ID Optic-id.com

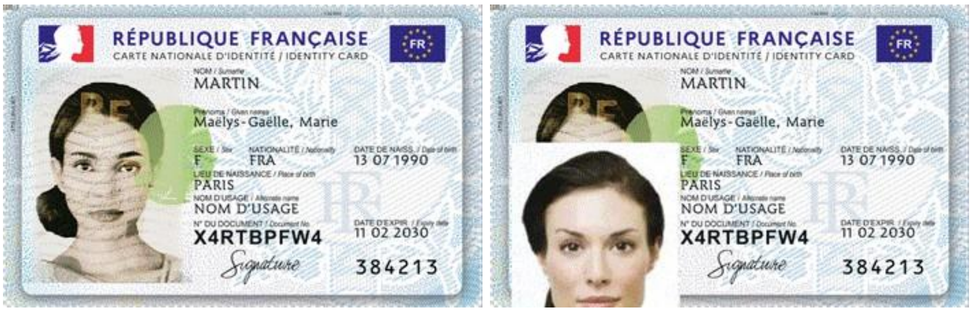
The essential evolution of identification procedures

I. The current procedures allow for identity theft.

To identify online, one only needs to send a video of an identity document and of his face to check that it looks like the photo on the document.

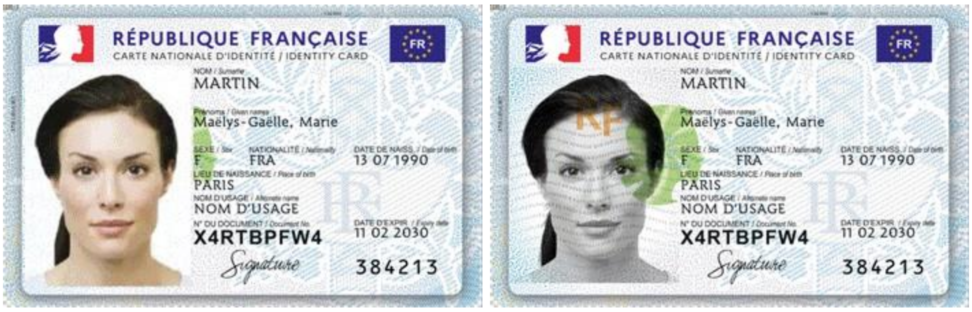
The verification of the document focuses on its known characteristics (layout, fonts, various details), but not on the photograph, which is the weak point. The comparison with the face of the person wishing to identify himself is therefore made with a photo that is not always that of the holder.

It is enough to photograph the identity card of a third party and replace the identity photo with an image editing software such as Photoshop,



RÉPUBLIQUE FRANÇAISE
CARTE NATIONALE D'IDENTITÉ / IDENTITY CARD
FR
NOM / Surname MARTIN
Prénoms / Given names Maëlys-Gaëlle, Marie
SEXE / Sex F
NATIONALITÉ / Nationality FRA
DATE DE NAISS. / Date of birth 13 07 1990
LIEU DE NAISSANCE / Place of birth PARIS
NOM D'USAGE / Alternate name NOM D'USAGE
N° DU DOCUMENT / Document No. X4RTBPFW4
DATE D'EXPIR. / Expiry date 11 02 2030
Signature
384213

and apply a layer simulating a hologram before printing the result on a sheet of paper with an office printer.



RÉPUBLIQUE FRANÇAISE
CARTE NATIONALE D'IDENTITÉ / IDENTITY CARD
FR
NOM / Surname MARTIN
Prénoms / Given names Maëlys-Gaëlle, Marie
SEXE / Sex F
NATIONALITÉ / Nationality FRA
DATE DE NAISS. / Date of birth 13 07 1990
LIEU DE NAISSANCE / Place of birth PARIS
NOM D'USAGE / Alternate name NOM D'USAGE
N° DU DOCUMENT / Document No. X4RTBPFW4
DATE D'EXPIR. / Expiry date 11 02 2030
Signature
384213

It is this document that is then presented to his Smartphone to identify someone.

Photos of authentic documents can be found on the *darkweb*, but it is also possible to carry out bulk operations using the database of remote identification service companies, since many of them keep photos of verified identity documents.

II. The consequences of identity theft are very serious

In France, a unique identification method (FranceConnect) provides access to many sensitive sites: income tax declaration, passport and national identity card application, change of address, health coverage, declaration of transfer of a vehicle, application for a certificate of registration of a used vehicle, declaration of retirement, declaration of a birth, declaration relating to work and social rights, local life, energy, housing, etc.

A fraudulent identification alone is therefore sufficient to carry out a large number of operations which can have very serious consequences for the person whose identity has been usurped.

