Biometrics on smartphones: stayin' alive

To protect consumers from hacking and online identity fraud, Morpho is once again raising the bar in biometric identification through liveness detection, which ensures the authentication of real persons, weeding out false fingerprints, photos or other artificial data.

 # PAYMENT
 # CONNECTIVITY
 # ACCESS CONTROL
 # IDENTITY

POSTED ON 05.03.16

Biometrics is quickly becoming the most practical and safe method to authenticate someone. It uniquely combines security and convenience of use for linking a user's unique identity to their smartphones and tablets. The phenomenon began with fingerprint recognition, made popular by Apple's TouchID, and is now opening up to other biometrics, such as facial recognition which is quickly developing on the mobile market. Both fingerprint and facial recognition are also key authentication technologies for sensitive of applications such as access control, payment authorization or border control.

To prevent biometric systems from becoming hacking targets using false biometric samples such as a photo of someone's face or a fake finger, Morpho is developing new methods of capture which integrate liveness detection. The ability to recognize a living and breathing person considerably strengthens the security and reliability of a biometric system. Morpho has been developing such technologies for several years now.

As early as 2013, Morpho was the first in the industry to certify its fake finger detection technology, capable of measuring the specific characteristics of real human skin.

Morpho is now innovating to support the rollout of facial recognition in commercial applications by **integrating liveness detection into its facial recognition technology**.

When installed on a smartphone, for example, a simple "selfie-check" enables users to verify their identities quickly and, of course, securely. Liveness detection ensures that the selfie-check is actually made by a live user, and not by using a photograph.

How does it work? To authenticate someone, the algorithms verify that the selfie taken by the user corresponds to the biometrics already registered into the smartphone. To do so, the user must move slightly his face in front of the camera, so that the technology can reconstruct a 3D form of the user's face. Morpho CEO Anne Bouverot recently demonstrated this technology during a keynote at the 2016 Mobile World Congress in Barcelona.

For highly critical applications, this new technology provides significant upgrades in security when combined with other biometric authentication factors such as "what the user owns" (e.g. a security token) and "what the user knows"

(e.g. a PIN code).