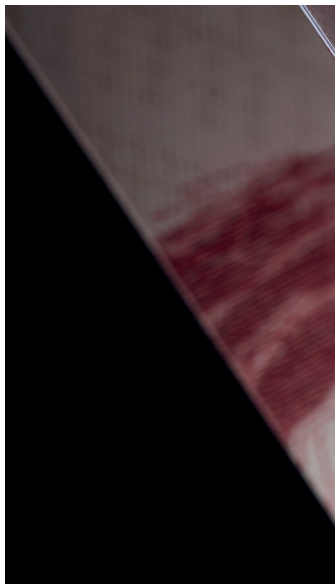
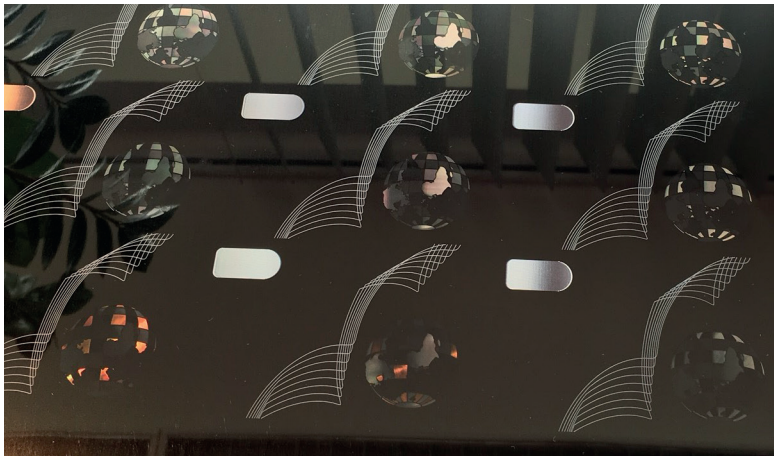


Figure 6:
Lamination plate for ID-1/3 cards with various surface security elements including holoPHOTIC®.



Cards can be personalised either in colour or in black-and-white. For polymer-based identity cards the latter can be considered the most secure technology, because the individual data are integrated in the card body after lamination and directly connected to the security printing. The positioning of the data can be determined in the card set-up. Colour personalisation has its drawbacks, because the known technologies are either surface-based or do not offer a connection between individual polycarbonate (PC) sheets if applied inside the card. New processes like the solvent-based 'in-melting' of colour pigments using liquid PC (inkjet) are restricted to pre-personalised individualisation or still lacking contrast and quality for first colour laser engraved personalisation.

Future prospects and summary

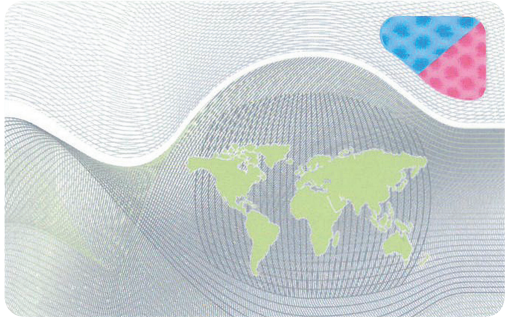
Highly secure identity cards including passport cards are and will remain an important product for identification and authentication purposes. Alternative means of identification such as mobile documents and cloud-based solutions are being developed, but face a number of problems in regard to the security/protection, verification and availability of personal data.

Physical identity documents already have many sophisticated security features, and further improvements in the quality of background printing enable a growing number of states to take the 'secure road.' In the case of non-chip cards, high-quality registered front-to-background printing and various other printing technologies such as offset and flexographic printing will be combined on a single printer. The silkscreen process for cards creates problems regarding the bond strength in multilayer card bodies, because the ISO requirements for inks without additional glues/adhesives are not achievable. Glues and adhesives are not a solution for identity documents with a validity of 10+ years, as they limit the lifespan of the document.

Regarding security features, there is a trend towards more complex and high-security features in background printing, card set-up, personalisation and graphical surface structure. Especially the relatively new transparent window element in PC cards offers numerous ways to increase the security of a document, by combining various advanced security features as well as production steps and produces highly secure identity documents.

References

1 *International Civil Aviation Organization - ICAO (2015). Doc 9303: Machine Readable Travel Documents. Part 2, Specifications for the Security of the Design, Manufacture and Issuance of Machine Readable Travel Documents. Current version: seventh edition.*
2 *Muth, O. (2012). Secure colour personalisation, Keesing Journal of Documents & Identity, Volume 39, pp. 23-27.*
3 *ISO/IEC 7810. Identification cards - Physical characteristics. International Organization for Standardization. Geneva, Switzerland.*



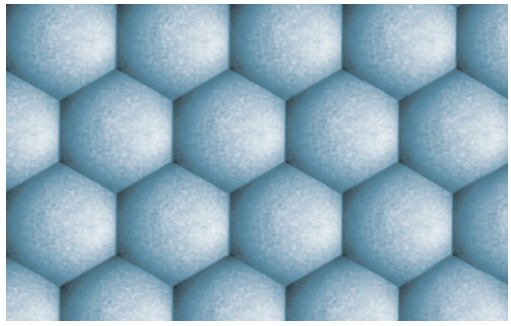


Figure 7:
3D security features Fly-Eye® on a PC card (left) and the lamination plate for producing the surface structure (right).