SECURE IDENTITY ALLIANCE

Passport Fraud Trends and Ways to Combat Them

Public Version
2021

Mentions

Secure Identity Alliance (SIA)
www.secureidentityalliance.org

Design
Design Motive Ltd

Photo credits
Shutterstock

Editorial review
Slingshot Communications

We would like to thank the many contributors to this paper. Without their valued inputs, it would not have been possible to create such a detailed analysis of today's secure documents, the threats they face, and the security features in place to mitigate risk.

Production
This report has been produced by the Document Security Working Group of the SIA:

Joachim Caillosse (Chair and Lead Author)
IN Groupe

Christophe Duriez, Aimane Ait El Madani and Thomas Poreaux
IDEMIA

Françoise Daniel and Philippe Jung
IN Groupe

Renaud Laffont-Leenhardt and Petri Viljanen
Thales

Michael Ruhland-Bauer and Tobias Rosati
Veridos

Christophe Halopé and Cosimo Prete
CST

Claudia Schwendimann and Andreas Zechmann
OSD

Frank Smith
SIA Observer (and former Deputy Director UK Home Office)

Patrick Butor
Independent Consultant (Former Head of French MoI security standardization & ICAO TAG TRIP Delegate)

Thank you
Our thanks also go out to France's National Document and Identity Fraud Office, and Interpol's Counterfeit Currency & Security Documents (CCSD) Branch for their thorough review of the report.

SECURE IDENTITY ALLIANCE

Contents

1.
Assuring the integrity of today's secure documents

With the integrity of today's secure documents under threat from increasingly sophisticated counterfeiters and fraudsters, the need to continually evolve and embed new security features is paramount. This is particularly critical for the passport and, as we see in this paper, considerable work is being done.

Authored by the eDocuments Working Group, the Secure Identity Alliance's (SIA) cross-industry task force responsible for guiding the design, manufacturing, issuance and verification of secure documents, the report provides an overall analysis of the document fraud landscape alongside useful guidelines and recommendations on how to strengthen a passport against attack.

The aim of this document is not to show real examples of fraud; authorized organizations already have access to such examples through restricted channels.

It is constructive to discuss the general principles of document security and a few selected examples publicly. However, in the interests of maximising security, the public version of this document avoids discussing detailed examples especially of most advanced techniques, which might be of greatest interest to forgers and counterfeiters.

The restricted, more explicit, version of this guide is limited to law enforcement agencies and authorities. It is accessible on the web page of the INTERPOL Travel and ID Documents Reference Centre, access to which is governed by strict rules and regulations. If you work for police, border control agency, immigration or other relevant governmental authority, please contact INTERPOL's Counterfeit Currency and Security Documents Branch for more details: CCSD@interpol.int

2. Introduction

Document fraud, specifically the counterfeiting and forgery of travel documents such as passports, represents a significant threat to everything from personal identity to national security. Crucially, it is also part of a much bigger picture. Europol's 2017 SOCTA Report draws a clear link between document fraud and international crime, and the European Multidisciplinary Platform Against Criminal Threats (EMPACT) cites the issue as one of its strategic priorities.

Document fraud is also a growing challenge leading some commentators to decry a growing passport fraud "epidemic"[1]. In 2020, nearly 100 million travel documents were reported lost or stolen[2] – suggesting the black market in stolen ID documents remains in a healthy state.

The consequences of illegally modified or reproduced travel documents are many and varied. From reputational damage to the issuing country and document manufacturer, to the numerous onward possibilities such as financial crime, drug trafficking, and terrorism, the creation and use of false travel papers can have an impact that goes far beyond personal inconvenience.

That said, personal identity theft remains a serious issue, and one which can have major consequences for those affected. Issuing authorities have a responsibility to protect individual citizens, as well as their national borders.

More positively, issuing authorities now have access to a greater arsenal of deterrents and countermeasures than they ever have before. Today, passports can be equipped with a range of security features that would have been all but impossible to employ just a few decades ago. From biometric chips to physical security features, continual innovation in document components has created a plethora of ways to prevent or highlight illicit modification.

Good document security design today relies on a mix of various expertise. Moreover, it relies on a spirit of unity and collaboration between the following:

- Document fraud and examination experts such as law enforcement bodies.
- Secure document design and manufacturing experts such as the SIA.
- Issuing authorities, who may or not have in-house expertise, and are accountable for both the creation and issuance of secure documents.

The practical reality, of course, is that many countries have limited resources with which to detect, analyze, and counter document fraud. As a result, there is a strong need for support.

As a not-for-profit global identity and secure digital services advisory body, the sharing of best practice guidance and advice is one of the fundamental roles performed by the Secure Identity Alliance (SIA).

We and our members are deeply invested in helping governments and issuing bodies tackle the ongoing threat of document fraud however we can, and our Document Security Working Group was created specifically to provide recommendations and guidelines for the overall design of secure documents.

This report is an example of our continuing commitment to the execution of best practice around document security. In it, you'll find deep analysis of the latest trends influencing both the prevention and detection of passport fraud. We seek to highlight the ever-present need to balance usability with security, and the growing number of ways that issuers can strive to stay one step ahead of the latest threats.

The information presented in this report has been collected and validated in collaboration with document examination experts from various organizations across the world. Typically, we have worked with national document fraud units including France's National Document and Identity Fraud Office, Central directorate of border police, and Interpol's Counterfeit Currency & Security Documents (CCSD) Branch.

We hope you find it useful.

[1] EU's passport fraud 'epidemic' – Politico, 28th January 2016

[2] https://www.interpol.int/How-we-work/Databases/Stolen-and-Lost-Travel-Documents-database

3. Passport booklets and fraud: an overview

3.1
Defining the passport

The primary purpose of a passport is as a travel document, granting the bearer the right to cross geographic borders. The strict controls around issuance have also given passports a secondary life as an identity document, however, giving holders the ability to do everything from open a bank account to vote. In some countries, for instance, the passport actually takes the place of a national identity card.

While they are governed by a range of restrictions and requirements for use, passports today are also designed to be convenient and interoperable between different authorities. This is made possible thanks to the standards and recommendations outlined by the International Civil Aviation Organization (ICAO) in its well-known Doc 9303, and other guideline documentation. In this documentation, the ICAO also defines "basic" (i.e. mandatory) and "additional" (i.e. optional) security features for passports.

Those security features now need to defend against threats both physical and digital. Preventing someone from modifying a portrait photograph remains important, but so too is the ability to ensure that an embedded microchip cannot be altered or counterfeited. And these dangers are not limited to passports alone – other types of travel documentation such as Laissez-Passer issued paperwork are subject to similar risks.

Naturally, these defensive measures must also be delivered with one eye on the cost of production. Typically, these secure and convenient travel documents must also be cost-effective, ensuring the need for a smart selection of economically attractive technical features.

Design continues to play a key role. A strong visual identity, one that enhances the country and its culture through its sovereign symbols, is a key element of the modern passport. So too does durability; a given for a document that must remain active and secure for up to 10 years of normal use.

3.2
How passport booklets are made

Thanks to ICAO Doc 9303, passports today are standardized documents with universal commonality across their basic characteristics. Most blank passports are manufactured and then personalized using similar techniques, mastered by world-class public or private companies.

3.3
The main components of a typical passport booklet

Passports now follow a broadly uniform design that includes the following key elements:

- **Cover** (front and back)
  These provide the first level of identification of the document. The cover may include an embedded electronic inlay (containing an antenna and a contactless secure chip).
- **Inner cover** (front and back)
  Also referred to as the "end-pages", with a secure printed background and numbering.
- **Data page**
  Usually positioned on the first inner page, though some passports still use the inside of the front cover for the data page (though this approach is strongly discouraged by both the ICAO and the majority of document examination experts[1]). The data page can be:
  - » Paper-based – always with a protective film/layer, usually holographic.
  - » Synthetic – made predominantly from polycarbonate. This can be electronic or not, a choice made by the issuing authority.
- **Inner pages**
  Intended for observations and visas, these pages are made of security paper and run between eight and 64 pages in total.

A passport also has other key manufacturing features, all closely linked to security:

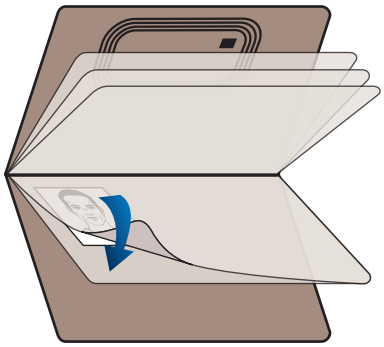
- A hinge connecting a polycarbonate data page with the rest of the booklet. This key component can also hold security features.
- UV fluorescent sewing thread, applied using a specific method, to bind the components of the booklet together.
- Numbering method(s) so that each booklet has its own unique document number (typically, letterpress printing combined with laser perforation).
- Graphical personalization techniques that contain the holder's data. These are found on the data page but sometimes on other pages too (an additional portrait image immediately after the data page, for instance).
- Laminate coating - typically a thin security film - used to protect the personalized information on a data page. This is used predominantly for paper-based data pages.
- Electronic personalization of the contactless chip, including the embedding of security mechanisms. These are explained in greater depth later in this report.

The position of the electronic component (antenna and chip) in a passport is ultimately left to the issuing authorities. Various technical solutions are available, and manufacturers of passport reading devices have adapted their products to cater to these configurations.

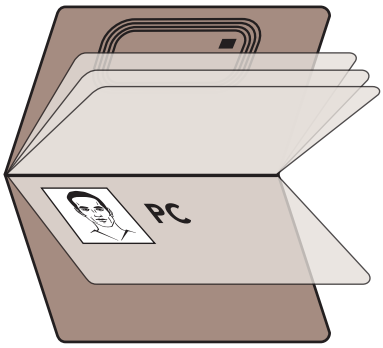
[1] The cover of a passport can be relatively easy to delaminate, helping forgers to disguise an attack on a data page.

3.4
Common passport booklet layouts

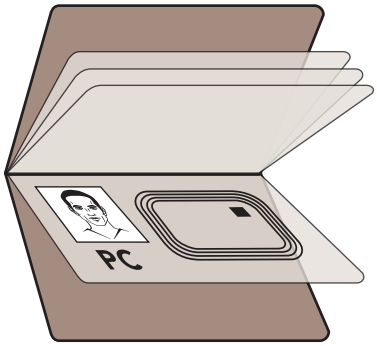
Today, passports tend to follow one of three layouts



1. Passports with a laminated paper data page, and electronics in the back cover



2. Passports with a polycarbonate data page and electronics in the back (or front) cover



3. Passports with an electronic polycarbonate data page

Some rare exceptions can be found, such as passports with the chip embedded in the middle of the booklet, for example.

