Biometric Authentication and The End of Passwords

*Biometrics is a proven identity authentication technology that is rapidly being adopted by states and the federal government for employees and constituents. In this Q&A, **John Fanguy**, federal sales director for iProov, addresses a variety of concerns that arise around biometrics and explains how the right solution strengthens security, improves the user experience and reduces operational costs.*

What's driving the increased usage of biometrics?

Individuals are becoming more comfortable with applying for things like driver's licenses and unemployment benefits online. At the same time, they see that passwords are not a very good solution because most breaches involve passwords. People are also becoming more comfortable with using biometrics to authenticate for basic things. Over 75% of U.S. consumers have used some biometric credential, even if it's a face ID on a phone.

And governments see biometric solutions quickly and successfully deliver on three major goals: improving access for constituents, reducing costs, and improving trust and security.

How does biometric presence assurance support stronger digital identities and Zero-Trust models?

The premise is that a digital identity should always remain the property of the person and not be owned or stored by the solution vendor. The key to that is passwordless authentication, which enables a user to access an account without needing to input a knowledge-based password. Genuine biometric presence assurance solutions are more secure, improve the user experience, and eliminate a lot of the cost and inconvenience associated with users forgetting passwords. The most secure versions of biometric presence assurance deliver on the most rigorous Zero-Trust requirements of the federal government — and, increasingly, states — as well as the most stringent NIST guidance.

What are some common misunderstandings about biometrics?

First, authentication is not identification. Constituents, employees and other users willingly enroll and then authenticate as they deem necessary to access services and other things. The solution is not used to identify random people in a crowd.

Second, it's important to understand the difference between "liveness" solutions and genuine presence assurance solutions. Liveness simply detects that a live person, rather than an image or mask of a person, is attempting access. A genuine presence assurance solution assures a real person — and the right person — is authenticating in real time. It's almost always the most appropriate solution for anything involving sensitive data or government-to-constituent interactions.

The third misconception is that biometrics are difficult to implement or use. Advanced solutions support thousands of different mobile devices, and users can authenticate themselves, on average, in fewer than eight seconds.

The fourth concern is that biases related to things like age, gender and disability are inevitable; however, the best presence assurance solutions achieve a success rate of 97% when it comes to avoiding bias errors.

What does the verification and authentication process look like?

There are two main steps. There's enrollment, which is voluntary and collaborative with the individual who wants to create the enrollment event. Then there's ongoing authentication, as needed, whenever the person desires a government service that uses a high-security, genuine presence assurance solution.