US Dept Defense

A member of the US Air Force scans a woman's iris in Afghanistan

IDENTIFY YOURSELF

Kevin Hung *explains why trust in digital identity depends on getting it right*

What if someone chopped off my finger? It's a question biometric technology companies get asked surprisingly often. In 2026, however, the concerns behind that question are felt very differently around the world. In February, MOSIP Connect landed in Morocco, bringing together government leaders, technologists, academics and Digital Public Infrastructure (DPI) advocates. MOSIP, the Modular Open Source Identity Platform, helps governments deliver one of the most fundamental public services: trusted national digital identity programmes.

In many developing countries, digital identity is not just something that's a luxury. It's very much a necessity for daily life. It enables access to healthcare, financial services and government programmes that would otherwise remain out of reach. For people living without reliable infrastructure, literacy or formal documentation, digital identity can remove barriers and enables inclusive access to essential services.

In so much of the Western world, the reaction is often very different. The moment digital identity is brought up, suspicion so often quickly follows. Biometric identity verification, in particular, is sometimes viewed with caution.

A 2025 survey by the Identity Theft Resource Center in the United States, found that while 87 percent of the 1,177 respondents had been asked to provide a biometric identifier in the past year, 63 percent said they had serious reservations about doing so. Despite these concerns, the global digital identity market continues to expand rapidly. The digital identity solutions market was valued at between $43-billion and $64-billion in 2025, with projections suggesting it could exceed $130–200-billion by the early 2030s. This growth reflects the increasing role digital identity plays across sectors such as financial services, healthcare, public services and border management.

Digital identity has become foundational to a wide range of services. Because these systems rely on highly sensitive personal data, governed by strict data protection regulations, maintaining trust in biometric verification processes is critical.

To ensure that trust, biometric liveness detection has become an important component of many identity verification solutions. Liveness detection adds an additional layer to authentication strategies by enabling biometric systems to distinguish reliably between genuine users and spoofing attempts. This technology is now widely deployed in multiple forms. The global face liveness detection market alone projected to surpass $250-million by 2027, according to a 2025 market report from Biometric Update and Goode Intelligence.

Liveness detection is designed to address the very concern that often starts the conversation: whether biometric systems could be fooled by fake outputs. By analysing characteristics that indicate the presence of living human tissue, liveness detection helps prevent attacks. In doing so, it helps strengthen confidence in biometric authentication systems. For countries building digital identity programmes, it provides an additional safeguard for critical infrastructure. For more sceptical audiences in developed markets, it offers reassurance that biometric security systems are designed to resist manipulation.

While biometric technology is sometimes associated with exaggerated fictional scenarios (like having your digit cut off), its real purpose is far more practical ensuring that digital identity systems remain secure, trustworthy and resilient.

Biometric authentication solutions have evolved far beyond simply matching a biometric sample to an image template. As attack techniques become more sophisticated, capable of tricking sensors into recognising fake inputs as legitimate authentication attempts, modern systems must also determine whether a biometric sample originates from a genuine human presence.

These attacks, known as presentation attacks, vary in complexity, expertise and cost. Small-scale attacks typically target individuals using easily produced replicas, while more advanced approaches focus on compromising systems at scale, including injection-style attacks designed to trigger false positives. Countermeasures against such attacks include analysing skin temperature, moisture, texture and electrical properties to distinguish between live and artificial inputs.

As digital identity becomes increasingly embedded in payments, public services and cross-border systems, the potential impact of biometric exploitation has grown significantly. For example the European Union's Biometric Entry / Exit System (EES) began its implementation in October 2025, requiring non-EU citizens to have fingerprints scanned and a facial image taken at border checkpoints. In this context, any exploited weakness in biometric systems can have wide-ranging and systemic repercussions.

As with most technologies biometric systems are governed by standardised testing and certifications. In the case of anti-spoofing biometrics, sensors must comply with ISO/IEC 30107, which defines the international framework for Presentation Attack Detection (PAD). This framework provides a common way to describe, categorise, and assess spoofing attempts, enabling systems to be designed and evaluated against known attack vectors. PAD testing assesses whether biometric sensors can reliably distinguish between bona-fide presentations and attacks using fake biometric samples.

