Biometrics – why the magic is in the software

When thinking of 'biometric authentication', what image comes into your mind? For most of you it will be a touch of a fingerprint sensor or a scan of your iris. Because of the way we, as humans, interact with the world around us, it is very easy to focus in on just the physical, the hardware, the biometric sensor.

But when we peek behind the magician's cloth, we are often surprised by what we find. As such, let's not overlook the software 'powering' biometric authentication.

The magic touch

The success of any technology hinges on the value it offers and its performance. No value? People won't use it. Poor performance? People will try it, before rejecting it.

Achieving this combination of value and performance when optimizing biometric solutions is only possible, however, when the whole solution is considered; hardware and software working in harmony. Of course, hardware design is fundamental to success, but the software is often where the real refinement – or rather, 'the magic' happens.

The extensive R&D poured into the development of fingerprint sensors in mobile phones is the perfect illustration of the value software has in driving mass adoption.

Making consumer concerns…disappear!

Speed, convenience, security, fraud prevention – the quality of the software is the difference between tap&go and tap&slow. It's all about the best UX with the lowest false rejection/highest acceptance rates possible.

Getting the right balance finds the sweet-spot by capturing the best image with the smallest sensor in the fastest time using the lowest power.

Much of the software's work focuses on optimizing image capture, when we boil it down. This is key to realizing the best UX: enabling consumers to touch at any angle, minimizing false rejections and crucially, nearly eliminating the chance of false acceptance.

But this is not a passive process and much has been done to make the software work so that issuers and consumers don't have to.

Pulling the rabbit out of the hat

Better quality software can reduce the processing power and memory that is needed on the device, reducing touch times dramatically. The best software, right now, is even allowing smaller sensors to be made, cutting the cost of solutions and giving device makers more flexibility for design and integration.

The software can also keep the sensor in standby mode, so it is ready to go whenever it is needed. It can also expedite the enrollment process by only needing a few images, to complete set-up, before learning something new each time the user authenticates. We also can't expect users to interact with the sensor the same way each time, and the software is what ensures a fingerprint sensor, for example, can be touched from any angle both at first enroll and for everyday use.

So next time you authenticate, think about the marriage of hardware and software that is working hard to get rid of PINs and passwords to make life simpler, quicker and more secure.