WHAT ARE THE KEY ELEMENTS OF A MODERN PASSPORT?

TABLE OF CONTENTS

INTRO

Over 40% of countries have decided **to switch to polycarbonate for the datapage** of their new electronic passports. While paper is still used for the datapage of many passports, the adoption of polycarbonate is **increasing every year**, as the synthetic substrate brings greater security and durability to the document.

When it comes to modernization and upgrades, we believe that electronic passports should be designed **with a thin polycarbonate datapage, combined with an electronic cover (eCover).**

GOVERNMENT EXPECTATIONS: MORE THAN JUST SECURITY AND EASE OF USE

Most countries now issue **electronic passports**. These travel documents must offer both **security and convenience**, while maintaining a good **cost/benefit ratio:**

Security

Security, to curb document fraud and identity theft. These two phenomena jeopardize internal security and citizens' ability to travel, and can have significant social and economic repercussions.

Convenience

Convenience is essential if users are to have a good experience at checkpoints. This criterion is mainly linked to the performance of the on-board electronics and the overall flexibility of the booklet.

Technologies

Technologies selected and combined to optimize the cost/ benefit ratio.

When choosing a supplier, authorities also demand and look for:

01

Outstanding **secure design**, to provide a **strong visual identity.**

02

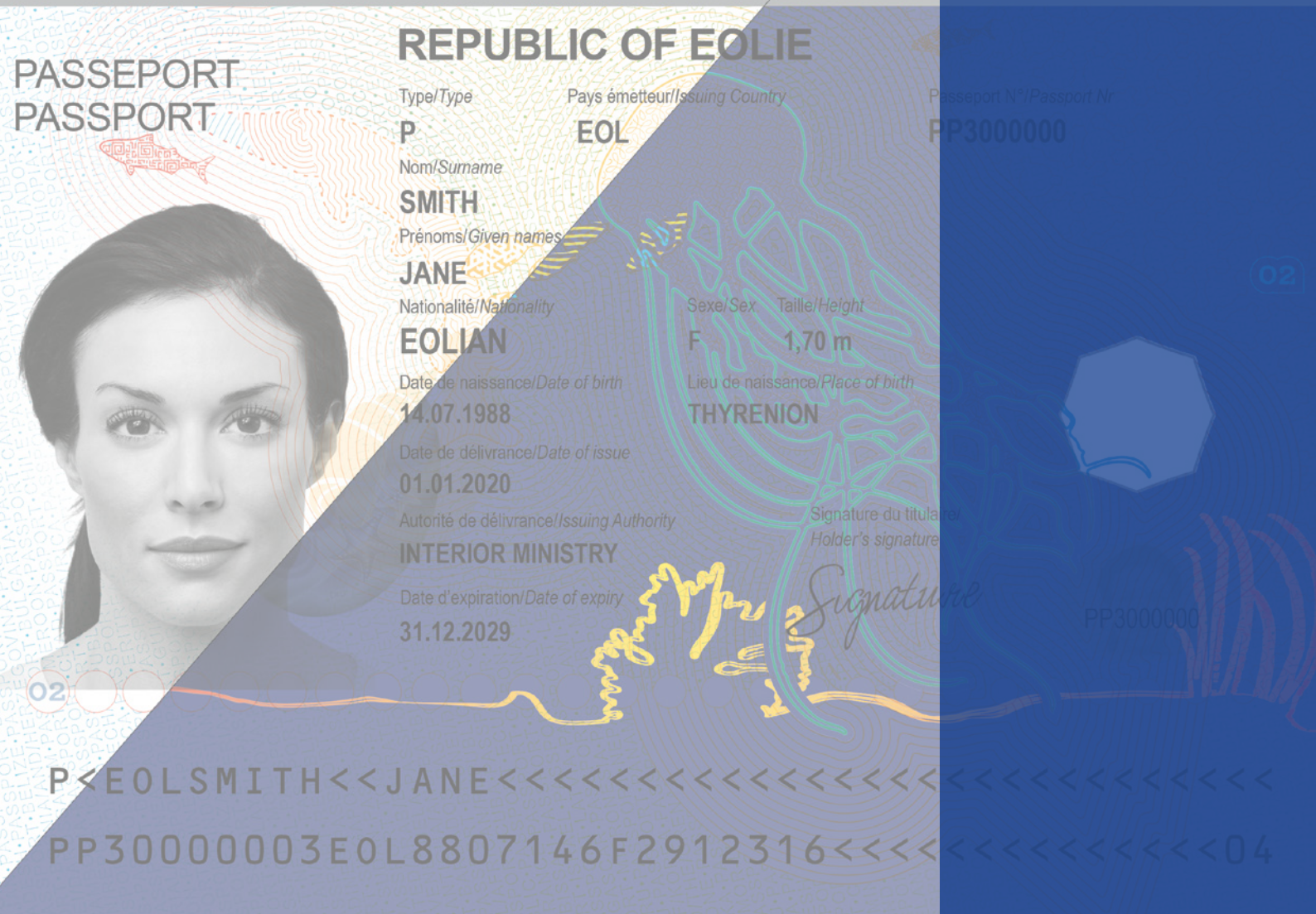
Technical options that **guarantee their independence**.

