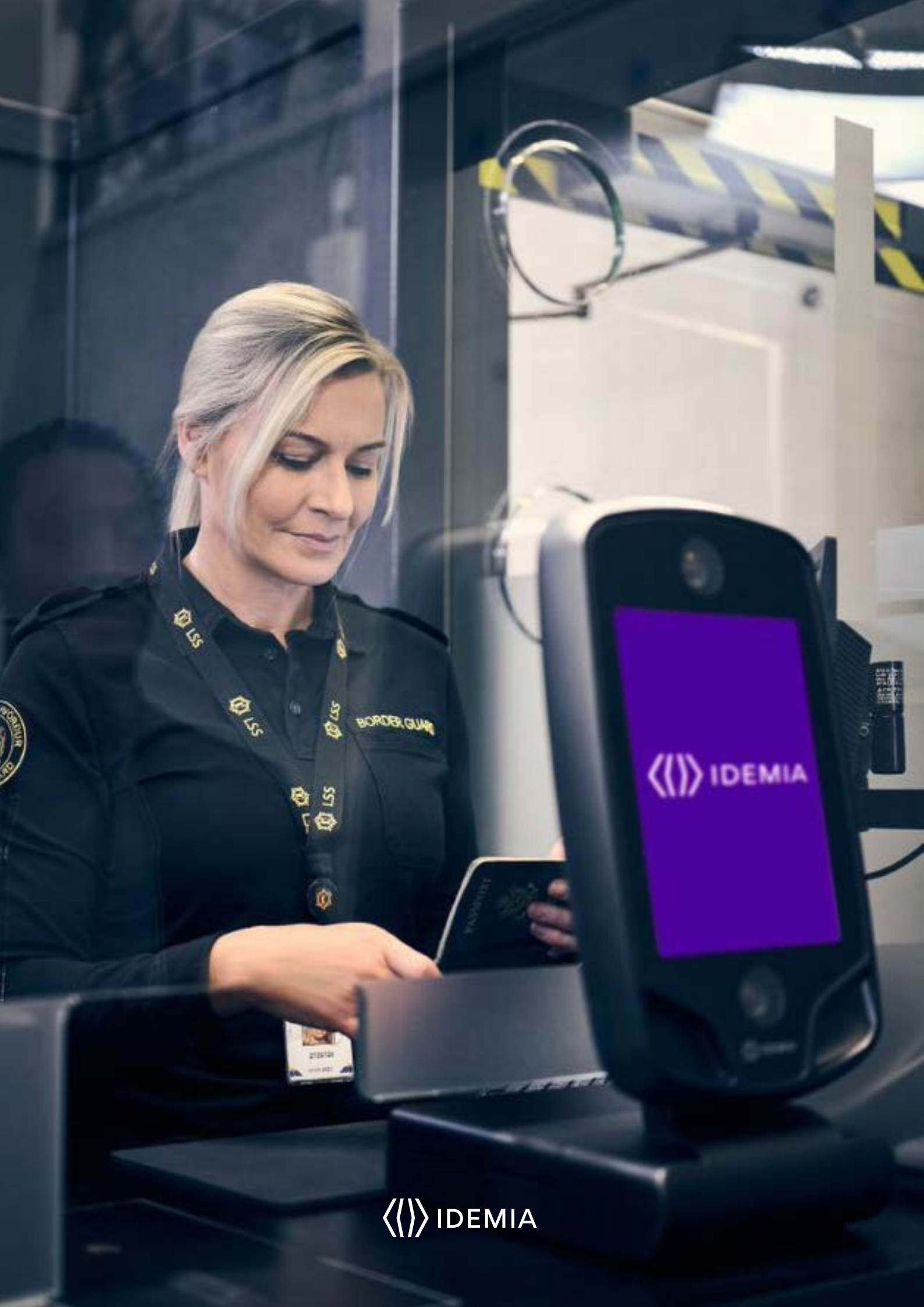


Securing ID credentials

selecting the right
secondary portrait



《》 IDEMIA

Executive summary

The truth is that ID fraud exists and will continue to exist in one form or another. With the advent of eServices, there has been an increase in ID related fraud and the pandemic has only helped facilitate ill-intentioned individuals, which is why ID issuers need to continually stay one step ahead.

The objectives of this paper are to understand why ID credential fraud continues to develop, and to guide governments and ID issuance authorities in understanding all available solutions.

We will take a look at the various forms of ID fraud being committed, the different levels of inspection required and the solutions that are currently available on the market. We will also define the strengths and weaknesses of each solution to provide an understanding of how efficient they are in combating fraud.

