IN GROUPE

THE KEY FEATURES OF A MODERN IDENTITY CARD

TABLE OF CONTENTS

INTRO

National identity documents have been around for over a century. From the simple piece of paper with a photo affixed to it, to the polycarbonate card incorporating electronics, identity cards have concentrated the best technologies so that citizens, businesses and governments can place their trust in them.

As mobile identity solutions gain in popularity around the world, we believe they should remain a companion to the physical credentials that are still issued. Physical credentials remain necessary for all those cases where proof of identity must be provided in an offline environment (in areas without internet coverage, for example). Above all, physical documents are the most inclusive method of identification, because not everyone has a smartphone.

Identity cards provide a link between the physical and digital worlds, thanks to the electronic component containing the citizen's digital identity. These physical documents give citizens secure access to online government and private services.

Modern identity cards must therefore be reliable, durable, secure and attractive, while offering good value for money:

To begin with, we will make general recommendations for selecting and combining security elements. Next, we will provide expertise on selecting the right communication interface. Then, we will present some key elements of a modern ID card, recommended to meet the needs of control authorities. In this instance, we will highlight the important role that the polycarbonate structure plays in security, as well as that of design and personalisation.

GENERAL RECOMMENDATIONS FOR CHOOSING SECURE COMPONENTS

DID YOU KNOW?

In 2023, 17,400 people were arrested with 22,300 fraudulent documents at the European Union's external borders.

Source : FRONTEX

To begin with, every government should require an identity card containing all the basic security features recommended by the ICAO.

In its Doc 9303 on machine-readable travel documents, the organisation lists all the security features that must appear on a travel document, classifying them as 'basic' or 'additional'.

Doc 9303 also covers ID-1 documents (i.e. cards) in part 5. The general recommendations for selecting security features can be applied to **all types of secure documents, from national identity cards to electronic passports and visas.**

In order to select and combine secure devices as effectively as possible, it is advisable to focus on the real benefits they provide; they must be cost-effective, with a good benefit/cost ratio, in order to increase the profitability of the project.

Consequently, a given government should have only a few additional security devices (ICAO Doc 9303), focusing on level 1 elements.

01

VISIBLE

No tools required for authentication (naked eye or touch).

02

HIDDEN

Authentication requires simple, widely-used inspection tools (UV lamp, magnifying glass, etc.).

03

LABORATORY

Authentication requires qualified examiners or laboratory tools (microscope, X-ray, etc.).

Security features that can be **quickly checked by human senses and/or through automated checks with standard equipment** (visible light / UV / IR readers) **should be used as a priority**.

Conversely, any feature that requires special equipment to be checked should be avoided. For example, a very specific ink label could be checked by just a few people in the field (such a feature is better suited to protecting branded commercial products such as tobacco).

Generally speaking, the number of level 2 and level 3 secure devices should be limited **to less than approximately 10%** of the total number of security devices. They are mainly used for second-line checks, in case of doubt.

Most security devices must be controllable by human senses (level 1) and have a high resistance to attack. They must also be easy to understand and quick to check, so that they can be effectively controlled in the field.

Finally, selecting the right security elements also involves selecting the right manufacturer.

Choosing a trusted partner **with extensive ID experience and robust industrial capabilities is essential to the success of the project**.

Certifications such as ISO 14298 (Intergraf), ISO 9001, ISO 14001, ISO 45001, ISO 27001 and ISO 37001 are guarantees of the manufacturer's commitment to quality, security, information systems management and the environment.

A government looking for a manufacturer to help it issue a new identity card would be well advised to demand **this kind of certification**, which testifies to the reliability of a potential new partner.

IN SHORT

Prioritise security features that are easy to control

Avoid security features that require special equipment

Choose a manufacturer with the right certifications, experience and capacity

The art of secure document design

Only graphic designers with real expertise in designing secure documents can bring an ID card to life.

All the visual elements must **work together** to produce a coherent, secure document. As a National Identity Card is often an object of pride, the graphics must be carefully selected to truly reflect **a country's identity.**

Co-design workshops are the best way to work with the manufacturer to create **aesthetically pleasing documents,** incorporating the security features selected and the symbols chosen.