03

Documents that comply with **international standards and recommendations**, and respect regional regulations.

OBSERVATIONS

GENERAL RECOMMENDATIONS FOR SELECTING SECURITY FEATURES



On **the choice** for **selecting security features**

To begin with, every government should require a passport that includes all the basic security features recommended by the ICAO.

In its Doc 9303 on machine-readable travel documents, the organization details all the security features that **must appear** on a travel document, classifying them as “basic” or “additional”.

Doc 9303 also covers **ID-3 documents (i.e. passports)** in part 4. The general recommendations for selecting security features can be applied **to all types of secure documents,** from **electronic passports** to **national identity cards and visas.**

In order to best select and combine security features, it is recommended **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.**

Therefore, a given government should only have a few additional security features (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.**

On the contrary, any feature requiring special equipment to be verified should be avoided.

As a general rule, the number of **level 2 and level 3 security feature** should be **limited to less than around 10% of the total number of security devices.** They are mainly used for second-line checks, in case of doubt.

Most security devices need to be controllable **by human senses** (level 1) and have a high resistance to attack.

They must also be **easy to understand and quick to control**, so that they can be effectively monitored in the field.

Finally, selecting the right security elements is also about selecting the right manufacturer.

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

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 passport would be **well advised to demand this kind of certification**, which testifies to the reliability of a potential new partner.

IN **SHORT**

Prioritize easy-to-control security features

Avoid security features requiring special equipment

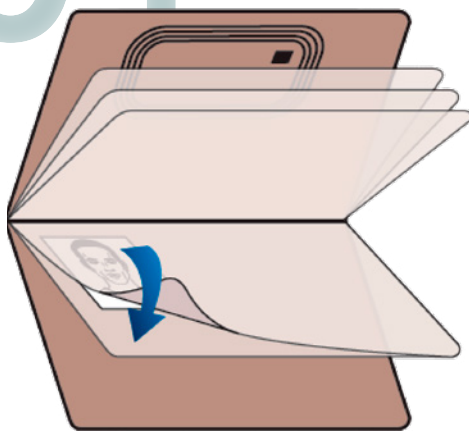
Choose a manufacturer with the right certifications, experience and capacity

THE MAIN TYPES OF ePASSPORT CONFIGURATIONS

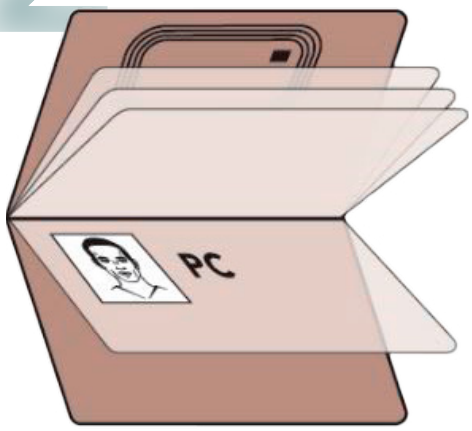
There are three possible configurations for an ePassport.