This paper clearly highlights that one of the most efficient security features is a secondary portrait that reinforces the security of the main portrait. It is difficult, if not impossible, to tamper with both the main portrait and the secondary portrait, as two different technologies are used. It is rare for fraudsters to understand and master both types of technology. And lastly, this paper raises the importance of opting for technologies that are not widely available to the public is optimal.

ID fraud is a reality; however, by using the right security features, governments can provide their citizens with ID documents that are fraud-proof.

Creating fraud-resistant ID documents using innovative security features

ID documents are of great importance; they permit people to prove their identity in person and online. Unfortunately, over the last couple of decades, document fraud has rapidly evolved, despite the prevention measures enforced by issuing authorities and document manufacturers. One of the reasons is because fraudsters now have access to sophisticated equipment and materials that help them create seemingly authentic ID documents.

We live in an increasingly digital world, and we are now able to access remote services from the comfort of our homes. However, if our data is not correctly protected, we are leaving ourselves wide open to ID theft and other ID related fraud. Fraudsters are always looking for new and inventive ways to breach security. To safeguard citizen data, ID documents should be regularly renewed and updated with new security features.

Regardless of the type of document and type of fraud, one thing is certain: the portrait is always impacted. Whether it is by adding a new portrait over the genuine one, passing as someone the fraudster resembles, or submitting the picture of someone else in the process of acquiring a new document, it all comes down to the portrait. The portrait is the main link between the document and its holder when performing identity verification.






The portrait needs to be clearly visible and devoid of any pattern that could hinder visibility when authenticated using a machine. To reinforce security, it is essential to focus on secondary portraits, as they confirm whether or not the main portrait is genuine and intact. The ID document needs to be highly secure and hard to reproduce, yet easy to inspect.

Reasons why ID fraud continues

An unfortunate fact is that fraud will always exist. Whether it is using a counterfeit or altered passports to cross borders, making electronic transactions using a stolen identity, etc.—fraud will happen. It has a devastating effect on governments, companies, and, in particular, on people.

In addition to official figures (border guards, law enforcement agents, etc.) verifying ID documents, there are cases when civilians also have to check an ID. The surge in the collaborative economy means that people can rent out their car, their country house and even their building tools in a few clicks. They need to be sure that the ID document they are presented with is authentic and that the holder is indeed the lawful owner.

Five different types of fraud

	Counterfeit	The complete fake reproduction of a genuine document made with non-genuine materials or using parts of genuine documents.
	Stolen blank documents	Genuine blank documents that have been stolen in order to personalize them with false information.
	Forgery	Falsification of personalized or affixed data on an ID document for example using morphing or photo replacement.
	Impostor	Use of a genuine document that does not belong to the holder, because the fraudster resembles the legitimate document bearer.
	FOG	Fraudulently Obtained but Genuine document with false data and/or morphed portrait.

1. Challenges related to human verification

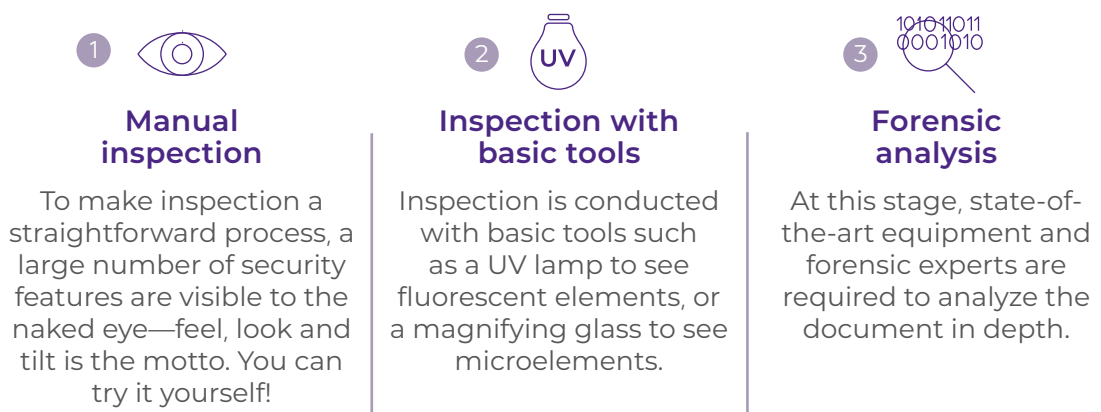
The number of use cases where untrained people must check ID documents is growing. Therefore, it is important that along with trained agents, civilians are aware of how to verify security elements on ID documents correctly.