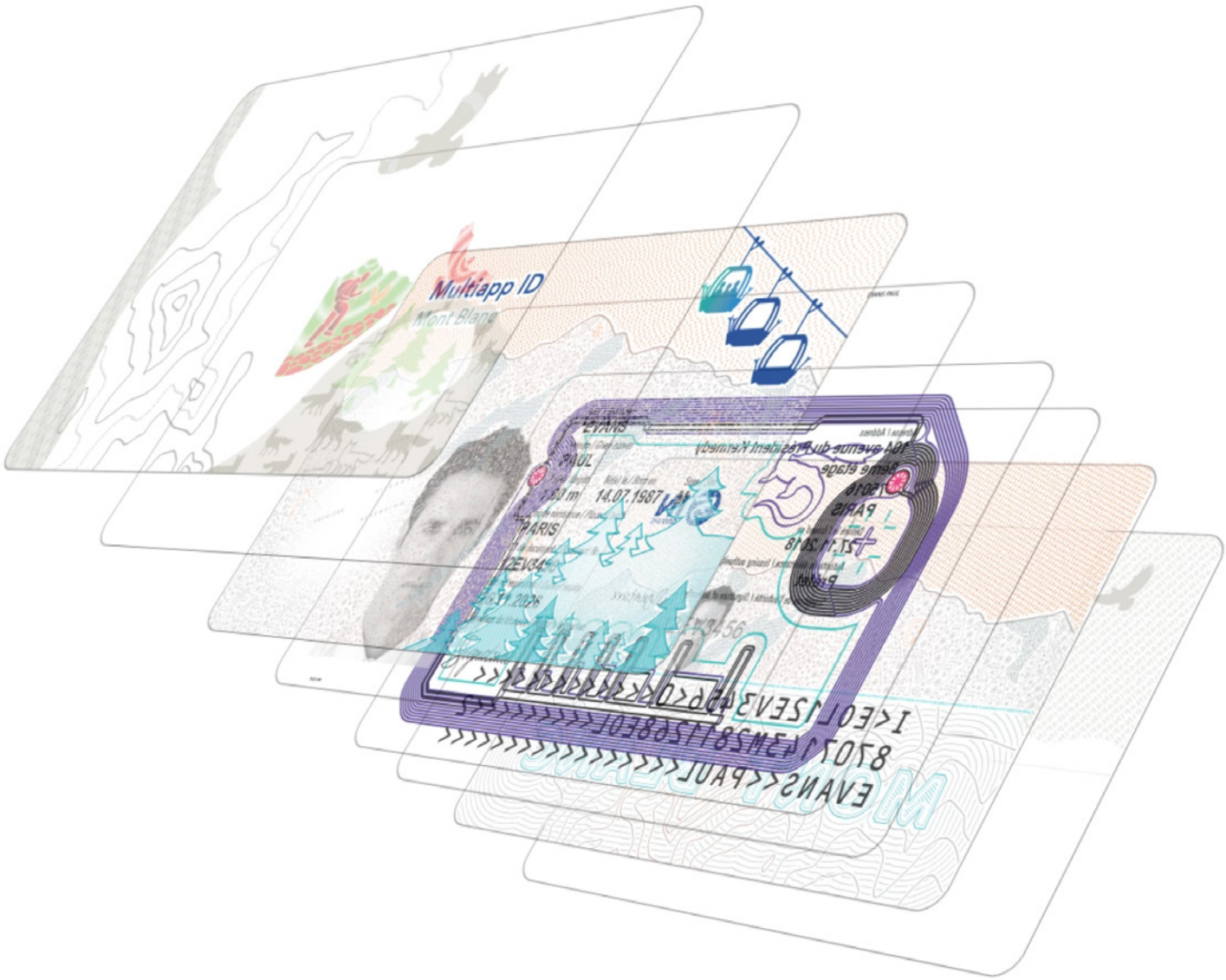
Renewing the design of documents **every 5 or 10 years** is also recommended, to stay one step ahead of fraud.

The card must be constructed in such a way that the polycarbonate layer to be personalised is underneath the offset-printed layer, so that **the security printing is above the personalisation.**

Attempts to falsify the portrait by scratching it would destroy the secure print. Offset-printed guilloches, visible or fluorescent under UV light, are a subtle way of providing protection without compromising the legibility of the portrait.

Good card designs integrate a **wide variety of security features** with apparent ease, ensuring that there are no interactions between them.

Efficient designs remain easy to control.