The illustrations below give a better understanding of these options. Once again, the choice is made by the issuing authority.

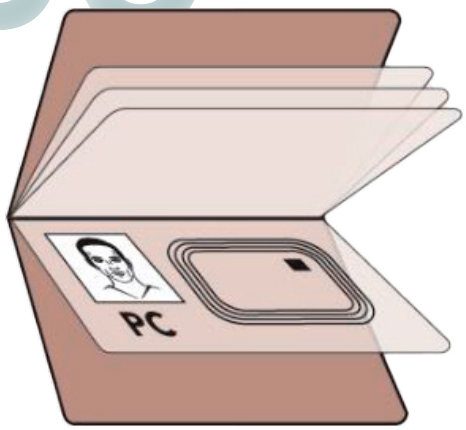
01 ePassport with paper datapage



02 ePassport with eCover



03 ePassport with eDatapage



A thin **polycarbonate datapage combined** with an **electronic cover**: the **best concept** for a modern **electronic passport**

The choice of configuration for a passport is a sovereign one, made by the issuing authorities.

Nevertheless, for their next generation of e-passports, IN Groupe recommends that governments issue booklets **with an electronic cover** and a **thin polycarbonate datapage**; and combine this with an additional, full-color, **personalized portrait image on page 3**.

In 2020 and 2021, two American countries with large populations chose this configuration for their new passports.

DID YOU KNOW?

More than half of all passports with a polycarbonate datapage have an eCover.

In fact, the use of a thin polycarbonate datapage has proved to be **an effective response to the issuing authorities' need** for greater security and practicality.

Practicality is linked to the booklet's flexibility. It can be maintained with a thin polycarbonate datapage (combined with a thin eCover) - an electronic polycarbonate datapage, on the other hand, will be thicker and less flexible:

- **Good flexibility** brings **greater durability** and improves the user experience. For example, opening the booklet flat makes checking more convenient, while closing the booklet completely is important for confidentiality.
- **Less flexibility** makes the datapage susceptible to breakage, and degrades the traveler's experience.

IN Groupe also recommends this concept because, in terms of security against document fraud, **it is more robust** than a booklet with an electronic datapage.