- › **Lack of training:** In a bid to secure ID documents, sometimes too many security features are added. This means that agents need to understand and remember how to check each feature, which can make verification a long and laborious process. Instead, a select few security features would be ideal along with some level of training on how to examine ID documents correctly. For example, basic training would be sufficient for a civilian renting out their car, and it would help increase confidence and limit doubt to the authenticity of the document.
- › **Limited practical tools:** In addition to a lack of training, few people have the necessary equipment to check documents such as a pocket magnifier or an ultra-violet lamp. Tools for in-depth verification, such as a multi-spectral microscope are exclusively available in laboratories and to second-line inspection teams at airports.
- › **Limited time to do the job properly:** Limited time is a significant factor when it comes to conducting ID checks, especially at congested airports. Therefore, border guards have to concentrate on specific aspects of the document.

There are other use cases, such as entering a stadium or a concert hall, where ID documents are rarely checked properly as the crowd is often excited and in a hurry. In public services, clerks need to provide a fast and efficient service to their customers; as a result, they too only have a few seconds to conduct ID checks.

Three levels of inspection

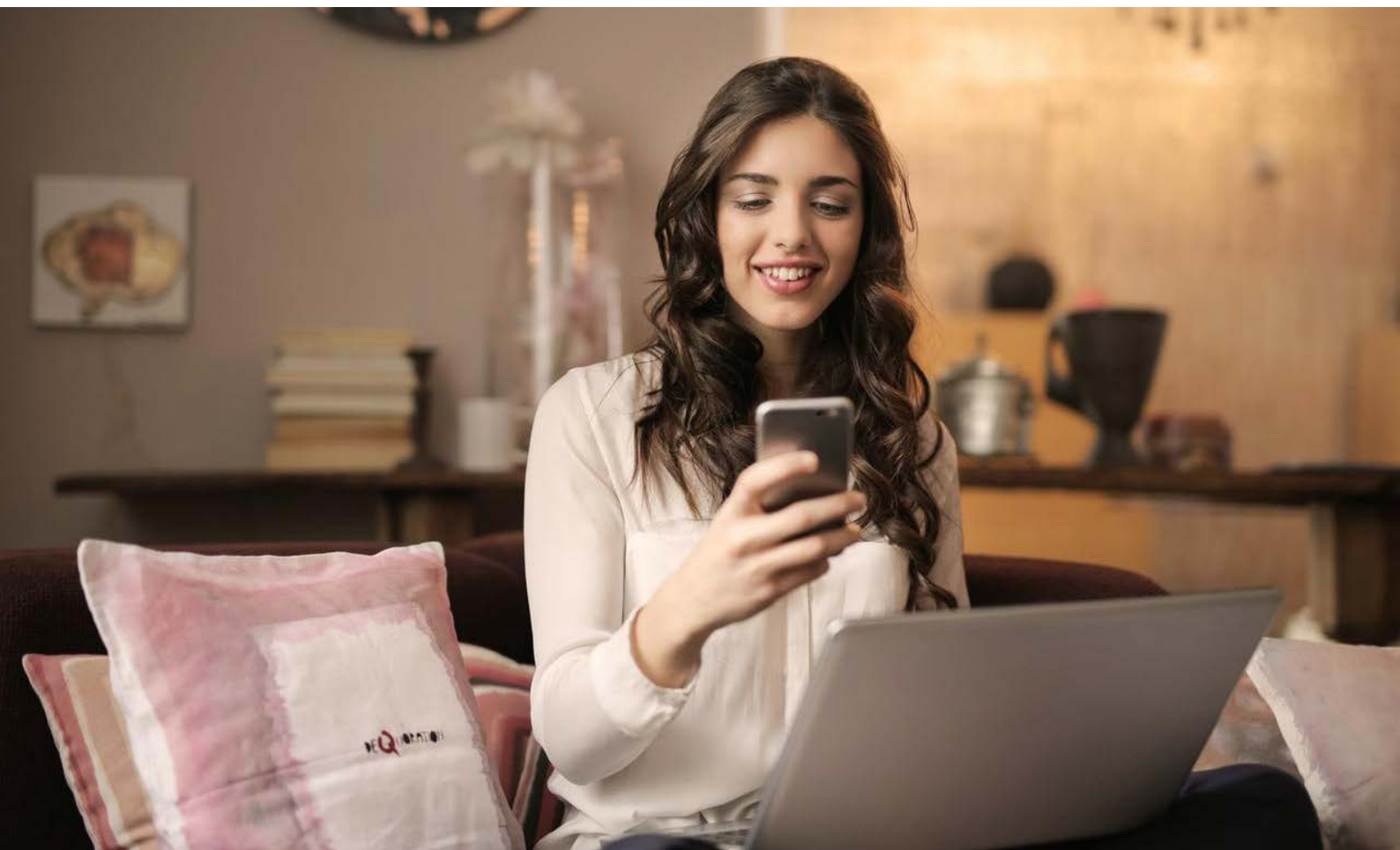
To combat the five types of fraud, the security industry advocates a three-layered approach for ID documents:



