

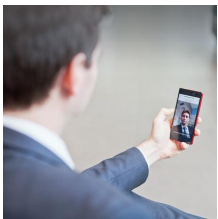
Securing our digital identities on our smartphones through biometrics

By Anne Bouverot, CEO, Safran Identity & Security

IDENTITY

POSTED ON 09.27.16

Recent studies show that people consult their smartphones up to 220 times per day, and are doing so more and more. **Mobility** is forever changing our online behaviors and with that, our **online identities**. As consumers we must prove who we are on a daily basis, and more and more digitally. Before we just needed credentials to access online services, but today we must link our digital selves to our physical selves.



As digital consumers we all want **frictionless experiences**, especially where **security** is involved. Yet current standards of **fighting fraud and identity theft** – such as complex passwords – remain a source of friction. Passwords may not be dead, but they have shown their limits. And there is one thing they can't offer which biometrics can – a unique and proven link between our digital credentials and physical attributes.

Biometrics is also "**privacy by design**", meaning that solutions are designed to inherently protect user privacy. Today's mobile security architectures provide a proven means to protect user data. Backed by organizations like FIDO (Fast Identity Online), the industry is specifying open and interoperable mechanisms to **reduce the reliance on passwords** to authenticate users.

Whereas once biometrics was considered intrusive, more convenient technologies are readily available. User acceptance is now becoming the norm, thanks to the use of fingerprint access to smartphones/tablets and the wide use of photos/videos online. Contactless technologies are growing, which are faster and more hygienic. And costs are going down, due to the wide availability of smartphones and affordable methods of biometric capture.

This unique combination of security and ease of use has enabled biometrics to become a technology of choice for both digital security and identity.

Fingerprint recognition is still leading the market, thanks to the introduction of sensors like TouchID which have truly democratized their usage. Yet as the need grows for more secure and confidential transactions, we need higher accuracy solutions and more universal methods which forego the need of a sensor.

The next step in biometrics for mobile is **facial recognition**, which has made staggering advances in recent years in terms of accuracy. Half of the world's population owns a phone with a camera, and now can gain access to the "**selfie-check**", the next wave in biometric authentication. Combined with facial recognition, the ubiquitous selfie now has a new purpose – protecting our digital identities! The most important factor in facial recognition is that it must be able to distinguish between a real person and a photo placed in front of the camera. This is where liveness detection comes into play, which ensures that the selfie is indeed a "live" picture.

In short, biometrics is a proven technology to seamlessly secure our digital transactions and identities. And the market needs those solutions now: as consumers we will soon store more on our smartphones and tablets than we ever did in our wallets, our bank accounts, or even our PCs.

Protecting those credentials and data is now possible, in just a snap.