III. To date, there are no regulations in many European countries

A. In France, the ANSSI's "Référentiel PVID" only requires a video

This document (available at https://www.ssi.gouv.fr/uploads/2021/03/anssi-referentiel_exigences-pvid-v1.1.pdf) only requires the acquisition of a video, without specifying how it should be taken. To date, only one PVID has obtained certification from ANSSI, the Parisian company UBBLE.

The world leaders, who operate in France, do not even seek this certification.
They only ask for photographs of identity documents, even easier to falsify than a video, and their clients are many major French banks.

B. The authentication of a hologram with the naked eye is almost impossible.

Authenticating a hologram consists of verifying that its appearance from a certain point of view and under certain lighting conditions is what is expected, and also verifying that this appearance changes when one changes point of view or lighting conditions.

Since the appearance of a hologram depends on the position of the light source, simply looking at the hologram without knowing the precise position of the light sources does not enabling a proper authentication. Therefore, a hologram cannot be authenticated in ambient light.

Artificial intelligence can be used with a machine learning algorithm trained using a dataset containing both images of authentic holograms and images of counterfeit holograms to enable it to learn to identify the distinctive features of authentic holograms, but again, it would be necessary to ensure that the acquisitions made during the authentication procedure have been made from a point of view and in lighting conditions similar to those of the images used for training the algorithm, which is impossible.

IV. The urgency is to make an effective procedure mandatory

A. The arrival of digital identity creates urgency

The current situation, which makes it all too easy to steel identities, engages the responsibility of the states, as well as that of all public and private companies that are satisfied with inefficient identification procedures.

The upcoming arrival of the future digital identity application creates urgency, because it will provide proof of identity, justify its majority, give a power of attorney, and connect to all services requiring identification.

eIDAS is set up to organize "secure electronic interactions" between the population, companies and administrations, but as it stands, it seems to be moving towards the exclusive use of NFC chips, which does not seem viable since many smartphones do not have NFC near-field communication capability, and that the NFC chip reading of many identity documents will not be allowed to individuals.

The visual authentication of printed or digital documents (presented on the screen of the Smartphone) will therefore remain for a long time as a major means of identification.

B. Verification of holograms is essential

The authenticity of the content of a printed or electronic document may be guaranteed by a visible electronic seal. In many cases, however, it is necessary to ensure that the original document is being dealt with. The authentication of optical security devices that cannot be reproduced by photographic means, such as holograms, is therefore essential.

It is for this reason that the identity documents of all countries include optical security devices, usually one or more holograms, and it is unreasonable not to verify them during remote identification.

The only tool available is the Smartphone, and it is very effective for verifying a hologram, because it allows you to verify that the appearance of the hologram from a given point of view and in given lighting conditions corresponds to what it should be, which the best trained human eye cannot do.

C. Gendarmes and police must have the means to authenticate identity documents

Mr. Julien Retailleau, head of department at the French Gendarmerie, explains that out of 100,000 gendarmes, only 600 had been trained in the authentication of identity documents, or zero comma six percent. M. Gilles Colas, a director and nalyst in document and identity fraud within the DEFDI of the Ministry of the Interior, announces that less than 4,000 police officers, *including "a good proportion at the #DCPAF for border control",* have received such training.

A very simple method can allow law enforcement to verify in seconds all the identity documents presented to them, with a smartphone application that automatically performs:

- **a first photographic acquisition to verify that the appearance of the hologram from a point of view corresponds to what it should be,**
- **and a second acquisition from a different point of view or in a different light to verify that the appearance has changed.**

Known methods allow a smartphone application to calculate the effect of flash lighting alone, by subtracting an image taken in ambient light without flash from an image also taken in ambient light but with flash. The comparison is then made with an image under the sole illumination of the flash. Such an image can also be acquired in the dark or calculated from the characteristics of the hologram.

D. Verification of holograms must become mandatory

To allow remote access to public services, the regulation must require the provider to authenticate holograms with this method.

Some verifiers use artificial intelligence to train algorithms to recognize holograms, but if this training is done without taking into account point of view and illuminance conditions, which is essential to compare the appearance of the hologram analyzed with that of the original under the same conditions, it is obviously without any interest.

Others simply check that the appearance of a document changes when the point of view or lighting is changed. This is not a reliable method because it does not make it possible to verify that the hologram is consistent with the original, that is to say that it has since a given point of view and under a given lighting the appearance that the original presents under the same conditions.

Latest publications:

- What future for identity businesses?
- Hologram authentication - the good practices

En français

- L'évolution indispensable des procédures d'identification
- Quel avenir pour les métiers de l'identité ?
- Authentification des hologrammes - les bonnes pratiques

28 avril 2023
Franck Guigan
f.guigan@optic-id.com
+33 6 14 63 93 36