

How do biometric identifiers measure up?

By [Henrik Nilsson](#)

24 Dec 2018

Strong customer authentication using biometrics is now part of the day-to-day. From 'selfie' authentication to voice recognition, fingerprint through to iris, our bodies have a range of unique 'modalities' that can be measured, each with benefits and drawbacks as authentication methods.



Henrik Nilsson, product manager at Fingerprints

In the age of open banking and rising demands for more secure customer authentication methods, biometrics is cementing its place in the payment world. But for biometric-secured solutions to succeed in the world of financial services, getting the right balance of high security and consumer convenience is essential. So, will fingerprints continue to dominate for payments?

At least our fingerprints won't age!

Fingerprint authentication is the analysis of the ridges and patterns of the skin on our fingertips. Fingerprints are highly unique to each individual and easily collectable. Unlike other identifiers, which can be prone to change through environmental factors, illness or aging, fingerprints are permanent throughout a person's lifespan.

Easily distinguishable and hard to duplicate, fingerprint authentication has comparatively low false-acceptance (accepting the wrong biometric data) and false-rejection (rejecting the right biometric data) rates. Other biometric identifiers such as face, voice and gait are more difficult to measure and can be prone to change, increasing rejection rates.

Efficiency, efficiency, efficiency

While other physical authentication factors such as eye (iris), vein and DNA are the most secure, the technological requirements far exceed those of fingerprint biometrics, needing more complex and expensive systems that will not work in payment cards, wearables and USB dongles.

The sensors required to scan vascular patterns, for example, can be large, expensive and require a lot of power, making processing requirements high and integration into smaller devices difficult. Similarly, the camera and software required to examine a face, or iris, cannot be fitted into small and limited processing powered devices like a card or wearable, and can also be costlier. Fingerprint sensors, on the other hand, are relatively small, cost and power efficient, making them much easier to integrate into a range of payment form factors.

Consumer convenience is key

To realise mass adoption of any technology, convenience and a positive UX is essential. Examining an eye, for example, can feel intrusive and a bit awkward, but is better suited for use cases where a touchless experience is wanted for instance on devices and in situations where many persons should be authenticated. Fingerprint authentication, on the other hand, is much more discreet and non-invasive, requiring a simple touch and can feel more 'private' and discreet for the user.

Similarly, the matching process of vein patterns takes considerably longer than fingerprint sensors that, having benefitted from years of R&D in the mobile world, can now be read and authenticated in under a second, in some cases like on the smartphone, even in a fraction of a second. This success in the smartphone world has also created consumer trust and familiarity in fingerprint authentication, providing the perfect platform for its wider adoption in the payment world.

Fingerprint on the pulse – what's next?

It is clear that fingerprint sits at the nexus of security and convenience, and can deliver the unified UX that is needed for effective payment authentication. Combining uniqueness and high security with simplicity, scalability and ease of use its success in securing mobile payments and mobile banking apps is just the beginning. Fingerprint sensors are easy to integrate into a multiple of form factors – not only because of their size, but the huge advances we've seen in their power efficiency and flexibility.

With trials ongoing across the globe, the biometric payment card is likely to be the next big fingerprint-secured solution to revolutionize the payments world. But the potential is limitless – from wearables to USB dongles – biometric security will soon be unifying the way we pay, all with a touch.

ABOUT THE AUTHOR

Henrik Nilsson is product manager at Fingerprints

For more, visit: <https://www.bizcommunity.com>