2. The digital domain: a target for fraudsters

While our world still has physical land boundaries between countries, the digital sphere enables global interaction that is less restrictive. It is, of course, more difficult to verify a person's identity online than face-to-face, which is why the digital environment is a target for fraudsters. They can request illegitimate social welfare, open a bank account using a fake ID (imposter scams), and even cross into a different country using a stolen passport. The list of abuse is endless.

The need to create an ID document that is relevant and verifiable both digitally and physically has led document producers to building new security concepts that are compatible with physical and digital environments.





IDEMIA
is committed
to creating
ID documents
that are hard
to reproduce,
yet easy
to inspect.

A truly robust security concept to create fraud-resistant ID documents

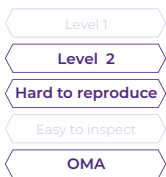
Aspects to be considered are:

- › **Document authentication** needs to be unambiguous using the detailed portrait
- › **Examination conditions** such as the type of lighting (daylight, artificial light or backlight), and the time available for document authentication
- › **The level of knowledge necessary** for the person inspecting the document (trained professionals or untrained civilians)
- › **Types of equipment needed** to inspect the document
- › Possibility of authenticating the document using **Optical Machine Authentication** (OMA)

IDEMIA's security concept consists of three main pillars:
PORTRAIT PROTECTION • DATA INTERLINKING • OPTICAL MACHINE AUTHENTICATION



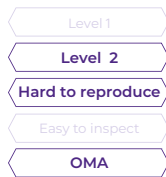
The next chapter focuses on how secondary portraits contribute to securing ID documents. Some features have been in use for many years, and those achieved using a classic inkjet printer or laser engraving personalization are more often subject to counterfeit and forgery. Therefore, we recommend new features that are more difficult to tamper with.



› **A solution specific to passports consists of creating a secondary portrait printed by a color inkjet printer on the paper data page** or the page facing the data page. The portrait has curvy lines made of letters and numbers that contain the bearer's personal data, such as the name and date of birth.

The letters and numbers vary in size within the curvy lines and are different for each document, and they can be used for OMA.

In order to be verified, this technology needs to be checked by a machine, which means that authentication with the naked eye is not feasible.

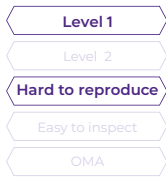


› **Perforated portrait including encoded data:** A laser can be used to perforate a portrait through the complete structure of the ID document. The portrait can bear a pattern at the bottom left or right-hand corner that contains personal data retrieved from the data page. This pattern can be read and compared to the pattern recalculated by software using the personal information found on the data page. This feature offers a visual element that can only be verified using an algorithm calculated by a machine.

2. Secondary portraits that combine personalization with other features on the document

Secondary portraits that allow unambiguous authentication with the naked eye are first choice and are very helpful for main portrait authentication. Optical effects such as movement and color variation are easy to verify without the use of tools.

2.1 Portrait engraved over an OVI® pattern



One example of a secondary image is a ghost image, which is engraved over an Optical Variable Ink pattern. Increased security is achieved due to the color-changing effect of the ink used for the ghost image. The portrait is quite low because of the limited shape and size of the printed pattern that the portrait must fit.



2.2 Using a lens structure to obtain a depth and relief effect

- Level 1
- Level 2
- Hard to reproduce
- Easy to inspect
- OMA



IDEMIA's Stereo Laser Image (SLI) is a portrait viewed from different angles using a lens structure to create an impression of movement when the document is tilted from left to right. Alphanumeric characters can also be engraved onto the forefront of the portrait to create a striking depth effect.

Once the SLI portrait has been verified, the examiner can confidently conclude that the main portrait is genuine.

2.3 Solutions with a window in the document

Secondary portraits can also be created in a transparent window.

- Level 1
- Level 2
- Hard to reproduce
- Easy to inspect
- OMA

› **Portrait personalized using a special ink:** The secondary portrait can be laser engraved below the surface of the document. A special ink that displays a gold aspect is used to personalize a negatively engraved secondary portrait that is complex to modify. When viewed in a transmitted light the portrait disappears and a pre-printed symbol appears that is also visible from the reverse side.

