FIDO Alliance Exceeds 50 Members in Eight Months, as Industry Drives Fast toward Open Standards for Universal Strong Authentication

Palo Alto, California – October 30, 2013 - The FIDO Alliance, an industry consortium revolutionizing online authentication with the first standards-based open specifications for overcoming password dependency with universal strong authentication, announces that it has exceeded 50 members. Launched in February, 2013 with six founding members, the alliance has grown rapidly with representatives from every continent comprising 11 board, 16 sponsor, and 26 associate members in less than eight months. Joining CrucialTec, Google, Lenovo, Nok Nok Labs, NXP Semiconductors, PayPal, Validity, and Yubico, newest board members are BlackBerry, MasterCard, and Oberthur Technologies. Founding associate member Agnitio has advanced to sponsor and is joined by new sponsor members Constratus, Eyelock, IDEX, Kili, MedImpact, Ping Identity, Plug-up, SecureKey, and WWTT. New associates include Aktiv-soft, Arxan Technologies, Authentify, Bio-key, Biomatiques, Certus, Cloud Star Corporation, DigiFLAK, Egistec, FaceBanx, findBIOMETRICS, GoTrust, ItsMe! Security, LaunchKey, LG Electronics, Natural Security, Toopher, ValidSoft, Yandex.

"The rapid growth of the FIDO Alliance and the quality of our membership reflect a thriving awareness of the demands for better authentication," said Michael Barrett, FIDO Alliance president. "We welcome our new members, and we continue to invite all who recognize the value of enabling the broad range of strong authentication methods and devices to join the Alliance and explore this emerging technology. Both Relying Parties and users need FIDO authentication to realize the full potential of the Internet."

Open FIDO specifications will support a full range of authentication technologies, including biometrics such as fingerprint and iris scanners, voice and facial recognition, as well as existing solutions and communications standards, such as Trusted Platform Modules (TPM), USB Security Tokens, embedded Secure Elements (eSE), Smart Cards, and Near Field Communication (NFC). The open specifications are being designed to be extensible and to accommodate future innovation, as well as protect existing investments. FIDO specifications allow the interaction of technologies within a single infrastructure, enabling security options to be tailored to the distinct needs of each user and organization.

Among the landmark achievements announced today, the FIDO Alliance has begun conformance and interoperability testing for FIDO Universal Authentication Framework (UAF) and Universal Second Factor (U2F) products. Members of the FIDO Alliance Technology Working Group (TWG) are implementing products to the working specifications and informal FIDO organized events have successfully begun testing to verify conformance and interoperability.

"The progress made since we founded the FIDO Alliance is impressive," said FIDO visionary and founder of Nok Nok Labs, Ramesh Kesanupalli, "The diversity and quality of the new

member organizations validates our belief that the lack of strong authentication is a critical problem, and can only be solved through broad industry consensus and a standards-based approach. This first phase of member interoperability testing is an important milestone for the FIDO Alliance. The work completed now will deliver a solid platform for our continued growth."

"As a founding member, Agnitio has seen the FIDO Alliance expand eight-fold in just eight months," said Mike Goldgof, VP Marketing for Agnitio, a global leader in voice biometrics and FIDO Alliance sponsor member. "As part of the alliance, Agnitio is thrilled to be a driving force in the global adoption of stronger standards-based authentication that is more secure, private, and easier to use."

The FIDO approach ensures that users and Relying Parties (RPs) have a variety of choices to implement better authentication that overcomes the prevailing reliance on passwords. The specifications emphasize a device-centric model. Authentication over the wire happens using public key cryptography. The user's device registers the user to a server by registering a public key. To authenticate the user, the device signs a challenge from the server using the private key that it holds. The keys on the device are unlocked by a local user gesture -- such as a biometric or pressing a button. The server has the choice of replacing the password depending on the choice of local authentication. FIDO protocols are designed with a core focus on privacy -- the key issued by a user's device to each account on each server is unique to avoid link-ability. If the user chooses to use a biometric local authentication, all biometric information stays local on the user's device and is not shared with the cloud.

The FIDO Alliance invites all companies and organizations to join the Alliance and become active members.

About The FIDO Alliance

The FIDO (Fast IDentity Online) Alliance, www.fidoalliance.org, 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 for better authentication that define an open, scalable, interoperable set of mechanisms that reduce reliance on passwords. Better authentication is stronger, private, and easier to use when authenticating to online services.

###

Media Contact:
Suzanne Matick
for FIDO Alliance

suzanne [at] matick.net
831-479-1888 Pacific time zone