3.5
Key entities in the manufacturing process

The bodies involved in passport manufacturer can generally be split into three camps. Some companies may be involved in all three of these areas at the same time by virtue of a diverse business focus or via subsidiaries.

i. **Public and private manufacturers of secure blank documents**
Responsible for the printing and stitching of a blank passport once all of the security components have been assembled. These businesses are the primary suppliers to sovereign states.

ii. **Security component manufacturers**
Security components include secure papers, polycarbonate pages, holograms, inks, sewing threads, electronic components, and more. Businesses operating in this field play a major role in furthering the security of a passport.

iii. **Personalization machine manufacturers**
Personalization machines include inkjet printers, thermal-transfer printers, laser toners, laser engraving devices, UV printing facilities, laminate fixings, and more. Providers here aid in the process of linking a blank passport to its holder.

3.6
Fraud: types, techniques, and objectives

When physical and electronic attacks are made on passports, fraud is almost certainly the final objective. Whether attempting to use someone else's identity or create a new, fake one, passport fraud is always orchestrated in pursuit of illegal activities.

Europol's 2017 SOCTA report[2] identifies eight priority crime threats as listed below. Document fraud is one of three "cross-cutting crime threats" that SOCTA says "enable or enhance all types of serious and organized crime".

- Cybercrime
- Drug production, trafficking, and distribution
- Migrant smuggling
- Organized property crime
- Trafficking in human beings
- Criminal finances and money laundering
- Document fraud
- Online trade in illicit goods and services

The latest SOCTA Report, published in April 2021 only serves to reconfirm this reality: "Document fraud is an enabler for most criminal activities… It's prevalence is partly due to the fact that it does not necessarily require sophisticated tools or excessive monetary investment."

> *Europol recommends focussing on three cross cutting crime threats with a significant impact across the spectrum of serious and organized crime – document fraud, money laundering and the online trade in illicit goods and services.*
>
> **Quoted from SOCTA report 2017**

The specific motive behind document fraud varies from incident to incident, of course. From "simple" financial crime, such as the opening of a false bank account, through to bigger threats like terrorism, fake and genuine documents alike can be used to support a wide range of illegal activities. The ubiquity of passport documentation ensures that everyone – from citizens to private and public organizations – are at risk from such activities.

There are four primary techniques used in passport fraud:

1. Counterfeiting

Counterfeiting is the unauthorized reproduction of a genuine document. Substitute materials and/or printing methods are used for either part or the whole of the booklet.

2. Forgery

Forgery involves the falsification or modification of a genuine document, fraudulently altering it to provide misleading information about the bearer or the validity of the passport. This threat applies to security features and holder data such as the bearer's portrait. Some forged documents are constructed using materials from legitimate ones[3].

Stolen blank documents that are then illegally personalized also fall into this category. These documents are genuine items that are then modified by the fraudster using the same technology that a legitimate body would. The result is a false, but potentially very genuine looking document.

Stolen blank documents are genuine documents stolen from the manufacturing site, or more generally from the place where documents are personalized. These documents can then be personalized by the fraudster using the same technology that a legitimate body would (alternative technologies that produce a similar outcome may also be used). The result is a fraudulent identity on a genuine looking document.

[2] SOCTA Report 2017 - https://www.europol.europa.eu/socta-report

[3] ICAO - Machine Readable Travel Documents, Seventh Edition, 2015 - Part 2: Specifications for the Security of the Design, Manufacture and Issuance of MRTDs - https://www.icao.int/publications/pages/publication.aspx?docnum=9303

3.
Identity fraud

Identity fraud involves the illegal use of authentic documents, and falls into two categories: impersonation and fraudulently obtained documents.

Impersonation (sometimes referred to as a "look-alike") sees an impostor using a genuine document and claiming to be the holder. The usurper may use a document which has been lost, stolen, or borrowed from an accomplice.

Fraudulently obtained documents come from the exploitation of potential flaws in the issuing process. This can include the use of "breeder documents" which are either forged, counterfeited, or belong to somebody else. Fraud of this kind is sometimes carried out in cooperation with a corrupt official.

Interpol has found cases where organised criminal entities have been able to fraudulently obtain genuine travel documents from officials involved in the document issuance process, through suspected abuse of position.

While we do not cover identity fraud in this report, we do stress the importance of watchlists and biometric controls, including those used in the issuing process.

4.
Pseudo documents

These are documents that appear genuine, but do not actually seek to replicate a real equivalent.

Pseudo documents typically take the form of:

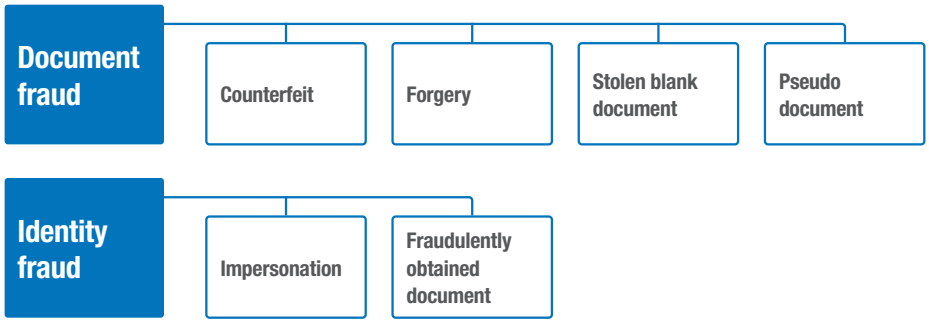
- Exotic or fantasy documents, complete fabrications issued by an imaginary state or organization.
- A camouflage document from a state that no longer exists or has been renamed.
- Fictitious documents that use the name of a real state or organization but are not genuine and do not have a legitimate equivalent.

While we do not cover pseudo documents in this report, it is worth noting that this type of fraud can be readily detected by consulting the lists provided by Public Register of Authentic Travel and Identity Documents Online (PRADO) in the European Union. Modern document readers are also able to detect such documents using ICAO country codes.

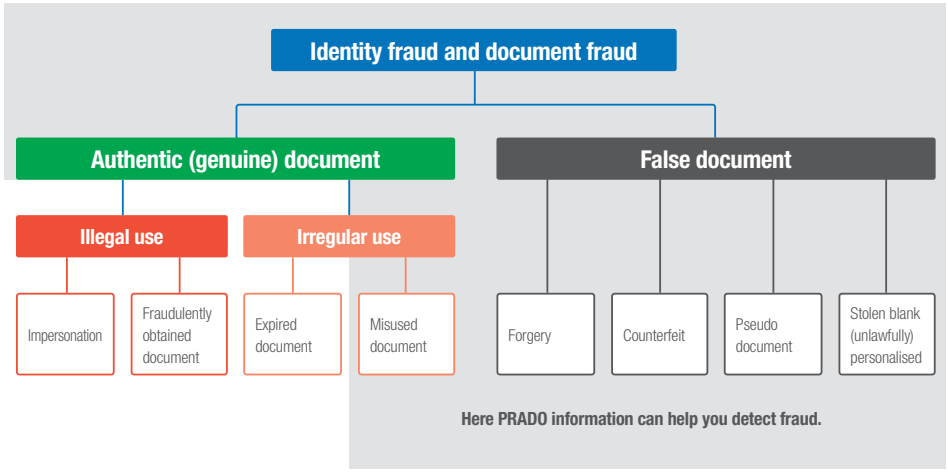
Counterfeiting and forgery are commonly known as "document fraud". This report focuses mainly on these threats. Identity fraud is not covered in this document because it is mainly linked to issuing and control systems, including breeder documents. Pseudo documents are omitted due to the relative rarity with which this technique is employed.

3.7
Classifying fraud

The diagram below provides a simplified fraud classification scheme. Note that irregular use of authentic documents (whether expired or valid) is not pictured.



While this diagram provides an overall summary of fraud types, alternative ways to classify fraud linked to identity and travel documents do exist. For example, the "identity fraud and document fraud" model was adopted by the European Union Document Fraud Risk Analysis Network (EDF-ARA 2012 Ref R023), and is also used by Frontex. This model is publicly available and can be found in the glossary proposed by PRADO [6].



PRADO refers to European Union regulation and to ICAO recommendations.

Interpol proposes another scheme, which presents travel document-related fraud in a relatively simple way. This approach is similar to the one used by Frontex.

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

The different types of document fraud[7]

Criminals and terrorists often make fraudulent use of both fake and genuine identity and travel documents in order to carry out illegal activities.

False documents

- Counterfeits – an unauthorized reproduction of a genuine document
- Forgeries – alteration of a genuine document
- Pseudo documents – documents which are not officially recognized.

Genuine documents

- Fraudulently obtained genuine documents
- Genuine documents misused by an impostor.

[7] typology used by Interpol. Source here https://www.interpol.int/Crimes/Counterfeit-currency-and-security-documents/Identity-and-travel-document-fraud

3.8
Document fraud in numbers

Precise statistics relating to document fraud are difficult to source; few are both publicly available and reliable enough to be trusted. There are exceptions, of course, and those gathered by the European Border and Coast Guard Agency and Frontex provide great insight into the document fraud landscape.

Risk Analysis – issued by Frontex on a yearly basis – is based upon monthly statistics exchanged by Member States within the Frontex Risk Analysis Network (FRAN). FRAN connects Frontex with Member States' risk analysis and intelligence experts, and the detection of fraudulent documents is one of nine key indicators[4] collected through the network on a quarterly basis.

In 2019, the number of fraudulent documents detected at external borders[5] was as follows:

- **Passports**
  3,582 out of the 7,536 fraudulent documents detected
- **Auth-impostor**
  27% (2019); other types of document fraud on passports = 73%

As was the case in previous years, the majority of fraudulent documents detected were discovered on air routes; on average, seven out of ten detections are made on these routes according to Frontex[6].

These statistics represent only a small percentage of fraudulent documents seized in total, of course. False documents are not only used to cross borders, but for a number of other criminal enterprises too.

