Best Practice Guidelines and Minimum Security Standards for Identity Documents

Recommendations for Advanced Document Design and Integration of Security Features

SECURE IDENTITY ALLIANCE

DSA
ENHANCING DOCUMENT AND IDENTITY SECURITY

INTERGRAF

Table of Contents

INTRODUCTION

Raising the Bar: A Practical Framework for Elevating Minimum Security Standards in Government Identity Document Issuance

Identity documents — passports, national identity cards, driver's licenses, and the many other credentials governments issue — are a critical element of modern global society. They enable people to prove who they are across a vast range of essential interactions: crossing international borders, opening bank accounts, boarding aircraft, entering government facilities, purchasing age-restricted goods, and countless other situations where trusted identification is a prerequisite for participation. In this sense, identity documents are not merely bureaucratic artifacts; they are the infrastructure of civic and economic life.

Of paramount concern is the alarming quantity, quality, and sophistication of counterfeit identity documents now pervasive across Europe, North America, and beyond. Fraudulent documents are instruments of serious harm: they facilitate identity theft, financial crimes including money laundering, worksite enforcement violations, and fraud linked to immigration-related offences such as human smuggling and trafficking. Manipulated and counterfeited credentials are also exploited by individuals connected to organized criminal networks — including international terrorist groups — specifically to reduce scrutiny from travel screening and border control measures. The threat is not abstract or distant. It is active, adaptive, and escalating.

Governments are continually under pressure to define security, technical, and design requirements that are both financially sustainable and genuinely effective — keeping their documents ahead of counterfeiters who are rapidly closing the gap. Drawing on a deep understanding of the technologies available to and actively used by the most sophisticated forgers, the authors of this paper aim to provide governments and document specifiers with best practice guidelines for the development and production of passports and identity cards that exceed minimum standards and are significantly more resistant to counterfeiting.

This paper is written for the practitioners and policymakers who bear direct responsibility for that resistance: the government officials, program managers, and technical leads overseeing identity document issuance. Its purpose is to raise the floor — to go well beyond the minimum standards. Not every issuing authority will adopt the same solutions, and not every context will support the same technologies. But every authority can aspire to a higher standard of security — and this paper aims to show what that looks like in practice.

What This Paper Is — and What It Is Not

This is not an encyclopedia of identity document technologies. It does not attempt to catalogue every available solution or provide exhaustive technical specifications. Instead, it is a practical guide to concepts, principles, and decision-making — focused on the "why" and "how" rather than the granular detail of every available option. Where technologies are referenced, they serve as illustrative examples of optimization rather than prescriptive mandates.

We acknowledge, plainly, that not all technologies are equal. Laser engraving, for example, offers a level of durability and tamper resistance that thermal personalization cannot match. Where authorities have the means and mandate to adopt superior technologies, they should. But we also recognize that procurement cycles are long, budgets are constrained, and transitions take time. For those authorities currently operating with less advanced systems, this paper offers guidance on how to extract the maximum security benefit from the tools at hand — and how to plan for future uplift.

Key Themes

Several themes run throughout this paper, each reflecting a critical dimension of modern identity document security:

- **Advancing the Physical.** The era of purely physical document security is behind us. Today's strongest identity credentials integrate physical security features with embedded digital elements — cryptographic chips & codes, Machine-Readable Zones, and biometric data — in ways that reinforce one another. This paper explores how issuing authorities can approach that integration thoughtfully, regardless of their current technical baseline.
- **Quality Control and Image Management.** A document is only as secure as its weakest process. As an example, portrait photographs — the primary biometric identifier in most identity documents — are a frequent point of vulnerability. Poor image acquisition, inadequate quality checks, and inconsistent enrollment standards can undermine even the most sophisticated personalization technologies. Effective quality control over photograph capture and management is not a peripheral concern; it is foundational.
- **Continuous Education as a Security Imperative.** Technologies evolve. Threat actors adapt. Standards develop. No document produced today can be considered permanently secure against the threats of tomorrow — and no practitioner trained five years ago can be assumed current without ongoing development. This paper therefore treats continuing education — through conferences, structured training programs, webinars, and peer exchange — not as an optional supplement but as an integral component of any credible security framework.

An Invitation to Raise the Standard

The recommendations and frameworks that follow are grounded in both established best practice and the practical realities facing issuing authorities around the world. They are offered not as criticism of current practice, but as an invitation: to examine existing standards honestly, to identify where improvements are achievable, and to commit to a trajectory of continuous improvement.

The holders of identity documents — citizens, travelers, residents — place considerable trust in the authorities that issue them. That trust deserves to be honored with the highest standards of security that each authority can responsibly achieve. We hope this paper serves as a useful tool in that ongoing effort.

1. DOCUMENT FRAUD PROBLEMS

Weak documents — from poor quality manufacturing or from deploying weak security features — can be falsified in a number of ways and used to achieve different goals. Therefore, the resulting consequences are equally diverse. To design documents more securely against counterfeiting attacks, it is necessary to consider the different types of attacks used by counterfeiters and understand the methods of forgery. Based on the knowledge of attacks and procedures for forging documents, suitable measures can be taken for the protection of documents. The design and construction of a secure document should be such that the success rate of any attempted attack on the document is minimized and, hence, the likelihood of detecting the attack in the situation/scenario the document is presented for the first time is maximized.

a) Risk and Consequences of Weak Documents

In this section, we illustrate why fraudulent documents are of interest to criminals, what they are used for, and the economic impact and damage that undetected fraud can have. It should be noted that especially in situations where the same eligibility may be proven by different documents, e.g. driving licenses issued by different states, counterfeiters only need to focus on the inadequately secured and lower quality documents to achieve their goal. Such documents can often be falsified or forged even by simple methods, without high probabilities of detection at the first line of inspection. The more prominent use cases for fraudulent documents are as follows:

- **Create a new identity**

  The person could be on a watchlist and may want to misrepresent their age and/or name, or to obscure their real identity to deceive authorities.

- **Open a fraudulent bank account**

  The person can open an online bank account under false pretenses using a digitally altered or “deepfake” identity credential which greatly facilitates financial fraud. It is estimated that a false ID is used for 3 to 5% of all online onboarding transactions. In the U.S. alone this represents millions of fraudulent accounts every year.

- **Facilitate international border crossing**

  This refers to terrorists or organized crime rings intending to illegally enter a country to carry out attacks or illegal transactions, or criminals that require travel (such as those involved in contraband or human smuggling/trafficking). Another example is the circumvention of visa requirements.

- **Claim social benefits**

  Individuals could apply for asylum, health, or social benefits, such as unemployment subsidies which the individual would otherwise not be entitled to. An additional use case could be the admission to a study program or to exercise a profession for which the person would otherwise not meet the requirements.

b) Types of Identity Document Fraud

Document fraud appears in various forms and serves different purposes. The complexity, quality and structure of fraudulent documents differ depending on, among other things, their use and purpose. The following types of forged documents can be classified:

Modified Documents

These are authentic documents that have been altered and can be divided into the following categories:

- **Forged Documents (Forgery and Alteration)**

  Definition: A genuine document that has been unlawfully altered.

  There are various types of forgeries, which are all based on changing the information on a genuine document. Fraudsters may change only parts or the entire set of personal and/or issuance data originally provided in the genuine document. Often, the portrait is of particular interest as it provides the most prominent link between the document and the person presenting the document. Hence, the portrait is a frequently encountered target of attack as it needs to be adapted to the appearance of the new bearer of the document. Depending on the use case, however, other data elements might be targeted as well, e.g. the date of birth, validity periods in the visa or the document number. The methods employed for falsification of genuine documents include:

  - Portrait substitution or subtle modification of the portrait image
  - Portrait substitution with a digitally morphed image created from the original image in the chip and the counterfeiter's image
  - Removal and replacement of individual data elements
  - Addition, removal and/or replacement of letters/numbers to alter individual data elements
  - Removal and/or replacement of authentic (data) pages, e.g. from another authentic document
  - Applying false stamps
  - For digital transactions: digitally altering or adding information to an image of a genuine document

  Note: Weak documents personalized with low cost commercially available equipment may allow counterfeiters to apply the same or similar technologies for personalization as those used in authentic documents, thus rendering counterfeiting more difficult to detect.

- **Blank Stolen Documents**

  Definition: Documents issued decentrally are often delivered to the issuing authorities as genuine blanks.

  When such blanks fall into the hands of fraudsters, e.g. by theft, they can be personalized by the fraudsters, often containing all the genuine security features to be expected in authentic documents. In this case, the properties of the documents' personalization or checking databases for lost/stolen document numbers may be the only possible pathways of detection. Besides this mode of attack, authentic parts of genuine documents may also become available to fraudsters, e.g. due to security flaws in the manufacturing supply chain, and be applied to otherwise counterfeit documents.

Illegitimate Documents

While modified documents are authentic documents that have been altered, illegitimate documents are entirely false creations. These documents can be divided into:

- **Counterfeit Documents**
  Definition: A complete or partial reproduction of a genuine document.

  Counterfeit documents are imitations or reproductions of authentic documents. Typically, a fraudster will obtain or create a template and insert fake information and photos. The attack is carried out by creating the entire document or data page from scratch, imitating the appearance of the document and its security features (incl. their behavior) as closely as possible to the corresponding authentic document. The quality of counterfeits encountered in practice differ with the level of expertise of the fraudster, the availability of materials and manufacturing/imitation/printing techniques and the intended fraudulent use case.

- **Fantasy or Camouflage Documents**

  Definition: A fantasy document is made to resemble an official document but is not issued by a competent or recognized government authority.

  For this purpose, fraudsters may create their own issuing authorities that don't exist or use known organizations or authorities which are not allowed to issue official documents. Camouflage documents suggest issuance by an existing official document issuance authority or an existing country while the corresponding authority does not issue such types of documents. The rapid development of so-called "AI" tools for use with well-known graphic design software greatly facilitates the creation of such documents, thus their prevalence is likely to rise.

Falsely represented documents

These are documents that may be legitimate or authentic, but don't belong to the person presenting them. Without sophisticated identity verification technology, they are the most difficult to detect. These documents typically come in two forms:

- **Fraudulently Obtained Documents**

  Fraudsters attack the application process of official documents by providing false information on their applications and/or tricking issuance authorities into issuing an official document based on fraudulent reasons/documents/information. In the process, false information and/or manipulated portraits may be incorporated into officially issued and otherwise authentic documents. Hence, the attack cannot be detected by inspection of security features.

- **Imposter Documents**

  The document itself is genuine, but presented by someone other than the legal holder of the document ("look-alike fraud").

Not all types of fraud presented above can be addressed with proper design and construction of security documents. Fraud types such as stolen blanks or fraudulently obtained documents require other measures, such as improving traceability and security of supply chain and storage or eliminating vulnerabilities of the application process and morphing detection algorithms. The following sections will, hence, focus primarily on the prevention of forgeries and counterfeit documents, which can be substantially improved by appropriate design and integration of security features in a document.

Finally, in many jurisdictions, the penalties for forging documents (especially if they are not those of the country where the forgery is physically done) can be low, as little as a financial penalty and a suspended sentence for a first time offense. The legal jeopardy for an institution such as a bank accepting a fraudulent ID are lower still, even nonexistent if the institution can prove “good faith”. This emphasizes the importance of maintaining the highest possible standards for document security.

2. SECURITY FEATURE CLASSIFICATION

Broadly, the term "security features" refers to a diverse group of technologies that make counterfeiting and alteration of documents difficult. Security feature definitions and taxonomies are available from the Public Register of Authentic Documents Online[1] (PRADO) and multiple sections of ICAO Doc 9303 8th edition, including in the Terms and Definitions of Part 1[2], Appendix A to Part 2[3] regarding human-inspectable security features, and Appendices B and C to Part 2 regarding machine-readable security features.

