7 questions about identity document verification and security features

IDENTITY

POSTED ON 04.21.23

While digital transformation of the ID landscape is already underway, this does not mean that physical ID documents are set to disappear. To combat illegal activities, governments must ensure that all citizens can actually prove who they claim to be—both online and in-person. Even in the digital world, the physical document remains the intrinsic link between a digital identity and the document owner. Physical IDs must not become an easy "backdoor" for fraudsters.

Identity document fraud is constantly evolving and can take on different forms, including counterfeiting, forgery, use of stolen blank documents, or Fraudulently Obtained but Genuine documents (FOG). Providing citizens with tamper-proof ID documents is critical and this means constant innovation as security features on a physical ID are considered obsolete after 10 years and easy to copy after 20 years.

#1 What are the key features of an identity document that makes it unique to its holder?

The portrait is probably the most important feature on an identity document because it helps to uniquely identify the cardholder. Therefore, securing the portrait using advanced security features while making such features easy to verify is absolutely vital. To do this, a secondary portrait is generally added.

An identity card also contains:

- Biographical data (name, first name, date of birth, etc.);
- Biometric data (usually fingerprints and/or iris) stored in the chip;
- The signature of the holder;
- A unique identifier (the ID card number);
- And the MRZ (Machine Readable Zone)—only on ID cards intended for travel purposes. The MRZ contains biographical data and document validity dates, etc., for optical scanning.

These are all elements that are unique to the cardholder and allow them to be identified.

#2 How to secure an ID document?

Security is provided at different levels:

- **The substrate**: polycarbonate – a material that cannot be separated once the different plastic layers have

been laminated – should be used to secure ID cards or the datapage of a passport to protect laser engraved personal data more effectively. In the case of passports, visa pages made of paper can contain multi-tone watermarks, security fibers, etc.

- **Secure printing technologies**: the structure can be covered with a complex background design using guilloche, intaglio (i.e., ink that stays at the surface of the paper and creates tactile effects) or negative and positive microtexts that are only visible under a magnifying glass.
- **Specific inks**: the ID may incorporate a fluorescent pattern that is only visible under UV light. It may also use Optically Variable Ink (OVI), which displays different colors depending on the angle.
- **Personalization features**: certain parts of the ID, such as micro-texts and document numbers, may use laser engraving to obtain a relief effect. Specific personalization techniques may also be applied to create color or grayscale portraits.
- **Operating System security**: i.e. the software security of the NFC chip that contains the holder's data – including the portrait – as well as an electronic certificate and the cryptographic key to secure this data.

#3 Why is the portrait such a key element of secure identity documents?

The portrait is the natural link between the document and its owner, hence the need to secure it. The first step is to ensure that the picture used on the document corresponds to the actual holder of the document. This is why the **identity enrollment process** is so crucial. The most effective approach is to capture live photos by an agent on the spot or through controlled and secured channels (accredited photographer or in a secure kiosk).

The second step consists in ensuring that the portrait on the document cannot be tampered with after issuance. One of the most advanced techniques consists in engraving the document holder's ID picture in color directly onto the identity document using a single laser beam. Moreover, **duplicating the main photo** in the same document using a different technology reinforces document security and helps prevent fraud because tampering would require the fraudster to master different techniques in order to modify the photos. A **secondary photo** may be directly embedded in the document or in a window. This can take various forms such as a color hologram or a 3D photo with floating characters in the forefront, for instance. **Interlinking personal data** (e.g., biographical and biometric data, the unique identifier or the signature) makes forgery almost impossible.

#4 Why security features must be easy to inspect

With the rapid increase in situations where ID checks must be performed, not only police officers but also public and private sector employees need to be able to verify the authenticity of an identity document. You may need to prove your identity during a job interview, to take an exam, to open a bank account, take out an insurance policy, or to access an age-restricted area, for example. ID checks are becoming even more critical due to the **large-scale adoption of digital services**. Hence the need to develop ID security features that can be easily checked in just a few seconds by experts and non-experts – banks or insurance officers, merchants, pharmacists or universities – with or without checking devices, in-person or online.

User-friendly security features must enable **different levels of inspection**: with the naked eye, using a simple tool such as a magnifying glass, or with a device such as a smartphone or a scanner. Training, tutorials, and communication about how to check an ID document also help combat fraud.

#5 Why is it important to continuously innovate with new security features?

Identity document fraud is constantly on the increase and can cause serious security problems for governments and reputational damage for businesses. The most common form of ID fraud is counterfeiting, i.e. a complete fake reproduction of a genuine identity document, either made from scratch or using parts of genuine documents.

Alternatively, blank documents may be stolen and completed using false information, or fraudsters may tamper with a genuine identity document, for example by using morphing or photo substitution—this third type of fraud is called "forgery". There is also an increase in the number of "imposters" using genuine identity documents belonging to people who look like them.