Annex Table 10. Fraudulent documents used

Detections on entry at the external borders, by country of issuance of the document and type of document

	2016	2017	2018	2019	Share of total	% change on prev. year	Highest share
Country of issuance							**Type of Document**
Spain	862	989	1 107	895	12	-19	ID Cards (37%)
France	783	1 030	944	817	11	-13	Passports (34%)
Italy	875	860	711	649	8.6	-8.7	Visas (29%)
Germany	469	504	412	443	5.9	7.5	Residence Permits (37%)
Turkey	69	117	276	315	4.2	14	Passports (95%)
Poland	886	740	404	272	3.6	-33	Visas (79%)
Greece	272	296	283	251	3.3	-11	ID Cards (34%)
Belgium	293	253	239	203	2.7	-15	Residence Permits (32%)
Senegal	78	91	75	192	2.5	156	Passports (98%)
Ghana	43	57	88	181	2.4	106	Passports (97%)
All Other	3 659	3 289	3 439	3 318	44	-3.5	Passports (68%)
Type of Document							**Type of Fraud**
Passports	2 764	2 885	3 130	3 582	48	14	AUTH-IMPOSTOR (27%)
Visa	2 124	1 856	1 454	1 179	16	-19	FALSE-COUNTERFEIT (47%)
ID Cards	1 166	1 309	1 461	1 163	15	-20	FALSE-COUNTERFEIT (45%)
Residence Permits	1 193	1 227	1 138	956	13	-16	FALSE-COUNTERFEIT (43%)
Stamps	832	710	602	496	6.6	-18	FALSE-COUNTERFEIT (85%)
Other	210	239	193	160	2.1	-17	FALSE-COUNTERFEIT (61%)
Total	**8 289**	**8 226**	**7 978**	**7 536**	**100**	**-5.5**	

[4] Indicators: detections of illegal border-crossing between Border Crossing Points (BCPs); detections of illegal border-crossing at BCPs; detections of suspected facilitators; detections of illegal stay; refusals of entry; asylum applications; detections of false documents; return decisions for illegally staying third-country nationals; returns of illegally staying third-country nationals). More information at: https://knowledge4policy.ec.europa.eu/dataset/ds00034_en

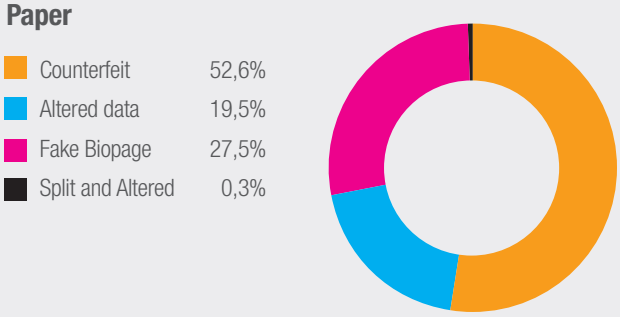
[5] "External border" refers to external borders of the EU and Schengen Associated Countries. Source: Frontex Risk Analysis 2020

[6] Frontex Risk Analysis for 2020

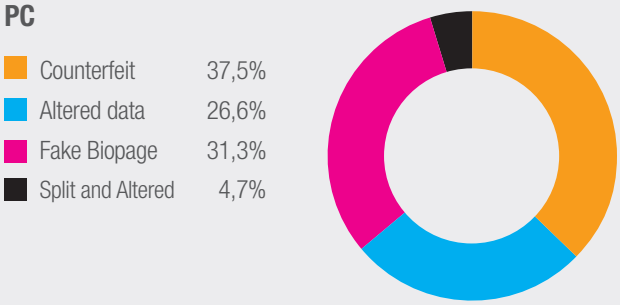
Some additional statistics have kindly been provided by Keesing Technologies[7] and are based on Authentiscan ID verification solutions – typically used by non-law enforcement organizations, public or private. As a result, the statistics do cover counterfeits and forgeries and are primarily related to Know Your Customer (KYC) objectives rather than border control.

Fraudulent passports – breakdown by type of datapage and document fraud

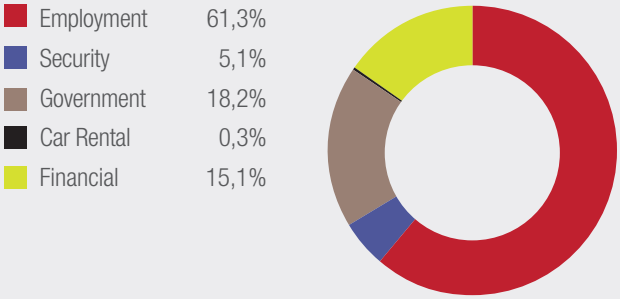
Paper



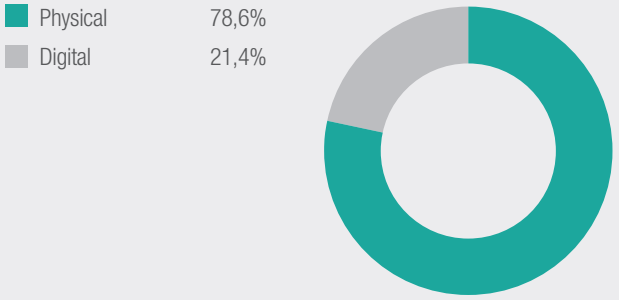
PC



Fraudulent passports – breakdown by industry



Fraudulent passports – breakdown by type of image



'Digital' attacks relate to images sent by a user (holder of the document uploads images - potentially altered - in the ID verification system). 'Physical' attacks relate to images taken in a live environment. This could be remotely by the user with a smartphone or with scanners on site. It is more difficult to assess if a document is genuine based on images sent by a user instead of generated by a trusted device.

The impact of Covid-19

While Covid's obvious impact on international travel has helped to slow the rate at which fraudulent documentation is being used – "only" 3,885 fraudulent documents were detected in 2020 according to Frontex[8].

[7] https://keesingidacademy.com/product/study/

[8] Frontex - 'Frontex 2020 in brief' – February 2021, https://frontex.europa.eu/publications/2020-in-brief-IrbE0G

3.9
Forgers and counterfeiters explained

Document forgers and counterfeiters can be principally described as criminal entrepreneurs supplying illegal commodity and/or providing illegal service. As such, they can be classified in several categories, depending on the level of investment, skillset and quality of their products. The below is the categorization proposed. Some experts would notice similarities with a possible classification of banknotes counterfeiters.

- **Unprofessional**
  Individuals tampering with elements of documents such as biographical data or information on visa pages, often in crude, unsophisticated manner or producing documents without attempting to simulate security features.
- **Semi-professional**
  Individuals using small-scale printing equipment (digital and traditional) and materials purchased on-line or in shops, with determination to simulate security features and ability to produce deceptive documents.
- **Professional**
  Individuals and networks with access to high-end printing and marking equipment and advanced technical skills, often able to produce or source design templates and emulated security features. Capable of producing deceptive counterfeit documents in large batches.
- **Sophisticated**
  Networks capable of producing highly deceptive counterfeit documents, with a great sophistication.

It remains difficult to provide an accurate and all-encompassing classification – due in part to the democratisation of document counterfeiting. Today, individuals can purchase templates in Photoshop and counterfeit materials such as holograms. This moves these individuals from the semi-professional to the professional category.

As mentioned earlier, motives are diverse, with fake ID able to be used to do everything from open bank accounts and mobile phone lines, to human and drug trafficking as well as money laundering and terrorism. As a result, the "quality" of a fraudulent document can vary considerably depending on what fraudsters are attempting to achieve.

In fact, the one thing that tends to unite forgers is their creativity. Preferring to make things easy, they will typically seek to replace smaller elements such as photos and document numbers while keeping the security features of a genuine document intact.

The same type of behavior can be observed in banknote counterfeiting. Since the document usually only needs to pass a quick check, there is little need for the whole document to be forged. As a result, document fraud is usually a mix of both counterfeiting and forgery (a genuine booklet with a fake data page, for instance).

Like many other illegal networks, forgers will seek to establish the same kind of production schemes that authorized bodies have access to. Document fraud today is facilitated by criminals who specialize in providing fake components, fake blanks, and unauthorized personalization.

The capabilities demonstrated by these forgers only serves to highlight the importance of the work done by law enforcement bodies to study and disable these networks wherever they exist. In particular, some recent law enforcement initiatives have been focused on what is commonly known as "forensic profiling of fraudulent documents". This approach looks to find similarities between various fraudulent documents seized at different places and times, and whether they may have come from either a single production source or component provider.

As Europol points out, "high quality counterfeit documents are primarily produced by highly specialized counterfeiters[9]", and document fraudsters are described as "specialized criminals offering document fraud as a service[10]", often belonging to fluid criminal networks.

About the distribution of fraudulent documents

Referring back to Europol once again, the law enforcement agency notes that "fraudulent documents are increasingly traded online and trafficked using post and parcel services", a trend which has been "accelerated by the COVID-19 pandemic".

One of the channels frequently used by criminal organisations for the distribution of fraudulent documents is the dark net. As law enforcement bodies have focused on dismantling these networks however, an increasing number of cases have started being linked to the open web. Included in those cases are pure frauds (scams), in which fraudsters are paid in advance and never send any document – genuine or not.

[9] SOCTA Report (2017)

[10] SOCTA Report (2021)

4. Exploring the classes of fraud

In this chapter, we look in greater depth at the most common types of document fraud; looking at the type and frequency of attack, how fraud occurs and recommended counter measures.

In the interests of maximising security, much of the detail in this section is excluded from this public document. This detail can be found in the restricted version produced for law enforcement agencies and authorities, and available for authorised personnel by contacting CCSD@interpol.int

4.1 Counterfeiting

4.1.1 Passport

Reproducing a passport from scratch to sufficient quality that it can pass as a genuine article is very rare. Most of the time, rather than trying to duplicate an original precisely, counterfeiters will imitate it to the extent that it can be used to deceive authorities and non-specialists.

In general, the most targeted passports are those that allow access to countries without an accompanying visa. Documents with weak security design are also prime targets since they are easier to imitate.

Documents with long circulation periods (10+ years) are also prime targets for attack. With more time to study and experiment on a document with various forgery techniques, forgers will usually find it easier to conduct a successful attack the longer a document has been in circulation. Even when a document has been modernized, some fraud attempts will continue as long as former versions continue to be used.

