

The changing face of identity verification

As identity protection becomes ever more important in a digital world, how are authorities meeting the challenge of ID verification? Erik van Dijk, Product Manager for card body material and security features, sets the scene.



Eric Vernazobres / Morpho

What are the big trends today in ID verification?

What's clear is that authorities still rely on the manual inspection of documents that feature high-resolution printing, watermarks and other techniques to prove an ID is genuine. However, we are quickly moving to machine-assisted verification, such as the document readers in passport 'e-gates' at borders. We are also seeing research into the storage of ID on mobile phones, with driving licenses as an early candidate, and the development of techniques for sending a photo of an ID to remote databases to check its authenticity against records held on Cloud servers. This opens up the possibility of new use cases for identity verification, such as employers verifying the IDs of job applicants, car rental operators checking customers' ID and age, or hotels checking the ID documents of their guests. So, verification is person-to-person, albeit with some help from machines; but is moving to mobile-to-person and also machine-to-machine.



What is driving this market for machine-assisted verification?

Firstly, it's about improving the efficiency and reliability of verification – i.e. checking that the document is genuine, that it hasn't been altered and that the bearer is also the owner. Today, this is only carried out manually in very specific cases, and the people involved are specialists. For checks at any scale, technology is clearly the way forward - as we can see in air travel, for example. With passenger numbers set to rise from 3.7 billion in 2016 to 7.2 billion in 2035, it will be important to speed up passport control without being limited by the number of experts available to check documents. Technology makes verification possible to non-specialists – including users themselves - or to machines.

If that's the case, why isn't this technology more popular?

For a start, not every document has an RF chip – whether it's a passport, driving license or some other form of ID. Secondly, not every device can read a chip. A smartphone would need a kind of connectivity known as Near Field Communication to do that – but not all smartphones offer NFC and some that do, such as the Apple iPhone, will not communicate with the chip. Finally, the chip or its antenna can be damaged; in some cases, that damage is done deliberately by a counterfeiter as a way of defeating the security checks inside the chip and ensuring that any inspection is only manual.

What's been holding back mobile and remote inspection?

Clearly, the security features developed over the last 50 years – which we call 'look, feel and tilt' -- are not really fit for a smartphone or remote examination from a server. When you look at a document with a smartphone, colors change, you cannot hold or tilt the document, any infra-red or UV light properties are lost and you can't magnify it - as you are limited to the resolution of the photo. So, the challenge we face is to ensure that security features to prove that a document is genuine can evolve with the changing way we actually check ID documents.

What are the options for using smartphones to check legacy IDs?

It's a mixed picture. By using special filters and spectrum analysis, there are ways of detecting low-quality counterfeit IDs from a smartphone. But for high-quality counterfeits, it's a lot harder; you need to use a high-end camera and some prior knowledge of the document, in terms of its content and physical characteristics. An added problem is that when you point the smartphone camera at a document, the photo will be taken at an angle, however slight. This photo must then be checked against an electronic record of the document - which obviously has no angles. Clearly, authentication has to allow for these differences in order to make the right call - and this technology is still at the development stage. But as algorithms and smartphone cameras develop, the situation will improve.

What about taking a video, rather than a photo, of the ID?

In theory, it would be technically possible to check certain elements of the ID. But using video mode, so that it's in focus and showing the whole document, is actually quite difficult. And because that process of trying to video an ID card would not be a very user-friendly task, I reckon there is less chance of finishing up with a usable record of the document. You would need to be trained for this and, of course, that's what we don't want – as the aim is to have checks that can be carried out by non-specialists.

So how can we enhance IDs to make automatic verification easier with a smartphone?

There are three ways to do that without a chip, but each has its downside. Firstly, you could add a digital seal to a document in the form of a 2D barcode that would hold data and prove its authenticity. The drawback is that barcodes are not allowed on passport data pages, and they lack the storage to hold a facial photo. Another option, called 'fingerprinting' is to add a microscopic feature or mark to a document that will make it unique. This will tell you if an ID is genuine, but not if it has been altered – by changing the date of birth or the facial photo, for example. Finally, there is 'digital marking' where personal data can be inserted, invisibly, onto a photo portrait. The catch here is that it degrades the quality of the image, which then makes identification of the person more difficult. Overall, we are making progress on using technology to help us with ID verification. But there is still a way to go.

How is OT-Morpho looking to bring innovation to this area?

We are developing a new form of verification that can be used offline and online, and from your own device – whether it's a document reader or a mobile phone. It will initially cater for passports, driving licenses and ID cards, and will later be enhanced to verify the future mobile IDs. Privacy by Design will be a key feature.



Erik van Dijk, Product Manager for card body material and security features at Morpho