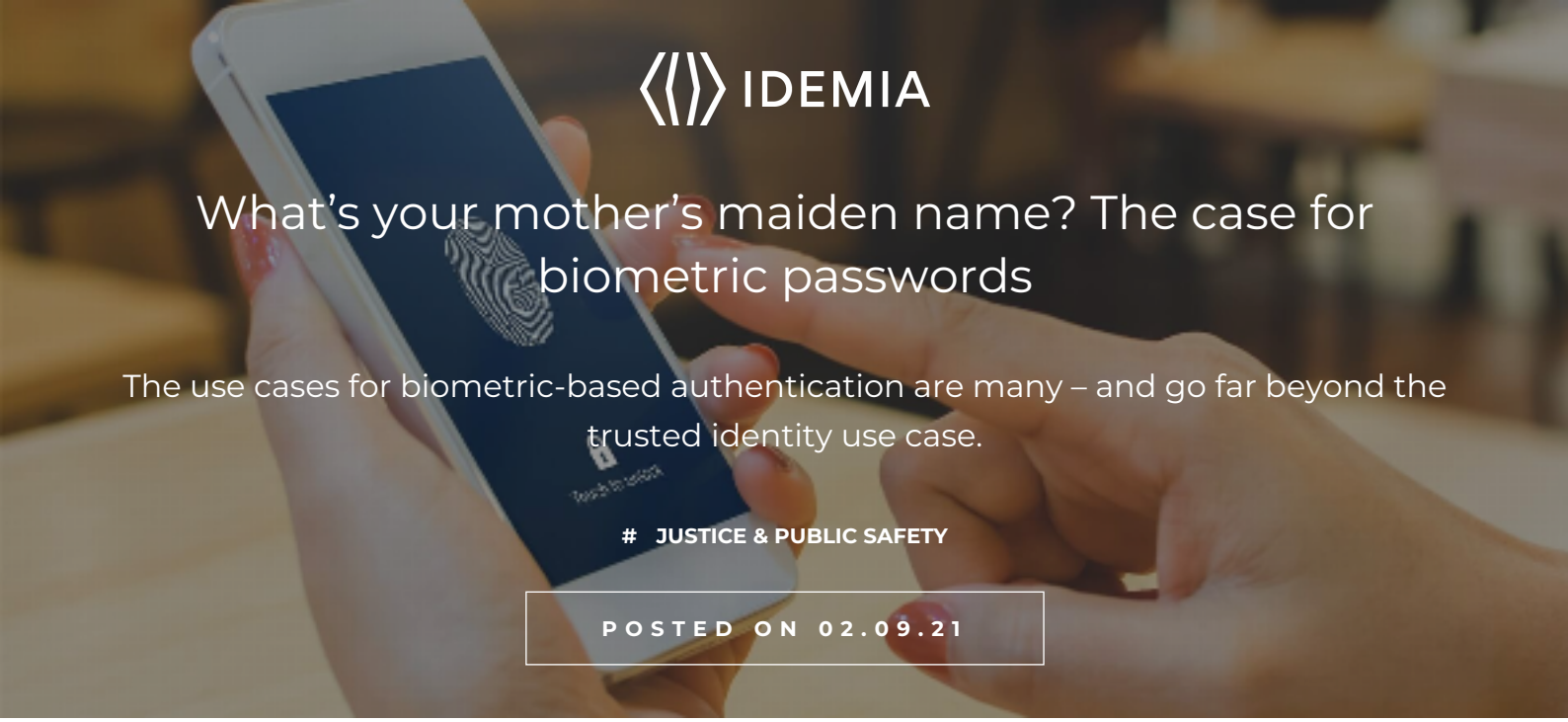
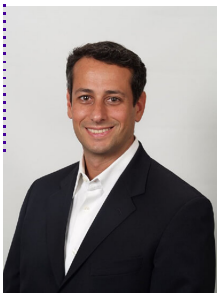


What's your mother's maiden name? The case for biometric passwords

The use cases for biometric-based authentication are many – and go far beyond the trusted identity use case.

 # JUSTICE & PUBLIC SAFETY

POSTED ON 02.09.21



The use cases for biometric-based authentication are many – and go far beyond the trusted identity use case.

Alejandro Lopresti, NORAM Regional Sales Director, IDEMIA

Biometrics: universal, unique, and immutable

In recent years, biometrics have been increasingly praised as a superior authentication solution to passwords – relying on the biological characteristics of an individual to verify their identity rather than on something that the user must remember.

Biometrics can be defined by three main characteristics:

1. **They are universal**: everyone possesses biometric data
2. **They are unique**: biometrics are unique to every individual – even in cases where people are nearly identical (including twins)
3. **They are immutable**: biometrics remain largely stable throughout one's life

Advantages of biometrics in authentication

Under current circumstances, digital tools participate in almost everything we do, from buying groceries online to studying and find entertainment or continue working. Today, biometric authentication is used in a variety of ways: from logging into phones or computers, to accessing sensitive data – and even to pay for groceries. In addition, in today's context where more and more people are performing sensitive transactions online, the security risks for sensitive transactions have intensified. With cybercriminal risks constantly looming, the need for secure authentication has never been higher.

Biometrics offer a number of advantages to increase the authentication security level:

1. **They are virtually impossible to lose**

2. **They are difficult to replicate**
3. **They are easy to use**

Depending on the sensitivity of a transaction, many organizations bump the security up one level higher – using multi-factor authentication methods to verify a customer's identity.

Using biometrics to verify someone's identity

During the "Document-Centric, Real-World Identity Proofing" process, a user captures an image or video snippet of their passport, driver's license or other government-issued ID via their webcam or, more typically, via their smartphone camera. This process allows to verify if the eID document is legitimate and has not been doctored or forged in any way.

Next, the photo on the document is compared with a "**selfie**" (still photo or short video) taken by the same individual. This process, also commonly referred to as "**liveness detection**," is a test to ensure that the person is physically present, and is not using a mask, photo or video. Convolutional Neural Network (CNN) deep learning algorithms are able to detect whether the selfie is a real selfie, at which point it performs face matching between the selfie and the picture on the ID document.

In doing this, service providers not only learn if the ID document is legitimate and the selfie matches the person on the document – they learn if the person is actually physically present and intentionally performing a transaction. On the other hand, users benefit from a seamless experience, with effortless usability, while protecting themselves against fraud.

The use cases for biometric-based authentication are many – and go far beyond the trusted identity use case. Biometric-based authentication can provide a means to freeze accounts, or send alerts to a user when suspicious activity is detected.

In the next (and last) article of this short series, I will go into where the use cases for biometrics are headed – and what it will mean for us as consumers.