Smart-card security—security features

To manage access authorization or to provide person-specific configurations, identification options are needed. These tasks are often realized by **ID or smart cards** using unique security and characteristic features consisting of several layers. They work, depending on configuration, with or without contact. Security features on smart cards are categorically divided into **physical** or **digital** as well as **visible** and **invisible**.

Security features on chip cards prevent the following threats:

- Unauthorized readout of information (confidentiality)
- Unauthorized change of information (integrity)
- Unauthorized withholding (availability)
- Unauthorized modification of identified data (authenticity)

**In this blog entry some important applied security features will be introduced.**

Photos:

![Smart-card example](image)

The **most obvious and widely used security feature** for personal identification is a passport photo. These are applied to the card in high quality through color printing, usually using the inkjet drop-on-demand method or sometimes through laser engraving and other techniques. Passport photos have the great advantage of functioning **without a reading device**. In addition, supplemental bio-metric data can be added to photos on driver's licenses or ID cards to render them machine-readable.

Ghost Images:

A ghost image is a semi-visible graphic, usually another photo of the cardholder, which is applied to the card. Sometimes ID numbers or logos with reduced transparency are also printed into the background of the card. The process is inexpensive and can be copied only with great difficulty.
Signatures:

In addition to photos, **reference signatures** on cards are also a common safety feature, including when paying by debit or credit card. Security signature fields **increase the copy protection** in that the signing area can be damaged obviously by friction or contact with chemicals.

Laser engraving:

Using different laser types with varying wavelengths, **names, card numbers or other inscriptions** can be engraved into cards in a manner that is easy on the card material. Through engraving, **labeling is not removable**. The process of engraving labels has simple and variable programming.
Barcodes:

Barcodes allow for computer-based precise identifying. They can be applied to cards in one or two dimensions especially cost effectively. QR codes can also be printed.

Embossing:

Through pressing the back of a card, the surface of the front becomes raised. Thus numbers, names or logos can be displayed 3-dimensionally. In addition to aesthetic appearance and practical use, for example manually carbon copying credit cards, the process also makes it difficult to copy cards. Furthermore, haptic features make it easier for visually disabled people to read cards.
Holograms:

A hologram is a 3-dimensional graphic using complicated methods of multiple layers and laser technology that can be placed anywhere on the card surface prior to lamination. Depending on the angle there is a different space of the image can be viewed. With an addition a matt layer reading the graphic becomes more difficult. The 3-D effect is inexpensive, durable and is considered to be difficult to forge.

Holographic overlays:

The surfaces of personalized cards are protected from scratching, color loss and destruction of electronic components using laminate layers. Holographic overlays are lamination layers with an applied structure of a holographic image. With this method, two or three dimensional images can be rendered.
Effect colors:

Using UV or IR active colors, lettering, designs, logos or even photos may be displayed that can be invisible in normal light. Cards that are labeled with UV or IR colors glow under ultraviolet or infrared light. Also so-called OVis (optically variable inks) are used, which change color depending on light. Another application of the effect colors are so-called thermochromatic inks. These change color or become transparent through applying heat, e.g. friction. Such imaging can only be produced through complicated printing processes or using blank cards with a special coating, which are then individualized by lasers. Moreover, these graphics can be implemented depending on the viewing angle. These procedures protect against color copying or scanning fraud.

Guilloche:

Closed, interwoven lines are applied to the surface of the front and back. The fine lines often form asymmetric patterns such as ellipses or circular paths. Manipulated cards can be identified by broken guilloche patterns. They can only be applied
during the manufacturing process and cannot be copied.

Microprinting:

Microprinting appears to be normal lines to the naked eye. With a character height of less than 0.3 mm, it is usually only readable under a magnifying glass or a microscope. Color and font can be freely selected. Through its fine structure, microprinting is **not able to be copied, but can only be printed.**

Magnetic stripes:

On many cards, there is a **cost-effective magnetic stripe coated with a metal oxide.** The data on it can be read electronically through swiping or inserting it in a reader. There are primarily two types of magnetic stripes in use: HiCo (high coercivity) and LoCo (low coercivity). They differ in the magnetic flux density required for reading and writing. **LoCo magnetic stripes** operate at about 30 mT, which are used in current debit and credit cards. Through relatively weak external magnetic fields, such as a poorly constructed speaker box, the information on these stripes can be erased. In contrast, **HiCo magnetic stripes** operate around 300 - 400mT and are highly resistant to external influences.
Microchips:

In comparison to magnetic stripes, microchips have the advantage of being not only passively readable, but also function actively with low processing power, their own operating system as well as readable and writable protected memory. Thus, these small microprocessors allow the use of complex encryption techniques. With advanced technology, microchips are now protected against the metrological reading of the applied encryption algorithm.

RFID:

While conventional microchips transmit data via contact, it can be achieved without contact using RFID inlays. The antenna in the card is supplied with energy by an electric field emanating from reading device. The contactless technology enables easy handling and a reduction of contamination as well as wear.
CLI / MLI:

CLI (changeable laser image) / MLI (multiple laser image) are floating images, which show different graphics depending on the viewing angle. Either individually or stacked, layers are irradiated from different angles with lasers. The use of CLI / MLI technology makes copying difficult and remains visually checkable. This technique is used, among other instances, on German driving licenses.

Invisible Personal Information:

Personal information is stored hidden on the data carrier, for example a birth date in the background of a passport photo. With the help of software encryption methods, unique characteristics are encoded and applied invisible to the human eye on cards. Only with special lenses and the appropriate software are the cards then able to be read by devices.
Summary

Today in many areas, ID and smart cards are able to be personalized practically and securely. The proliferation of these smart cards will increase strongly in the years to come, which also means a rise on the demands of the security features of these cards. Copy and fraud protection can indeed be realized in many ways, whereas the security of the card is only established through the entirety of the applied features. In addition to optical characteristics, cryptology and software play an increasingly important role. Through improved chips, new materials and sophisticated software solutions, the usability and security of individualized plastic cards increase.

card personalisation [1]

Source URL: https://www.ruhlamat.com/en/company/blog/smart-card-security-security-features

Links