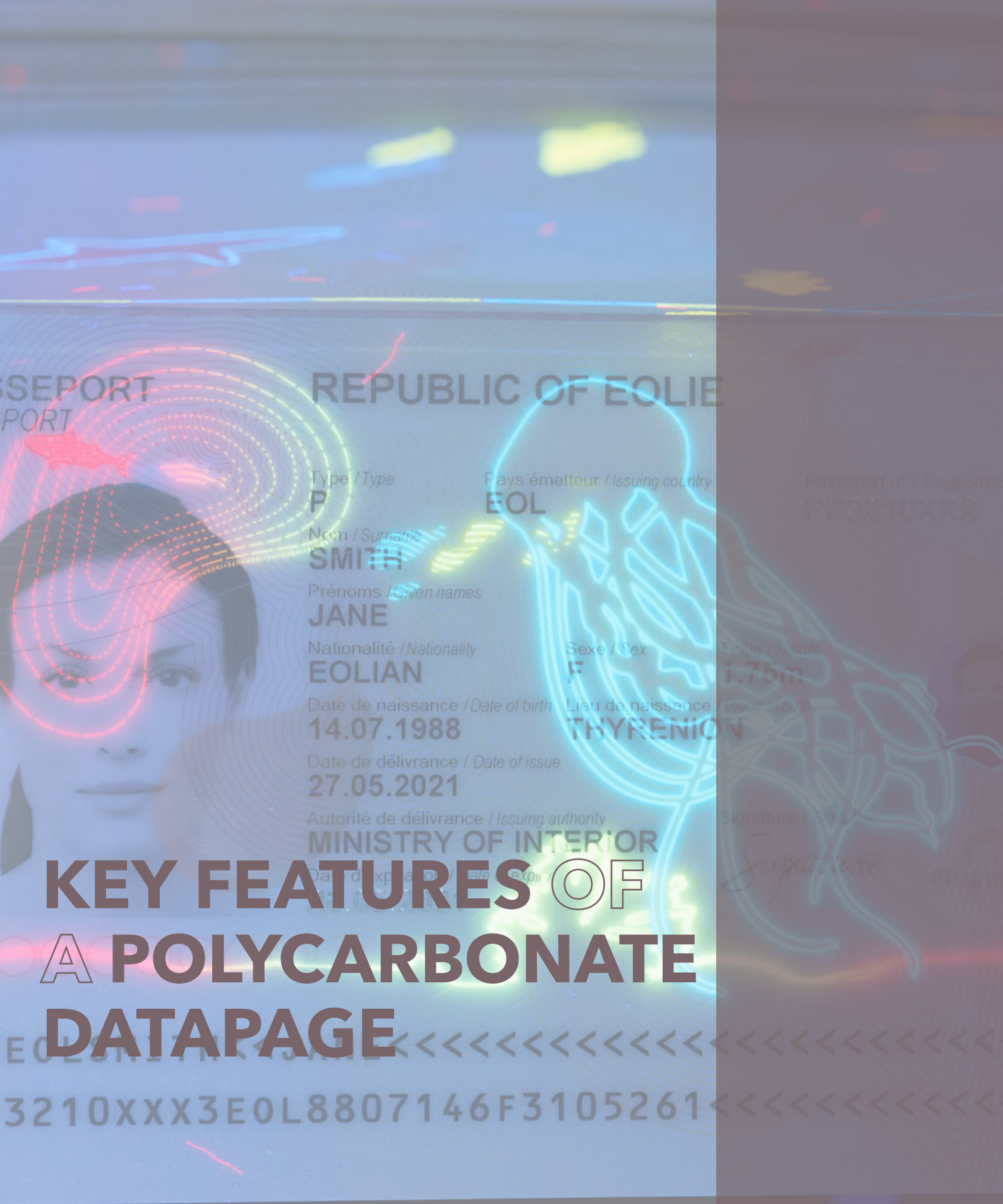
- **A thin datapage** makes it easier to verify **the metallic sound** typical of polycarbonate (which is less obvious with a thick data page). What's more, these structures make it possible to integrate economically interesting Level 1 security features, such as a watermark.
- **Security** is also enhanced when the holder's data is well distributed between the polycarbonate datapage (with the physical portrait image) and the electronic cover (chip containing the digital portrait image): a strong unique link is created. With an electronic polycarbonate datapage, all the data is concentrated in a single component: this weakens the unique link between the polycarbonate datapage and the rest of the booklet.

Finally, a thin polycarbonate datapage combined with an eCover is both **an economically attractive and reliable configuration**.
Indeed, with an inlay integrated into an eCover, less secure chips are wasted during manufacture than with a polycarbonate datapage.

IN SHORT

Choose a thin, flexible datapage

Distribute key data on the datapage and in the eCover



KEY FEATURES OF A POLYCARBONATE DATAPAGE

Example of a personalized aluminum “watermark” protecting the photo.

A construction that prevents layering, incorporating specific security features

As recommended by ICAO Doc 9303, all synthetic data-pages must be manufactured with a “construction that prevents layering”.

In particular, it is important to protect **the portrait area,** which is the first target of counterfeiters.

In addition, specific features need to be integrated within the polycarbonate structure to actively **mitigate abrasion attacks** through the back of the datapage.

This can be a kind of visible “watermark”, as such a Level 1 feature is **easy to check** with the naked eye and can be personalized with a national symbol.

Example of a hinge with a customized visible security feature (CHI)

IN SHORT

Use a hinge molded between layers of polycarbonate

Add Level 1 security to the hinge

A flexible, secure and customizable hinge

The polycarbonate data-page hinge must be thin and flexible enough to prevent the booklet from opening. This is very important in terms of practicality.

In terms of security, we recommend using a structure **with a hinge molded between the polycarbonate layers fused together**. This method guarantees secure incorporation of the datapage, with high resistance to tearing or bending and better detection of page substitution.