As with the modes of document fraud described in Section 2, this guidance focuses more on security feature classification rather than on enumerating an exhaustive list of technologies. In addition, Doc 9303 Part 2 Appendix A illustrates several methods of classifying security features, which are described below. These methods are not in competition with one another, and issuers should consider all of them to be important to the process of designing a new document.

a) Role in Combating Counterfeiting

One way to classify security features is according to their roles in combating counterfeiting and alteration[4]. Not all security features perform similar functions and a security feature that provides strong protection against counterfeiting may be weak against alteration, or the reverse. For example, watermarks are typically regarded as a defense against counterfeiting, while including multiple bearer portraits is usually a defense against alteration. However, fragile watermarks can also be added to passport data pages for tamper evidence, and if several bearer portraits are added at different locations using different personalization technologies, then a counterfeiter must work harder to simulate them and is at greater risk of error. Similarly, diffractive optically variable image devices (DOVIDs) combat counterfeiting because of their graphical complexity and bright visual effects but combat alteration when they intersect with one or more of the portraits in ways that promote visible damage to the DOVID if the portrait is manipulated. These examples are just illustrative; ideally, every security feature should be optimized for its capacity to fulfill several functions at once.

b) Inspection Levels

A prototypical security feature classification method is by inspection level[5]. Visual features verifiable with the naked eye are Level 1/Overt (e.g. watermarks and color shifting ink), features requiring simple tools are Level 2/Covert (e.g. microtext or ultraviolet features), and those requiring elaborate tools and special expertise are Level 3/Forensic (e.g. chemical taggants). Any ID document requires a balance between straightforward security features for lay users and more sophisticated technologies that counterfeiters are seriously challenged to simulate or cannot locate at all. Issuers can begin by partitioning security features between each of these categories, with an emphasis on Level 1 features that are accessible in

[1] https://www.consilium.europa.eu/prado/en/prado-glossary.html

[2] ICAO Doc 9303, 8th edition, Part 1, pp 8-25

[3] ICAO Doc 9303, 8th edition, Part 2, pp App A-4 through A-15

[4] ICAO Doc 9303, 8th edition, Part 2, pp App A-2

[5] ICAO Doc 9303, 8th edition, Part 2, pp App A-3

diverse conditions. Individual features can fall under more than one of these categories; some of these are discussed below under Section 5, Design Principles and Strategies.

c) Feature Location

Doc 9303 also divides security features according to their location on or in the document, i.e. their association with specific physical components of the document or a specific part of the document's manufacturing and issuance workflow[6]. These categories include substrate features, printed elements, surface-applied or integrated features, serial numbering, other copy protection and personalization/ issuance techniques. Distributing security through different aspects of a document's construction, while avoiding concentration of many security features in a single part of the document to the neglect of others, puts much higher barriers in the way of counterfeiters who would need to master all aspects of the document's construction instead of just graphic arts.

d) Designing for —and Interacting with —Machine Readers

Yet another way security features can be categorized is by their interaction with document machine readers. As explained in the 8th edition of Doc 9303 Part 2[7,8], both data security features (e.g. MRZ, 2D-barcodes such as PDF-417 or Data Matrix Code) and visual/physical security features can be inspected and authenticated by readers. While ICAO provides international standards to make data features interoperable across borders, visual/physical security features for human and machine inspection are designed differently by each issuer and security feature manufacturer. Nonetheless, because document reader systems typically capture a combination of visible, UV, and IR images, embedding specific UV and IR characteristics enables readers to identify fraudulent documents (in most cases, readers need access to a library of genuine document images for comparison). Substrates, print, personalization, and security features can all play a role in improving compatibility with machine readers, if this is considered and optimized for when a document is designed. Ideally, artwork and security features should be affirmatively designed to create a highly distinctive 'reader signature' that counterfeiters will be challenged to mimic.

It is important to differentiate between the document readers described above, which are designed to check UV, IR and other features, and consumer cameras that are not explicitly intended for security document verification. For example, a webcam or smartphone camera used in a remote video identification process ("Video Ident") cannot check UV, IR or various other security features. If this limitation is known to a counterfeiter, then counterfeiting efforts can ignore features inaccessible to such a camera. Entities authenticating documents are cautioned that video or other digital inspection workflows do not allow for robust security feature inspection.

Many security features can perform different functions across more than one of these categories, and issuers should seek to embed this multifunctionality whenever feasible. Examples of such optimizations are presented below under Section 6, Design Examples.

---

[6] ICAO Doc 9303, 8th edition, Part 2, pp App A-4

[7] ICAO Doc 9303, 8th edition, Part 2, Appendix B

[8] ICAO Doc 9303, 8th edition, Part 2, Appendix C

3. MINIMUM STANDARDS

Document security is not maximized by meeting an arbitrary threshold for a certain quantity of security features without also considering the role each feature plays against different modes of attack, where it is placed in the document, how it is integrated with personalization, artwork and other features, and how it is inspected. Objective standards regarding the components used in a security document's construction, and the presence or absence of basic and advanced security features, provide a minimum floor that is the foundation for later design optimizations.

ICAO Doc 9303[9] and the E.U. passport regulation[10] describe minimum standards for each part or process of a travel document. Within each category, security feature technologies are partitioned between "basic features" that issuers are recommended to incorporate, and "additional features" that may or may not be included based on considerations such as the present counterfeiting threat as well as stipulated budgets. Importantly, security features can simultaneously be placed in both categories, depending on how they are implemented. In addition to feature implementation, the feature and security print designs are also of great significance to how documents resist counterfeiting and alteration workflows.

Document design principles can be divided into two groups, which are each addressed in separate sections below. The first section on Technical Design Principles describes strategies relating to the physical and manufacturing characteristics of the document and its security features. The second section about Ergonomic Design Principles includes strategies that help users locate and authenticate security features quickly and easily.

[9] ICAO Doc 9303, 8th edition, Part 2, pp App A-4 through A-15

[10] EU Council Regulation 2252/2004

4. TECHNICAL DESIGN PRINCIPLES

This section describes four technical design principles that should be viewed in combination and not as alternatives. It is highly recommended to integrate all these concepts into a document design simultaneously, while further ensuring that the guidance in the Ergonomic Design Principles section below and a security feature classification scheme (see Chapters 3, 4) are also observed. Precisely how these goals are executed is a matter of discretion and priorities rather than absolute rules.

In this context, it is useful to consider counterfeiting and forgery from the perspective of the forger. Forgers are first and foremost efficient and will seek to expend the minimum amount of effort for the maximum gain. For example, a driver's license from any E.U. state is valid in any other E.U. state, so for the purpose of illegally driving a motor vehicle a forger will forge or counterfeit the license document which is the easiest to attack.

A counterfeit document is also subject to far fewer technical constraints than issuing authorities, among them:

- A criminal can spend as much time as needed to make a single fake, while industry must make tens of thousands of whole documents every day. Handcraft is the norm in ID fraud and opens endless possibilities in feature substitution or subversion.
- For a Polycarbonate travel document as an example, the criminal is unlikely to use lamination (or even polycarbonate for that matter) and will prefer gluing the layers as this brings a cascade of benefits in terms of substitute materials and consumables which do not have to survive 180°C lamination temperatures.
- A counterfeit document does not need to survive ten years as typically a few weeks is all that is needed. Poor lightfastness is fine for a fake.

Industrial production does have some technical benefits, however:

- Once properly set up, registration can be very good. This is difficult to replicate by hand. As an example, visible duplex printing is an advantageous feature, especially if it can be achieved on several different layers of the card construction.
- A small counterfeiting / forgery operation cannot be a jack-of-all-trades like an established integrator. Thus, combining features from vastly different domains, i.e. physical + digital will be challenging for a criminal.

a) High Technical Demands

Security printing must use superior equipment, materials and expertise that counterfeiters are challenged to mimic. The main priority of a document manufacturer should therefore be adherence to high technical sophistication and high quality control standards, since quality control problems can result in genuine documents being suspected as counterfeits and a less-than-consistent quality can confuse document users and inspectors. Manufacturers should embrace security designs that are technically demanding, e.g., in terms of high-resolution artwork, material integration, and registration between multiple printing steps. In many cases, a manufacturing or issuance workflow that is simple or convenient for a genuine document issuer is also easier for counterfeiters to attack.

Offset printing may provide the best illustration of what “technically demanding” means. Offset printing is a widely used commercial printing process that is accessible to counterfeiters. To address this, in security printing, offset is implemented using methods and press capabilities for which there is little demand in commercial printing markets. For example, advanced security offset printing usually includes line art instead of halftones, spot colors instead of process colors, inks with special visual properties, high resolution plate capabilities, high registration press capabilities (**Figure 1: Zambia 10 Kwacha Banknote**), split fountain color transitions, simultaneous offset for front-to-back register, microprinting, partitioning of artwork between offset and intaglio printing, etc. Even counterfeiters that do have access to offset printing technology and skills may be challenged to mimic these specialized security printing techniques. Similarly, security substrates, security features and personalization methods should also be technically challenging and/or using materials with restricted accessibility.

Figure 1: Example illustrating registration of multicolor offset printing and intaglio printing (Zambia 10 Kwacha Banknote — Credit: KEESING TECHNOLOGIES)

b) Integration of Document Components

A security document is more than the sum of its parts and integrated security features are more difficult to attack than isolated security features. When possible, designers should integrate 1) materials, 2) manufacturing processes and 3) design together such that the composite product can only be manufactured with all three elements in place. This prevents counterfeiters from attacking individual elements in isolation or using simple low-cost equipment to simulate the output of a security document manufacturing workflow that requires a complex manufacturing and issuance infrastructure.

A simple example is metallic ink microprinting (**Figure 2: Thailand Passport**). Metallic ink can provide some protection against digital counterfeiting because it cannot be simulated by most home/office printing devices. However, metallic ink can be purchased commercially by counterfeiters, so if viewed strictly as a raw material it would appear to be of limited security value. Similarly, microprinting provides some security against digital counterfeiting, but inkjet printer resolutions continue to improve, and some can simulate the fine details of spot color microprinting. To improve the security value of both features, metallic ink can be applied using a printing process capable of the high resolution and fine line detail needed for microprinting, such as offset. Combining the two features together, such that they cannot be counterfeited separately, is more difficult to simulate than either component alone.

Figure 2: Example of metallic ink (Data page of Thailand Passport)

In similar fashion, metallic ink, UV-reactive ink, split fountain printing and simultaneous offset are often regarded as distinct security features. In security printing environments where the necessary infrastructure is available, these features can be integrated together into a single design that requires two special inks and two specific printing press hardware capabilities to execute correctly, making it impossible for a counterfeiter to simulate each feature effectively in isolation (returning again to **Figure 1: Zambia 10 Kwacha Banknote**). Additionally, color shifting inks and/or UV fluorescent inks could be included in a multicolor intaglio design that also contains microprinting; intaglio or tactile features, applied by the card lamination process, could be positioned over DOVIDs or a colour-shifting ink patch to provide zone security over multiple levels of the card construction and prevent harvesting; or various security features could intersect with high-permanence portraits or other personalization data to prevent portrait substitution. The majority of overt optical features function more effectively (are more visible) against a dark background, thus laser engraving applied during the personalization step, can be used to locally enhance the visibility of a DOVID or a surface OVD such as a Reflective Optically Variable Image Device (ROVID) applied by lamination. Such a solution not only protects against misuse of stolen, blank documents but can also advantageously make the excellent registration between laser engraving and other card features visible.

An enhanced example is the integration of combination DOVIDs, where the embedded DOVID is partially metallic and partially transparent. The metalized portion can be personalized via laser ablation (birthdate/initials, document number) while the transparent portion reveals the underlying security print features and/or personalization (photo and/or personalized data) on the document. Additionally, the design of the DOVID and the structures within it can be integrated with the document design such that together they complete a design.