To address such issues, security features have been and continue to be developed to create tamper-proof identity documents as fraudsters gain access to more sophisticated technologies such as laser engraving and inkjet and 3D printing. In the fight against illegal activities, innovation is crucial for **staying one step ahead of the fraudsters** and complying with international standards (notably ICAO standard for passports). Moreover, highly secure ID documents and strong border control processes make mean **passports with a higher security ranking**, making it easier to obtain visa waivers. Last but not least, using a trusted physical document is a solid basis for **creating a secure digital identity**.

#6 How to verify the authenticity of an identity document?

There are 3 levels of human inspection:

- **Level 1: visual inspection with the naked eye.** The inspector examines the document to assess if it is genuine and checks that the photo matches the individual presenting it.
- **Level 2: ID check using a simple device such as a UV lamp or a magnifying glass.** The use of a device increases the degree of certainty.
- **Level 3: forensic inspection using a dedicated device or machine.** This involves a detailed examination of the document's paper, ink, printing, stitching, and laminate to determine if it is genuine or not. It can also involve comparison with an official database.

ID checks can also be automated thanks to **Optical Machine Authentication (OMA)**, which allows experts or non-experts to perform a thorough ID check with a simple device like a smartphone or a scanner. The user just needs to take a scan, a photo or a video to perform a global check of the design, a specific check of Optical Security Features, as well as a consistency check between the data in the Machine-Readable Zone (MRZ) and printed data. With OMA, the non-expert can immediately ascertain whether the ID picture and biographical data are genuine, or if they have been altered or substituted. Overall, OMA ensures **more reliable ID verification** than human inspection.

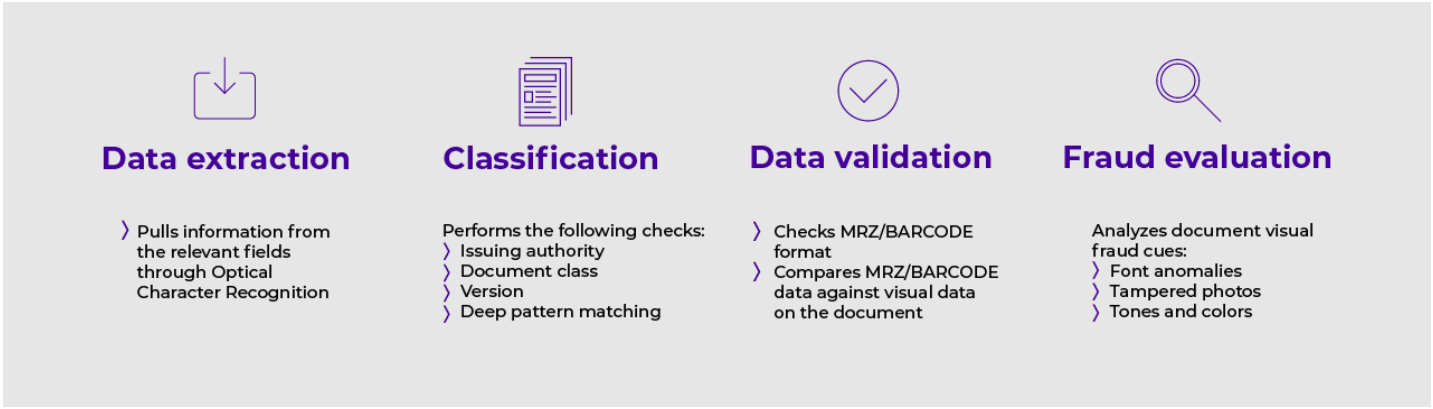
OMA covers 2 main types of verification: either by phone (OPA) or scanner (OSA):

- **Optical Phone Authentication (OPA)** can only check security features visible with simple smartphone cameras, such as diffractive motion effects based on the viewing angle.
- **Optical Scanner Authentication (OSA)** allows static controls using cameras at multiple wavelengths (visible and infrared light).

#7 How to verify a physical identity document remotely?

In today's digital world, a secure physical ID document (identity cards, driving licenses, passports or residence permits) must be **verifiable remotely** as well as physically, face to face. This is typically done using optical document verification. The document holder is guided and **assisted by a smartphone app** to take an optimal photo of their document, making it possible to extract the document holder's photo, read printed data using Optical Character Recognition, and extract data from the MRZ. A video recording of the document may also be requested to increase the level of certainty: the holder must then rotate their identity document in front of the camera to verify its authenticity.

Each document is analyzed according to its specific security features (secure printing techniques, specific inks, customized features, etc.) to ensure these features are valid and in the right place. Techniques may include data extraction, classification, data validation and fraud evaluation.



In addition to – or instead of – optical document verification, **chip reading using NFC technology** may be used in a remote identity verification context to guarantee even stronger verification of the ID document.