> *When new versions of identity documentation are issued, fraudsters may take the easier route of attacking the old design – still valid and in wide circulation for many years to come. It may be hard to avoid this, though some issuers may try to mitigate this if required to some extent, e.g. by reducing the duration of passports from ICAO's maximum of 10 years (some choose 5 years); or by introducing an interim upgrade to the design and security features, e.g. after only 5 years rather than waiting for the full 10 year cycle.*
>
> **Frank Smith**
> Ex-Deputy Director, UK Home Office

When checking whether a document is genuine, controlling authorities can both check and contribute to several databases.
Examples include:

- PRADO (Public Register of Authentic Identity and Travel Documents Online), a publicly accessible database created by the Council of the European Union.
- iFADO (Intranet False and Authentic Documents Online), also set up by the Council of the European Union. Access is strictly limited to certain enforcement bodies.
- Edison TD (Travel Documents), a reference database of travel documents and other travel-related materials developed by the Dutch authorities in cooperation with several other authorities including Interpol. This registry has three levels of access: public, LEA (Law Enforcement Agencies), and Expert (a selection of forensic laboratories), each providing further details about the genuine document. The 194 Interpol member countries are connected to this database via its secure communication network called I-24/7.
- Documentchecker, a reference database developed by Keesing Technologies (Netherlands), used by public or private organizations to fulfil their legal obligations: Know Your Customer (KYC) and Customer Due Diligence (CDD).
- Dial-Doc (Digital INTERPOL Alert Library – Documents) is a joint INTERPOL-G8 initiative which allows countries to share alerts produced at the national level on newly detected forms of travel document counterfeiting. Through comparisons with images and descriptions of counterfeit documents submitted worldwide, the system makes it possible to strengthen international police cooperation in identity control and the fight against fake documents.
- Many additional initiatives from law enforcement bodies exist to collect, produce, and share national alerts with a focus on the key detection points.

Some of these reference databases (PRADO and Edison TD in particular) have been made widely available via the web in order to provide any interested party with a stronger chance of determining whether a document is genuine or not. High quality images and further information on genuine security features are only available to authorized bodies, however.

> *In contrast to the long tradition of strict confidentiality around document security features, [these] initiatives aim to raise public awareness on document fraud and to support anyone who has to check a document. Some observers fear that these public and overt references would help forgers in their endeavour, but they do not provide high-quality images of documents or detailed descriptions of security features. Only low-level forgers would potentially learn something from these websites*[11].
>
> **Simon Baechler**
> Doctor of Forensic Science, University of Lausanne
> Head of forensic science and crime intelligence, Police neuchâteloise

To further aid in the fight against fraud, the ICAO recommends that issuing authorities share physical specimens and basic information about passport security features with the main organizations maintaining reference databases, and with the manufacturers of document readers: "In addition to sending to receiving states, it is a good idea to send specimens to the organisations that offer a secure reference database of images of passports and their security features[12]."

The facilitation of identity checks is a social responsibility for issuing authorities, one that aims to provide greater convenience for citizens and drive usage of e-services. Improved access to reference databases delivers benefits that include:

- Increased awareness of the document security features to look for (thanks to high-quality images) and quicker identification of those features; even automatic checks can be performed using templates, for instance.
- Reduced waiting time at control points and easier digital onboarding for travellers.

Typical counterfeiting attempts can be separated into two categories: one targeting the secure materials used in passport creation (basis components), and the other involving the imitation of manufacturing techniques and related security features (e.g. security printing).

[11] Baechler, S. Document Fraud: Will Your Identity Be Secure in the Twenty-first Century?. Eur J Crim Policy Res 26, 379–398 (2020). https://doi.org/10.1007/s10610-020-09441-8

[12] Guidance for Circulating Specimen Travel Documents" (ICAO, Version: Release 1, March 2016)

Substitute materials

The complete reproduction of a passport will involve substitute materials. These include paper, polycarbonate, inks, laminates, sewing thread, hinge (for polycarbonate data pages), and the relevant cover material.

Some fraudsters (a very small group) will try to reproduce most of the components or materials. Others will have limited knowledge and little means to try and counterfeit everything. As a result there are many different cases of counterfeits, and the overview below is indicative rather than exhaustive. Treat it as general guidance rather than a specific set of considerations. It is worth noting that the best counterfeits aren't always detected, even by highly trained and experienced controllers. With only a few seconds to analyse the validity of a passport, well produced counterfeits do occasionally make it through.

Let's look at some of the materials involved in counterfeit reproduction.

Paper	**Watermark** One of the first security features that requires control, counterfeiters tend to use two tone watermarks with simple designs or simulation of the watermark via printing. This results in poor detail. When printed, a fake watermark may be visible under UV light. This should not be the case for an authentic one. Quite often, counterfeiters will use generic watermarks, with non-customized designs that do not correspond with genuine ones.
	Security fibers Very often, counterfeiting of security fibers is achieved through printing. Visible fibers have the same appearance (no variation in the depth), and can be found in the same place on different pages. This is not the case with randomly spread genuine fibers, making counterfeit ones relatively easy to spot.
	Security thread Transparent and micro printed polyester threads are mostly counterfeited by printing. Fraud attempts of this nature are rather easy to identify as - just like security fibers - a genuine security thread is embedded inside the paper substrate instead of the surface – where it is visible without transmitted light.
Polycarbonate	While some counterfeit polycarbonate cards (ID-1 format) have been found in the field, there is currently no significant complete counterfeiting of polycarbonate data pages. Polycarbonate materials are available on the public market, of course, and could thus be considered less secure than a material like security paper. Polycarbonates specially made for laser engraving are more difficult to counterfeit, however, and some now allow for the application of greater security controls such as controlled UV fluorescence. This is different from fluorescence thanks to the addition of optical brighteners.
Cover	Made either from paper or textiles, the cover needs to offer a high level of durability. The cover material used for passports is very similar to the one used in the book publishing industry. As a result, the cover alone is rarely something that can be relied upon as a way to confidently authenticate a document. Some experts do pay lot of attention to the cover since it serves as the first contact with the document for front line officers. Normally the passport should be taken closed before any inspection and – as a result – the feel of the cover and a quick check of the sides of the booklet can help to detect something wrong before inspecting the interior.
Sewing thread	This security feature is rarely counterfeited. When reproductions are used, blue coloration under UV light or a lack of fluorescence altogether will help to identify them. Most genuine sewing threads use less available UV fluorescent colors such as red.
Laminates (for paper data pages)	Because modern laminates are highly complex materials, counterfeiters tend not to try and duplicate genuine articles, but create false equivalents that are good enough to pass with authorities and citizens. And while holographic techniques have made the counterfeiting of paper data pages more difficult, the efficiency of these methods relies on the integration of new and highly secured devices. This leads us to stress the importance of maintaining clear communications with the police on how to recognize common forgeries. For personal (paper) data pages, the ICAO recommends using a laminate on the whole page.
Optical variable features	Counterfeiters prefer to keep the security features on the surface of polycarbonate data pages, and for good reason. Holograms are now a widely-used optical variable feature, and when counterfeited they are usually of poor quality and likely to fail a check by a professional.

Imitation techniques

Reproducing a passport also means recreating the techniques used in its creation. This stretches from the security background (i.e. printed security features) to the various manufacturing techniques and security features used on authentic documentation.

Scanners, image modification software, and printing technologies (such as inkjet, laser, and sublimation) all play a role here. With consumer-level technologies offering ever-higher resolution counts, counterfeiters now have a better arsenal with which to simulate identity documents than ever before.

Let's look at some of the techniques used.

Cover	Hot stamping is a commercially available technique, mainly used for identification and the embellishment of travel document booklet covers. It is not always mastered by counterfeiters, however, and a poor gold foil hot stamping (with poor definition and/or adhesion) should be enough to trigger the in-depth review of a document. Additional UV fluorescent printing and embossing on the cover surface are used less frequently, and will not necessarily be recognized by a controller.
Security printing and security inks	With higher resolution technologies increasingly available, counterfeiting becomes easier. Minimum magnification of x15 is now required to see the difference between a security printing and a counterfeit.
Sewing method	The sewing method used for passport booklet binding is not complex in itself. At the same time, not all counterfeiters have perfected it, resulting in lower sewing quality which is likely to set off a more detailed check.
Laser perforation	Mechanical laser perforation can be reproduced but its use is becoming increasingly rare. Conic perforation counterfeiting is on the rise on the other hand, but is much more difficult to replicate when the perforation is not uniform (i.e. using different shapes like circles and squares).
Personalization	Counterfeiters often use inkjet and laser printing technologies to manufacture false paper data pages.

Recommended countermeasures

Fraudsters tend to employ the techniques they know best, especially when the materials and means to employ them become more widely available. As a result, innovative new security features that surprise fraudsters play a major role in making certain features much harder to replicate.

Some highly complex security features have been used for decades, of course, and are yet to be counterfeited. Every security feature has a lifecycle, and some require evolution rather than reinvention.

Organizations like the ICAO regularly seek out information about state-of-the art security features, using them to shape the guidelines they provide to governments around the world. This is vital; there is no panacea nor flawless security feature that works in every situation.

Good security relies on a combination of several features interacting with each other. The right mix of technologies can make document fraud very complex, while still fulfilling the needs of the end user – an easy-to-use, but hard to replicate document, for example.

When considering whether to apply a new security feature to a document, the experts involved should take a few key issues into account (NB: points are not listed in order of importance):

- The security level, and whether the new feature can be detected with the naked eye. Some features can be controlled with several security levels, up to three according to traditional classification.
- Whether it can be controlled with OMA (Optical Machine Authentication). This developing technology assists in document verification, and some security features are suitable for or designed specifically for OMA.
- How easy it is to control the feature. Some experts believe that a good security feature should be:
  - » Easy to explain (some features are very intuitive and require nearly no training).
  - » Easy to understand and memorize.
  - » Easy to locate, recognize and control (authenticate) – the most critical aspect is the total time it takes.
- How resistant to fraud it is. A good security feature, in general, is:
  - » Hard to imitate (with alternative technologies)
  - » Hard to produce (full counterfeiting).
  - » Hard to get (the fraudster would need to source the same product from a specialized supplier). Some features are hard to get because the minimum order quantity is high, and hence the price to source it is equally significant.
- Visual aspects, and the impact on the readability of personalized data in particular. The easiness with which the feature can be embedded and combined into the entire document design is important, too.
- The security of the supply chain, from production to transport.
- The impact on the total cost of the document. There is no general rule in this area, because every technology has its own cost model. Typically, the link between cost and quantity varies a lot from one security feature to another – and even between suppliers.
- Exclusivity, or market availability. Can the security feature be supplied by one company only, or can equivalent alternatives be found from other trusted suppliers? Limited supply equals greater security – in theory at least.

About the classification of security features

While there is no international norm when it comes to the classification of security features, a three-tier system is generally accepted as a suitable starting point for their evaluation. These tiers are as follows:

- **Level 1:** checks can be made with human senses under natural daylight, and without the use of any specialized tools. The controller will tilt, observe, or feel the feature to authenticate it.

- **Level 2:** controllable using a simple verification tool, which will be widely available. Most commonly, this will be a UV lamp (UV-A 365nm) or a magnifier (x10).

- **Level 3:** verification demands a specific tool and/or forensic (laboratory) means – typically, a microscope and/or a video spectral comparator.