It is also a **construction resistant to layer separation**, as recommended by ICAO. Conversely, when the hinge is fixed to the datapage using gluing technologies, it is potentially easier to separate it from the datapage, and **the risk of page substitution is therefore higher.**

In addition, the hinge must incorporate a **highly resistant, uniquely customizable and easily verifiable security feature**.

Without this Level 1 feature, the hinge would be easier to counterfeit or replace without leaving evidence of tampering.

Example of an asymmetrically shaped window

IN SHORT

Link the two sides with an asymmetrical transparent window

Repeat key data in the window

An **asymmetrical** transparent **window**

To effectively link the two sides of the polycarbonate datapage, we strongly recommend including a transparent window.

With a window, light can pass entirely through this area, creating **a link between the two sides of the datapage.**

A window can be **laser-customized** with the wearer's data (for example, an additional portrait image). This is an effective feature for protecting the datapage against counterfeiting and delamination attacks, which is why almost half of all newly issued (modernized) passports with a polycarbonate datapage feature a transparent window; this trend is on the **increase**.

To make the window much more difficult to imitate, its structure should be asymmetrical, with two complex shapes of different sizes.

The window should also feature visible, UV-fluorescent printed security backgrounds to add complexity and facilitate verification - so you can see a continuity of print, just like **in a transparent border found on some ID cards.**

Example of a security background printed in visible offset to protect the portrait area.

Security printing to protect the portrait area

This security layer must consist of a visible and invisible (UV-fluorescent) rainbow print in two different colors, all offset printed.

The main image of the portrait is **the most important data** to protect. One way of protecting it is to laser-engrave the data under the security background.

Another security feature is to print optically variable ink on the reverse side of the datapage, behind the photo; any modification from the rear would leave a trace of manipulation.

IN SHORT

Protect the portrait with visible and invisible security features

Example of a DID™ Inlay

A transparent **DOVID** to protect the **portrait area**, with **robust Level 1 security** features

Effective and essential protection against photo substitution and alteration requires a visible security device covering the portrait area.

IN Groupe recommends integrating a **transparent DOVID** into the polycarbonate structure.

To make checks easier and quicker, it is strongly recommended that the DOVID incorporates at least one level 1 security feature that is particularly robust (against counterfeiting) and **easy to check.**

This could be a clear color change when the document **is tilted,** combined with a **3D optical effect or a movement that is difficult to reproduce.**

Example of a DID™ Shape

To provide advanced protection against counterfeiting and tampering, IN Groupe has made it possible to integrate **larger, more complex DOVIDs.**

They can cover more data, up to the entire surface of the datapage if required. These DOVIDs can be made up of several optical elements of varying shapes, deliberately distributed over all or part of the datapage surface.

More of the holder's data is protected by the various Level 1 holographic elements, making it more difficult to imitate and reuse the DOVID.

These DOVIDs also **increase the possibilities for security concepts**, as designers can integrate more national symbols with optical characteristics of trust (requested by law enforcement agencies).

IN SHORT

Choose a DOVID with a highly robust Level 1 security feature

Add complexity by using multiple scattered holographic element

Example of tactile embossing

Some **tactile** and **optical characteristics** obtained during **lamination**

All polycarbonate-based documents must feature tactile lamination elements on the surface of the datapage to facilitate authentication and better detect forgery attempts such as the addition of a transparent overlay with a false portrait image.

IN Groupe recommends the following security features: **tactile embossing** to protect the portrait, **lens for MLI** (Multiple Laser Image), **matte/gloss effect**, **guilloches and microtext**, and a **super- tactile element** on the side of the page for quick finger control.

Laminating features should also be **integrated on the reverse side** of the structure, to combat attempts at tampering from the rear.

IN **SHORT**

Use tactile and optical lamination effects on both sides of the datapage

Carefully select and position security elements

Example of a Bright Color UV print

Invisible **fluorescent inks,** a **new vision**

Ultraviolet (UV) fluorescent inks are a well-known and reliable security feature used by law enforcement agencies to combat the falsification and counterfeiting of identity documents.

UV-fluorescent inks are usually treated as iridescent or single-color inks.