More generally, since ID documents are about ten times thicker than paper-based documents of value (such as banknotes) they offer a wide range of optical interaction possibilities between layers, especially when the document design incorporates a clear window. For example, a “moiré-magnifier” type feature incorporating structures embossed during lamination on both surfaces of a clear window, when combined with a laser engraved secondary portrait within the card construction, will pose great difficulties for forgers and the counterfeiters.

c) Utility in Multiple Inspection Conditions

Designers should include security features that are inspectable at multiple levels: overt, covert, and forensic, with a priority on readily accessible overt and covert features. In addition to increasing the difficulty of simulation, these can either be checked in environments where no tools are available, or examined with greater scrutiny at the covert level when circumstances allow. For example, the presence or absence of an embedded security thread can be checked at the overt level by visual inspection of the document, but if circumstances warrant then further inspection of the thread properties can be done with magnification or a UV lamp to show the thread’s UV response (**Figure 3: Swedish passport**).

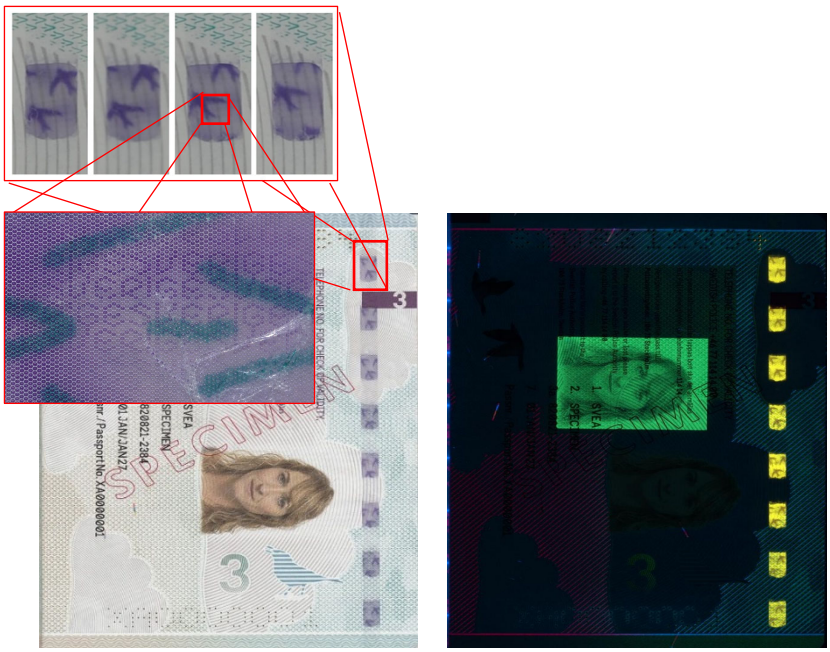


Figure 3: Multiple inspection conditions in this example of a Swedish passport (page 3): microscopic investigation of microtext (top left), Visible inspection at multiple viewing angles (bottom left), and inspection under UV illumination (right).

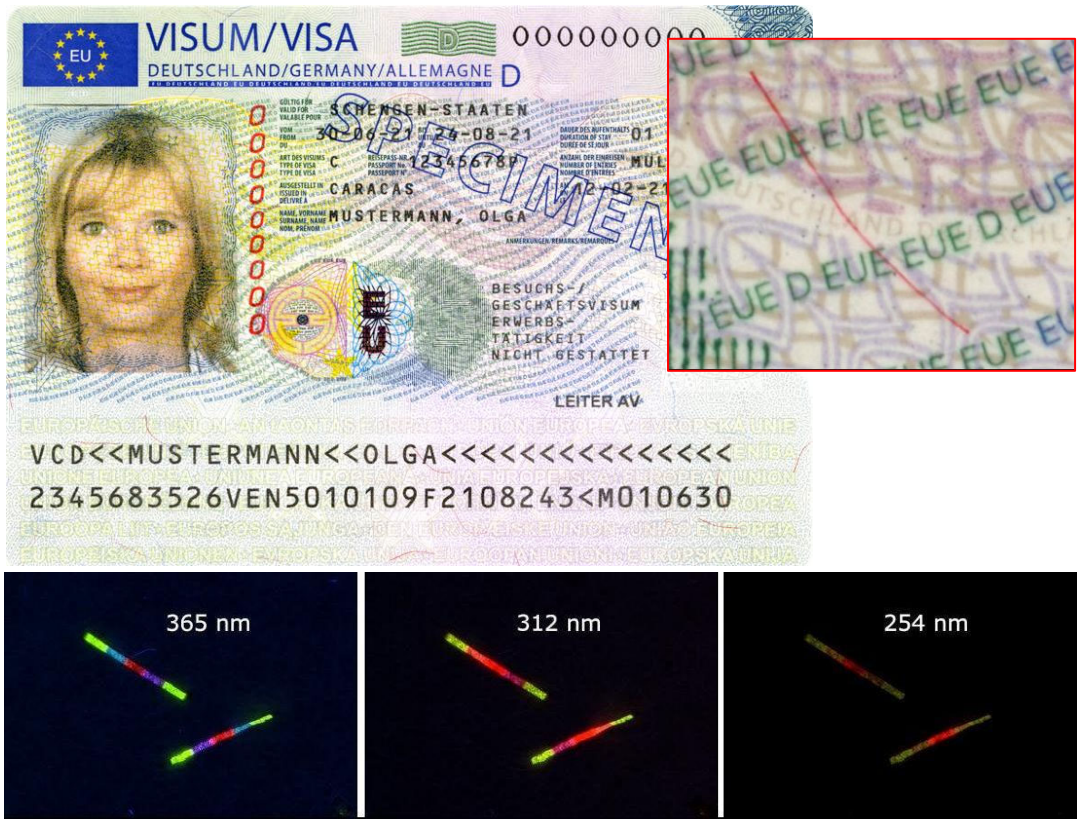


Figure 4: Example of security fibers in an EU Schengen visa sticker: Visible (top right) and invisible fibers with different UV responses at different UV wavelengths (bottom)

If the thread were also a carrier for a forensic feature, it would play a role at all three levels. Another example of a feature that functions at multiple levels are visible security fibers that also feature a UV response, and potentially carry a forensic functionality (**Figure 4: E.U. Schengen Visa**).

Microprinting deserves a special mention because it can be implemented at low cost into any other security feature capable of carrying artwork (offset print, intaglio print, planchettes, security threads, DOVIDs, etc.). It should be added to every possible document component to convert as many overt security features as possible into dual overt/covert features. Similarly, UV and IR responses can be added to many security feature types and should be considered for the same reason.

Despite their important role as an emergency backstop against highly sophisticated counterfeiting attacks, forensic security features are inaccessible to most document users. This limits their utility for routine document verification that takes place outside of laboratory environments. Nonetheless, the inclusion of forensic feature(s) into identity documents is imperative.

d) Resistance to Both Counterfeiting and Alteration

Generally, resistance to counterfeiting is supported by design and manufacturing complexity that make genuine document artwork and security features challenging to simulate with commercial materials and techniques. In contrast, alteration resistance is produced by high permanence personalization methods like laser engraving that are hard to remove from a document once applied, in addition to manufacturing processes that prevent delamination or layer separation within synthetic substrates, and overlaying document components in ways that inhibit harvesting of security feature materials. In each of these cases, permanence is key, and the goal is to make every aspect of the final document irreversible such that attempts to change or remove one component results in damage to that and other components. In this context, an ID document should ideally consist of the same material throughout all layers and be laminated together by heat and pressure. If an ID consists of different laminate materials, then a mechanical or chemical method exists to split it.

One of the most common and effective methods for preventing portrait substitutions is intersecting security features such as DOVIDs (**Figure 5: U.S. Permanent Resident Card**) and tactile plate features (**Figure 6: Dutch passport**`) with portraits.

Figure 5: Example of a transparent portion of a DOVID overlapping the portrait. U.S. Permanent Resident Card.

Figure 6: Example of static microprint tactile feature (Dutch passport).

This prevents forgery by laminate superposition and provides unmistakable tamper evidence for portrait erasure or substitution. For both examples, it is the visual complexity and high manufacturing requirements that help the features resist counterfeiting, but it is the placement of the feature to overlap the portrait area that provides alteration resistance. As the primary portrait is by far the most checked feature on an identity document, a DOVID or surface structure overlapping the photo creates a barrier to anyone attempting photo substitution or alteration.

e) Self-Assessment of Government Documents

The eDocument Scheme for Evaluating Physical Security (eSEC) is a tool designed by SIA's Document Security Working Group and other experts in the ID documents sector to help governments develop secure eDocuments, functioning as a self-assessment tool to evaluate the physical security of current documents, assess the security impact of additional design changes, and understand what is required to build a secure eDocument. Built on three years of research and informed by decades of cumulative expertise, the eSEC 2.0 platform evaluates more than 150 security features — including the latest generations — and offers a structured self-assessment process to help document issuers and designers evaluate existing or planned documents to ensure balanced and well-rounded security features.

5. ERGONOMIC DESIGN PRINCIPLES

This section will explore four ergonomic design principles that illustrate how better design can make document examination easier: signaling users, clustering similar features, branding to the issuing authority and contrast optimization. User training on security feature recognition and inspection is a constant problem for many issuers, and design strategies that signal the presence of security features or make them easier to inspect can help. These strategies should be implemented concurrently with each other, and with the Technical Design Principles above, and follow the schema described in the Minimum Standards and Security Feature Classification sections. Just as with the technical design principles, these ergonomic design principles can be implemented in many ways and designers have considerable discretion.

a) Signaling Users

Security features can be designed in ways that alert users to their presence and facilitate easier inspection. This can be done by including large, bold security features as well as by the harmonious integration of features into the document in ways that draw the attention of document users — or a decidedly isolated position of features that visibly contrasts with the rest of the document design.

Specific types of features, such as advanced DOVIDs, are particularly suitable for overall design integration and broad coverage, which facilitates a storytelling approach that will help even untrained individuals to draw their eyes toward the feature and its motifs and use it for document verification. How each security feature is made accessible to users can differ for various document types or user populations, and bespoke criteria could be used for each feature type. An easy way to do this is to incorporate static printed elements which are identical to design elements on the DOVID (**Figure 7: integration of DOVID elements and printed elements)** as this informs the user what should be seen on the DOVID. This extends to other security elements such as micro perforation, and silkscreen printed security inks.

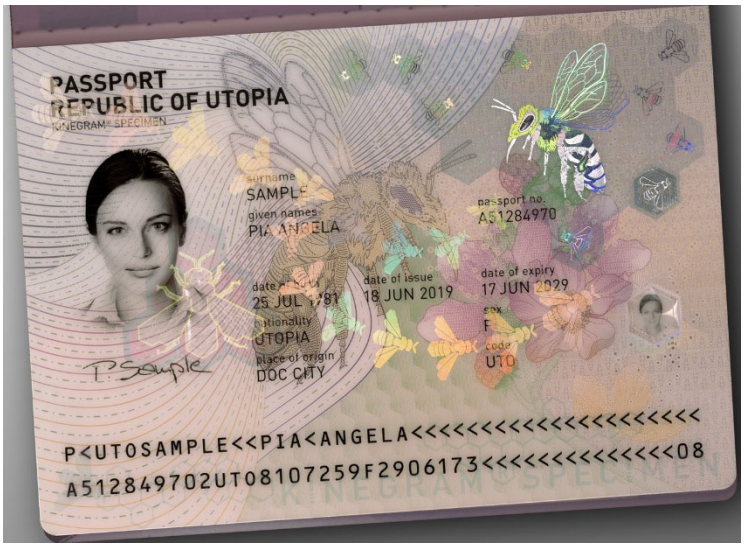


Figure 7: Integration of DOVID elements and printed elements

Another example, microprinting, is a popular and inexpensive feature — however, its placement in an unfamiliar document is not obvious and document users must search the document with magnification to determine whether and where microprinting is present. Solutions for better microprinting ergonomics include typical locations — for example, at the edges of larger graphics or in signature lines — or including large microprinting patterns throughout the document artwork, so users don't have to search. Another solution is to include variable size microprinting that shows a progression in font size to help users identify the location even before reaching for a magnifier (**Figure 8: Czech passport**).