Divided view
of a polycarbonate card

There are **several methods** to help the control authorities authenticate a document. For example, a continuous line can help verify iridescence (in visible and UV light).

Another trick is **to superimpose visible and UV prints**, so that authentication is intuitive.

This is known as **a register design.**

In the example below, the crest of the mountain is visible in both visible light and UV light.

It is also part of the iridescence, to give controllers a line to follow and make it easy to see where the colours mix.

IN SHORT

Opt for a design that represents the country

Use guilloches (visible and invisible) on the top of the portrait to protect it

Make the design easy to check

DID YOU KNOW?

Today, 2 out of 3 countries have a polycarbonate identity card

Polycarbonate : the best choice for **identity cards**

Identity documents must meet two main requirements: resistance to time and use (durability), and resistance to attack (security).

Polycarbonate meets both these needs **perfectly**.

It has a **high level of mechanical and thermal resistance**, and can be used to personalise the data at the heart of the card, as well as incorporating security features to combat counterfeiting and falsification.

Over and above **the durability and security aspects**, the card format, known as ID-1, is generally popular with the general public because it is easier **to carry around in a wallet.**

A polycarbonate card is made up of several layers of polycarbonate of different thicknesses that are fused together during the lamination stage. During this stage, pressure and heat are applied to allow the layers to fuse together, without the use of glue or adhesives (unlike other substrates such as PVC).

After that, it is **virtually impossible to separate them**, as any attempt to do so would irreversibly damage the layers and render them unusable.

After this stage, **it becomes impossible to separate the layers from each other,** and any attempt to do so would damage them irreparably, rendering them unusable. Polycarbonate cards are also **highly resistant to external damage** caused by the environment. Extensive laboratory tests are carried out on documents to certify their resistance to extreme conditions (hot or cold climates, dry or damp environments).

It is important to note that the polycarbonate used in the production of an ID card is **specially treated**: it must not contain any whitening agents, so that it does not react under ultraviolet (UV) light. This means that under the light of a UV lamp, only the UV inks will be visible, making it easier to check.

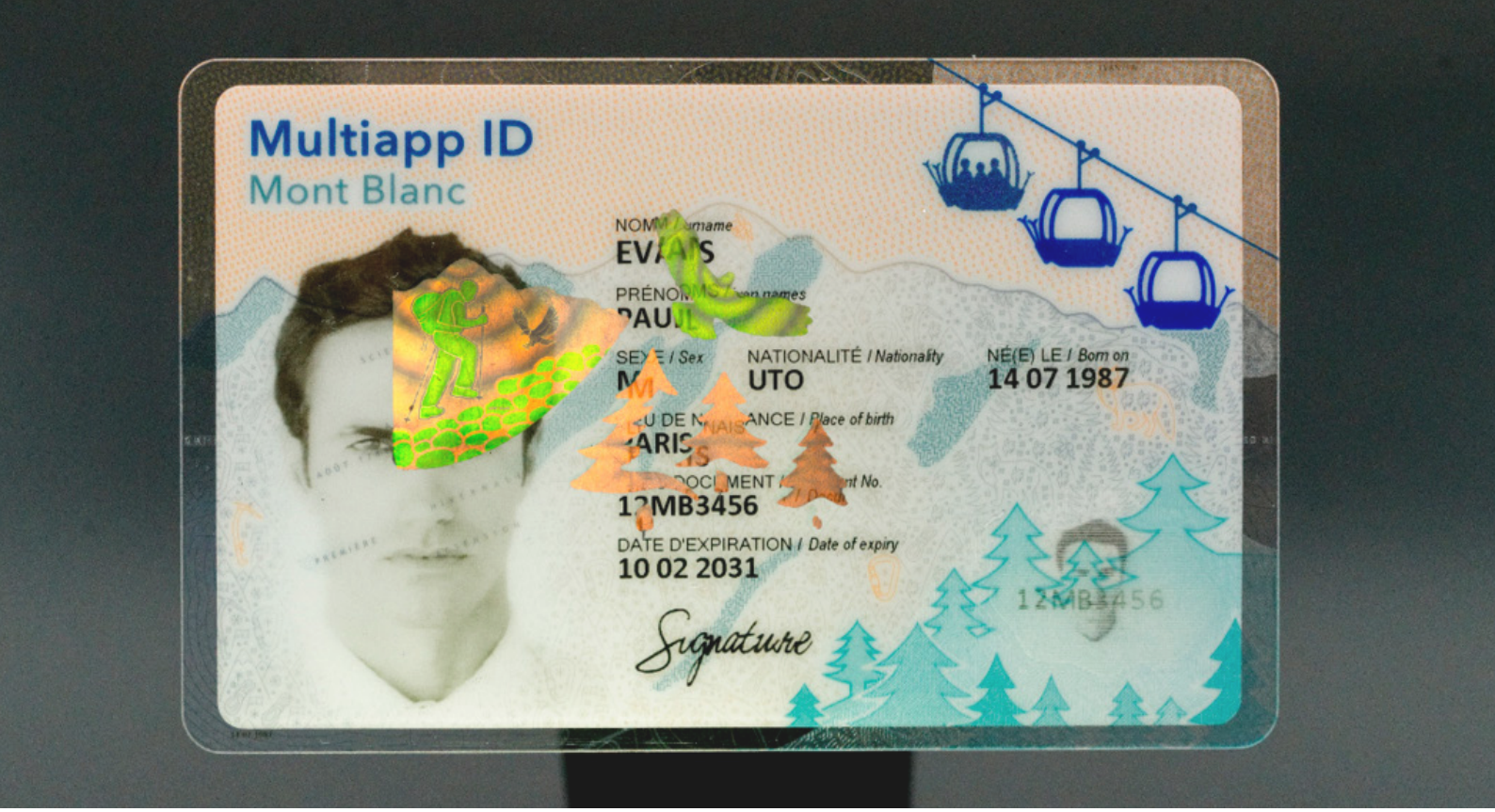
An effective way of preventing delamination attacks is to have **a transparent area on the card**. By allowing light to pass through, the two sides of the card are connected.

