Lenovo, Nok Nok Labs, PayPal, and Validity Lead an Open Industry Alliance to Revolutionize Online Authentication

The FIDO Alliance (Fast IDentity Online) Standards Will Allow Users the Option to Replace Passwords with Authentication Methods that are More Secure and Easier to Use

Palo Alto, California – February 12, 2013 - 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."

Why FIDO? Why Now?

The FIDO Alliance is a revolution in authentication methods that today's markets demand. Though many authentication systems and point solutions existed before the FIDO Alliance, they have been proprietary, difficult and costly to manage, and/or insufficient to scale. The FIDO Alliance's objective is to be all-inclusive, embracing both existing and new authentication methods and hardware with the FIDO open protocol. FIDO-compliant smartphones, tablets, PCs and laptops can replace password dependency and exposure of sensitive user information by automatically and transparently providing user credentials when they're required.

50 billion internet-connected devices are predicted to be in the marketplace by 2020, according to Cisco Systems. The FIDO protocol approach inherently supports consumerization trends, by allowing end users any choice of authentication method. At the same time, FIDO shifts control to providers, who can make authentication user-transparent and limit the risk of fraud. Any site will be able to effect stronger account and transaction security, and improve their users' experience with more convenience, better privacy and fortified protection of persons and assets.

Today, users are often required to remember a selection of security questions, enter a unique ID with a main password, and potentially use a software or hardware token, as well. Most users have a handful of slightly varied passwords they use to access multiple sites and accounts. This cross-use of passwords poses serious risks if one account is compromised and user credentials are exposed to potential fraud across the range of a user's accounts. Providers are invariably implicated when data is breached and personal information is exposed at a site or within an application. Repeated attempts to outline better security practices and change user behaviors haven't succeeded.

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.

The FIDO Alliance and standards create the open, non-proprietary and flexible authentication protocol framework that lowers costs to deploy and improve returns on investment by using

devices and systems already in the marketplace to authenticate users. Today, more and improved security options have become available and at better prices. Considering new market dynamics and the risk problem FIDO solves for users and providers, broad market adoption of secure authentication is now set up to succeed.

The FIDO Alliance invites all companies and organizations to become active members. Members will define the market requirements and contribute to the FIDO specification. Interested organizations are encouraged to go to www.fidoalliance.org to find out more and to join the FIDO Alliance.

About The FIDO Alliance
The FIDO (Fast IDentity Online) Alliance was formed in July 2012 to address the lack of interoperability among strong authentication technologies, and remedy the problems users face with creating and remembering multiple usernames and passwords. The Alliance plans to change the nature of authentication by developing standards-based specifications that define an open, scalable, interoperable set of mechanisms that supplant reliance on passwords to easily and securely authenticate users of online services.

###

Quotes from FIDO Alliance Founding Members:

Biometrics

Biometrics – finger, hand/palm, face, voice, iris—represent something everyone has with them at all times. The FIDO Alliance calls attention anew to the range of biometric options that identify who a user is. By enabling dynamic discovery of FIDO-compliant biometric devices, the FIDO Alliance manifests remarkable advantages to biometric users and manufacturers of biometric devices and systems, as well as device manufacturers who want to incorporate biometric recognition technology into their systems and devices to enable FIDO-compliance.

Agnitio, http://www.agnitio-corp.com/

"Agnitio is committed and passionate about fighting for Internet citizens worldwide against identity fraud and criminal activity. The FIDO Alliance facilitates our global opportunity to equip users with the convenience of using their voice to automatically authenticate instead of having to remember and enter passwords, especially when they're on the go," said Agnitio CEO Emilio Martinez. "What is more natural for Agnitio users than authenticating while speaking to their FIDO-compliant mobile devices? Voice Biometrics is the most natural way to ease and secure the authentication process anytime and anywhere, using a mobile phone or any FIDO-enabled device."

Validity, http://www.validityinc.com/

"As device and digital consumption continues to grow exponentially, so does the challenge of maintaining privacy and ease of use," said Sebastien Taveau, FIDO Alliance Board Member and CTO for Validity Sensors. "PC manufacturers have already recognized the power of leveraging a fingerprint for authentication, and with the upcoming release of fingerprint sensors in mobile devices, now is the time for the FIDO Alliance to bring together the hardware, software and applications that create a seamless user experience with a much needed new approach to security."

Relying Parties -- Those who must authenticate and secure users against identity theft, financial fraud and abuse

All FIDO Alliance members have a stake in making online authentication work, but none moreso than those who must authenticate and secure the billions of online and mobile users who rely on their services and risk exposure every time they logon or access sites and services. These FIDO Alliance members – the Relying Parties are at risk along with their users, until user authentication is made secure with FIDO standards.

PayPal, https://www.paypal.com/

"PayPal authenticates 7.5 million transactions every day and we take our customers' security very seriously," said Bill Leddy, Principal Security Strategist, PayPal. "We recognize that user authentication must go beyond passwords. With FIDO, PayPal's customers will have more choice and stronger methods of authentication including biometrics, USB security tokens and one-time passwords. By collaborating with the industry to create open authentication standards such as FIDO, we can make authentication simpler and stronger for Internet users everywhere."

Server and ValidationVendors

The FIDO Alliance establishes the standards that make online authentication open to all to compete in every market with FIDO-compliant hardware and software products. FIDO-compliant servers and processors enable inherent features and functions of FIDO authentication and automate delivery of secure credentials throughout the FIDO ecosystem.

Nok Nok Labs, http://www.noknok.com

"The formation of the FIDO Alliance addresses a longtime, critical need for technology providers and their users: stronger security that is easier to use," said Phillip Dunkelberger, CEO of Nok Nok Labs, a founding member of the FIDO Alliance. "From day one, through our Unified Authentication Infrastructure, we are developing solutions that will deliver-on the vision of the FIDO Alliance. We are excited to see the launch and expansion of the Alliance."

Systems and Device Manufacturers

FIDO Alliance membership enhances opportunities for PC, mobile and other systems and device manufacturers to influence the FIDO standard. As these manufacturers incorporate FIDO-compliance, the market opportunities expand for their products, as widespread adoption of standards-based FIDO authentication ensues.

Lenovo, http://lenovo.com/us/en/

"Lenovo products have earned a reputation for outstanding security features and designs," said Mark Cohen, Vice President and General Manager, Ecosystem and Monetization, Lenovo. "Recognizing that our customers wanted more than just passwords for authentication, we began shipping ThinkPad PCs with integrated fingerprint readers nearly a decade ago. We are excited about the new FIDO standard because it enhances both security and convenience, enabling biometric and other forms of authentication to take place directly between the user and the service that he or she is trying to use."

Media Contact:
Suzanne Matick
for FIDO Alliance
suzanne [at] matick.net
831-479-1888 Pacific time zone