ICONS designed by the Secure Identity Alliance to represent the three security levels

Some experts consider that a fourth level exists, pertaining to features that are kept secret by the document or component manufacturer as an additional security level. And, with mobile phones now in the hands of almost everyone, some classify this as level "1.5". The three levels outlined above should be treated as a guideline, rather than the rule.

Controls can be made either at the "front line" (with usually only a few seconds available) or at "second line" (for deeper analysis that demands more time). As a result, some security features are not suitable for first line controls. Professionals involved in the conception of document verification guidelines should always consider this difference.

About the availability of security features

Some technologies and security features are only available from a few certified document manufacturers or component suppliers. While this is good for document security, it also means that some proprietary technologies can be exclusive to a single supplier, carrying a risk of customer lock-in that needs to be assessed and managed.

Issuing authorities are aware of this concern and know that it is their responsibility to consult with providers on the technologies that have active patents. And, just because a feature is exclusive to one vendor, that doesn't mean that an issuing authority should automatically avoid the use of that technology.

When modernizing a document, the right balance has to be struck between holistic security and the use of proprietary technology. When assessing the options open to them, governments will find great benefit in working with certified bodies; SIA members, for example, hold "security certification(s) and certification(s) of information technology security, recognized by the Member States of the European Union[13]".

[13] https://secureidentityalliance.org/about-secure-identity-alliance/join-us/types-of-membership

An analysis of security features, materials, and manufacturing techniques

Security features	Level	How they aid fraud prevention
UV dull substrate	**2**	"UV dull paper, or a substrate with a controlled response to UV, such that when illuminated by UV light it exhibits a fluorescence distinguishable in colour from the blue-white luminescence used in commonly available materials containing optical brighteners". This is the definition given by the ICAO and such a basic feature is an effective countermeasure against low quality counterfeits.
Watermark (paper)	**1**	Multi-tone paper watermarks (sometimes called "cylinder mould" or "shadow" watermarks) with subtle changes in tone (more than two tones) and both lighter and darker areas. This is not possible to reproduce by printing, and not as commonly available as two-tone watermark paper (produced on Fourdrinier paper machines). Additional security features: » Specific watermark for the data page » Thin electrotype including page numbering
Security fibers (paper)	**1-2**	Multicolor, visible and/or invisible UV fluorescent security fibers randomly dispersed in paper. Not possible to achieve by printing.
Security thread (paper)	**1-2**	Easier to identify in transmitted light, ideally placed on the side of the page. Alternatively, this can be placed close to the hinge to facilitate authentication when checking the watermark. Cleartext metallic threads are more complex to imitate, and fluorescence in one or several colors increases the difficulty of replication. Window-threads – seldom used in passports – are amongst the most difficult security threads to imitate. This is because they are embedded partly in the paper and also appear on the surface. Additional optical properties are sometimes present. Note: if embedded, a window thread should typically be positioned on page three or inner cover pages.
Transparent window in polycarbonate data page, with optical variable device	**1-2-3**	Data pages are most commonly made by fusing polycarbonate layers together. One way to make these structures more difficult to forge, and faster to authenticate, is to include one or more transparent ("see-through") areas in the thickness of the structure. This often takes the form of a window, of variable size and shape. Sometimes, it may be asymmetrical. Additional security is conferred by a background printed with an optically variable or metallic ink and/or laser engraved personalization (e.g. personal data of the holder, image).
Security polycarbonate	**1-2-3**	Polycarbonates specially made for laser engraving are more difficult to counterfeit, and some polycarbonate materials allowing additional security level controls are now available.
Offset Printing	**1-2**	A high-quality and detailed background design using guilloches, micro text, and other complex graphical features only available through specific software.
Intaglio printing	**1-2-3**	Printed on the inside front and/or back covers of a passport booklet, intaglio printing can include hidden patterns (e.g. latent images), tactile features, and micro-texts.
Optical variable inks	**1-2-3**	Printed on transparent areas of a polycarbonate data page, optical variable inks make for easy authentication at first line.
Hot foil stamping on cover	**1**	With sufficiently high-definition design and quality, hot foil stamping becomes difficult to reproduce. Due to the wide availability of this technique, however, some do not consider hot stamping to be a security feature.
Embossing lamination with an optical effect and/or micro text	**1-2**	Difficult to reproduce, and easy to detect by its absence through touch or oblique light (low-angled). Special tools are required to verify the presence of micro texts, however.
Optical variable color shifting embossing	**1-2-3**	A combination of tactile lamination with some kind of security polycarbonate, and/or secure optical variable inks in transparent areas (e.g. clear window).
Sewing thread	**1-2-3**	UV fluorescent sewing thread with up to three plies of different UV colors are recommended (avoid UV blue fluorescence alone).
DOVIDs (for both paper or PC data pages)	**1-2-3**	DOVID (Diffractive Optically Variable Identification Devices) are one of the most commonly checked features during ID verifications.
Laser perforation (booklet numbering)	**1**	Laser perforated holes with different shapes (e.g. circles, squares, and triangles are much more difficult to counterfeit than mechanical or conical holes with just a single shape.

Security features specifically linked to personalization

In the area of personalization, special machines are used to add further security to blank passports. This is vital, because the data page is the most commonly attacked component of a passport booklet. Personalization technologies are specially adapted for paper or polycarbonate pages, and only their careful combination offers the highest level of security.

It is highly recommended to show multiple bearer portraits in a passport booklet, preferably using various technologies. These should be of a sufficient size to facilitate easy control. This can be facilitated through Multiple Laser Images (available for the polycarbonate data pages) or via an additional portrait obtained by laser engraving or perforation. These latter machines are available solely to certified security manufacturers.

Many solutions can be used to embed color portraits on polycarbonate pages. Laser engraving can be applied to the core of the layer, as can color printing. A combination of black laser engraving with color printing can also be used on the surface of the data page.

Another possibility around personalization is to print an additional color portrait on page three (after the data page). This is natively protected by the security background (with visible and invisible offset features), and security can be enhanced with additional security measures such as:

- Transparent and colorful holographic portraits (a level one security feature).
- Portraits made from micro-text (level two feature, requiring verification with a magnifier).
- Portrait protection through digital technology (a guarantee of the authenticity of the portrait, with data sealed into an interoperable Visible Digital Seal).
- Hidden information embedded in the portrait (level three security feature, checked with a specific filter).

Color portraits are useful against document fraud as a whole (counterfeiting or forgery), and specifically against identity fraud. Color may also help police officers to authenticate the person by matching the photo to the bearer.

Security features	Level	How they aid fraud prevention
Combination of different personalization techniques	**1-2**	The use of different technologies to print the portrait makes counterfeiting more complicated. An example would be using laser engraving for the main portrait on a polycarbonate data page, and combining this with color and/or UV fluorescent printing on page three.
Color portrait for polycarbonate data page	**1-2**	Color portraits for polycarbonate as a whole are relatively new technologies, and have not yet been mastered by counterfeiters.
Tactile laser engraving (for polycarbonate data pages)	**1**	Tactile features are typically used to personalize document numbers or expiry dates, data which is likely to be modified by counterfeiters.
Personalization in transparent area	**1-2**	The most commonly used security feature is a portrait in a transparent window. This is easy to authenticate (very intuitive), and enhances the security brought by the transparent area.
Personalization in lenticular structure	**1**	TThe most commonly used feature here is a MLI (Multiple Laser Image), embedding a portrait image and key data (e.g. expiry date).

4.1.2 ePassport

Some alert reports point to fake chips being used in counterfeit passports. It is difficult to quantify the phenomenon, but these alerts suggest the existence of (more or less) advanced fake chips that simulate the behaviour of official chips. "More or less" in this instance means that logically, with a robust standard control device, fraud will be detected by signalling (that passive authentication has not worked, for instance).

As one border control document and identity fraud expert stressed to us, "the problem is that many border guards are largely unaware of the threat. As a result, if they have been inundated by false positives previously, they will tend to ignore the messages sent by the system. Popularization work is therefore essential."

In the meantime, documents with counterfeit chips continue to circulate. These sometimes contain only a BAC, DG1, and DG2 but no EF. SOD[14] (i.e. no signature). Other travel documents with a chip containing data in DG1 and DG2 and signed "UTOPIA" have also been observed. Naturally, these do not correspond to any real country.

Usage of these documents remains infrequent and, if a reading device is up to standard, it will signal the problem. But their existence must be taken into account nonetheless.

As our border control contact explained to us during the writing of this report, it is therefore important that:

- Devices are developed that reduce false positive rates as much as possible so that the police have confidence in the system and act on the messages sent to them. Comprehensive messages on detected anomalies should be delivered so as to ensure that police officers remain active in the detection of fraud and/or the removal of doubt.
- Agents should receive better training on the challenges of controlling the electronic component of electronic Machine Readable Travel Documents (eMRTDs).

As can be inferred from the examples above, potential counterfeit on the electronic part of a passport is directly linked to the age of its secure components: its software, operating system (OS), and integrated circuit (IC).

Because of this, compliance with electronic security standards and recommendations is the surest way to preserve the integrity of electronic chips. For instance, states that implement biometric passports with Extended Access Control (EAC) as defined by the ICAO guarantee their citizens the highest level of security. The various security mechanisms recommended by the ICAO for the electronic components are detailed in another section.

In order to make sure that only trustworthy documents are delivered, the OS and IC contained in an electronic passport must be security certified (Common Criteria) before issuance. The Common Criteria security certificates only demonstrate that a product met the requirements at the time of certification of course, and do not have any meaning with respect to their effective security at a later date.

The electronic passport generally has a long validity period, usually ten years. The lifetimes of an embedded software and a chip are longer than the validity period of the identity document itself, however.

In order to ensure the effective security of OS and IC components at any time, some countries are implementing security surveillance processes that allow for the monitoring of the embedded software and chip. This allows them to check on the potential erosion of security in those components across the entirety of their lifetime.

Monitoring of this kind can inform risk management plans. It allows issuing authorities to anticipate the end of life of an OS or an IC, and enact migration to new generations. Additionally, it enables issuing authorities to define contingency plans that include scenarios tailored to the level of the security breach they may encounter.

[14] Elementary File (EF) / Document Security Object (SOD)

4.2
Forgery

4.2.1 Cover

Replacement of the cover only

Some forgers will try to switch a cover from an ordinary passport to a diplomatic one in order to avoid having to present a visa when crossing a border. To achieve this, they will merely add a new cover, or remove the existing one in order to replace it.

This kind of fraud can be detected primarily by paying attention to the identification marks that characterize the diplomatic passport booklet. Typically, wording clearly marking it as a diplomatic document will be printed on the data page, both on the front and reverse side.

From a prevention standpoint, issuing authorities should make the cover removal as complex as possible using appropriate basis materials and gluing methods. The paper for the inner covers should be sufficiently fragile so as to make tampering obvious.