Any attempt to tear the card will leave traces on the transparent area (it will become opaque, the offset print will not line up, etc.). Having a transparent area around the borders of the card will make it all the more difficult for fraudsters to attack.

It is also possible to laser personalise the card with the cardholder's details (e.g. date of birth in micro-text) to enhance security. The secure background must be continuous between the opaque part of the card and the transparent area. A strong visual element straddling the two parts ensures that the card has not been split.

In addition, polycarbonate gives access to **a whole range of security features** created at the lamination stage. These elements make it easier to **authenticate the document and help detect forgery** (by adding a laminate with a false portrait printed on it, for example).

All polycarbonate cards should have **tactile elements** (guilloches or micro-text, on the portrait if possible), a **matt/ gloss effect and a super tactile effect near one border of the card** to allow rapid detection by touch.



Thanks to polycarbonate, we can also incorporate an optically variable mark and more specifically a **DOVID (Diffractive Optically Variable Identification Device)**.

This device, placed **above the portrait area**, provides effective protection against the substitution and alteration of photos.

To facilitate and speed up checks, it is strongly recommended that a level 1 security feature be incorporated into the DOVID, as this is often the first security feature checked on an ID card. This could be a clear and obvious colour change combined with a 3D optical effect (relief) or a movement that is difficult to reproduce.

The latest-generation DOVIDs now feature several holographic elements of different shapes scattered over the portrait area, instead of a single round patch. This protects biographical data as well as the portrait area, and opens up new design possibilities.

IN SHORT

Use UV dull polycarbonate

Add complexity with a complex transparent zone

Opt for a DOVID with a strong level 1 characteristic

CHOOSING THE RIGHT COMMUNICATION INTERFACE

ID cards have long been used for identification, but this is no longer their only purpose.

In recent years, governments have sought to add new use cases to physical identity documents to give citizens **easier access to services** (in person and online). Several national electronic identity cards use a contactless interface.

This has been made possible by **technological advances** and the **inclusion of an electronic chip inside the document.**

Contactless cards are used in a number of identification applications, such as **travel authorisation**. The chip contains biographical data following the recommendations of ICAO Doc 9303 for international operability (first name, surname, gender, date of birth, nationality, card number, expiry date, etc.). Citizens holding such an identity card, called a Travel ID, can use it to travel within a community of countries, as they would with a passport.

Travel IDs are often required by law. This is the case, for example, in the Economic Community of West African States (ECOWAS), or in the European Union.

