Working paper

OPTAGLIO®
OPTICAL MICROSTRUCTURE TECHNOLOGIES

The strongest possible protection is not the most expensive one

Clever anti-counterfeit solution for polycarbonate cards

Mass immigration, terrorism and general deterioration of security situation underline the necessity of absolutely reliable identification and authentication of persons. The latest development has confirmed that no technology can eliminate the need for secure physical documents. Current requirements on anti-counterfeit protection are higher than ever before.

We therefore witness a massive transfer from paper-based documents to more advanced technologies. More than 120 states that either issue plastic e-ID cards or are preparing their issuing. According to Acuity Market Intelligence, 3,6 billion people will be equiped with such personal documents by 2021.

Polycarbonate challenge

Counterfeiters shift their focus on those who stick to the older protection technologies. In some cases, they will be successful. Consequently, the frequently attacked documents will not be accepted as fully trusted and their holders must expect more detailed checks. This situation brings new challenges for partners of governments, such as security printing companies and card producers. To meet all requirement and keep their position of preferred suppliers, they need to ensure the following.

- Counterfeiting or tampering of documents is either impossible or sufficiently difficult and expensive to deter attackers.
- The appearance of the documents demonstrates technological forwardness of the issuer. The holders can be proud of their documents.
- The production process ensures that documents are delivered on time and quality, with strict adherence to all security rules. The documents have sufficient durability
- The process of document issuing and personalisation is smooth, well organised, without any security risk and ensuring irreversible and unalterable personalisation.

The following text is focused on aspect a), anti-counterfeit protection. Other requirements will be discussed in separate documents.

Successful attacks and requirements on protection

The criminals attacking documents are successful if the fake is accepted as a genuine document during at least one check. It results that the following aspects need to be covered:

- The document.
- An inspecting person – his/her skills, motivation, training, information received technical support etc.

Attackers often focus on guards with the lowest level of skills and experience, unsufficient motivation, nonfunctional infrastructure and weak knowledge of the particular kind of document. The protection has to ensure that the fake is not accepted even under such conditions.

Therefore it is necessary to cover the following areas:

DOCUMENTS with the critical features

- Imitation and/or copying is impossible
- Distinctive protective elements
- Protective features are distinctive and can be identified by intuitive inspection
- The documents support automated checking (machine reading, comparison with information in centralised database etc.)

TRAINING OF INSPECTING GUARDS

- Ability of determination if the document is genuine based on visual inspection
- Ability to use electronic checking tools

“ Counterfeiters shift their focus on those who stick to older protection technologies.“

It is important to cover also inspections in other countries and/or non-members of law enforcement system. Some inspectors will see the particular document for the first time in their life. Therefore it is necessary to provide them with information on the main protective elements. Tools such as Keesing documentchecker database are handy, but it is unlikely that the supervising person has paid access. Basic information about protective elements should be therefore available on the Internet.

Role of physical document in authentication scheme.

ELECTRONIC ENVIRONMENT

- With functions covering automated check of genuineness as well as check against a black list
- User friendly

Defense strategy

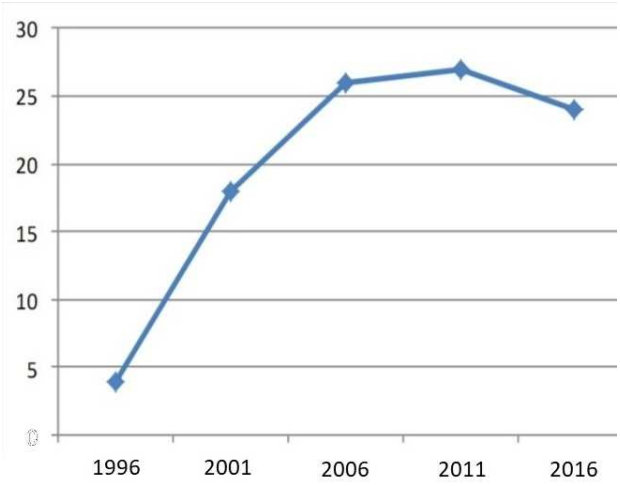
Absolute security can be reached only scarcely ever and for short term. However, it can be ensured that costs for any attacker are sufficiently high to deter. Anti-counterfeit protection has always been based on this assumption. From delicate fabrication of old coins trought printing with red ink to the latest nano technologies, protective technologies are focused on dramatic rising costs of imitation.