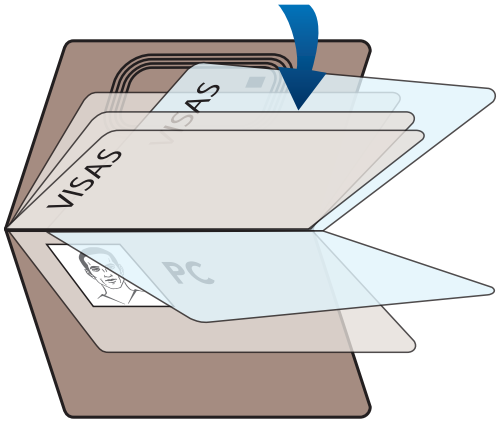
4.2.2 Booklet

The removal or replacement (substitution) of entire visa pages

In passport booklets, visa pages are subject to two categories of fraud:

i. The visa page is cut out and repositioned in a different place in either the same or another booklet. This is usually done in order to disguise the fact that one page has been cut out, because it contains – for example – an expired visa issued by the country in which the traveller is staying. The missing page is then replaced by another page of the same booklet, or from another booklet.

ii. The visa page is split into two thin sheets. The purpose of doing this is to avoid having to reinsert a complete sheet in the passport booklet.



Example of a visa page replacement (complete four-page sheet)

Removal/replacement (substitution) of visa stickers

Forgers will remove visa stickers from a passport booklet and affix them in another because they grant access to a certain territory.

Visa stickers are usually self-adhesive, and fraudsters use heat and chemical products to dilute that adhesive. Heat softens the glue, making it easier to lift and remove the sticker when done slowly and carefully.

There are three ways to prevent this kind of manipulation:

i. Pre-cuts should be implemented in the visa sticker, oriented in different directions, to create physical weaknesses in the visa sticker.

ii. Chemically reactive agents can be included in the paper of the visa pages and the sticker itself.

iii. Security inks can also be used to print background artwork.

Removal of stamps

Fraudsters usually try to remove stamps present on visa pages using chemical means, by using a rubber, or by scratching. To prevent these threats, the following countermeasures can be employed:

i. Use solvent-sensitive inks to print the background artwork that will react to chemical products or water.

ii. Chemically reactive agents can be included in the paper of the visa pages, producing a staining effect when activated.

iii. Use ink that disappears when rubbed off. Part of the security background will be removed when the stamp is tampered with.

iv. Make the paper substrate fragile enough to create visible damage should a fraudster attempt to scratch away personalized data

4.2.3 Paper data page

A. Whole data page substitution

The datapage is removed and replaced by a fake page containing fraudulent data. Fake sewing thread may also be used. The forgers seek to imitate the original look of the datapage and paper, even if the printed and holographic patterns are not completely right.

Data page forgery can be fuelled by a range of factors:

- Low security blank data pages, which are easy to counterfeit.
- Low security protection films or layers (laminates).
- Laminates stolen as a result of insecure storage.
- Low security sewing (stitching) methods and/or sewing thread.
- Low security numbering methods, especially for inner pages.
- The absence of an electronic chip in the cover (containing a genuine digital portrait image, and protected with state-of-the-art cryptography mechanisms).
- Making the booklet too easy to open and reassemble without leaving tamper evidence.

4.2
Forgery (continued)

Recommended countermeasures

Security features not linked to personalization

Security features	Level	How they aid fraud prevention
Data page **1. Unique design** **2. Unique watermark (different from the watermark used on the inner pages)**	**1-2**	1. A unique design makes it impossible to use an inner page as a replacement; using rainbow offset printing is a basic recommendation. 2. As above, a unique watermark prevents inner pages from being used; using a two-tone watermark is a basic recommendation.
Secure laminate, with at least one robust level one security feature	**1**	Quick and easy to authenticate, and counterfeiters cannot easily imitate it.
Sewing **1. Programmable sewing method (lock-stich, with thread stitched back at the ends)** **2. UV fluorescent sewing thread**	**1 - 2**	1. When the booklet is reassembled, a stitched back at the end is even more difficult to reproduce using the same holes. 2. UV fluorescent sewing thread is a basic recommendation; such threads are difficult to source or imitate, especially complex ones (e.g. red under UV 365nm light).
Inner page numbering **1. Conical laser perforation** **2. Geometrical laser perforation**	**1**	1. When the booklet is reassembled, inner pages cannot be perfectly aligned. As a result, the laser perforated holes of the various inner pages will not be perfectly aligned either. This can be detected fairly easily. 2. Geometrical laser perforation (holes made of different shapes) are more difficult to imitate with heated needles.
Thin paper for inner cover pages	**1**	Thin paper must be resistant and durable but frangible enough to be partially destroyed if separated from the cover.

Security features linked to personalization

Security features	Level	How they aid fraud prevention
Additional portrait image(s) printed after the data page	**1-2**	Attempting to modify this image may activate specific security features embedded in or on the paper.
Electronic chip with genuine portrait image protected by cryptography mechanisms	**2**	This genuine digital portrait is nearly impossible to modify, and a fake replacement (printed on the data page) may be detected. If the chip is damaged or destroyed to try and circumvent this, it may raise doubts about the integrity of the passport and legitimacy of the holder.
Additional personalization technology	**1-2**	Most paper data pages are personalized with inkjet or laser printing methods. Adding some data with additional personalization technology (e.g. invisible UV fluorescent printing) will make page replacements more likely to be detected..

B. Picture (portrait) modification or replacement

Several techniques can be used to forge a portrait photograph onto a passport data page. Below we present the main ones seen in the field, and basic countermeasures.

- **Direct overprinting on top of the laminate (no removal of the genuine photo)**
  Since the fake photo is added on top of the laminate, some optical features protecting the portrait area will no longer appear genuine. This can typically be detected using an angled view (oblique) with side light, and checking whether the laminate sits on top of the portrait image as it should. As a result, the quality of the secure laminate optical features is key to detecting such attacks.

  In addition, a well-designed security background (both visible and UV fluorescent) protecting the portrait area will help with detection.

- **Laminate removal and/or reuse**
  Forgers typically practice chemical or physical attacks in an attempt to delaminate and remove the security laminate in order to access the data within with only minor destruction. They may try to reuse the laminate, but most of the time it will be destroyed due to its thinness (a few microns width only).

- **Chemical attack and replacement (after direct access to the photo)**
  On paper data pages, a basic recommendation is merely to use an appropriate chemical reagent. Should the photo become accessible (something that is nearly impossible with a well-designed, thin security laminate), the chemical sensitizers will ensure that the attack is made evident.

C. Some cases that are not explored further in this report

- **Use of a visa page to forge the paper datapage**
  While cases of this kind have occurred in the past, today's datapages are designed to be highly specific, particularly in relation to the printed security design. It is recommended that the watermark has a specific design too, which may be as simple as orienting the central image (e.g. a coat of arms) differently.

- **Transparent film/layer with a fake portrait image**
  A similar technique to that used to forge data on polycarbonate data pages is applied here. As with direct overprinting, a close look at the optical features (especially with side light) makes this type of fraud attempt easier to detect.

- **Abrasion from the back of the paper**
  In this case, the watermark would likely be partially destroyed. Attacks of this kind – and countermeasures against them – are discussed in more detail below.

- **Splitting and partial replacement with a fake datapage (front side only)**
  Classic countermeasures are most effective in this instance: watermarking with some thin areas (leaving tamper evidence when split), high-quality security backgrounds, and highly secure laminates.

- **Laminate replacement with a fake**
  In these attacks, forgers try to imitate genuine security laminates with available holographic techniques. Sometimes they will even attempt to do so using non-customized holographic foil.

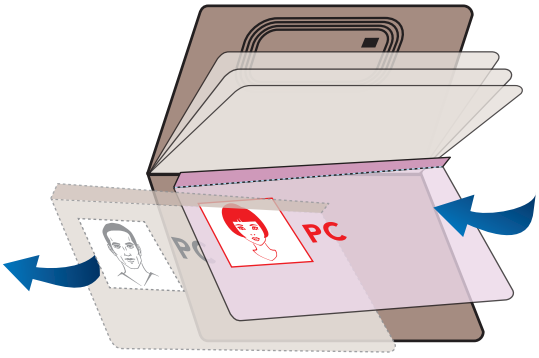
  The use of counterfeit lookalike laminate is usually done with only a raw reproduction of the main design elements. As a result, it will be lacking in some details and be without the most robust and specific security features such as simulated (virtual) reliefs, image switches, and/or two-color permutations.

  Covert features like microtexts will not be reproduced perfectly either, and may sometimes be missing altogether.

4.2.4 Polycarbonate data page and e-data page

A. Data page removal and replacement with fake data page, hinge, and sewing threads

There are several circumstances under which polycarbonate data pages may become suitable targets for forgers, with activities including taking the passport apart and reassemble without leaving evidence of tampering, and/or taking out the electronic chip.



Example of a polycarbonate data page removal and replacement

Recommended countermeasures

Security features not linked to personalization

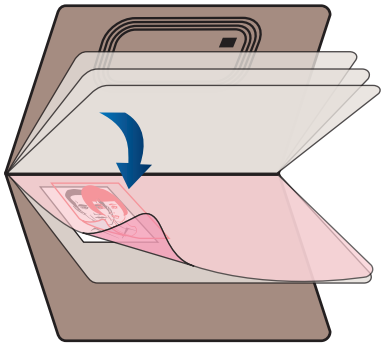
Security features	Level	How they aid fraud prevention
Blank data pages	-	Please refer to the recommendations to limit counterfeiting.
Optical variable features	1-2-3	A highly secure optical variable feature with at least one robust level one security feature.
Hinges	1-2	Well-designed hinges are hard to separate from the data page body without leaving evidence of tampering.
Sewing (stitching) methods and/or sewing thread	1-2	
1. Programmable sewing method (lock-stitch, with thread stitched back at the ends)		1. When the booklet is reassembled, a stitched back at the end is even more difficult to reproduce using the same holes.
2. UV fluorescent sewing thread		2. A UV fluorescent sewing thread is a basic recommendation; such threads are difficult to source or imitate, especially complex ones.
Numbering using conical and geometrical laser perforation through the inner pages	1	When the booklet is reassembled, the inner pages cannot be perfectly aligned.
Thin paper for inner cover pages (e.g. 90gsm)	1	This paper is resistant and durable but fragile enough to be partially destroyed should the cover be removed.

