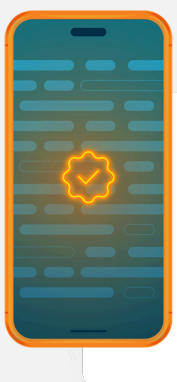
Decoding Biometric Testing Frameworks in the Age of AI Attacks

AI Attacks Are Reshaping Digital Identity Security

1 The Threat Landscape Is Exploding

- Injection attacks increased by 1,151% in one year
- Deepfakes can now be created in 30–40 minutes
- iOS devices are no longer considered “safe by default”



2 What’s Driving New Regulations?

- eIDAS 2.0
- NIST SP 800-63-4
- WCAG accessibility standards

3 Key Shift: “Liveness” → “Genuine Presence”

Old approach:

Is the user alive?

New approach:

- Is the user physically present?
- Is the video stream authentic?
- Has the device been compromised?

4 Why Independent Testing Matters

Vendor claims alone are no longer enough.

- Modern assurance requires:
- ISO 30107-3 testing
- CEN TS 18099 certification
- Independent labs
- Continuous retesting

5 Defense-in-Depth Is Essential

Strong systems combine:

- Device security
- Injection attack detection
- Deepfake detection
- Backend AI monitoring
- Ongoing threat intelligence

“A static yearly test is not enough anymore.”

6 The Future of Biometric Security

Winning strategies:

- Continuous testing
- Transparent AI models
- Multi-layered defense
- Human authorization verification
- Bias & demographic monitoring

Final Takeaway

No single certification proves full security.

Organizations need:

- Independent validation
- Layered protection
- Ongoing monitoring
- Compliance with evolving standards