To enhance document security, we have developed **Bright Color UV.** This technology synthesizes the three RGB colors: red, green and blue, which are **superimposed to create a realistic image**. Millions of combinations are possible.

It is compatible with laser engraving and embossing elements. The registration between the visible and the surface represented by the BCU makes it possible to secure a large part of the document data.

In addition to security, Bright Color UV **brings aestheticism and modernity to design.**

THE COVER, A COMPONENT IN ITS OWN RIGHT

Better protection for passport cover

Fraudsters are becoming increasingly skilful, using every part of the passport to create a new one.

The cover of a passport identifies the country at a glance. Yet this component is **rarely secure**. At its best, it features a tactile effect or UV-fluorescent ink, poorly controlled due to lack of time.

Traditionally, passport stamping consists of a simple, permanent image.

IN Groupe recommends that the cover be secured easily and intuitively with Dynamic Gilding. By tilting the document, the image previously integrated in a large area of the cover disappears and another one appears.

On the choices for electronic cover

The selection of the electronic components integrated into the eCover **is essential to guarantee both security and practicality**, but also **performance** (for example, rapid automated control at border crossings) and independence - governments are looking for robust but open technological options, enabling them to limit indirect costs.

The chip and the operating system: performance and independence

Various security mechanisms (BAC, SAC, EAC, AA, PA) guarantee strong, appropriate protection of the chip's contents.

Thanks to these state-of-the-art security mechanisms, the chip is protected against various attempts at document fraud: unauthorized access to contents, duplication, falsification or eavesdropping.

IN Groupe is totally agnostic when it comes to choosing the contactless chip and the operating system (OS). This means we can source these strategic e-components from a number of different suppliers to select the optimum stand-alone solution.

Depending on the project we're working on, we can establish minimum technical recommendations for the contactless chip and OS.

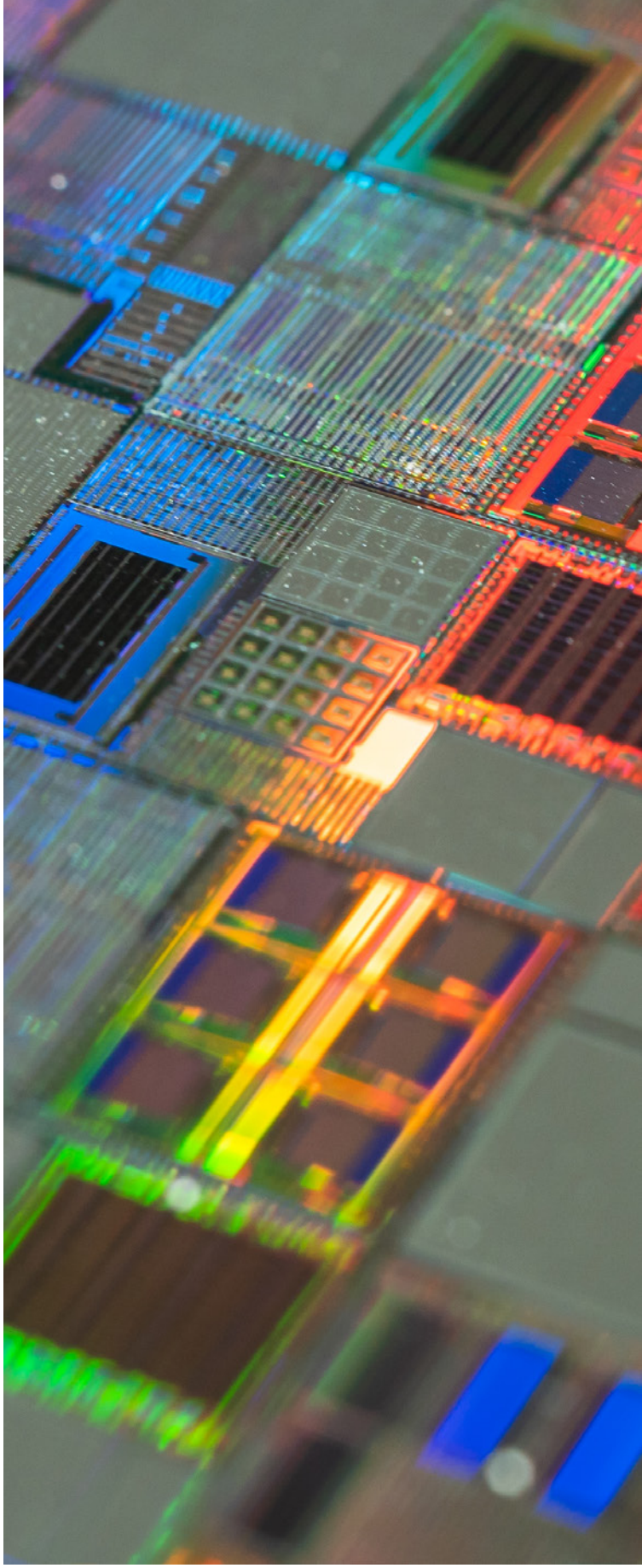
These specifications are always based on proven technologies.

