National ID Cards: Multi-Technology Solutions for a Changing World

The Case for the Multi-Technology ID Card

Increasing the security and utility of national ID programs is one of the most pressing concerns of governments around the world, driving the evolution of advanced ID solutions and encouraging innovation across all areas of the industry. As a result, sophisticated credentials featuring layers of visual, physical and digital security have become a key mechanism helping governments to protect their citizens and their borders and to streamline the delivery of a wide range of services.

In this paper, we will attempt to outline the benefits of how the use of both on-card visual security elements, combined with in-card, chip-level security, provide protection for citizens and Governments alike against counterfeited IDs and widespread identity fraud.

Identity Document Fraud

Over the last 20 years, there has been a global shift from attack of the document to attack of the application process. This has largely been the result of the strengthening of document security, including digital imaging, thin-film diffractive laminates, laser engraving and electronic defenses. Despite this trend, document attack remains widespread and appropriate defenses must continue to evolve to meet it. Figure 1 (below) is a diagrammatic representation of the multitude of threats to ID documents.

The criminal has increasing access to the components and technologies they need to simulate or alter identity documents. Lasers, polycarbonate, specialist inks, manufacturing equipment and holographic origination systems are all available, together with more traditional printing and stamping processes.

In the war on fraud, an understanding of vulnerability in both current and next-generation documents is a vital part of creating a future-proof solution. Success requires close collaboration between all stakeholders: designers, manufacturers, issuers and document examiners such as those from immigration and police authorities.
Principles of Secure Document Design

Although technology evolves, some principles of identity document security have been well established and unchanged over several decades:

- Documents need to be difficult to simulate and alter, and easy to verify with confidence. Ideal security features are easy to identify and verify, and therefore easy to train.
- Features may be overt, covert or forensic in nature. They should be distributed throughout the document: within the substrate, the security print, the personalization and the RFID chip.
- The overall design of the document helps ensure the features work together in an effective defense network. PC materials, electronic inlays, lamination plate design, embedded diffractive devices, security print design, security inks, personalization hardware and personalization layout need to be considered holistically to achieve an aesthetic identity document that is technically secure.
- Security relies on a mix of:
  - Novel materials with restricted availability
  - Specialized engineering delivering unique structures and with precise registration of features to each other
  - Secrets and knowledge – confidential know-how of the genuine manufacturing processes
- Personalization security features are particularly strong, defending against alteration as well as simulation. They require particularly close collaboration between document manufacturer and personalization technology vendor, in order to deliver high quality and consistent features that challenge the criminal.

Combination Technologies Produce Secure, Functional ID Cards

Over recent years, increasing emphasis has been placed on the combination of technologies. This may be achieved by combining security features to improve resistance to simulation and alteration, or by including multiple technologies within the ID document. This combination philosophy has been driven by a variety of benefits for the issuer, the examiner and the user:

- Multi-functional documents, allowing citizens to access many Government services
- Improved security, where the network of defenses is strengthened by new “super features”
- Authentication of identity in a range of scenarios; visual, machine-readable, offline and online
- Improved durability, where technologies combine to optimize protection of electronics and document lifetime
- Increased return-on-investment (ROI) where documents last, and stay secure, for longer
Concept to Reality

While the concept of a multi-functional card is simple, the reality is very difficult to achieve. Considerable industry knowledge and design skills, together with technical and manufacturing expertise, must be employed to ensure that the end result conforms to international standards in terms of size, security, functionality, durability and interoperability. In addition, the multiple technologies built into the card must be complementary and not contradictory. With ever-increasing technical complexity, achieving optimal card design is not a trivial matter. Nevertheless, such cards offer a more cost-effective, efficient option than multiple single-purpose credentials, and help ensure the highest standard of security is implemented to future-proof the document against the largely unknown attacks of the next decade.

Evolution of Secure ID Solutions

The security technologies available today offer different benefits to the issuer, the examiner and the user. Some enable a secure and convenient interface to government agencies, whilst others provide resistance to criminal attack. ID solutions are evolving at pace in both these areas; security and functionality.

Security features take many forms and the technologies must defend against both counterfeiting and alteration. They are typically located visibly and invisibly throughout the document:

- Within the physical card
  - Diffractive holographic structures (OSM, holograms, Kinegrams™)
  - Windows, lens structures (Changeable Laser Image)
  - Security print (optically variable inks, ultra-violet fluorescent inks, rainbow “split-duct” printing, microtext, guilloche, as in Figure 2 below)
  - Personalization features (laser microtext, ImagePerf™)

Figure 2: A small list of card body security features.
Customized combination of technologies on a single card delivers greater security and value than a multi-card solution. This combination is the principle for the next generation of secure ID cards.