Figure 8: Variable Sized Microtext (Czech Passport — Credit: KEESING TECHNOLOGIES)

b) Clustering Similar Features

Security features are inspected in a variety of ways and common viewing conditions include inspecting using transmitted light, tilting for overt features, and magnification or UV light for covert features. Each inspection method is applicable to multiple security feature types, so designers should consider placing security features that are inspected in the same way in proximity to one another. This can allow multiple features to be inspected simultaneously and can help lay users locate similar features in unfamiliar documents.

An example is the placement of microprinting from different printing steps in the same microscopic location. This can be limited to static microprinting impressions from multiple offset or intaglio plate impressions, or it can include personalized laser engraved microprinting in synthetic substrates.

Another example is planchettes containing embedded security fibers and/or graphics. Similar to microprinting, security fibers are sometimes challenging for document users to inspect because the document substrate must first be searched for the location of a tiny fiber that may be concealed by the document artwork. This can be easy if many security fibers are present but difficult if the security fiber density is low, which is sometimes the case. When a security fiber is found, it is still not clear whether there are security fibers of other colors or with other properties elsewhere in the substrate. Clustering security fibers together at high density in a planchette (**Figure 9: Clustering of planchettes and security fibers**) helps alleviate this problem because planchettes are physically larger and easier to locate than individual fibers.

Additionally, because the fiber density is high, each planchette contains the full suite of security fibers such that document users must only locate one planchette to see all fiber types together and need not search for each one individually.

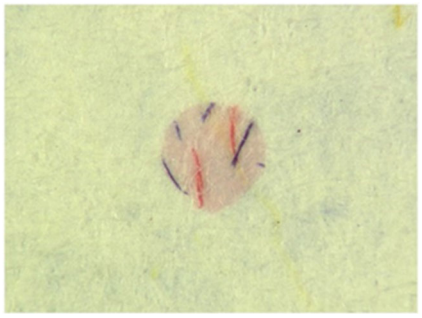


Figure 9: A planchette containing security fibers (Credit: KEESING TECHNOLOGIES)

c) Branding to the Issuing Authority

Security documents contain a blend of components that can carry images or text artwork, such as offset or intaglio printing, microprinting, security threads, watermarks, static tactile plate features, planchettes (**Figure 10: Nigerian passport**) and DOVIDs (**Figure 11: Swedish Passport**).

Figure 10: Example of a planchette (left) and a security fibre (right) with issuer branding visible under UV illumination (Nigerian passport)

Figure 11:Example of a DOVID with issuer branding (data page of Swedish passport)

Just as issuers should look for opportunities to insert microprinting wherever it is technically possible, every area of imagery is also an opportunity to insert issuer branding. Associating each document component to a specific issuing authority makes it more challenging for counterfeiters to repurpose generic commercially available materials into counterfeits. Including consistent issuer branding across multiple document components also provides clarity for document users. A common example is to use an image of the same historical figure as a printed portrait, watermark or a DOVID each in different locations in the document. (**Figure 12: French Passport**) and (**Figure 13: Canadian PRC**).

Figure 12: The same historical figure is incorporated in different components/features of the French passport: The watermark (left) and the DOVID (right).

Figure 13: Repeated image (PR card clock) in visible, DOVID, Embossing, UV (Canadian PRC)

d) Contrast Optimization

Both low contrast and high contrast concepts are important in security document design. In designing artwork for better resistance to digital counterfeiting processes, areas of low contrast between substrate and artwork colors, or between artwork from multiple printing steps, may inhibit scanning or process color hardcopy reproduction processes. But when considering user ergonomics, designing for higher contrast can help users locate and differentiate between various document features.

A good example is the design of UV components, which could include UV responses from security fibers, a security thread and printed artwork. If these components all respond to the same UV wavelength, it could confuse document users as to how many features are present. If these components all respond in different UV wavelengths, they will stand out from one another, and it will be apparent that three separate features are present (**Figure 14: Polish Driving License**).

Figure 14: Example of different design motifs visible under different UV wavelengths. On the front side of the Polish driving license, additional instruments become visible at 313 nm UV illumination (right) compared to standard 365 nm UV (left).

Another aspect of contrast of particular significance to UV features is brightness. Because the visibility of UV features is highly dependent on ambient lighting conditions and the type of UV light source used, UV features should be designed to produce a UV response that is as bright as possible so they can be used in as many circumstances as possible. This example was specific to UV-reactive features but could be extended to other security features. For example, high contrast between a visible security fiber color and the color of the substrate will help users locate fibers more easily, while low contrast between fiber color and substrate color will conceal the fibers and make them hard to find and inspect.

Finally, to combat the increasing ubiquity of UV fluorescent inks it is useful to combine them with IR dropout or anti-Stokes inks (**Figure 15: Anti-Stokes (IR fluorescing) print**) in a graphically coherent manner by registered silkscreen printing for example.

Figure 15: Anti-Stokes (IR fluorescing) print (Credit: Thales)

6. DESIGN EXAMPLES

The prior sections on design principles illustrated some high-level design concepts that should be considered to maximize the effectiveness of security features and the identity documents they protect. The purpose of this section is to provide additional context about how these design principles combat specific counterfeiting or alteration attacks.

ICAO Doc 9303[11] provides a list of nine discrete threats to the security of travel documents. Although the Doc 9303 guidance is specific to travel documents (like passports), many of the recommendations may be extensible to identity cards, vital records or other documents. The threats include:

- Counterfeiting a complete travel document
- Photo substitution
- Deletion/alteration of data in the visual or Machine-Readable Zone of the MRP data page
- Construction of a fraudulent document, or parts thereof, using materials from legitimate documents
- Removal and substitution of entire page(s) or visas
- Deletion of entries on visa pages and the observations page
- Theft of genuine document blanks
- Impostors (assumed identity; altered appearance)
- Tampering with the contactless IC (where present) either physically or electronically

In addition to the above threats described in ICAO Doc 9303, two additional items are considered here:

- Tampering with cryptographically signed data structures encoded in a two-dimensional barcode
- Improperly issued/improperly obtained

In every case where a document optimization or implementation strategy is recommended, it should be associated with one or more of the above risks. Accordingly, each risk is addressed as a standalone topic in its own subsection below, with its own unique set of strategies and solutions.

The inclusion and optimization of security feature technologies can be constrained by substrate and personalization technology selections made in the early stages of a design process, and potential security features and design solutions are dependent on document construction. For example, anti-counterfeiting strategies appropriate for a plastic identity card may not be applicable to a paper visa, and features used in a thick plastic passport data page may not work in thin paper data pages. Importantly, counterfeiting technologies continue to evolve, and, as a result, mitigation strategies will need to evolve to address the needs and use case of specific security documents. This is particularly important considering the long validity periods of most travel documents (up to ten years).

a) Counterfeiting a Complete Travel Document

Contemporary identity and travel documents are complex manufactured products that contain substrates, inks, adhesives, stitching threads, electronics, security feature components and other materials that are sourced from different vendors, and which have their own supply chains. The large number of commercial and proprietary materials and manufacturing processes needed to assemble a

[11] ICAO Doc 9303, Part 2, pp App A-2.

complete security document make it a challenge for all but the most skilled and well-funded counterfeiting operations to attempt a highly deceptive counterfeit of a well-designed document.

One way that issuers achieve good security against counterfeiting is implementation of a broad variety of security features across different document components and for different security functions. For example, distributing security features across the substrate, artwork and personalization does not permit counterfeiters the convenience of focusing on only one of these components. To counterfeit such a document requires knowledge of all aspects of the document and access to technology to simulate many different feature types. Often, the number and complexity of features means a counterfeiter is forced to make compromises and/or take shortcuts, leading to errors and easier detection.

Another common practice is the use of security manufacturing and design processes that are different from commercial graphic arts workflows and technologies available to and employed by counterfeiters. For example, artwork in security documents is typically made of intricate fine lines instead of the halftones common in commercial printing. Similar thinking is applied to substrate design, selection of personalization technologies, raw materials and consumables, and other aspects of a document to ensure that identical document components are not readily available from commercial sources. Not all components and manufacturing processes in a document must be proprietary, but options should be explored especially in design contexts (such as artwork) that can be implemented without much cost. In this regard and in view of the "handcrafted" nature of most counterfeits, print in register such as visible duplex printing can (in combination of course with other features) be a highly cost effective option to enhance anti-counterfeit robustness.

A third common strategy is liberal application of branding so that each document component visually signals a link to the document's nationality, issuing authority and/or document type, either through text or imagery. Vehicles for communicating branding include not just visible and UV artwork, but also watermarks, security threads, DOVIDs (holograms etc.) and other optically variable devices, laminates, embossing, etc. (**Figure 16: Canadian Permanent Resident Card**). Including branding throughout these elements makes it more difficult for counterfeiters to source branded simulation materials, re-use genuine materials and increases risk for those counterfeiters that attempt to use generic materials that do not feature issuer branding.

Figure 16: DOVID with brand (Canadian Permanent Resident Card)

b) Photo Substitution

Rather than take the time and incur the expense of counterfeiting a complete identity document from scratch, counterfeiters may find it easier to change the identity by replacing or altering the bearer portrait. This risk is typically mitigated in one of three ways: selecting high permanence personalization methods, intersecting the portrait with security features for tamper evidence, and applying multiple bearer portraits with different technologies (**Figure 17: German ID Card**).

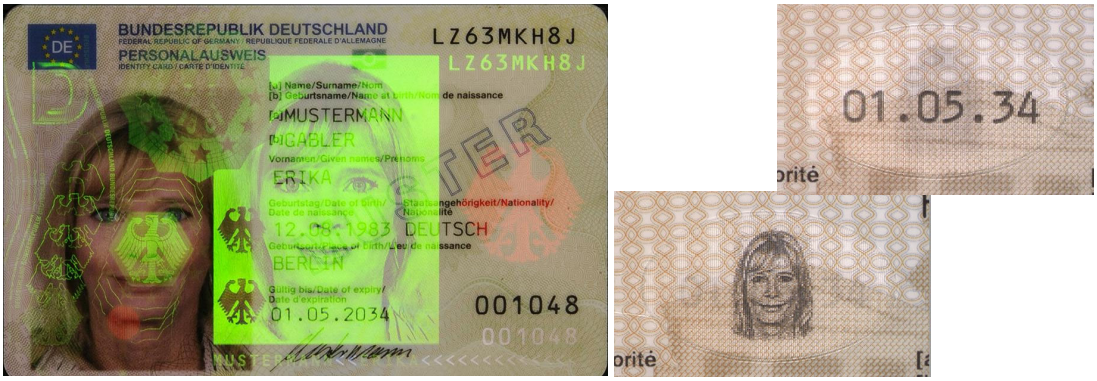


Figure 17: Example of incorporating multiple bearer images with different technologies. Besides the main portrait in inkjet-based technology, the secondary portraits In this German ID card are incorporated as DOVID and changeable laser image features.

Seized forgeries of this type are often identified thanks to the secondary portrait (**Figure 18: Forged Norway passport)**.

Figure 18: Forged Norway passport with different secondary portrait in MLI from tampered main photo (Credit: Joop van HOLLEGIE / Koninglijke Maréchaussée NL)

Thus, Protecting the primary portrait against tampering and adding at least one secondary portrait during the personalization step will defend against this type of fraud. For ID-1 documents, a small high resolution secondary portrait will prove difficult for the criminal to tamper with. Passport formats offer a wider range of possibilities for protection, such as a microperforated portrait on the datapage or placement of an alternate portrait on the paper page adjacent to the datapage which greatly increases the challenge of fraudulent tampering since the personalization methods and render are different for polymer and paper.