As government identity documents become more sophisticated and support an ever-increasing variety of use cases, it is becoming increasingly necessary to include support for the contact interface in addition to the contactless interface.

This is called dual.

All transactions pass through a single chip linked to these interfaces, so that citizens can meet their day-to-day needs with the interface that best suits their habits.

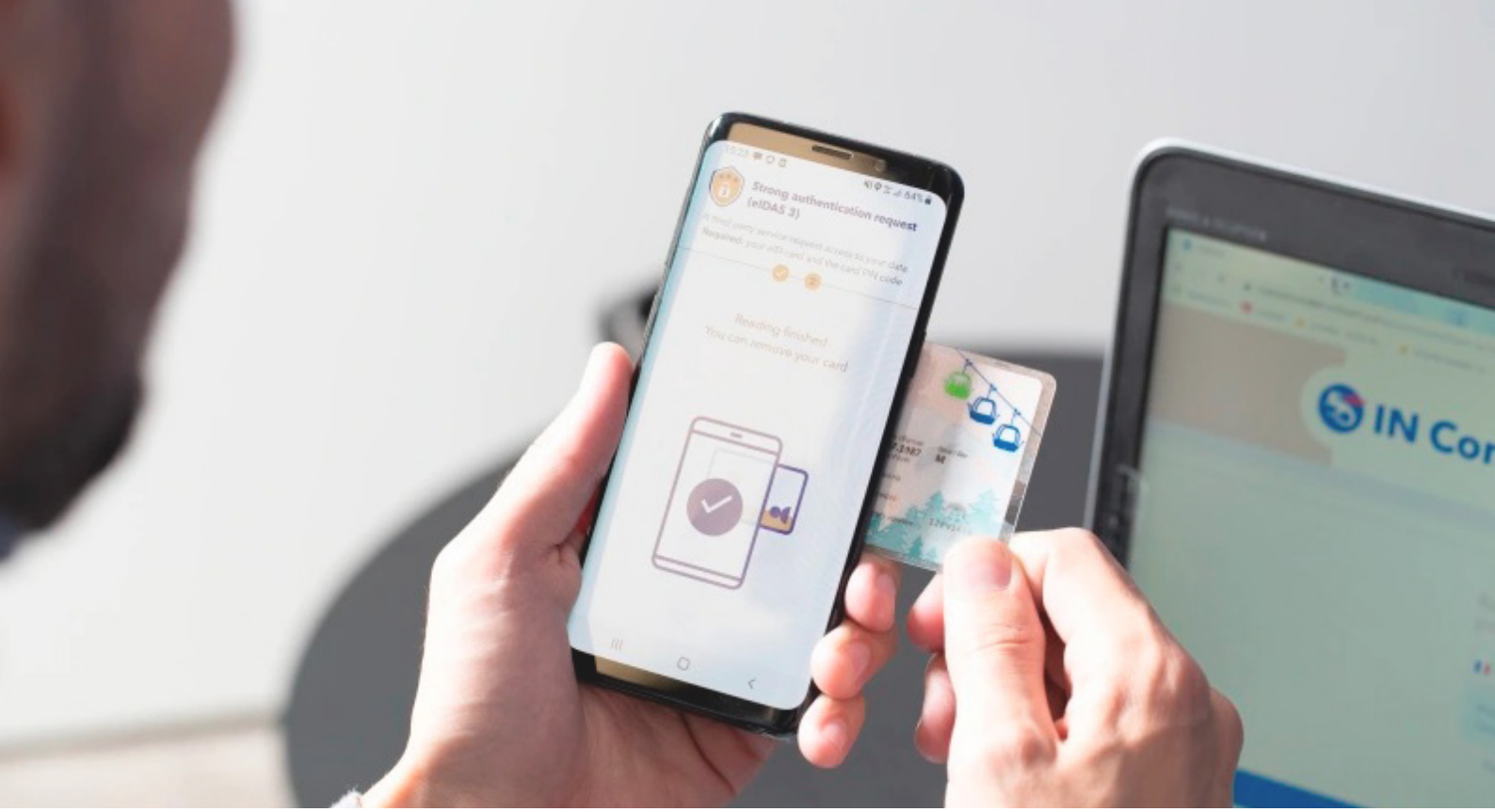
Dual cards offer by far the greatest **flexibility and interoperability** with existing applications.

