

INTERVIEW



According to Andrew Bud, CEO of iProov, 2019 has been a period of inflection points and rapid growth for the company. With many recent highlights, we spoke to Andrew to find out what the future holds for iProov and the wider biometrics industry...

What challenges are organisations facing today that you feel biometrics can help to solve?

Whether as consumers or as employees, users no longer expect to have to interact with a service in person. Whether it's setting up a bank account or accessing health records, we expect to undertake these tasks digitally, sat at home on our own sofas, without being compelled to engage in an in-person interaction. Shorter attention spans and broader expectations of digital inclusion both demand quick, simple and easy interactions. However, while remote digital service is convenient for the end-user, it creates risk for the organisation. Traditional authentication methods such as passwords, security questions etc can be easily lost, stolen or forgotten. Businesses are under pressure to assure their own cyber-security, comply with regulatory standards and create trust between themselves and their users.

Good biometric solutions create a safe digital environment. Biometrics remove the risk of forgetting or losing login credentials, allowing users to assert their identity with something only they have and can never be separated from. Increasingly, businesses are adopting biometrics to offer the best, most effortless journey for the end-user, whilst meeting high standards of cyber-security.

What do you feel the most exciting innovation is for biometric technology at the moment?

We're very excited by the potential of contactless palm biometrics, a modality that is new to the

market. They have some great advantages. For example, palms are an anonymous biometric - you can't identify someone just by seeing their palm - and therefore great for applications where privacy is paramount.

Historically however, palm authentication required costly, specialist hardware and hence its field of application was rather limited. So this year we launched iProov Palm Verifier, the world's first contactless, device-independent palm authentication solution, protected by iProov's Flashmark Genuine Presence Assurance.

How important is liveness detection for authentication solutions using biometric technology?

Genuine presence assurance is absolutely crucial to biometric authentication - in fact we believe that it is the core value of unsupervised biometric authentication. Biometrics are not passwords - they aren't really secret. Their value lies in the uniqueness of the genuine article, so that is what must be assured. It's important to carefully define "liveness detection": does it refer to liveness as opposed to inanimacy, the attack mounted by physical artefacts like masks, otherwise known as PAD? Does it refer to liveness rather than recorded or synthetic imagery, providing what we call Real-time Detection (RTD)? Or does it contrast with deadness, a requirement we encounter from time to time and have a few problems certifying? All these

defences must be in place to assure genuine presence. Without genuine presence, there can be no security. Of course, in supervised environments, like airports, the risk is much lower: the use of screen images or image injection into hardware is less of a threat.

Replay attacks have until now been an underestimated threat. The injection of recorded or deepfake synthetic video directly into the app datastream represents a real and scaleable threat. The emerging generation of low-cost, low skill deepfake generation apps just makes this clearer.

What is your view of how biometrics can support the increased usage of digital identity and the importance of protecting it?

Clearly there are many challenges in the creation, acceptance and business modelling of digital identities. But strong authentication lies at the heart of any digital identity system, whether centralised, federated or self-sovereign. All these systems require the user to prove their right to assert their identity attributes. So we partner with digital identity providers across the world and across the ecosystem. A user may have many digital identities - but they all belong to one person, who has one set of biometrics that cannot be shared, lost, copied or stolen...if genuine presence is assured. That's why we see that the assurance of genuine presence lies at the very heart of the whole digital identity ecosystem.

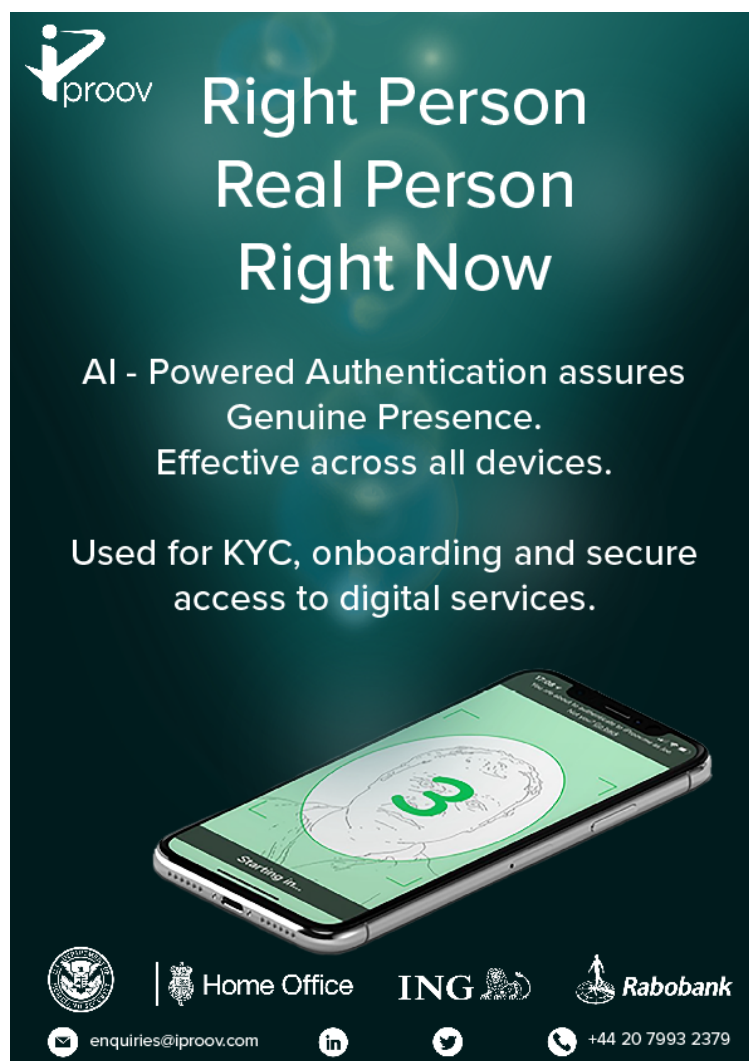
How, in your opinion, can new technologies and regulations support authentication and satisfy the greater demand for security and trust?

Firstly, regulation must recognise that, thanks to advances in deep learning, biometrics now outperform people, so that regulations requiring human engagement in identity verification or authentication are obsolete and indeed retrograde. Naturally, the performance of biometric systems must be measured to confirm that they are up to the job. At iProov we use trusted auditors, like the National Physical Laboratory, to review our own thorough and extensive attack testing and performance results, to confirm their thoroughness, coverage and integrity. This is the way many security standards are

constructed, and the way we think regulation will go. In future, we expect to see auditors review our processes for responding to new attacks, since incident response is a crucial part of any cybersecurity system. Clearly privacy must also be protected, but as long as we are covered by the GDPR, or an equivalent regulation, there is more than adequate protection for users and for data controllers.

For those looking to deploy biometric technology what would you advise them to consider?

There are three key questions that need to be thoroughly considered: (1) Is the solution usable? (2) Is the solution device independent? (3) Can the vendor assure that the remote user is genuinely present at the point of the transaction? Above all, you must be sure that your user is the right person, a real person, and that they are genuinely present right now.






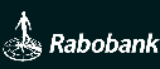
iProov





Right Person Real Person Right Now

AI - Powered Authentication assures Genuine Presence.
Effective across all devices.

Used for KYC, onboarding and secure access to digital services.



 Home Office  

 enquiries@iproov.com    +44 20 7993 2379