| For the contactless chip and module, we generally recommend :

- **Optimum thickness** for integration in thin inlays.
- **High capacity** for efficient performance
- Products with **recent Common Criteria certification**

| For the OS, we generally recommend :

- **SAC/EAC** support for biometric passports
- **Fast personalization time**
- **Fast, complete reading** of chip data
- **Recently Common Criteria-certified products**
- **Advanced protection** profiles



EN SHORT

Select robust yet open technology options

Choose an eCover for enhanced data protection thanks to repeatability at different points in the booklet

LAST BUT NOT LEAST: PERSONALIZATION

Certain physical characteristics are integrated at the critical personalization stage.

IN Groupe has the experience to **produce blank documents** and to set up and operate personalization centers for **small or large volumes of identity documents.**

To facilitate security operations, we recommend designing e-passports that can be personalized on different machines.

Personalization by laser engraving at the heart of the structure

A passport with a polycarbonate datapage can be personalized by laser engraving at the heart of the structure.

The quality of the input portrait image and the personalization technology, both **software and hardware**, strongly influence the security provided by the grayscale photo.

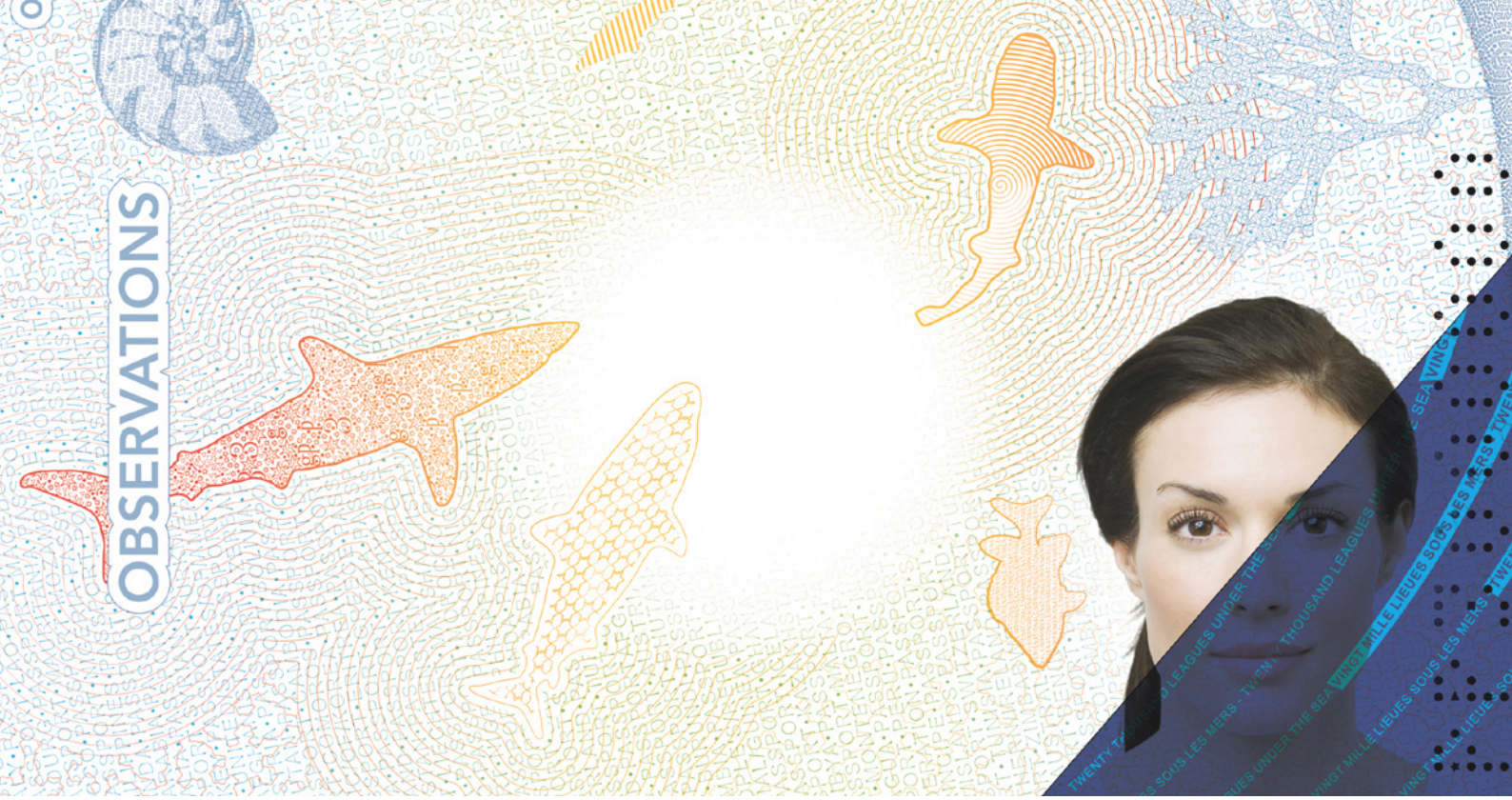
With the right technology, high resolution, contrast and sharpness can be achieved, enabling easy inspection in the field, whether physically or remotely.