LIVENESS DETECTION MUST BE TREATED AS A DESIGN PRINCIPAL RATHER THAN AN OPTIONAL FEATURE

However, adherence to standards alone does not guarantee resilience. ISO/IEC 30107 deliberately avoids prescribing specific detection techniques, recognising that attack techniques will continue to evolve. This flexibility encourages innovation across hardware, software and machine-learning-based approaches, but also places the responsibility on vendors and deployers to implement robust, multi-layered defences.

Collecting the data to attempt to create a spoof fingerprint can happen in a number of ways. These can range from anti-latent (removing the print from the sensor itself) through to non-cooperative spoofs like lifting the print from a glass.

Biometric spoofing attacks occur at the point of sensor input, where a fraudulent biometric trait is presented in an attempt to deceive the system. Liveness detection extends PAD by analysing whether the fingerprint originates from a living human rather than a synthetic or manipulated replica. A wide range of different materials can be used to create these replicas, including: silicone, Play-Doh, gelatine, white glue and latex.

Without effective liveness detection, even high quality sensors can be bypassed if the spoof is sufficiently realistic, allowing the core matching algorithms to produce false positives.

Leading biometric authentication technologies combine advanced sensors with sophisticated software and biometric algorithms to ensure strong liveness protection and attack resistance. From a hardware perspective, some sensors measure physical characteristics that are inherently difficult to replicate. For example, technologies that assess thermal response and electrical conductivity at the point of contact add critical layers of verification that significantly raise the barrier for attackers.

By simultaneously scanning fingerprint ridges and analysing thermal output the sensor can accurately

detect live human fingerprints. This combination creates a strong defence against many spoofing methods, as most synthetic materials fail to replicate the heat transfer properties of a real human finger.

This approach eliminates simple non-conductive or non-thermal spoofs such as rubber replicas. Latent prints are analysed at the image level and utilise template matching, with the most recent verification template stored in non-volatile memory. Plausibility checks are performed prior to comparison to prevent replay or injection-style attacks.

EVEN HIGH-QUALITY SENSORS CAN BE BYPASSED IF THE SPOOF IS SUFFICIENTLY REALISTIC

When combined with anti-spoofing software and sophisticated biometric matching algorithms, these sensors can deliver a comprehensive PAD solution that remains effective even against more sophisticated spoofing techniques.

Biometric authentication is now embedded in everyday consumer services as well as critical national infrastructure. As attackers develop more advanced spoofing capabilities, robust liveness detection is essential. Organisations deploying biometric systems must treat liveness detection as a core design requirement rather than an optional enhancement.

By combining physical sensing techniques with PAD algorithms and software-based liveness detection, biometric system providers can deliver resilient, future-proof authentication solutions that maintain security, trust and scalability over time.

Are all sensors made equal? No, some fingerprint sensors take biometric security a step further by actively emitting a small amount of heat and measuring how it transfers across the fingerprint's ridges and valleys. This enables the sensors to build a precise 3D fingerprint image while reliably distinguishing real human skin from fake materials. This thermal technology delivers built-in liveness detection, high image quality and low power consumption, in a thin form factor. Designed to perform in demanding environments, these sensors work consistently indoors and outdoors, in bright sunlight, humidity, extreme temperatures and with challenging fingerprints, making them a secure, future-proof choice for high-security applications.

INCREASED PRESSURE

As digital identity systems continue to expand across financial services, public infrastructure and border management, the stakes for getting biometric authentication right are only increasing. A vulnerability in one system is no longer an isolated technical issue; it can quickly become a matter of public trust.

This is why liveness detection must be treated as a fundamental design principal rather than an optional feature. Standards such as ISO/IEC 30107 provide an important framework, but resilience ultimately depends on how biometric technologies are implemented in practice. Systems that combine advanced sensing capabilities with intelligent software and algorithmic protections are far better equipped to resist both simple spoofing attempts and more sophisticated attacks.

For governments deploying national digital identity programmes, strong liveness detection helps safeguard critical infrastructure and protect citizens' identities. For users, particularly in regions where scepticism about biometric technology remains high, it provides reassurance that authentication systems are designed with security at their core.

In the end, the goal of biometric technology is to ensure that when a system asks: "Are you alive?" and: "Are you really you?", the answer can be trusted. Getting that right determines whether digital identity systems can continue to be widely adopted in the years ahead ●

Kevin Hung, Director of Field Application Engineers NEXT Biometrics – has over 11 years experience in semiconductor product and testing across Teradyne and ChipMOS.

Countermeasures against presentation attacks include analysing skin temperature and moisture to distinguish between live and artificial inputs

Picture credit: AdobeStock