The best example of high permanence personalization is laser engraving, a popular method for personalizing plastic cards or plastic passport data pages. Laser engraving is regarded as a high-security process because it penetrates deep into the card body, making it very difficult to remove without causing substantial damage. This creates a problem for counterfeiters because portrait substitutions are more difficult to execute, and easier to detect, if the original genuine bearer portrait cannot be removed from the document. In paper documents pigment inkjet formulations are typically regarded as offering higher permanence than dye inkjet formulations, with toner generally at greater risk of alteration than inkjet. These risks are often mitigated by applying the transparent portion of an embedded DOVID or a DOVID laminate over the portrait (see below) or placing tactile features across the portrait (Figure 19: Canadian Passport). Importantly, counterfeiting methods change over time and the conventional personalization security practices of today may not be adequate against tomorrow's attacks.

Figure 19: Transparent part of DOVID and tactile features over portrait (Canadian Passport)

Intersecting portraits with security features for tamper evidence provides clearly visible traces in case of portrait removal, alteration or obscuration. In laser engraved plastic documents it is common for the portrait area to be intersected by visible and/or UV artwork, clear textured surface artwork (which may itself display optical features) and a transparent DOVID. These features do not interfere with the penetration of laser engraving deep into the card body during personalization, such that any effort to change the portrait results in damage to, removal of, or discontinuities in security features that intersect the portrait area. In paper passport data pages, security features intersecting the portrait area often include underlying visible and UV artwork and a security laminate containing a DOVID. In paper documents that do not contain laminates (such as visa labels), visible and UV artwork, dry embossing, or fracture cuts are some options for security features that can intersect the portrait area.

The third method of preventing portrait substitution is multiple integrated portraits. All identity documents have at least one primary portrait (and all e-passports have an electronic portrait stored on the chip), but many issuers include second, third or even more portraits. To provide meaningful value against portrait substitution, each portrait should be applied with a different personalization method to force counterfeiters to simulate multiple technologies. Some common examples of technologies used for additional portraits include personalized halftones, UV printing, laser perforation and laser engraving in a clear window in a plastic card, but there are many other options for issuers to consider. Generally, the primary portrait should be large and of the highest resolution practically possible. Better a large, high-res monochrome portrait than a smaller, lower-resolution color one.

c) Deletion/Alteration of Data in the Visual or Machine-Readable Zone of the MRP Data Page

In most identity documents, the portrait and text data are applied in the same personalization steps using the same personalization technology, so some of the above strategies for protecting portraits from substitution can also be extended to text data. These include selecting a high permanence personalization method, which is often laser engraving in plastic cards or pigment inkjet for paper documents, though other personalization technologies can also be implemented securely. In laser engraved plastic documents a common strategy is to introduce tactile laser engraving in some data fields, which makes the data even more challenging to alter. Bearer data can also be intersected with visible or UV artwork, clear plate texture artwork, or a DOVID, all of which can provide tamper evidence if data is altered. Just as how multiple portraits make portrait substitution more difficult, in ICAO-compliant identity documents data is repeated between the Visual Inspection Zone (VIZ) and Machine-Readable Zone (MRZ). If data is altered in only one location, the VIZ and MRZ will not match, and the alteration can be easily detected. If data is altered in both the VIZ and MRZ, two alterations are required, and the risk of detection is increased.

d) Construction of a Fraudulent Document, or Parts Thereof, Using Materials from Legitimate Documents

Another shortcut some counterfeiters prefer over attempting to manufacture an entire identity document from scratch is to “harvest” security features or components from genuine documents and recycle them into a counterfeit. If successful, this can result in a more deceptive counterfeit than would be possible if the counterfeiter were working only with commercially available materials. However, genuine documents can resist this type of attack in two ways: using irreversible processes in document manufacturing/issuance and making security features hard to recycle even if they are harvested.

One example of an irreversible manufacturing process common in plastic identity documents is a solid card body in which the layers are bonded (laminated) together with heat and pressure, and which contain no adhesives, since this construction prevents counterfeiters from separating the card layers and removing components. Thin laminates used to protect personalization in paper passport data pages are intentionally fragile, preventing them from being separated and manipulated independently of the data page. Laser perforating the passport number through all the visa pages in a passport permanently ties all visa pages to bearer data in the genuine book. Features designed to self-destruct if modified, such as stitching threads that are bonded together after stitching, or fracture cuts, also fall into this category.

Just as intersecting bearer portraits with security features impedes portrait substitution as described above, intersecting security features with each other is a way to prevent harvesting. Some examples include applying intaglio artwork or dry embossing over a DOVID or a windowed security thread to provide tamper evidence if these features are harvested. Laser engraving can also be intersected with other features for harvesting resistance. Above, in the context of preventing portrait substitution and text data substitution, laser engraving was described as a high permanence personalization process that is difficult to remove once applied. Viewed differently, laser engraving also helps prevent harvesting because any document component, such as a DOVID, that is laser engraved, is permanently marked with personalization data from the original document, making it difficult to harvest and recycle the component into a counterfeit featuring different bearer data. In some cases, this strategy can be employed using personalization methods other than laser engraving (**Figure 20: Swiss ID Card**).

Figure 20: Personalized laser engraving of the DOVID of the Swiss ID card.

e) Removal and Substitution of Entire Pages or Visas

Preventing substitution of visa pages considers two risks: substitution of pages from one passport to another, and repositioning within a single passport. Preventing substitution between passports is addressed by marking every visa page with the passport number (or other personalization data specific to that book). This is typically done by laser or mechanical perforation. Preventing transposition of pages within a passport is achieved by clear display of page numbers both numerically in visible art, UV art, and the watermark, and graphically through tabbed numbering to provide a visual cue when a page is out of order (**Figure 21: Canadian Passport**).

Figure 21; Examples of altered perforation (Canadian passport)

Passport stitching is also a relevant security feature that can be customized by multiple thread colors, stitch type, UV response, twist and other characteristics. Unstitching and restitching is required for many types of page substitution and is indirectly revealed if one or more of the security characteristics of the stitching are disrupted (**Figure 22: German Passport**).

Figure 22: Example of genuine stitching thread (German passport).

f) Deletion of Entries on Visa Pages and the Observations Page

Entries on an observations page are applied by a document issuing authority during personalization, but visas and stamps are applied post-issuance by consular and/or border control agencies of other governments. Accordingly, these must be considered as two separate technical problems. Regarding the observations page, the issuing authority can apply observations text with personalization technologies more resistant to physical and/or chemical removal (typically pigment inkjet for a paper observations page) over both visible and UV background art. For visa pages, document issuers do not control the chemistry of the wide variety of stamp inks or visa labels adhesives used by foreign governments, but the surface characteristics of visa page paper can be engineered to maximize compatibility to the greatest extent possible. Additionally, mechanical alteration risks to visa page entries can be reduced by inclusion of fine line visible and UV artwork that covers the entire surface, and chemical alteration risks can be reduced by additional of chemically sensitive elements in the substrate.

For passports that have a signature panel on an interior page, the bearer's signature is another example of a post-issuance element that can be protected from alteration using strategies like those for the visa pages. Additionally, some issuers apply dry embossed artwork through the signature area to reduce the risk of mechanical alteration.

g) Theft of Genuine Document Blanks

The risk of theft of document blanks can be reduced through providing sufficient physical security measures, vetting staff that have access, and auditing blanks throughout their storage, issuance and disposition. But risks presented by theft of blanks can also be reduced by distributing security features throughout document components so that not all the security is in the blank. For example, custom data fonts, duplicate bearer data printed in UV, custom halftones in portraits, check digits, perforation technologies and others can be integrated into the personalization system and will be applied at the time of personalization (**Figure 23 – Norwegian Passport**). Counterfeiters in possession of stolen blanks do not also have access to the personalization system and cannot counterfeit these features easily.

Figure 23: Examples of features providing additional mitigation for risks presented by theft of blanks. The Norwegian passport shows a secondary portrait in the UV on page 3 and another laser perforated portrait and personal data on the data page.

Even if blanks were stolen, counterfeiters would not have access to the personalization system and would not have access to security features that are added during personalization. Also digitally signed personalized information inside 2D-barcodes can be checked to verify an authentic issuance. Another option is to adopt a centralized issuance workflow in which the document body is manufactured when the personalization is applied, which prevents theft of blanks because no blanks are ever transported outside of the issuance facility.

h) Impostors (Assumed Identity or Altered Appearance)

Unlike physical counterfeiting and alteration attacks that leave physical evidence that an identity document is fraudulent, impostors present a genuine document that was issued to a different individual as if it were their own. This fraud cannot be detected by inspection of physical security features because the document is genuine and unaltered. The focus of impostor detection shifts to a comparison between

the document bearer to any biometric information recorded in the document, either in printed or in electronic form. Identity documents almost always include a facial image but may also contain other biometric modalities, such as fingerprints or iris.

Document issuers have a variety of strategies to improve the utility of biometric images to facilitate impostor detection by making them easier to inspect. As described above, portraits applied using high-permanence personalization technologies such as laser engraving provide greater confidence that a substitution has not occurred and that a document is neither counterfeit nor altered. Given that assurance, the next step is to consider biometric inspection ergonomics, and document issuers can include enlarged portraits that are optimized for contrast/color and ensure good quality control throughout document personalization steps to make them as easy to inspect as possible. Finally, live capture of applicant portrait images in environments controlled by the issuing authority, and the use of biometric systems to detect multiple applications by a single individual, help ensure that only images of real humans are included in issued documents.

i) Tampering with the Contactless IC Either Physically or Electronically

Tampering with the contactless IC (Integrated Circuit) in security documents refers to the manipulation of the chip's functionality or data, either physically or electronically. Here's a breakdown of the potential attack vectors:

Physical Tampering

a) Chip damage or destruction: An attacker could try to damage or destroy the chip to prevent it from functioning correctly or to trigger a specific response.
b) Chip removal or replacement: An attacker might attempt to remove the contactless IC from the document and replace it with a fake or modified chip.
c) Physical probing: An attacker might use physical probes to access the chip's internal components, allowing them to manipulate the data or functionality.

Electronic Tampering:

a) Eavesdropping: An attacker could try to intercept the communication between the contactless IC and the reader device, potentially allowing them to steal sensitive information.
b) Replay attacks: An attacker might record and replay the communication between the contactless IC and the reader device, attempting to trick the system into accepting the replayed data as legitimate.
c) Data manipulation: An attacker could try to manipulate the data stored on the contactless IC, such as modifying personal data, authentication credentials, or other sensitive information.
d) Side-channel attacks: An attacker might exploit information about the implementation of the contactless IC, such as power consumption or electromagnetic radiation, to deduce sensitive information.
e) Fault injection: An attacker could intentionally introduce faults or errors into the contactless IC's operation, potentially allowing them to bypass security mechanisms or extract sensitive information.

To mitigate these types of attacks, security document issuers and manufacturers can implement various countermeasures, such as:

a) Secure chip design: Implementing secure design principles and using tamper-resistant materials to prevent physical tampering.
b) Encryption and authentication: Using robust encryption and authentication mechanisms to protect data and prevent unauthorized access.
c) Secure communication protocols: Implementing secure communication protocols, such as secure authentication and encryption, to prevent eavesdropping and replay attacks.
d) To ensure authenticity and integrity of the personalized data stored in the IC, digital signature schemes such as Passive Authentication defined in ICAO Doc 9303[12] must be implemented.
e) Intrusion detection and response: Implementing mechanisms to detect and respond to potential tampering attempts, such as monitoring for unusual activity or triggering alarms in case of suspicious behavior.

By understanding the potential attack vectors and implementing effective countermeasures, security document issuers and manufacturers can help protect the integrity and security of contactless ICs in security documents.

j) Tampering with Cryptographically Signed Data Structures Encoded in a Two-Dimensional Barcode

Cryptographically signed data encoded in 2D-barcodes are similarly vulnerable as the data content in an IC, most often similar data structures are used. To verify the digital signature using the Public Key Infrastructure (PKI) available, not all certificates necessary might be contained in the 2D-barcode itself, therefore access to a certificate repository might be needed to apply the full chain of trust.

k) Improperly Issued/Improperly Obtained

Within the EU, one method for improperly obtaining a document is to find a local indigent who is unlikely to travel and to walk this person through the passport application process, recovering the authentic document at the end of the process in exchange for money. Another well-known method is the fraudulent purchase of real documents from a traveler who then reports it as “lost” or “stolen”. In most developed countries, nationals can replace such document through consular channels within a day or two at a considerably lesser cost than the black market rate for a genuine document.