DID YOU KNOW?

The name field in the passport MRZ allows a maximum of 39 characters in the top line.

Laser-engraved tactile personalization

The structure of the polycarbonate datapage **must be compatible** with tactile laser personalization, a highly effective and cost-effective security feature. Typical data to be protected with such an additional feature are expiry date and document number.



Additional **color photo** on **page 3**

For security purposes, ICAO recommends incorporating "personal data printed on an inside page in addition to the information page".

In general, this can and should be an additional large portrait image printed on page 3. A growing number of issuing authorities are using this simple and effective security concept. Indeed, this additional color photo **creates a strong physical link between the datapage and the booklet**, which become more difficult to separate (many forgery attempts are based on substituting the datapage with a fake one).

This cost-effective security feature also provides good protection against photo substitution and alteration.

IN **SHORT**

Choose a manufacturer with experience in setting up personalization centers

Use laser engraving with tactile effects

Use an additional color photo to create a strong physical link between the datapage and the booklet

Moving towards a more responsible passport

The environmental and health impacts of everyday products are at the heart of our concerns. Climate change and the recent health crisis have alerted us to the need for action.

For several years now, banknote manufacturers have been developing **specific treatments in the paper mass to give it anti-bacterial, anti-fungal and anti-virus properties.**

These technologies have now been tested and validated in the laboratory, providing a barrier against the development of fungi and bacteria in extreme conditions of temperature and humidity.

We recommend integrating an anti-bacterial, anti-fungal and anti-virus solution into the paper product's mass, without any visual impact on the passport's appearance. This solution should reduce viral concentration **by at least 100 times**.

It must be produced in an environmentally-friendly manner (ISO 14001-accredited factory and compliance with EU biocidal products regulation n°528/2012).

Similarly, as part of our sustainable development approach, we have chosen to use **biosourced inks for printing on polycarbonate and vegetable-based inks for paper.**

This has a direct impact on the environment, but also on the health of users, who are not exposed to the risks associated with the solvents present in mineral inks.

THE RIGHT TO BE YOU

Keep in touch and learn more information about us ➜

v1.0