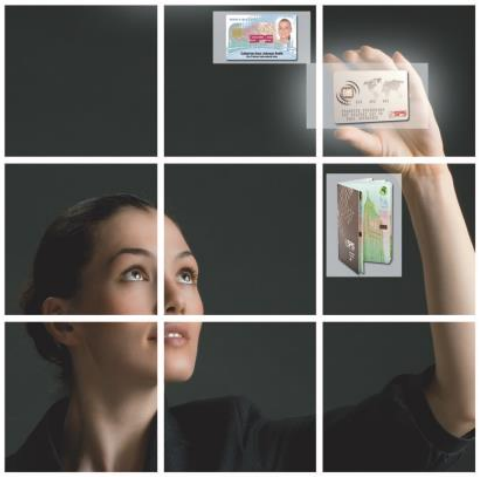


RELIABLE TECHNOLOGY

*WHITE PAPER*

# MARKED MODULES AND ANTENNAS: PHYSICAL SECURITY FEATURES FOR GOVERNMENT

National ID cards have evolved and are now part of a global identity management ecosystem. They are evolving into multi-purpose ID credentials, having multiple functions: allowing a citizen to prove his/her identity, border control, access to eGovernment services, … To fulfill these multiple demands, governments are now issuing more and more complex security documents that combine physical security features with electronic chips. As ID cards provide more services, they become a prime target for counterfeiters.

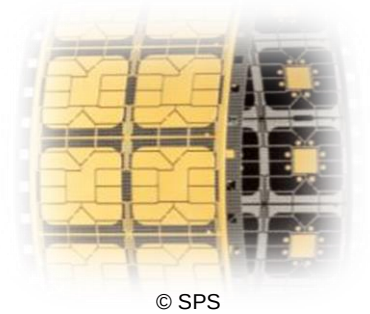
Answering these concerns, SPS proposes a secure industrial solution to government authorities: marked modules and antennas that provide efficient level 1 and level 2 security features. These security features guarantee to governments that their documents are unique, and their modules cannot be replaced. This way, law enforcement officers can check that documents that are presented are genuine in an easy and efficient manner.

Several types of smart cards are now in use:

- Contact cards, to be inserted in a smart card reader,
- Contactless cards, that communicate up to a few centimeters from a reader equipped with an antenna,
- Hybrid cards, equipped with both a contact and a contactless chip,
- Dual interface cards, where one chip can support both communication modes.

ID document issuance is to be considered as a complete system, in which secure procedures will ensure that secure documents will be issued. Efficient design for a security document is based on the combination of several security features, belonging to all levels, in order to withstand fraud attempts. The objective is to ensure law enforcement officers, immigration and customs officers, are able to determine if a document is genuine and the data it carries is authentic.

## Module presence



© SPS

SPS unique manufacturing process is based on a micromodule, which includes the chip. The same process is applied independently from the type of smart card manufactured: contact, contactless or dual interface. As all national ID cards manufactured with this process include a micromodule, this one becomes a security feature: only genuine cards issued by the authority bear a micromodule with the official design.

It has been experienced that fraudsters attempted to scan and print a genuine card image on a blank card body, especially in the case of a contactless card. Such a fraud attempt is easily detected as a printed micromodule image gives a totally different touch feeling from an authentic metal-coated micromodule.

## Marked module

© Imprimerie Nationale

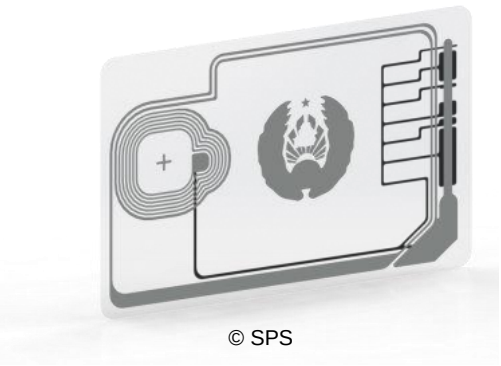
The surface of the module of a national ID card shows a specific mark referring to the issuing authority. Thanks to marked modules, the module look and feel becomes unique to a government and to an application. The marking brings consistence to the global card design, showing national symbols, such as flag, coat of arms, etc. The module marking is done by copper etching with nickel/gold electroplating in a controlled industrial environment and supply chain. A marked module is extremely difficult to reproduce without these industrial-grade secure means.