In last two decades, the strategy of anti-counterfeit protection was based on:

- Production of more and more sophisticated and expensive elements. It can be demonstrated, e.g. on changes in guilloches and holograms. The prevailing trend is towards intricate optical effects.
- Adding more and more additional protection features. Each version of each document includes elements that have not been applied before. On some documents, there are more than 30 security features, including guilloche patterns, clear windows, watermarks, serial numbers, micro perforation, printing with special inks, UV ink blockers, laser ablated generic patterns, microprint and offset microprint.

Strong but not confusing

However, the second point faces an issue of inspection. If there are too many security elements on a card, the inspecting person can be confused. The very latest tendency, therefore, leads to decrease in a number of features.



Number of elements on identity cards according to start of issuing. Source: Keesing Tehnologies

The best strategy consists in an implementation of a limited number of elements. Some 3 – 5 of them should be easily identificable during an intuitive visual inspection.

The following levels of inspection need to be covered.

- **Primary inspection** with the naked eye, without a need for special user training. Elements on this level are often called Level 1 elements. Most of the standard security items such as guilloches, watermarks, embossing and holograms are in this group.
- **Machine reading**, including comparing of biometric data from readers with information saved in the document, eventually check against database.
- **Detailed inspection** on a different level, including forensics.

"If there are too many security elements on a card, the inspecting person can be confused."

It is critical to cover four kinds of attacks:

- Manufacturing of a fake document, including imitation of all security elements.
- Removing of security elements and their application into a new card.
- Tampering with personalisation data.
- A stolen document is used by a wrong person.

Implementation of security elements integrating them into polycarbonate

A lot has been said and written about benefits of polycarbonate as the substance for ID cards production. However, specific polycarbonate features create also challenges for card manufacturers.

The card is laminated at the temperature of 180° C, which some security elements cannot sustain. It is especially aggravating that PET foils, the common material for holograms printing, are irreversibly damaged at such temperature.

Polycarbonate has a low ability to connect with other materials. In some aspects, it is a strong benefit because it results in stability. On the other hand, it complicates integration of heterogenes security elements. A layer enabling removal of a security element can grow up at the at material boundary easily. Bubbles or other abnormalities complicating visual access to security elements difficult can appear as well.

Therefore any effort to select and integrate of security elements need to deal with these polycarbonate specifics. From almost unlimited choices in protection elements, the attention should be drawn to the following ones.

"A layer enabling removal of a security element can grow up at the at material boundary easily."

POLYCARBONATE

counterfeiting is thus created. Moreover, the producer needs different types of polycarbonate for different layers (e.g. personalisation layer).

Another anti-counterfeit bareerr can be built throught sealing of protective microparticles into polycarbonate. A range of microparticles can be applied with different levels of resistance, from simple strings up to microholograms.

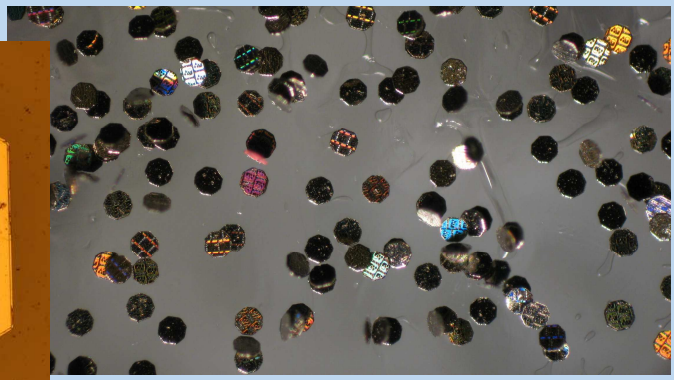
HOLOGRAM

There is a range of holograms providing very different protection levels. Every hologram needs to resist two basic kinds of attacks: imitation, and removal from a card. The basic defense principles will be shown on the most advanced solution in the market – Optaglio OVMesh.