- **Microcontroller IC chips** verify and control transactions between the credential and its outside world through the reader. It may contain biometric, personal, or account data that individuals need to effectively process transactions. There are three types of secure IC chips that may be used on identity cards — contact, contactless and dual interface.

- **IOSM** is a tamper-proof, highly counterfeit-resistant visual and physical security feature that can also display the personalized data of the credential holder, such as a facial image or other personal information.

### The Optical Security Media (OSM) Difference

The real power of OSM security comes from its unique instantly recognizable appearance coupled with its receptivity to laser personalization, as shown in Figure 3 below. By virtue of being exceptionally difficult to simulate yet easily verified without the need for magnification or specialist forensic devices, it provides a strong defense against the twin threats of counterfeiting and data alteration.

- Ultra-high resolution (up to 24,000 dpi) security patterns and images
- Covert diffractive image

Figure 3: Evolution of OSM design.

A personalized laser-engraved image cannot be removed, erased, duplicated, simulated or altered. Additionally, after more than 30 years and with over 100 million cards issued in global circulation, there remain no known cases of OSM being successfully compromised.

Several cards issued for major ID programs are using an OSM stripe: including Indian state vehicle registration cards supporting both ID authentication and records/payment management, and Saudi Arabia’s national ID card program employing a combination of contact chip and optical security media. In this instance, Saudi Arabia uses the card as both a citizen national ID and a token for the streamlined delivery of a variety of government services, such as e-banking.
Delivering the Multi-Technology Credential

One of the recent ID program examples of using a multi-tech OSM card is the Ireland Passport Card (Figure 4). This card is the first and only passport card deployed in Europe for border crossing. It allows Irish citizens to travel across Europe without their traditional passports. Citizens can obtain the card by applying online or through a smartphone app that allows the applicant to submit a compliant photo from a mobile device. In addition, payments for the passport card are made through a secure payment gateway.

Figure 4: Multi-technology OSM cards combine both an OSM laser-engraveable strip and a RFID microcontroller chip within the same card body.

With the release of the DBond™ technology, contactless inlays can become thinner thus enabling the integration of contactless smart card technology together with OSM. Some of the key advantages to our multi-tech OSM card approach include:

- An extremely counterfeit-resistant platform for the highest level of security
- The ability to leverage a client’s existing infrastructure
- A platform for the delivery of any required application or service
- Integrated technologies that improve the way in which existing public services can be provided
- Rationalized resources and reduced costs for government agencies, citizens and businesses
- Simplified processes and procedures for delivery

The multi-tech OSM card is applicable for nearly all ID credential applications for a variety of Government-to-Citizen programs, such as national/personal IDs, driver’s licenses, vehicle registration cards, e-government services, other government-issued cards.

Electronic security features might also include:

- Different security levels for different applications on the secure crypto-controller chip
- Two-factor authentication: something you have (card) and something you know (password)
- Three-factor authentication: added biometric information to verify “something you are”
While the power of the CPU and crypto-processor of the secure microcontroller alone provide multi-factor authentication and security controls that could be used for access control, data storage and even payment, the addition of OSM technology greatly enhances the card’s visual and physical security, acknowledging that the majority of ID card inspection and examination today is visual. OSM also delivers a forensic-level authentication capability and greatly enhances counterfeit resistance.

The integration of OSM with smart card technology brings a series of advantages, all of them offering a high return on investment in the credential (Figure 5) by combining two or more functions on a single card.

![Figure 5: OSM technology combined with DBond technology on the same card.](image)

**The Multi-tech OSM One Card Solution**

In response to the increasingly complex ID requirements of governments worldwide, HID Global offers secure microcontroller-based smartcard ID solutions for contact, contactless or multiple interface environments.

The foundation of the smartcard ID platform is a set of features, technology, partnerships and consulting services that meet the most complex technology and functionality requirements, complying with exacting standards across a breadth of applications, and supported by our unmatched industry expertise in design, manufacture and issuance of secure ID card programs. Our multi-tech OSM card is an example of a product that uses this platform to provide trusted identities for a variety of applications.

Our continuous innovation programs ensure that we offer partners and customers the most advanced, highly secure credentials and solutions available today.

HID’s global experience in advanced secure credential technologies place the company in a unique position to assist any client planning a major ID card program that will utilize technology combinations to achieve their security and service goals.

If you’re interested in learning more about our multi-technology solutions, download our brochure [here](https://www.hidglobal.com/border-protection) or visit our website at [https://www.hidglobal.com/border-protection](https://www.hidglobal.com/border-protection).