Security features linked to personalization

Security features	Level	How they aid fraud prevention
Personalization security features for the data page	-	Several approaches can be used to make counterfeiting of the page more difficult. Among these are: » Personalization using lenticular structures. » Hidden information (typically in a portrait). » Tactile personalization. » Windows with personalization. » Laser perforation.
Additional portrait image(s) printed after the data page	1-2	The genuine portrait image may not be modified, or the attempt to modify it may be detected because specific security features are embedded in or on the paper.
Electronic chip with genuine portrait image protected with cryptography mechanisms	2	This genuine digital portrait is nearly impossible to modify and comparisons with the fake portrait (printed on the data page) may lead to detection. If the chip is rendered non-functional (it can be intentionally destroyed), this may raise the doubts about the integrity of the passport and legitimacy of the holder.

B. Data and/or picture modification

Data or picture modification typically relies on the application of a transparent film containing fake information.



Example of a transparent film used to modify a portrait image

Recommended countermeasures

Security features not linked to personalization

Security features	Level	How they aid fraud prevention
Visible and invisible (UV fluorescent) printed security background overlapping the portrait area	1-2	May be less visible (or at least different than expected) once covered with the transparent layer, and will be much less visible under the fake photo.
Optically variable ink near the portrait area	1	May be less visible once covered with the transparent layer.
Hologram/DOVID overlapping the portrait area, including optical variations (i.e. matte/glossy)	1-2-3	Once covered with the transparent layer, may be less visible with optical variations disappearing.
Tactile lamination (embossing) features	1	May be less obvious to touch once covered with a transparent layer; may disturb the application of the fake layer.
Lamination (embossing) features including optical variations (i.e. matte/glossy)	1	Optical variations may disappear once covered with the transparent layer.

Security features linked to personalization

Security features	Level	How they aid fraud prevention
MLI or CLI (a tactile feature) that can contain an additional portrait image	**1**	May feel less obvious once covered with the transparent layer; may disturb the application of the fake layer; the genuine image may not be modified.
Tactile laser engraving of key data (e.g. passport number or expiry date)	**1**	May be less obvious to touch once covered with the transparent layer; may disturb the application of the fake layer.
Additional portrait image(s) laser engraved or perforated in the data page structure and/ or printed on an inner (paper) page	**1-2**	This genuine portrait image may not be modified, or the attempt to modify it may be detected because specific security features are embedded in or on the paper (chemical sensitizers, security background, information based on passport data embedded in the genuine portrait).
Secure personalization technologies	**1-2-3**	Some new technologies embed visible features that are complex to imitate with a fake photo on a laminate. These can be linked to color, resolution, or the combination of laser and embossing on the portrait area, for example.

C. Direct overprinting on top of the polycarbonate data page

Since the fake photo is added on top of the genuine image, some optical features will no longer appear genuine.

Thanks to this, forgeries of this kind can typically be detected with low doubt using coaxial light. Without access to such tooling – a reality for the majority of frontline staff – document examination experts recommend that border control personnel check the portrait area using a side view. This is usually the best way to notice that the main portrait image is not personalized where it should be.

Recommended countermeasures

As with fraud attempts that use transparent overlay, the most effective security features against direct overprinting include security printed backgrounds (especially visible) or DOVIDs embedded on top of the portrait area (overlapping some of it). This is complex to design effectively, because these security features must not hide the portrait either.

Additional portrait images will also help to make detection easier, especially if they are large enough and secure against manipulation. The third page of a passport booklet (usually following the data page) has room available for this and is increasingly seen as a “second” data page.

D. Abrasion from the back of the data page

This type of forgery is commonly applied against synthetic cards. The document is ground from the back in order to remove some of the security layers and provide access to the portrait area.

Recommended countermeasures

In addition to secure offset backgrounds (both visible and invisible), several security features can be used to make fraud attempts more challenging and easier to detect. The following are comparatively easy to embed within a secure design:

- The addition of tactile and/or optical lamination features to the reverse side.
- Optically variable ink behind the portrait area (usually printed only on the front side).
- Security features on a layer inside the data page structure.
- An MLI lens on the front side. Should the additional portrait image also be erased and replaced, it would be unlikely to show movement when tilted.
- A transparent window with additional portrait image. Attacking this image from the reverse side would leave tamper evidence.
- Additional portrait images on page three or behind the main portrait area (reverse side). Special equipment and extra personalization time are required in both cases.

Of course, it is highly recommended that controllers inspect the reverse of a datapage whenever possible.

4.2.5 ePassport (forgeries on contactless chips)

Intentional deactivation, damage, or chip replacement

Forgery of a passport booklet involves altering key details to make the document suit the new holder. Often, this will mean disabling the micro-controller to prevent border officers from matching the chip content with the document, and thus spotting inconsistencies in either the portrait or other data.

Sometimes, fraudsters may add a micro-controller with data from the "new holder" signed by a fake issuing authority. This can be effective when border control is not checking against the ICAO Public Key Directory (PKD), or when the issuing authority does not publish its certificates in the PKD. This is the same method that is used when doing a full counterfeit of the passport booklet (as described above).

Replacing a genuine contactless chip with a fake is done in order to take advantage of the weaknesses of a system which may not cross check physical security features and personal data. This type of attack was most common in the 2010s.

Since strong security mechanisms are present in passport chips today, forgers rarely aim to modify or replace them. Most of the time, fraudsters will instead attempt to destroy or deactivate the chip in order to make the personal data impossible to verify. Again, tampering of this kind is often used by fraudsters wishing to pass themselves off as the genuine bearer or, in the case of a forged portrait on the data page, to avoid the portrait on the chip being checked.

We recommend that non-functioning chips should always be treated as suspicious. Border officers should check the document for any sign of tampering, such as indentations on the cover, where a void will be clearly visible when viewed using reflected light. Microwaving a travel document can also leave visible burn marks, another sign to check for.

Chips should be systematically and thoroughly verified during an inspection, and checked with all possible security devices.

It is also highly recommended to secure chips using the guidelines established in ICAO Doc 9303, specifically parts nine, 10 and 11. This promotes the following techniques:

- **Passive Authentication (PA):** by allowing digital signatures and country certificates to be checked, this mechanism ensures that a passport has been issued by a legal government and not manipulated.
- **Active Authentication (AA):** an encrypted algorithm verifies that the chip has not been cloned thanks to a challenge/response mechanism.
- **Basic Access Control (BAC):** prevents skimming and mitigates the risk of eavesdropping between chip and inspection systems by using a secure communication channel. This protocol is weakened by the use of algorithms SHA-1 and 3DES, however.
- **Supplemental Access Control (SAC):** this mechanism is similar to BAC in that it protects data exchanges between the chip and the terminal, and allows the terminal to access the data groups that are not biometric. SAC is highly recommended because it is based on more recent and robust cryptographic mechanisms than BAC.
- **Extended Access Control (EAC):** this mechanism allows the terminal to access the data group storing the biometric data of the holder – their fingerprint and retinal scan. The portrait, sometimes considered as biometric data, is stored in data group two and requires only BAC or SAC to be accessed.

As noted earlier, fraud on the electronic part of the passport is directly linked to the age of its secure components. In order to make sure that only trustworthy documents are issued, embedded software and chips contained in electronic passports are security certified with the Common Criteria before their issuance.

Nonetheless, it is highly recommended to implement a security surveillance process that provides lifetime monitoring of the chip and ensures effective security.

4.3
The specific case of morphing

Facial morphing represents a very serious threat to ID security, which is a key component of national and international security. By blending the facial features of two people, fraudsters are able to produce a morphed photo that could potentially fool highly trained agents and sophisticated facial recognition systems.

Studies have proven that both trained humans and machines struggle to detect morphed photos with a high level of confidence. This creates a risk that morphed photos will go undetected during the ID application process, resulting in Fraudulently Obtained but Genuine (FOG) passports and ID cards that two people could use for fraudulently claiming services and for travelling around the world.

Furthermore, many measures currently in use to protect ID photos from morphing are insufficient. This should present major cause for concern for ID-issuing authorities. In order to combat this ongoing and ever-changing threat, governments need to remain agile and open to new and innovative prevention, protection, and detection measures.

The best way to reliably protect against morphing attacks is to take a three-pronged approach that includes preventing FOGs from being issued in the first place, protecting ID photos from manipulation, and detecting mismatches between live images and morphed ID photos using the best biometric algorithms available.

The first step is to ban the acceptance of printed photos and take control of the photo capture process to prevent morphed photos from successfully infiltrating ID applications. Secondly, to protect photos in existing IDs from morphing attacks, the most advanced ID photo security techniques must be used.

Finally, to support these solutions and reinforce national and international security, governments should also deploy leading-edge biometric systems at security and other ID checkpoints. As biometric algorithms improve, these systems will increasingly help border agents, law enforcement officials, and other authorities to catch fraudsters, criminals, and terrorists before they are able carry out their plans.

To summarize, the best defence against morphing attacks is to combine the following solutions:

- Ban printed photos, and capture live photos on-site or through controlled and connected photographers and photo booths.
- Protect the photos in identity documents by implementing strong security features.
- Deploy cutting-edge biometric recognition systems at ID checkpoints.

5. Various field factors to take into account

Fraud is an ever-evolving landscape, and issuing authorities should keep a close eye on the changing dynamics that shape it. Below, we discuss some of the key issues influencing the future of document fraud.

Factors boosting fraud

- **Professionalization**
  (the increasing capabilities and technological access of forgers) Inkjet printing and dye sublimation have largely been mastered and are now regularly used for document counterfeiting. Sometimes, even offset printing and laser engraving can be employed, typically by 'professional' forgers who likely have an involvement in the production of fake banknotes as well.
- **Availability of standard or sophisticated secure materials**
  Reports of document fraud have begun to mention some entry level security inks or security papers, as well as fake holographic laminates (created primarily through the use of dot matrix technology).
- **Availability of confidential information**
  Everyone involved in the security chain plays a part in maintaining the security of information in restricted areas, taking into account the degree to which the recipient "needs to know" before sharing anything. All SIA members raise awareness within their organizations about the importance of managing confidential information, and are governed by the highest security certification frameworks for both production sites and the information technology used. These certifications are recognized by the Member States of the European Union.
- **Low security documents**
  The purpose of this report is to raise the importance of secure documents, focusing on the main risks identified.
- **Availability of equipment and products on the open and dark web**
  Even "finished" documents can be found for sale in certain places.