Not only can dual interface cards communicate in contact and contactless modes, but data can also be shared **between applications**, depending on the security rules defined at the design stage.

Dual interface cards combine the best of both worlds, because they can use both **contact and contactless infrastructures**, while guaranteeing consistency because they contain a single set of data.

DID YOU KNOW?

More than 120 countries have electronic identity cards.
A third of them
are dual-use cards.



A dual identity card can also be used **to derive a Mobile ID in the citizen's smartphone.**

Thanks to the certificates included in the chip, Mobile ID creation is both **simple and secure**. Citizens use dedicated kiosks or their smartphone as an NFC (Near Field Communication) reader and enter the card's PIN code to digitally store the data in the device. Once this has been done, the user can access their **digital companion** (a digital copy of the ID card) to prove their identity offline.

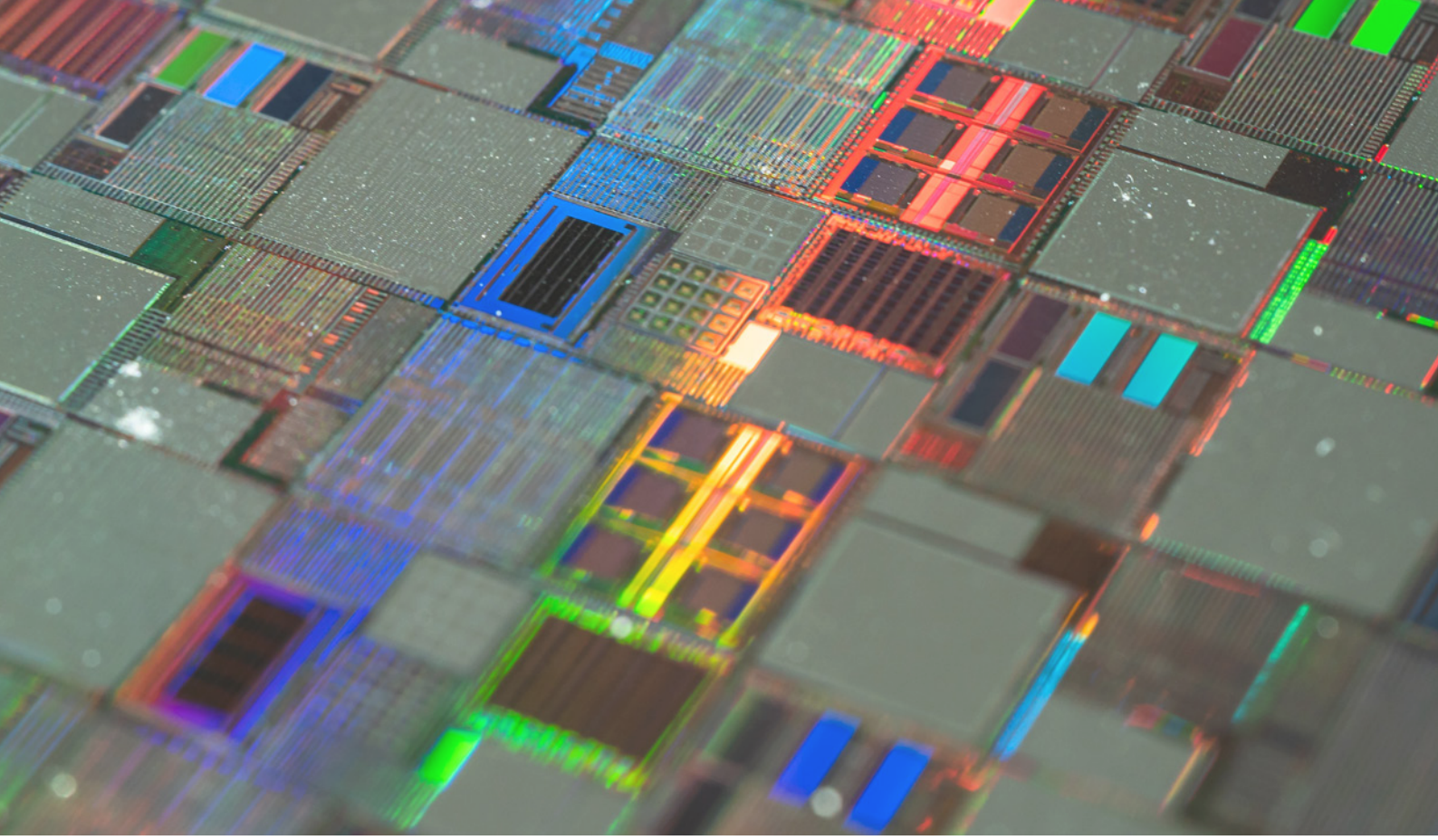
But the best thing about Mobile ID is that it can be used as a means of **authentication to access online government services.**

Dual cards enable governments and citizens to benefit from the security of smart cards combined with the flexibility of contact and contactless communications.

