fido ALLIANCE

fidoalliance.org

BEAM: Infrastructure, Culture, Community / CLASSIFICATION: Luminary

2025 LUMINARY
DEEPFAKE & SYNTHETIC IDENTITY PRISM

Growth & Resources	Market Presence	Impact & Influence	Unique Positioning	Business Model & Strategy	Biometric Commitment	Deepfakes & Synthetic Identity Leadership	Total	Average
5.75	5.50	5.83	5.67	5.50	5.83	6.00	40.08	5.73

The FIDO Alliance was founded in early 2013. Its radical vision of mobile-first identity preceded the mobile biometrics revolution sparked by Apple's Touch ID by a matter of months. An acronym for Fast Identity Online, FIDO advocated a privacy-first paradigm of public key cryptography based authentication, evangelizing a call for the "death of passwords" that would allow users to move beyond knowledge-based authentication (KBA). Flashforward to 2025, and FIDO is the world's preeminent voice in the evolution away from passwords, thanks to the passkey credential, which allows users to sign in with device unlock features, including biometrics, rather than usernames and passwords.

Strengthening the Authentication Foundation

Passwords, even when paired with additional security factors, can be circumvented without the use of deepfakes. Passkeys are a practical and deployable alternative. Many relying party organizations have already adopted them, but they aren't widespread enough to defend users in the face of generative AI-enhanced phishing schemes. That's why FIDO introduced the 2025 Passkey Pledge—a voluntary commitment for vendors and service providers to demonstrate measurable actions enabling the deployment, adoption, and use of passkeys. Signatories include tech giants like Google and Apple, universities and public agencies, household names like Ikea, and Prism Luminaries like Daon and IDEMIA. By bringing organizations together to hold each other accountable, the pledge is a tangible community effort to strengthen the foundation of strong authentication, enabling the entire ecosystem to benefit.

Taking Testing Seriously

Passkeys can use biometrics for authentication, and those biometrics need to be deepfake resilient. On a fundamental level, deepfakes are presentation attacks, and the efficacy of presentation attack detection is determined by third-party testing. FIDO offers two biometric evaluation certification programs—Biometric Component Certification and Face Verification Certification—both of which test solutions for accuracy, demographic bias, and importantly: liveness. This helps participating vendors benchmark their technology without having to participate in rallies or competitions, while relying parties are presented with an easy-to-understand assurance that a product meets standard requirements to protect against modern forms of synthetic fraud.

A History of Adaptation in the Face of Evolving Threats

The FIDO Alliance has been grounded in reality through more than a decade of strong authentication advocacy, providing protocols and frameworks for practical applications based on the state of the industry. While many identity vendors generate discourse that puts passwords firmly in the rearview mirror, the fact is that KBA is still widely used and getting more vulnerable by the day. Through its standards, initiatives, certifications, and commitment to a simply stated mission, FIDO moves deliberately, building a passwordless foundation on which further innovation can thrive.

For a complete list of FIDO Alliance members, visit https://fidoalliance.org/members/

Contact The FIDO Alliance:

fidoalliance.org/contact