Improperly Issued/Improperly Obtained Security Documents refer to documents that are issued or obtained through unauthorized or fraudulent means:

Scenarios:

a) Bribery or corruption/ Insider threats: An individual bribes or corrupts a government official or document issuer to obtain a security document without meeting the necessary requirements.
b) Identity theft: An individual steals or uses someone else's identity to obtain a security document.

[12] ICAO Doc 9303, 8th edition, Part 11

Countermeasures

a) Robust issuance procedures: Implementing strict and transparent procedures for issuing security documents, including thorough background checks and verification of applicant information.
b) Identity verification: Implementing robust identity verification processes, including biometric authentication, to ensure that the individual applying for the document is who they claim to be.
c) Quality control measures: Regularly auditing and monitoring the issuance process to detect and prevent any potential corruption or exploitation.
d) Public awareness campaigns: Educating the public on the importance of security documents and the risks associated with improperly issued or obtained documents.
e) Training and education: Providing training and education to government officials and document issuers on the importance of security documents and the procedures for issuing them.
f) International cooperation: Collaborating with international partners to share best practices and coordinate efforts to prevent the misuse of security documents.

By implementing these countermeasures, governments and document issuers can help prevent the improper issuance or obtaining of security documents, reducing the risk of identity theft, transnational major and organized crime, terrorism and other security threats.

7. SECURITY AND TECHNOLOGY PRINCIPLES

The security and integrity of identity documents depend fundamentally on the materials from which they are constructed. Unlike ordinary printed products, identity documents must withstand years of physical handling, resist sophisticated forgery attempts, and incorporate layers of authentication features that can be verified both visually and with specialized equipment. This chapter examines the full spectrum of substrates, components, and printing technologies that together form the foundation of a modern high-security travel document, from the outermost cover material to the innermost paper pages and embedded electronic components.

Each material used serves a dual purpose: it must meet demanding functional requirements — durability, flexibility, heat resistance, and compatibility with bonding and lamination processes — while simultaneously acting as a carrier for one or more security features. Cover materials, chip inlays, high-security papers, polycarbonate data pages, laminates, and visa vignettes are each subject to their own minimum standards, carefully calibrated to ensure that the finished document remains stable and tamper-evident for a service life exceeding ten years. The interaction between these components is equally important; weak points at material interfaces can create vulnerabilities that skilled forgers may exploit.

Security elements are organized across three levels of increasing complexity and exclusivity. Level 1 features — such as diffractive optically variable image devices (DOVIDs), color shifting inks, and tactile surface elements — are designed for straightforward, unaided visual authentication by border officers and the general public. Level 2 features, including UV and infrared printing and microtext, require simple handheld tools to verify, while Level 3 forensic elements such as anti-Stokes properties, nanofeatures, and bi- or tri-fluorescent inks are detectable only with specialized laboratory equipment, providing a final line of defense against the most sophisticated counterfeiting efforts.

Underpinning all of these components are the security printing techniques — intaglio, offset, screen printing, and letterpress numbering — that apply these features with the precision and consistency demanded by high security document production. The following sections describe each material and technology in detail, outlining both the minimum standards that any compliant document must meet and the advanced options available to issuing authorities seeking the highest possible level of protection.

a) Cover Material [Polyacrylate Coating]

Plastic/polymer is applied to a paper/cardboard base material. On the one hand, the plastic/polymer coating must be flexible and heat-resistant so that a structural insertion (e.g.: a grain similar to a leather surface), an embossing in further processing (gold embossing, blind embossing) is possible; on the other hand, it must be resistant and stable so that a use of more than 10 years is possible. In addition, the coloring of the cover material should also be stable and have high lightfastness.

- The coating shall be printable (printing of UV elements or colors).
- The paper/cardboard base material must have good bonding (bonding with chip inlay or endpapers) in the manufacturing process.

The following security elements can be integrated with the cover material:

- Standard:
  - Surface texture, UV printing, foil stamping, blind embossing
- Advanced elements:
  - UV printing elements with different fluorescent colors when switching between UV-A, UV-B and UV-C light (bi- and tri-fluorescent colors).

Minimum standards for cover material:

- High durability (>10y), heat resistant, printable, able for embossing, good workability for bonding processes, good color fastness

b) Chip Inlay

- The chip and the antenna structure must be able to be embedded in a stable and fixed manner and must not slip or be damaged during processing.
- If the chip is placed in the cover, the material of the chip inlay must bond well with the cover material and the paper of the attachment so that it is not possible to manipulate or remove the chip without destroying it.

Minimum standards for chip inlay:

- Embedded chip and antenna, good workability for bonding processes

c) High-Security Paper [Substrate End Page, Substrate Data Page, Substrate Visa pages]

- The composition of the paper may consist of a mixture of cellulose fibers and cotton fibers and/or admixed synthetic fibers.
- The paper must not exhibit UV fluorescence (UV dull).
- The paper may have a watermark (ideally a multitone cylinder mould watermarks, pixel watermarks, highlight watermarks, or electrotype watermark; Multitone watermarks can be combined with pixel and highlight watermark variants that make them difficult for forgers to copy or counterfeiting).
- If paper fibers are integrated, the paper fibers can show a specific color both in incident light and under UV light or in combination. Special coloring fibers can also be multicolored (rainbow fibers) or change color under different UV wavelengths (bi- or tri-fluorescent fibers).
- To indicate manipulation attempts with chemical substances, a chemical safeguard (pigments) should be present in the paper, which causes a color reaction upon contact with special substances/chemicals (including polar and apolar solvents, acids, bases, bleaching).
- A security thread (made of plastic, metal, or paper) may be embedded in the paper structure. These security threads can contain various elements (diffractive effects, UV fluorescence, microtext, etc.). By using window structures in the paper, these elements can be made even more visible or embedded into the design.
- The paper can also be coated with special inks to create special effects.
- Planchettes can also be embedded into the paper.

The following security elements may be integrated in the paper:

- Standard:
  - Watermarking, fibers (visible under VIS and/or UV light), pigments for chemical sensitivity/ pigments for chemical protection
- Advanced elements:
  - Special security fibers (UV-reactive fibers with different fluorescent colors when alternating between UV-A, UV-B and UV-C light (bi- and tri-fluorescent colors), Rainbow fibers), security thread (with or without window cutouts), surface coatings, planchettes, plastic core film (special paper).

Minimum standards high security paper (passport booklet):

- No UV fluorescence (UV dull), watermark (e.g., multitone watermark), security fibers (UV- and/or VIS-active fibers), chemical reactive pigments (chemical sensitivity) (**Figure 24: Swedish Passport**)

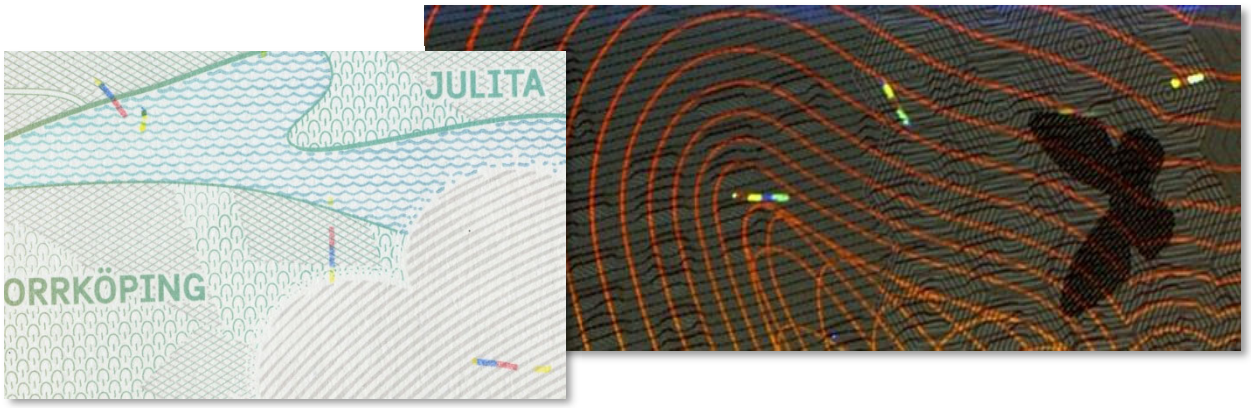


Figure 24: Candy cane fibers in visible and UV

d) Synthetic Substrates (Passport Data Pages & ID Cards) [Polycarbonate]

Polycarbonate (PC) is the preferred substrate for synthetic passport data pages and secure identity credentials due to its structural and security properties. When laminated at approximately 180°C, all layers fuse into a single, inseparable monoblock unit — eliminating adhesive interfaces that could be exploited for delamination. This high lamination temperature also functions as an inherent manufacturing barrier, as counterfeiters typically rely on adhesive bonding and cannot replicate the authentic construction process. The material exhibits no UV fluorescence and maintains physical and chemical stability for over 10 years under routine handling conditions.

Polycarbonate is uniquely compatible with laser engraving personalization, which penetrates deep into the card body and cannot be removed without causing irreversible visible damage — making it the most permanent available personalization method. Any attempt to alter data or portrait imagery will visibly damage intersecting security features such as DOVIDs and tactile elements, providing immediate tamper evidence. The substrate also supports the full range of security printing techniques, including UV/IR inks, guilloches, microtext, window elements, MLI/CLI, color-shifting inks, anti-Stokes elements, and tactile surface structures, all integrated cohesively across document layers.

Minimum standards for synthetic substrates (for passport data pages and ID cards):

- No UV fluorescence (UV dull), high durability (>10y), heat resistant, printable, receptable for embossing, uniform structure (monoblock) after lamination process to ensure a high stable and forgery-proof product

e) Composites of Paper and Polymer

- Composite of security paper and polymer material (physiochemical compound)
- Security paper is cotton based with integrated features, e.g. with watermarks, security fibres, security threads, foils
- The polymer core can be used to generate (semi-) transparent windows in any position on the document
- Also, polymer coated paper can be a secure substrate providing range for a complex mixture of features.

f) Processing a Polycarbonate Data Page in the Booklet

The polycarbonate data pages must allow for additional processing steps, especially regarding the process of sewing the data page in and the die-cutting process of the booklets. The following security elements can be integrated in a polycarbonate data page:

Standard:

- UV printing elements with different fluorescent colors when viewed with UV-A light, IR printing elements with different IR appearance when viewed with IR light, security printing (guilloches, microtext, artscreen elements), raised surface structures such as, tactile elements, line art or microtext, special effect inks (including color shifting ink).

Advanced elements:

- UV printing elements with different fluorescent colors when switching between UV-A, UV-B and UV-C light (bi- and tri-fluorescent colors), thermochromic inks, anti-Stokes elements, DOVID elements , window elements, (Multiple areas, complex shape, asymmetrical window, Combined with color shifting inks), MLI or CLI elements, surface laminated optical features), ICI elements, transmitted light elements, different surface textures (raised, recessed, matte).
- Layer of secured optically variable polycarbonate with visible color shift into transparent areas and UV fluorescence visible on the edge of the datapage under UV light.

Minimum standards polycarbonate data pages (for passport booklet):

- High durability (>10y), uniform structure (monoblock), standard security features (UV color printing, IR color printing and special printing elements e.g., guilloches, microtext, art screen elements), surface structure, ideally protecting personalized data and the reverse side of the portrait area, using special effect colors (e.g., optically variable inks)

g) Laminates [Plastic Films]

The laminate shall be tolerant regarding further processing and a long shelf life (>10 years). The laminates for hot lamination must be able to withstand the corresponding temperatures during application and the applied safety elements must not be damaged or impaired during the lamination.

