IDEMIA

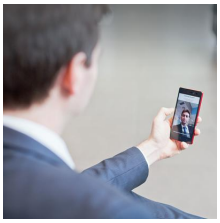
Look! No PIN!

Blog post 2/3 - By Philippe Le Pape, identity and security expert, VP Partnerships and Presales within the Digital Security and Authentication Division of Safran Identity & Security (formerly known as Morpho).

IDENTITY

POSTED ON 06.30.16

When discussing **two-factor authentication**, we touched on what makes for **strong authentication**: something that the user knows, something the user possesses, or something inseparable from the user. We could redefine 'something inseparable from the user' as 'something you are', as the human body provides numerous excellent ways for identifying an individual. Fingerprints, for example, have been used by police agencies around the world as a method of identifying suspect criminals since the end of the nineteenth century.



Biometric authentication uses physiological identifiers (e.g. fingerprints, facial recognition or iris scans) to confirm an individual's identity. As such, a biometric system is essentially a pattern recognition system; an individual's biometric data is verified against a previously stored example of that individual's template. Fundamentally, biometrics provide the only way to link an individual's physical identity to their digital identity.

A typical biometric system contains five main components: a sensor to capture and digitize data, signal processing algorithms that form the biometric template, a data storage unit, a matching algorithm that compares new templates to those previously recorded and stored, and a decision process that uses the results of the matching algorithm to accept or reject a new individual.

The type of **biometric authentication** used is determined by the target application, including the sensitivity and risk associated with the digital secured transaction. Data privacy management is even more crucial where user authentication takes place in the cloud. Any biometric system, especially one that involves a component of interconnectivity, must be very carefully designed to prevent the loss or interception of user **biometric data**. Typically, systems incorporate cryptographic safeguards to prevent the interception of biometric data while it is being communicated. Similarly, where a biometric template is stored on a device, it is protected by cryptographic and encryption tools.

Identification based on biometric characteristics is superior to traditional passwords and PIN based methods in several key ways:

1. Ease of use:

- Identification based on biometric techniques obviates the need to remember a password or carry a token. Moreover, the software and hardware are designed for ease-of-use; even in lighting conditions where mobile screens are hard to read biometric techniques are easier to use than entering traditional passwords.

- Biometric technology gives accurate results with minimal invasiveness; typically a simple scan or a photograph is usually all that's required.
- Biometric identification is extremely quick, which is another advantage over other traditional passwords, especially on mobile devices with small keypads.

2. Increased security:

- Personal characteristics, such as **fingerprints** and **iris scans**, provide unique and accurate identification methods. These features cannot be easily duplicated, nor directly exploited to steal identity, which means a high level of security and only the authorized person gets access...

Biometrics has evolved from niche military applications, to broadly used criminal justice applications and, more recently, as a widely used civil identity solution. Today, biometric data is already used to manage and protect the unique identity of individuals and fight against fraud. As an example, in the UK, Safran is supporting the government's new GOV.UK Verify program, which provides a way for citizens to prove who they are online so that they can safely and securely access a range of digital government services, such as renewing driver licenses or filing taxes. (Ref. 6) Identity verification is linked to different Levels of Assurance according to the kind of information provided by the applicant. The highest level of assurance (Level 4) is subjected to specific processes, including the use of Biometrics, to further protect the identity from impersonation or fabrication.

A similar scheme – Idensys – is being piloted in the Netherlands.

We'll conclude this series with the following article **The Mobile-powered Planet (3/3)**, by looking at how mobile technology can provide a solution for civilian identity problems and the role of R&D as we move into the future.