The marked module is a security feature that makes the ID card different from regular cards such as SIM cards or banking cards. It ensures the module cannot be replaced by a standard module taken from another easily available card.

It has been experienced in the past that fraudsters were able to remove the module from a card, , and insert it on an existing ID card. When authentic ID cards bear a marked module, a module taken from another card can easily be identified as a counterfeit.

## Marked antenna

For contactless, hybrid and dual interface cards, SPS unique manufacturing process is based on EBooster®, the electro-magnetic coupling of a small module-sized antenna and a large card-sized antenna, laminated inside the card structure. For National ID documents, the antenna is designed on request, which allows including aluminum etched distinctive signs in it. Typically an antenna distinctive sign can be a national symbol, an acronym, or a second embodiment of the national symbol already part of the marked module or the card surface. Such a distinctive sign is visible by transparency, just by exposing the card in front of a light. An antenna with a distinctive sign becomes an anti-counterfeiting feature, as a fraudster is not able to reproduce an antenna designed with industrial means within a controlled supply chain.


© SPS

To control these distinctive signs, a law enforcement officer needs to have the knowledge of the presence of the sign, and just to be equipped with a light, such as a mobile phone torch. In a way, a marked antenna brings to the plastic card the same type of security as watermark on a paper document.

The marked antenna is an easy to implement and easy to control level 2 security feature. In addition, as a hidden symbol controlled by law enforcement officers, it brings them into an inclusive confidence circle with the government they represent.

## Conclusion

The presence of a physical micromodule on an ID document is part of its security, as it makes the document harder to counterfeit, but is easy to control without any equipment.

Marked modules and marked antennas improve significantly robustness against counterfeiting. They bring uniqueness and security as they are specifically designed and managed in an industrial secure environment and supply chain. Marked modules and marked antennas can be implemented in any National ID document, and bear the same image, reinforcing the presence of government symbols.

## *Customer testimony*

**"**The micromodule includes a specific mark that can be a reference to the issuing authority. In addition to participating in the graphic design of the document, this mark is an easy and fast level 1 ("open domain") means of authentication. This specific mark brings consistence to the document and prevents fraudsters from using standard modules to make counterfeit cards.

This security is completed by another characteristic, which belongs to level 2 ("closed domain") as it is accessible thanks to an equipment. Antenna design can be personalized with a logo, only visible to officers in charge of control and trained to control it with simple tools such as a mobile phone flashlight.

This additional security constitutes a hidden trap to potential fraudsters, using the same idea as the watermark, the oldest and most robust of security printing techniques. In addition, being a hidden recognition sign between the issuing authority and the control officers, the marked antenna reinforces the confidence circle embodied in identity documents.**"**

***Head of Document Fraud Expertise, Government law enforcement organization***.

## *Background information*

ID card security features are unique: holograms and holographic foils, indent printing, embossing, intaglio, laser perforation, rainbow and guilloche, or the inclusion of a shadow photo, are made specifically upon a government requirement and each design is dedicated to a single government and type of card. The same requirement applies to level 2 security features: microprint, watermark, OVI (optical variable ink), UV/IR or specific ink marks, are unique to a government and a type of card.

The evolution of manufacturing technologies for National IDs has led to a similar evolution in terms of control methods.

<u>Control methods for ID documents are structured in levels:</u>

- Level 1 requires no specific equipment, and is accessible to the casual observer, for instance holograms, guilloches or OVI are level 1 security features,
- Level 2 requires simple equipment and/or methods that can be taught to a wide audience, including every law enforcement officer, immigration and customs officers, … For instance a UV lamp is needed to reveal UV printing on an ID document and a smart card based ID document requires a reader,
- Level 3 requires a specific knowledge about the existence, function and effect of a given security feature and laboratory level means of control are necessary.