Optaglio OVMEsh holograms are created through

Microholograms

Microscopic particles (from 40 micrometers) appear as metallic dust at first glance. Viewed through a magnifier, regular shapes, engraved letters and holographic surface can be seen. Microscopy inspection reveals a complete hologram with all visual effects.



e-beam lithography with extremely high resolution (more than 2,5 million DPI) using mathematic algorithms that cannot be derived back from a ready hologram. These holograms include special visual effects that cannot be imitated using other technologies. There should not be too many visual effects in a hologram. From inspection point of view, it is optimal that the guard:

- Identifies the illusion object immediately;
- Checks the correct move of the illusion object while tilting of the hologram;
- Makes sure that under special lighting (red light, intense light, sharp angle, etc.) an expected change appears, such as emerging another visual object, lettering, etc.

Optaglio OVMesh holograms consist of thousands of miniature part. During lamination of the card, melted polycarbonate flows between the parts of the hologram ensuring perfect integration of the hologram into the card, without any heterogeneous adhesive. Any attempt for hologram removal results in its disintegration into the miniature parts.

"...melted polycarbonate flows between the parts of the hologram ensuring perfect integration of the hologram into card."

The hologram can have any size, up to the full face coverage of the card. It is important, among others, for enabling of implementation of distinctive and recognizable visual effects.

The holographic layer can include any combination of transparent holograms, metallic holograms, and free space. Laser writing through the holographic layer is thus enabled.

TRANSPARENT WINDOW

At first sight, it can look simple but production of a card with a transparent window poses a technology challenge for the manufacturer, and it is even more challenging for potential counterfeiters. A specific segment needs to be cut from the colored layer of polycarbonate and replaced by transparent polycarbonate.

It is recommended that the transparent window should be combined with other security features, such as laser written picture of the card holder. The hologram is the strongest available measure for this purpose. At first level inspection, the guard sees just the transparent windows. At more appreciate view, he/she can see the transparent hologram in the window. Optaglio OVMesh Unlimited product is beneficial here because it enables to place any combination of metallic and transparent holograms on any position of the card.

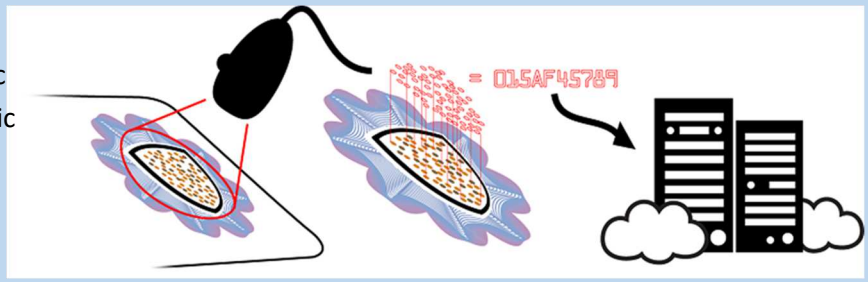
What is OVMesh

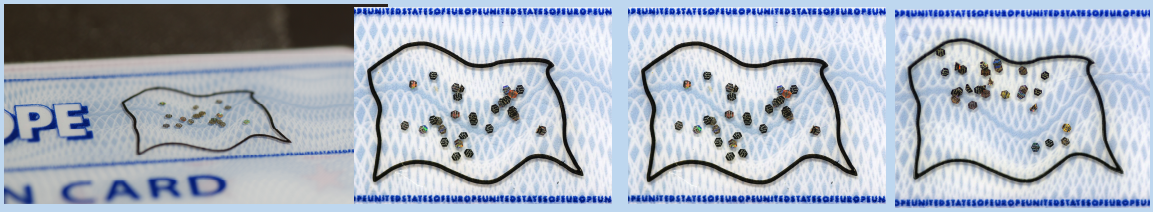
Optaglio OVMesh is delivered in three versions (Exclusive, Unlimited, Smart). Card manufacturers and integrators select between them according to batch size, holograms space, and selection of transparent holograms, metallic holograms, and microholograms.

All versions have the following features:

- Perfect integration of hologram into card, without application of heterogeneous adhesive
- Melted polycarbonate flows through the hologram during card lamination
- Application of all special visual effects developed by Optaglio

OVImage is a product for identification of individual cards without sending biometric or other sensitive personal data over public networks. It differs from other solutions based on microparticles position by using microholograms. Impenetrable anti-counterfeiting resistance is thus reached.