The adhesive for bonding the laminates to the paper must be selected in such a way that it does not interfere with the security elements in the paper (including chemical protection) and enables the best possible bonding between the laminate film and the paper (protection against splitting laminate film/paper). The following security elements can be integrated into the laminate:

Standard:

- DOVID elements, UV printing

Advanced elements:

- UV printing elements with different fluorescent colors when switching between UV-A, UV-B and UV-C light (bi- and tri-fluorescent colors), thermochromic inks, anti-Stokes elements, special effect inks (such as color shifting inks).

Minimum standards laminates (for passport booklet):

- High durability (>10y), heat resistant, printable (for applying security features), standard security features (using special effect colors (e.g., UV color printing, optically variable inks)

h) Diffractive Optically Variable Image Devices (DOVID)

Diffractive optically variable elements must be applied well and stably to the corresponding products. For this purpose, the choice of adhesives (adhesive layer) must be made in such a way that the best possible bonding is achieved for the substrate.

DOVIDs are primarily a high security level 1 (overt) feature, displaying complex optical technologies yet easy to observe and authenticate. Nevertheless, DOVIDs can also address security levels 2 (covert) and 3 (forensic).

Their diffractive effects such as movement, image flips, transformations, color permutation or virtual 3D effects should be individually defined. Special care should be taken during the selection of diffractive effects and technologies as well as their integration. Diffractive effects include movement, image or color flips, transformations or virtual 3D effects and may be achieved with different technologies. The effects should be individually defined and suitably harmonized with the DOVID's design motifs (e.g. a coat of arms, a national symbol).

More importantly than design motifs, however, is the consideration of the capabilities of counterfeit DOVIDs in order to maximize security. A DOVID with many colorful movements and transformations, for example, might be easier to counterfeit and lead to highly deceptive counterfeits even if it contains few high-security effects. DOVIDs designed with the focus on security, employ different technologies and effects, but with placement, integration and area/prominence carefully considered for each effect (**Figure 25: Canadian Passport**).

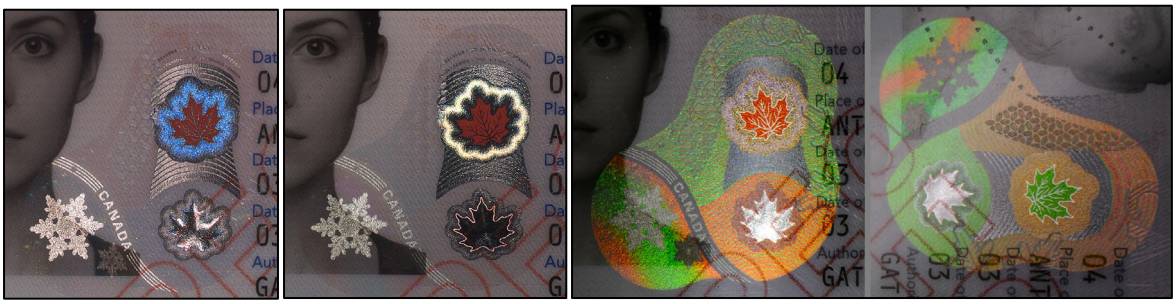


Figure 25: The DOVID of the Canadian passport at different viewing angles, rotations and illumination conditions revealing the different DOVID effects/features and technologies used.

As mentioned in the b) Integration of Document Components chapter, combination of such optical features within the DOVID design and the overall design of the document enhances its security level by facilitating its authentication.

In addition to their diffractive effects, the elements themselves can also have additional characteristics:

- Metallized elements
- UV printed elements
- IR printed elements
- Microtext and nanotext elements
- Anti-Stokes elements

Minimum standards for DOVID elements:

- High durability (>10y), inherently counterfeit resistant, integrated with other security features and design, and easy to authenticate

i) Visa/Vignettes for Passport Booklets

High security paper [cotton fibers, pulp, synthetic fibers; adhesives].

- The paper must not exhibit UV fluorescence (UV dull).
- The composition of the paper must be defined and may consist of a mixture of cellulose fibers and cotton fibers and/or admixed plastic fibers.
- Fibers (colored security fibers of paper or plastic) may be mixed with the paper fibers. These fibers can have a specific color both in incident light, under UV light or combined. Special coloring fibers can also be multicolored (rainbow fibers) or change color under different UV wavelengths (bi- or tri-fluorescent fibers).
- To indicate manipulation attempts with chemical substances, there should be a chemical safeguard (e.g. pigments) in the paper that causes a color reaction when in contact with special substances/chemicals.
- The adhesive and the adhesive application shall be selected in such a way that it ensures good bonding in use but does not lead to adhesive leakage or deactivation of the adhesive in processing (e.g., when exposed to high temperature (hot stamping) or high pressure (intaglio printing). The adhesive in the raw material should not lead to interference with safety elements (among others with the chemical protection). The adhesive should have an appropriate durability so that the bonding is given for the duration of the use of the product.

- The backing material selected must be well suited for the intended use and easily removed during application.
- Fracture cuts might be applied to prevent the unlawful removal and re-use of the sticker.

Minimum standards high security paper (visa):

- No UV fluorescence (UV dull), security fibers (UV- and/or VIS-active fibers), chemical reactive pigments (chemical sensitivity), stable and forgery-proof bonding after sticking in passports

j) Security Printing Techniques

- Offset printing — wet offset and dry offset. In dry offset, water sensitive inks can be used. These can be used as a security element (water sensitive element). Dry offset method can be used for polymer printing and paper. The digital offset color technique is excepted.
- Intaglio printing — this technique is preferred to print tactile elements and special color effects (e.g., color shifting inks).
- Screen printing — this technique is preferred to print special color effects elements (e.g., color shifting inks).
- Letterpress printing for numbering — numbering is used to create unique numbers on documents. The number on the printed sheet has a squeezed edge effect typical of letterpress printing.
- Copy protection
  - Microtext/micro letter printing[13]
  - Artscreen printing
  - Fine guilloche printing
  - Optically variable inks
  - UV-fluorescence inks
  - Anti-Stokes inks
- Numbering
  - Personalization (decentralized vs. centralized/issuing technique)

k) Advanced Security Features

- Level 1
  - Guilloche printing
  - Microperforated variable data
  - Color shifting ink / material
  - Security fibers (VIS visible)
  - DOVID element
  - Tactile surface element
  - Surface optical feature (ROVID element)
  - Complex window(s)
- Level 2
  - UV printing
  - IR printing
  - Security fibers (UV reactive)
  - Microtext
  - Artscreen element
- Level 3
  - Anti-Stokes properties
  - Nano features
  - UV bi- and tri-fluorescent ink

[13] Usage of fonts optimized for microtext usage is highly recommended. Microtext fonts support rich details, which help to identify manipulations.

8. SUMMARY: DOCUMENT SECURITY CHECKLIST

a) Cover Material (Polyacrylate Coating)

- ☐ Coating must be flexible and heat-resistant to allow structural insertion (grain/leather surface texture).
- ☐ Coating must support embossing in further processing (gold embossing, blind embossing).
- ☐ Coating must be resistant and stable for a use life exceeding 10 years and matched with a corresponding high quality and durable stamping foil .
- ☐ Coloring must be stable with high lightfastness.
- ☐ Coating shall be printable (UV elements and colors).
- ☐ Paper/cardboard base must have good bonding capability (with chip inlay and endpapers).
- ☐ Must support surface texture, UV printing, foil stamping, and blind embossing (standard security elements).
- ☐ Must support UV printing with bi- and tri-fluorescent colors (UV-A, UV-B, UV-C) as advanced security elements.

b) Chip Inlay

- ☐ Chip and antenna structure must be embedded stably and fixedly — no slipping or damage during processing.
- ☐ Chip inlay material must bond well with cover material and paper attachment.
- ☐ Chip must not be removable or manipulable without destroying it.
- ☐ Must support embedded chip and antenna with good workability for bonding processes.

c) High-Security Paper (Substrate End Page, Data Page, Visa Pages)

- ☐ Paper composition may consist of cellulose, cotton, and/or synthetic fibers.
- ☐ Paper must exhibit no UV fluorescence (UV dull).
- ☐ Paper should include a watermark — ideally multitone cylinder mould, pixel, highlight, or electrotype watermark.
- ☐ Security fibers, if integrated, must show specific colors in incident light and/or under UV light (including rainbow/multicolor fibers and bi- or tri-fluorescent fibers).
- ☐ Paper must include chemical safeguard pigments that produce a color reaction upon contact with polar/apolar solvents, acids, bases, and bleaching agents.
- ☐ A security thread (plastic, metal, or paper) may be embedded, optionally featuring diffractive effects, UV fluorescence, microtext, and/or text.
- ☐ Window structures may be used to enhance visibility of security thread elements.
- ☐ Paper may be coated with special inks for special effects.
- ☐ Planchettes may be embedded in the paper.

d) Synthetic Substrates — Data Page (Polycarbonate)

- ☐ Plastic printing stock must ensure good printability.
- ☐ Must be suitable for lamination processes.
- ☐ Must exhibit high stability with a shelf life exceeding 10 years.
- ☐ Must be compatible with standard security printing techniques.
- ☐ Must be compatible with embedding of DOVIDs and other security features.
- ☐ Plastic must not exhibit UV fluorescence (UV dull).

- Composite must be uniform and form a monoblock (e.g., 100% PC) after lamination — no weak points or splitting.

e) Composites of Paper and Polymer

- Must be a physiochemical compound of security paper and polymer material.
- Security paper must be cotton-based with integrated features (watermarks, security fibers, threads, foils).
- Polymer core must be capable of generating (semi-)transparent windows at any position on the document.
- Polymer-coated paper must support a complex mixture of security features.

f) Polycarbonate Data Page Processing (in Booklet)

- Must allow for a sewing process to integrate the data page with the booklet.
- Must allow a die-cutting process for the booklet.
- Must support standard security elements: UV printing (UV-A fluorescent colors), IR printing, guilloche, artscreen, tactile elements, line art, microtext, and special effect inks (including color shifting ink).
- Must support advanced elements: bi/tri-fluorescent UV inks, thermochromic inks, anti-Stokes elements, DOVIDs, window elements (multiple, complex, asymmetrical, combined with color shifting inks), MLI/CLI elements, surface laminated optical features, ICI elements, transmitted light elements, and varied surface textures.
- Optically variable polycarbonate layer must display visible color shift into transparent areas and UV fluorescence visible on edge under UV light.

g) Laminates (Plastic Film

- Must tolerate further processing and maintain integrity for a shelf life exceeding 10 years.
- Hot lamination laminates must withstand corresponding temperatures without damaging applied security elements.
- Adhesive must not interfere with security elements in the paper (including chemical protection).
- Adhesive must ensure strong bonding between laminate film and paper (protection against splitting).
- Must support standard security elements: DOVID elements, UV printing.
- Must support advanced elements: bi/tri-fluorescent UV inks, thermochromic inks, anti-Stokes elements, color shifting inks.

h) DOVIDs (Diffractive Optically Variable Image Device)

- Must be highly durable (>10 years) and easy to authenticate.
- Must be applied stably and securely to corresponding products.
- Adhesive layer must achieve best possible bonding to the substrate.
- Must function as a high security Level 1 (overt) feature — complex yet easy to observe and authenticate.
- May also address security Level 2 (covert) and Level 3 (forensic).
- Diffractive effects (movement, image flips, transformations, color permutation, virtual 3D) must be individually defined.
- Effects must be harmonized with design motifs (e.g., coat of arms, national symbols).