Factors lowering chances of detection

- **Too many security features**
  Some experts have likened overcomplicated passports to a Christmas tree overloaded with ornaments; they may appear impressive, but are also entirely impractical. Too many verifications can prove to be counterintuitive.
- **Limited time to make checks at front line**
  This is the primary reason why document examination experts call for security features that can be intuitively authenticated in seconds, without tools.
- **Lack of tools to aid in checks (limiting the chance to verify details)**
  Frontline staff should not be undermined by a lack of technology. Even smartphones – with their capability to zoom, magnify, provide additional lighting, and scan contactless chips – could serve as an additional checking tool, for instance.
- **Lack of knowledge and training of controllers for document examination**
  Typically, fraudulent documents usually have some similarities between them. This is the reason why some law enforcement bodies circulate alerts highlighting a few key detection points. Even some basic training sessions can empower controllers to detect the majority of forgery attempts.
- **Low levels of standardization (highly specific documents require different controls)**
  ICAO recommendations propose the introduction of standards in order to increase interoperability and facilitation of travel. Some regional initiatives also enable additional standardization for similar documents (e.g. EU regulations for documents like the resident permit card). This remains quite disjointed though, especially for passport booklets.

6. General recommendations and additional measures

In addition to the component and technique-specific security measures outlined in the previous chapter, general fraud prevention best practice also plays a vital role in maintaining document security.

Below we present some general recommendations and additional measures which should be taken into account by document manufacturers when designing a new passport booklet. (NB: points are not listed in order of importance).

- Do not rely on one security feature alone. Modern passports offer many different validation techniques, and these are most effective when used in combination. As the ICAO clearly points out in Doc 9303 (Part 2), "although some features can offer protection against more than one type of threat, no single feature can offer protection against them all. Likewise, no security feature is 100 per cent effective in eliminating any one category of threat."
- Use the most secure materials, printing and manufacturing techniques, and personnel as your budget allows for, and ensure that there is balance between all involved factors.
- The best protection comes from a combination of different security features. The key is to balance defence with data page readability, in particular. Many options should be considered here, including the following combinations:
  - » Offset printings (rainbow), visible and invisible landmarks, in register.
  - » Intaglio printing with an optical variable ink (e.g. for the inside front cover).
  - » Watermarks, which are easier to control if every inner page uses a blank area (a kind of window) as embedded on banknotes.
  - » Laminates (for paper data pages) or lamination plates that integrate multiple security elements.
  - » Optical variable color shifting embossing.
- While the combination of multiple security features is advised, too many can make verification unintuitive. Balance and common sense are key. In the field only a few security features (some experts say four to five) are needed to verify the authenticity of the passport booklet and the integrity of the main portrait image.
- Make the most of every security feature by optimizing the way it is embedded in the overall passport design. Tactile features should be embedded where the fingers will naturally hold or take the document, for example. This is one area in which the experience of the document manufacturer can prove to be very useful. A close collaboration between document examination experts and passport manufacturers is highly valuable here, too.
- In general, when it comes to the distribution of security features across the three security levels, it is recommended that:
  - » Issuing authorities should focus on level one security features, as they represent more than 90% of controls made in first line. Only a few are likely to be checked, so they should be strong and intuitive enough for cursory examination by anyone who knows what to look for. Highly trained and well-equipped examiners are a minority, and forensic specialists belong to an even smaller skilled population.
  - » Embed a few level two features such as micro-texts and UV rainbow printing. These should be designed to bring confidence and ease to second line inspections.
  - » Utilize level three security features sparingly; one or two is generally enough. These will only be used in very specific cases and require specific tooling to validate. Significant doubt about the authenticity of the document, or the need to produce unquestionable proof of counterfeit or forgery in front a judiciary authority, will be required to trigger these. Keep them highly confidential.

6
General recommendations and additional measures (continued)

- Distributing the features throughout the various booklet components requires prioritisation. It is highly recommended that issuing authorities protect the data page, portrait areas, and additional portrait images above all else. Some key data should also be duplicated and embedded using special features (e.g. the document number or expiry date personalized on page three, in a MLI lens and/or with tactile laser engraving).
- Some security features allow several levels to be embedded at the same time, and many features enable authorities to fight both counterfeiting and forgeries at once. Features should be selected to facilitate a broad spread of defences. This makes integration easier while limiting the number of features that need to be checked
- Documents should be designed for checking both by humans and the machines that assist them. Some security features are hybrid and can be controlled both by humans and machines, typically by comparing a given document with templates under VIS/UV/IR lights (UV and IR fluorescent printed backgrounds are in the scope).
- Embedding the same main security features and components in ordinary passports and other ID-3 format travel documents (e.g. diplomatic/service passports) makes life easier for controllers. With fewer specificities to deal with, they will generally require less training, and be able to make quicker and more reliable checks. A level of homogeneity for secure design features also enables document manufacturers to offer better prices and delivery times while keeping the bar high enough to deter counterfeiters. By way of example, while a 48 page diplomatic passport (instead of the 32 found in an "ordinary" document) can be useful, if there is also a request for an electrotype watermark with page numbering, then it means that two versions of a customized security paper will need to be produced (32 + 48 inner pages). This can present significant extra cost. Some exceptions do make sense, however. Emergency passports – which may not have all the security features of the ordinary passport – offer one such example.
- With regard to unique numbering on blank passports:
  - » Blank passport booklets should never leave the production facility without a unique number.
  - » Security features should be applied after personalization. Failing this, personalization should be a complex process using security features which require niche equipment.
  - » Use a chip in the document and verify its data.
  - » Keep control of the enrolment and issuance process.
  - » Store documents safely and apply relevant security measures and a four-eye principle for access to blank documents.
  - » Connect to Interpol MIND/FIND and SLTD databases, and report all stolen document numbers to invalidate their use for international travel at once.

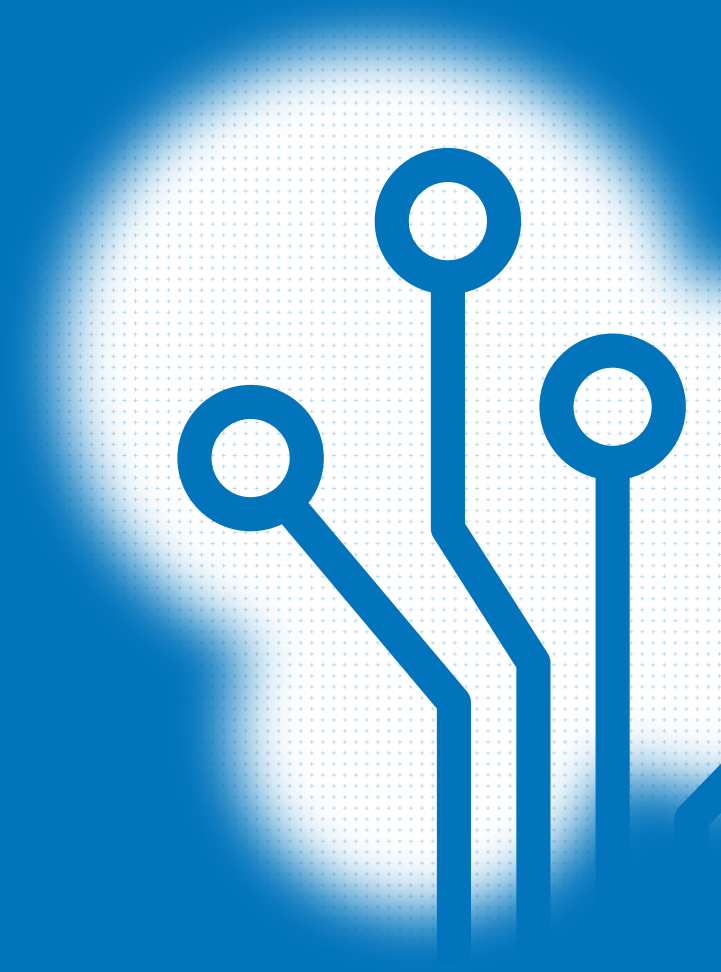
7. Conclusion

The document fraud landscape is becoming increasingly complicated, and requires a strong appreciation of a much bigger picture in order to navigate successfully. Successful controls now hinge on a variety of fast-moving factors that range from the operating methods of fraudsters to new and sometimes highly complex technology.

This paper was designed to help readers gain a better understanding of those factors, as well as a stark reminder of the stakes relating to document fraud. When fraudsters win, we all lose.

The recommendations made here are drawn from some of the world's leading document security experts and sources, and we would encourage anyone involved in the issuance, control, or design of passport booklets and other forms of identification to heed their guidance. As discussed above, the number of security features is less important than the overall art of secure design; less can be more when applied effectively.

One tool that may prove useful when evaluating the effectiveness of security features included in your own documentation is the SIA's own eDocument Physical Security Evaluation Model (eSec). First launched in 2017, eSec provides organisations with a way to better assess how security features like datapages and photos should be distributed across different parts of a passport booklet. An updated and optimized version of eSec is scheduled for 2022.

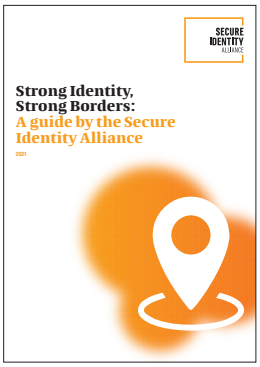


Other reports by the Secure Identity Alliance:

https://secureidentityalliance.org/ressources/publications

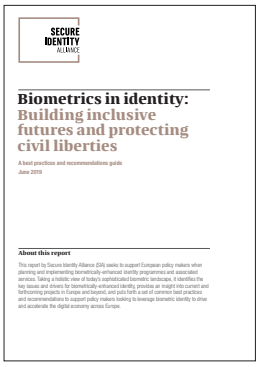
Giving Voice to Digital Identities Worldwide

Providing unprecedented 'on the ground' insights and perspectives, the study produced in partnership with onepoint gives a unique voice to stakeholders from 25 innovative sovereign digital ID schemes. Their shared learnings highlight the guiding principles and good practices that are critical for driving usage, adoption, and success – regardless of the digital ID model adopted.



Strong Identity, Strong Borders

Looks at the need for border authorities to balance security and protection with efficient and frictionless passenger experiences. In addition to the major drivers shaping the future of the border control space, the report looks at the vital - and complex - role played by identity management, highlighting some of the evolutionary technologies incl. automation, biometrics, mobile, and bringing those solutions to life in the form of case studies from around the world.



Biometrics in identity: Building inclusive futures and protecting civil liberties

This report seeks to support policy makers when planning and implementing biometrically-enhanced identity programmes and associated services. Taking a holistic view of today's sophisticated biometric landscape, it identifies the key issues and drivers for biometrically-enhanced identity, provides an insight into current and forthcoming projects in Europe and beyond, and puts forth a set of common best practices and recommendations to support policy makers looking to leverage biometric identity to drive and accelerate the digital economy across the world.

SECURE
IDENTITY
ALLIANCE