IN SHORT

Choose dual cards for a wide range of use cases

Use a dual card to easily create a Mobile ID



On the choice of chip

The recent health crisis illustrated the need to connect via the network to complete administrative procedures.

Similarly, border crossings have been **greatly accelerated by the use of eGates**, which support electronic documents.

Citizens have to prove who they are and what they are entitled to do on the basis of **electronic documents.** How can you trust someone on the Internet if they use identifiers/passwords that are available on the dark net for a few pennies?

In addition to what they know, users need to bring something they can trust in order **to multiply the means of authentication** and prove that they really are the person they claim to be.

The chip in a smart card is an all-in-one piece of hardware containing **highly secure silicon and software,** combined to prevent even the most sensitive data from being leaked.

These are the most secure elements designed and deployed today **for automated or online authentication.**

As well as being carried in the pocket, the chip contains internal logic that enables additional authentication methods such as biometrics or personal data to be added.

IN Groupe recommends incorporating **a recently CC-certified product** into the card and carrying out a **security assessment of the chip every two years** to ensure that it remains free of vulnerabilities.

DOC 9303

A Doc9303-compliant application is designed to cross borders quickly and securely so that citizens can have a drink or a meal before their flight.

MOC

A Match On Card (MOC) application stores face or finger templates in the chip and matches any external templates in the chip, making the operation very fast, convenient and confidential.

PKI

A PKI-based application stores government-issued certificates for online authentication and signature, for tax returns for example

CC

Common Criteria (CC) certification is the world's most advanced security scheme, proving that the chip will withstand the most invasive attacks for at least ten years.

IN SHORT

- Use a recent chip for your card
- Choose a Common Criteria certified chip to avoid security breaches
- Evaluate the security of the chip every two years

Other **interfaces**

When the project does not allow the integration of a chip, it is necessary to turn to another interface. IN Groupe offers a secure biometric code.

This secure biometric code is a **2-dimensional barcode** generated in high density **to increase the amount of information stored on a reduced surface**. This technology can store **biographical data** such as the bearer's surname, first name or date of birth, a photograph and fingerprints.

In order to meet the security requirements of the biometric code, **two cryptographic mechanisms** are used to achieve the highest standards:

- **the digital signature**, which authenticates the issuer and guarantees the integrity of the data it contains
- **encryption by scrambling and offuscation**, to ensure total confidentiality of the data for the bearer.

The biometric code is quickly decoded using a standard camera (e.g. a smartphone) and an application available to law enforcement agencies on Android and iOS.

LAST BUT NOT LEAST: PERSONALISATION

IN SHORT

Choose a manufacturer with experience in setting up customisation centres

Repeat key data and use a large, high-resolution portrait

Use laser engraving with tactile effects

The purpose of an identity card is to store personal information that enables a person to be identified with certainty.

The certainty of identifying another person derives from the security of the ID card **itself.** This means that personal information must be stored **securely** on the card.

Polycarbonate helps issuers achieve this objective. As we have seen, the construction of the card itself, in several layers of polycarbonate, allows the interior of the card to be personalised directly using **laser engraving technology.**

Several features such as security printing, lamination features and DOVID will protect the data.

For added security, it can be useful **to repeat key data**. For example, the expiry date or document number is easily repeatable in a Multiple Laser Image (MLI), some text data can be laser-engraved as micro-text on the card, and an additional portrait image can be laser-engraved in a lighter shade (known as a ghost image).

The structure of the card must also be compatible with laser-engraved tactile personalisation, a very cost-effective security feature.

All of these elements combine to make forgery attempts more difficult, as fraudsters have to modify several pieces of data in **different places**, using **different technologies**.

THE RIGHT TO BE YOU

Keep in touch and learn more information about us ➜

v1.0