Lenovo, PayPal, and Validity lead an open industry alliance to revolutionize online authentication

February 12 2013

(Phys.org)—Leading Internet companies, system integrators and security providers have formed the FIDO Alliance (Fast Identity Online) to revolutionize online authentication with an industry supported standards-based open protocol. FIDO Alliance founding member organizations Agnitio, Infineon Technologies, Lenovo, Nok Nok Labs, PayPal, and Validity are developing the specification and FIDO-compliant products.

The Internet requires users to confirm their identity to logon and access many online accounts and services. Current password authentication is weak due to reuse, malware and phishing, and leaves enterprises and end-users vulnerable to financial and identity theft. FIDO's standards-based approach automatically detects when a FIDO-enabled device is present, and offers users the option to replace passwords with authentication methods that are more secure and easier to use. The FIDO Alliance encourages and invites participation from all companies and organizations that want simpler, stronger authentication.

The FIDO standard will support a full range of technologies, including biometrics such as [fingerprint scanners](#), voice and [facial recognition](#), as well as existing authentication solutions and communications standards, such as Trusted Platform Modules (TPM), USB Security Tokens, Near Field Communication (NFC), One Time Passwords (OTP) and many other existing and future [technology options](#). The open protocol is designed to be extensible and to accommodate future innovation, as well

as protect existing investments. The FIDO protocol allows the interaction of technologies within a single infrastructure, enabling security options to be tailored to the distinct needs of each user and organization. As more organizations join the FIDO Alliance, more use cases and technologies will become part of the solution.

"The Internet—especially with recent rapid mobile and cloud expansion—exposes users and enterprises, more than ever before, to fraud. It's critical to know who you're dealing with on the Internet. The FIDO Alliance is a private sector and industry-driven collaboration to combat the very real challenge of confirming every user's identity online," said Michael Barrett, FIDO Alliance president and [PayPal](#) Chief Information Security Officer. "By giving users choice in the way they authenticate and taking an open-based approach to standards, we can make universal online authentication a reality. We want every company, vendor, and organization that needs to verify user identity to join us in making online authentication easier and safer for users everywhere."

"At the core of National Strategy for Trusted Identities in Cyberspace (NSTIC) is a call for the private sector to lead in developing open technology standards that will enable a more trusted and secure Identity Ecosystem. The new FIDO Alliance has pledged to do just that," said Jeremy Grant, who is leading the implementation of NSTIC as Senior Executive Advisor for Identity Management at the National Institute for Standards and Technology (NIST).

"I am excited to see what the FIDO Alliance's members can do to deliver the kind of usable, cost-effective, privacy-enhancing, interoperable strong authentication innovations envisioned in the NSTIC."

"IDC forecasts the strong authentication market to realize more than $2.2 billion in revenues alone by 2016. This demand is driven by social networking, internet, cloud and mobile, all of which will require higher

and higher levels of authentication by governments, corporations and consumers," said Sally Hudson, IDC Research Director, Security Products and Services. "We believe that standards based, automated solutions such as those advocated by FIDO will contribute greatly toward making this a reality."

The FIDO Alliance is committed to overcoming prevailing limitations by developing an [authentication](#) ecosystem with a standardized, global protocol and necessary interfaces. With users free to select any FIDO-compliant token type, even devices previously considered proprietary can be adapted for use, and new vendors with new protocol-compliant devices easily become part of the marketplace.