The details of the portrait are rather limited, lowering the efficiency of this feature and its authentication.

- Level 1
- Level 2
- Hard to reproduce
- Easy to inspect
- OMA

› **Portrait in a window using a specific material:** Transparent windows provide an increased level of security when combined with tamper-proof personalization and exclusive materials that are not readily available to the public. A new material that is compatible with laser engraving and has optical properties can be used to fill the window, which is located at the core of the credential. When examined under a light, the color of the inserted material varies depending on the brightness of the colored background. The color also varies depending on the light from a torch or UV lamp being shone through the window from the front or back of the document.



This feature offers a fair level of efficiency against counterfeiting and forgery both at level 1 and level 2.



- Level 1
- Level 2
- Hard to reproduce
- Easy to inspect
- OMA

› **Color portrait in a transparent window creating a relief and depth effect:** IDEMIA's LASINK™ is a laser engraving technology that generates secure high-quality color portraits on polycarbonate identity documents. Its distinctive linear pattern makes it instantly recognizable and adds an extra layer of security to the portrait. In addition to mastering polycarbonate laser engraving, fraudsters would also have to be able to forge the specific LASINK™ techniques—a feat that is almost impossible to achieve.

A LASINK™ color portrait combined with an SLI lens structure in a transparent window is an efficient fraud prevention method.

It is extremely difficult to create a LASINK color portrait, as its cyan, magenta and yellow color matrix is personalized by a perfectly registered laser engraving of the image. When a light is shone through the window, it creates a 3D effect, attracting the attention of anyone looking at the document. In this case, there is no need to be an expert to compare the secondary with the main portrait and/or the person claiming to be the legitimate bearer of the document in case of in-person ID verification.



2.4 Color portrait in a DOVID

- Level 1
- Level 2
- Hard to reproduce
- Easy to inspect
- OMA

Diffractive Optical Variable Image Devices (DOVID) are well-known security features that display eye-catching dynamic and kinetic effects. Grayscale laser engraving on DOVIDs has been done for many years.

It is now possible to laser engrave color images, allowing unambiguous authentication.

The portrait appears polychromatic when it is examined at a specific angle. At other angles, the secondary portrait appears in various monochromatic representations. The DOVID substrate can be located next to the main portrait to make comparison easier. It can also consist of a transparent section that partially overlaps the main portrait offering high-end optical security patterns (such as the ones supported by DID™) to enhance the security of the main portrait.



Key takeaways

The portrait is the strongest link between the ID credential and the person claiming to be the legitimate holder of the document. A growing number of situations require the authentication of ID documents, and it is critical to address this securely and conveniently for all use cases. The table opposite summarizes the positive aspects and limitations of the different solutions available on the market.

Secondary portraits with animation effects are most efficient in the combat against fraud. They can be easily authenticated by everyone, yet are hard to reproduce for fraudsters. Verifying the secondary portrait using OMA further facilitates authentication and adds an extra layer of security.

Security features that are hard to produce, yet easy to authenticate in all circumstances are key to providing robust ID credentials. Such credentials facilitate the person checking the ID (trained professionals and untrained civilians), both in face-to-face and online situations.



Properties and limitations of secondary portrait solutions

Feature		Rating (-) for weaknesses (0) fair (+) premium	Level 1	Level 2	Hard to reproduce	Easy to inspect by untrained people	OMA
Secondary portraits using personalization only	Portrait visible under grazing light	-	✓	-	✓	✓	-
	Portrait containing hidden data IPI™	0	-	✓	✓	✓	-
	Portrait of patterns calculated with bearer's data	-	-	✓	✓	-	✓
	Perforated portrait by laser with encoded data	-	-	✓	✓	-	✓
Secondary portraits that combine personalization with other features on the document	Portrait engraved over an OVI® pattern	-	✓	-	✓	-	-
	Portrait offering a depth and relief effect	+	✓	-	✓	✓	-
	Portrait engraved on a special ink in a window	0	✓	-	✓	-	-
	Solutions with a window Portrait engraved in an Optically Variable Material	0	✓	✓	✓	✓	-
	Color portrait with depth and relief effect in a transparent window	+	✓	✓	✓	✓	-
	Color portrait in a DOVID	+	✓	✓	✓	✓	-

Securing ID credentials

<https://www.idemia.com/id-security-features>



All rights reserved. Specifications and information subject to change without notice.
The products described in this document are subject to continuous development and improvement.
All trademarks and service marks referred to herein, whether registered or not in specific countries, are the property of their respective owners.

Join us on     

www.idemia.com