- Security focus must take precedence over visual complexity — design must maximize resistance to counterfeiting.
- Must be integrated with the overall document design to enhance authentication.
- May incorporate additional characteristics: metallized, UV printed, IR printed, microtext/nanotext, and anti-Stokes elements.

i) Visa/Vignettes for Passport Booklet

- Paper must exhibit no UV fluorescence (UV dull).
- Paper composition must be defined — may consist of cellulose, cotton, and/or synthetic fibers.
- Security fibers may be mixed in, showing specific colors in incident/UV light, including rainbow and bi-/tri-fluorescent fibers.
- Must include chemical safeguard pigments causing a color reaction upon contact with chemical substances.
- Adhesive must ensure good bonding in use without leakage or deactivation under high temperature (hot stamping) or high pressure (intaglio printing).
- Adhesive must not interfere with chemical protection or other security elements.
- Adhesive must maintain bonding for the full duration of product use.
- Backing material must be well suited for intended use and easily removed during application.
- Fracture cuts may be applied to prevent unlawful removal and reuse of the sticker.

j) Security Printing Techniques

- Offset printing (wet and dry) must be supported; dry offset shall allow use of water-sensitive inks as a security element; digital offset color technique is excluded.
- Intaglio printing must be supported for tactile elements and special color effects (e.g., color shifting inks).
- Screen printing must be supported for special color effect elements.
- Letterpress printing must be used for numbering, producing unique numbers with squeezed edge effect.
- Copy protection features must include: microtext, artscreen, fine guilloche, optically variable inks, UV-fluorescent inks, and anti-Stokes inks.
- Numbering must support personalization (decentralized and centralized/issuing techniques).

k) Advanced Security Features by Authentication Level

Level 1 (Overt):

- Guilloche printing
- Microperforated variable data
- Color shifting ink/material
- Visible (VIS) security fibers
- DOVID element
- Tactile surface element
- Surface optical feature (ROVID element)
- Complex window(s)

Level 2 (Covert):

- UV printing
- IR printing
- UV-reactive security fibers
- Microtext
- Artscreen element

Level 3 (Forensic):

- Anti-Stokes properties
- Nano features
- UV bi- and tri-fluorescent ink

9. ANNEX

The following are technical references related to the construct of secure identity documents — The Best Practice Guidelines and Minimum-Security Standards for Identity Documents draws key elements from these references:

1. ICAO 9303 — https://www.icao.int/publications/doc-series/doc-9303
   International standard that defines specifications for machine-readable travel documents (MRTDs), such as passports, visas, and ID cards.
2. ISO/IEC 7810 — https://www.iso.org/standard/70483.html
   This document specifies the physical characteristics of identification cards including card materials, construction, characteristics and dimensions for four sizes of cards.
3. ISO/IEC 18013 (Driver's License Standards) — https://www.iso.org/standard/63798.html
   This document prescribes requirements for an ISO-compliant driving license (IDL).
4. EU COUNCIL REGULATION 2025/1208 — https://eur-lex.europa.eu/eli/reg/2025/1208/oj/eng
   Regulation to strengthen security for E.U. citizens' identity cards and residence documents to combat forgery.
5. EU COUNCIL REGULATION 2252/2004 — https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=celex:32004R2252
   Sets mandatory security standards for passports and travel documents issued by E.U. Member States
6. EU PRADO Glossary — https://www.consilium.europa.eu/prado/en/prado-glossary.html
   Technical terms related to security features and to security documents in general

10. WHO WE ARE

a) Document Security Alliance (DSA)

The Document Security Alliance (DSA) is a nonprofit association created by government agencies, private industry, and academia with the goal of identifying methods to improve security documents and related procedures to help combat the growing acts of fraud, terrorism, illegal immigration, identity theft, and other criminal acts. The organization brings together collaborative expertise from over 125 government, industry, and academic organizations, representing more than 400 individual members dedicated to improving the security and authentication of critical value documents.

DSA is committed to identifying threats to legitimately issued documents and their production and issuance processes, as well as identifying technologies that would help secure those processes and educating partners on document security issues. DSA provides valuable insights into the vulnerabilities of identity documents such as driver's licenses, passports, and immigration documents, informing both government and private sector policies and helping to set higher security standards.

DSA operates around three core pillars — Secure, Enforce, and Educate — to address the full lifecycle of document security challenges. DSA is active in public outreach. Its public safety Identity Security Campaign, known as #NoFakeIDs, supports the security and education components of the DSA's mission, with materials including posters, fliers, and social media deployed in airports, universities, law enforcement training, and local communities. DSA also serves as a resource for governments seeking to build their understanding of existing solutions and provides support on issues ranging from counterfeiting to the security of travel and identity documents.

b) INTERGRAF

Intergraf is a trade association promoting and protecting the interests of the graphic industry at the European level, representing 22 member federations from 21 countries. The organization was officially founded in 1930 in Berlin as the International Bureau of the Federations of Master Printers, before being moved to London in 1946 and ultimately relocated to Brussels in 1984, when it was transformed into Intergraf. Today, Intergraf advocates for Europe's printing industry toward the European Union, working with E.U. policymakers to support the sector's competitiveness through advocacy, information sharing, networking, campaigning, social dialogue, and E.U. projects.

The printing industry that Intergraf represents is a significant economic force, with printing companies employing more than 550,000 people across Europe in creative, digital, and technical jobs, spread across more than 100,000 European printing companies. Intergraf The scope of the industry is broad, encompassing everything from books, newspapers, and magazines to food packaging, medicine labels, voting ballots, and identity documents. As part of its mission, Intergraf also provides targeted services to the global security printing community, helping solution providers and institutional end users respond to the challenges they face in an increasingly competitive environment.

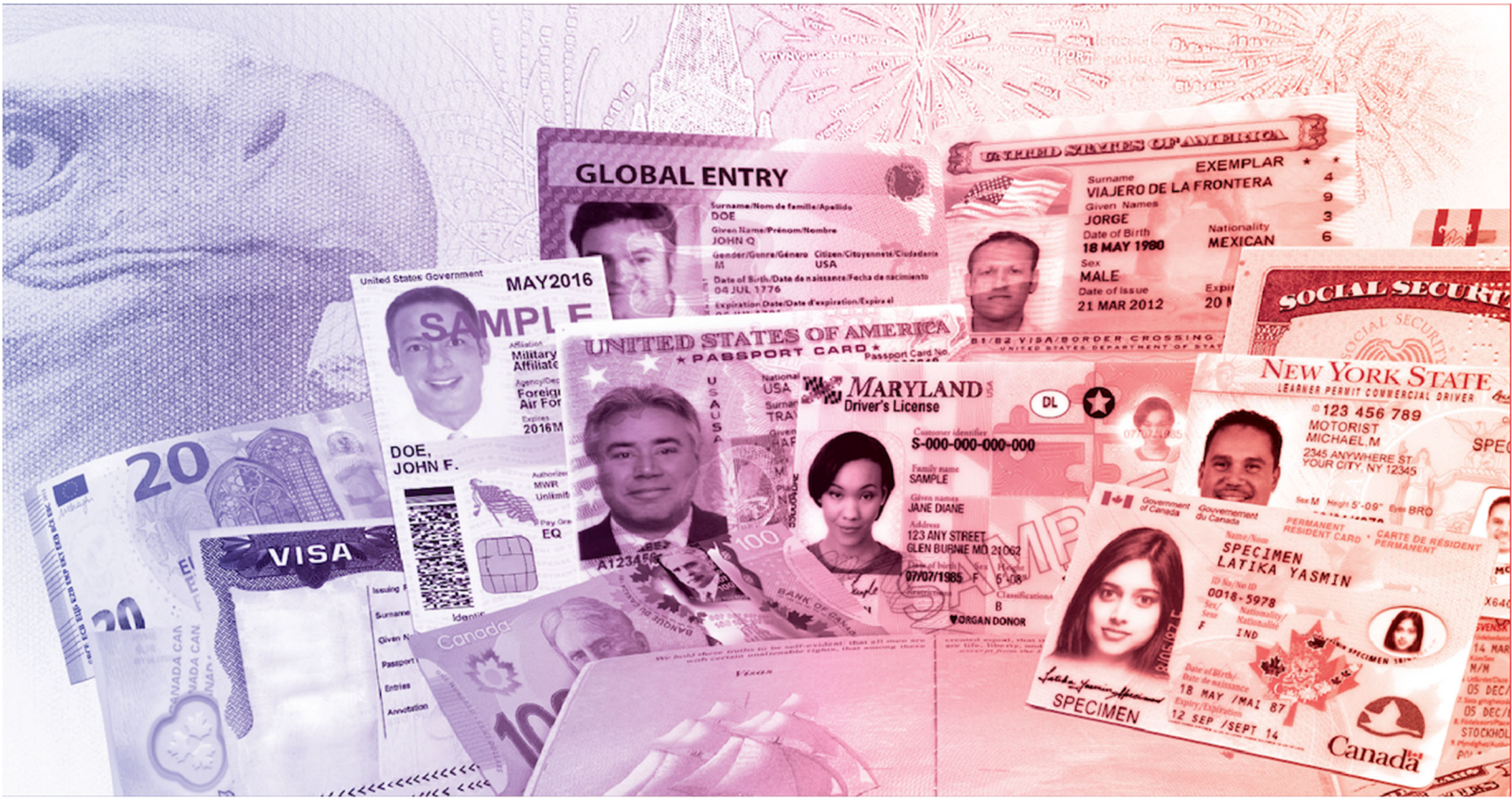
A particularly notable area of Intergraf's work is its role in security printing standards and certification. At the heart of this work are two complementary certification schemes: ISO 14298, which applies to security printers and hologram manufacturers and establishes requirements for managing security printing operations, and Intergraf 15374, which is designed for suppliers to the security printing industry to ensure those providing materials, components, machinery, or software also maintain rigorous controls to safeguard supply chain integrity. Intergraf is also a founding member of the World Print & Communication Forum (WPCF) and administers the WPCF Secretariat in Brussels, serving as a collaborative platform for the world's major printing associations to promote the development and prosperity of the global printing industry

c) Secure Identity Alliance (SIA)

The Secure Identity Alliance (SIA) is an expert and globally recognized not-for-profit organization that brings together public, private, and non-government organizations to foster international collaboration, help shape policy, provide technical guidance, and share best practice in the implementation of identity programs. SIA's mission is to unify the ecosystem of identity and unlock the full power of identity so that people, the economy, and society thrive, with the association supporting its members' activities across four broad pillars: Identity for Good, Outreach, Open Standards Development, and Industry Services and Solutions. The organization aligns its work with major international frameworks, including the UN's 2030 Agenda for Sustainable Development, the Charter of Fundamental Rights of the European Union, and the OECD Recommendation on the Governance of Digital Identity.

SIA is dedicated to supporting sustainable worldwide economic growth and prosperity through the development of trusted digital identities and the widespread adoption of secure, offering support and expertise to allow government agencies and other public bodies to implement their digital ID projects and realize the wide range of economic, public health, electoral, and sustainability opportunities offered by the shift to digital service provision. The Alliance's members' technologies cover over 85% of the world's population through multiple applications, and the organization firmly believes that strict adherence to high ethical standards is key to meeting the challenges and reaching the full potential of digital identities and secure eServices, to the benefit of all stakeholders.

A central pillar of SIA's technical work is its Open Standard Identity APIs initiative, known as OSIA. OSIA is a set of interfaces (APIs) that enables seamless connectivity between all building blocks of the identity management ecosystem, independent of technology, solution architecture, or vendor, and has been recognized as an official International Telecommunications Union (ITU) standard. SIA's workgroup programs offer expert advice and pragmatic guidance on designing, manufacturing, issuing, and verifying convenient and cost-effective secure documents, supporting the provision of legal trusted identity for all, and driving the development of inclusive digital identity services necessary for sustainable worldwide economic growth and prosperity.



FOR MORE INFORMATION:

DSA
ENHANCING DOCUMENT AND IDENTITY SECURITY

https://documentsecurityalliance.org/

Contact: secretariat@documentsecurityalliance.org

SECURE IDENTITY ALLIANCE

https://secureidentityalliance.org/

Contact: https://secureidentityalliance.org/contact/

INTERGRAF

https://www.intergraf.eu/

Contact: intergrafconference@intergraf.eu