PERSONALISATION

Personalisation is currently a relatively weak point in card protection. The counterfeiters can change the picture of card holder quite easily. They can rewrite laser personalization. Other personalization technologies that are more tampering resistant are either very expensive or still in pilot phase.

Moreover, personalization is dependent on a seamless and faultless process of transfer of personal data from front office to the center, document creating and its delivery to the right person, sometimes over hundreds or thousands of kilometers. Some specific situations need to be also covered. What if an applicant dies during the card personalization? What if he/she moves, changes family name, etc.? Current situation in Cameroon where hundreds of thousands personalized ID cards are gathered at local police stations without central control shows that even a small mistake in process definition can have a severe impact.

Nevertheless, personalization is an essential process for any personal card. Without personalization there is no connection between the particular card and a person and card is not an authentication tool. It seems that the best solution available now consists of writable polycarbonate layer, laser writing and chip with information about holder covered with a hologram, and possible check against a central database.

CHIP OR OSM

Laser personalization mitigates a risk of using the document by a wrong person, but it is not able to eliminate this risk completely. Stronger protection can be ensured through storing biometric data in the card, or more precisely in a chip or OSM element (Optical Security Media). During the identity check, biometric data from the card are compared with the real person.

It is handy to cover the chip with a self-destructive transparent hologram to prevent its change including data record. Any attempt for chip manipulation results in irreversible disintegration of the hologram. Optaglio OV-Mesh product, already mentions, is very useful for this purpose.

CENTRAL DATABASE

Checking against a central database would be an even stronger tool. However, transfer of biometric data over a public network is seen as unacceptable practice by most of the security experts, even if it is encrypted.

This issue is covered by Optaglio OVImage product. Microholograms are randomly scattered in a predefined area of the card. Their position on each card is unique so that even the manufacturer cannot produce the same card again. The position of microholograms is saved into a database. During identity check, their position is reread and compared against the database record. Neither biometric data nor sensitive personal data are transferred over the network. If the database was compromised, attackers would not gain access to biometric data.

“ ...transfer of biometric data over a public network is seen as unacceptable practice, even if it is encrypted.“

Well considered concept is the key

Although existing best practices are transferable, there is no „the best solution“ for all documents and environments. It is critical that all security elements form a consistent unit and that this unit meets all technology requirements as well specifics of culture, customs, infrastructure, and way of inspection that is not only written in guidelines but can be enforced.

Card architects should consider mainly the following issues.

- What types of attacks can be expected
- Lifecycle of a document
- Expected speed of document issuance, including personalization
- Volume of cards issued
- Specific culture limits regarding biometry data taking
- Adding new functions in future, such as using ID card as a social security card
- Public expectations on document appearance
- Way of identity checks
- ICT infrastructure available.

If you are looking for the most suitable solution for your documents, it is the time to contact Optaglio Consulting Practice. We are helping experts and managers from governments, card producers, and integrators. Backed by proven delivery of protection for tens of millions documents, extensive project management experience and excellent knowledge of the market, we are ready to meet you and discuss particular issues.

Optaglio Consulting Practice has no motivation to promote an expensive solution. Thanks to close cooperation with Optaglio Labs, we see over the horizon of current products and requirements. We aspire to find the best option for your project and your country.

“It is critical that all security elements form a consistent unit that meets all technology requirements as well specifics of culture, customs, infrastructure, and way of inspection.“

Libor Šustr is the Technical Manager in OPTAGLIO. He graduated from Brno Technical University and participated in tens of projects focused on ID cards, passports, and other documents protection. He can be reached on e-mail libor.sustr@optaglio.cz

Petr Hampl is a sociologist with more than 15-year experience from information security companies. Among others, he worked on one of the biggest European projects of trusted documents handling. He can be reached at petr.hampl@optaglio.cz

OPTAGLIO is a leading global provider of advanced optical security devices and the market leader in e-beam lithography. During almost 25 years of our history, we have delivered more than one billion of holograms to governments, financial institutions and other organizations in more than 50 countries around the world. Our unique technology has been broadly recognized as the industry standard for optical security. OPTAGLIO, certified to relevant international standards, operates under strict 24/7 security supervision. Our comprehensive security system covers people, processes, data and facilities. The company is a member of International Hologram Association (IHMA) through which it registers all its security devices and holograms in the central security register, in London.