What future for identity businesses?

I. The two upheavals to come

A. Digital identity

The future digital identity application announced by the European Commission aims to create a secure, interoperable and user-friendly online identification system for EU citizens, allowing them to access online services across the EU with a single login, eliminating the need to create and manage multiple user accounts for different online services.

In particular, it will make it possible to provide proof of identity, to justify one's majority, to give power of attorney, and to connect to a very large number of public or private services. The same thinking is under way in other parts of the world.

As it stands, many seem to be moving towards the exclusive use of NFC chips, although the chips of many identity documents are not allowed to read by individuals and many smartphones do not have near-field communication capability.

Consultations are ongoing, but the future remains uncertain, as many challenges are to be expected relating to the safety of operations and the establishment of a system that operates worldwide.

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

B. Quantum computing

Quantum computers, if cryptography systems are not improved in time to adapt to the post-quantum world, will be able to access critical data from states, companies and individuals by breaking all passwords.

The hackers' strategy known as *"SNDL - Steal Now Decrypt Later",* which involves downloading encrypted data knowing that they will only be able to read it when quantum computing algorithms allow its decryption is already underway. It will cause a lot of damage that could prove fatal in the field of identity, especially since it could well be foreign states attacking our identity systems to disrupt our entire economic, administrative and social life at once.

Democratic countries must organize now so that their identity systems can withstand the attacks that will one day be enabled by quantum computers. We can therefore already foresee that they will gradually switch to means of identification using neither encryption nor passwords.

II. The consequences for issuers of means of identification

Chips of passports and identity cards, payment cards and other documents will become vulnerable to quantum computing, and printed or digital versions of these documents will no longer be well protected by industrial devices repeated in number that are too easy to simulate by future computing. It will be the end of holograms, embossing, watermarks, optical graphics, microtexts, color change effects and other means that are predictable by software.

The solution is probably the reading of a PUF *"Physically Unclonable Function"* according to an unpredictable procedure. A PUF is difficult to clone or reproduce because it is a unique and irreversible characteristic of a physical object, such as the variation in its properties depending on how it is observed. A person or computer that is asked to examine a PUF in different randomly selected ways at the last moment cannot predict the result to be transmitted.

PUFs can be unique in their optical characteristics, such as metallic paint, varnish with randomly distributed glitter, color-changing ink mixing of different characteristics, sandblast frosting on a glossy surface, bubble code, and many other techniques. They are easy to analyze by any smartphone with a camera.

They can also be unique by their electrical and/or magnetic characteristics, and be included in any computer, identity card or payment card, and more generally in any object equipped with an electronic means of measurement.

III. The consequences for identity verifiers

While the best identity verification companies will continue their operations successfully and maintain their long-term leadership, some of them who thought this business was an Eldorado but did not perform a high-quality service will be affected by the change.

Many identity service providers only check the known characteristics (layout, fonts, various graphic details) of the documents presented without authenticating the hologram affixed to an ID photograph, whereas it is easy to check that the aspects of the hologram from two different points of view corresponds to those of the original from the considered points of view. Others do not compare what they see with the description of the original hologram. In both cases, their “selfie” compares the face of the person seeking to be identified with a photo that may have been replaced by that of a fraudster.

Some think to compensate for these failures by using artificial intelligence to carry out these checks, which is of no interest since simple algorithms are more efficient to verify known characteristics, and others seek to enhance their image by talking about blockchain which is also irrelevant. Many identity verifiers will therefore arrive weakened by the announced changes.

Identity verifiers will lose their document verification activity, which will be replaced by very simple procedures for reading and transmitting data according to an unpredictable scenario transmitted in real time.

The disadvantages of identification by morphological features could also cause them to lose their activity of morphological verification by "selfie". These known disadvantages are the risks to personal data, and the impossibility of replacing a corrupted feature with a new one (to take an example, a fingerprint fraudulently used by a third party can never again be used by its legitimate holder). In this area too, the solution could well be hardware keys such as PUFs that have the advantage of being easily repudiated and replaced.

The identity verifiers who will survive these upheavals are those who will have taken into account in good time the announced changes, and acquired solid strategic positions in niches by having enriched their identification services with other functions such as access control, payment, electronic signature, online and face-to-face voting, access control to intranets, social sites and multimedia services, verification of regulatory compliance of transactions undertaken, or for example additional checks such as address, employment or income status, credit history, criminal history, and others relevant references for the operations envisaged.

April 19 2023
Franck Guigan
f.guigan@optic-id.com
+33 6 14 63 93 36

Latest publications:

- The essential evolution of identification procedures
- 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