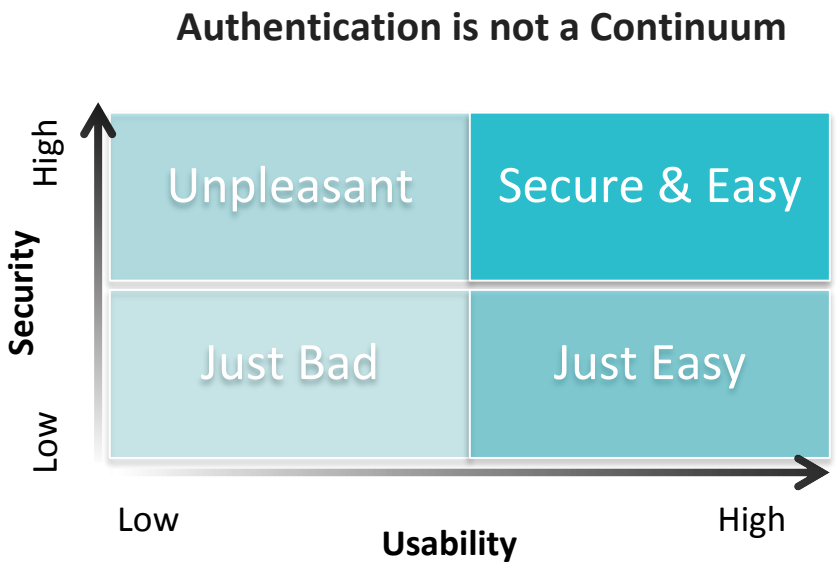
Overview of the FIDO Alliance:

For the overwhelming majority of organizations, user-ID and password authentication has proven to be the path of least resistance in terms of initial deployment. Countless experiences over the last decade have taught organizations that login credentials are not particularly secure. For consumers, it's not easy either, considering that it's virtually impossible for each of us to remember the numerous passwords we're now required to use in our daily lives. According to Microsoft, the average internet user with 25 accounts, performs 8 logins using 6.5 passwords daily. Organizations cannot adequately secure password and PIN authentication and their risk and costs are mounting at $5.5M per data breach, $15M yearly in password resets, and $60 per token replacement.

Information Security professionals tend to believe that authentication is a continuum – it could be described as easy to use, if insecure at one end, and hard to use, but secure at the other. You simply pick your level of security and then dial up the corresponding level of pain that you will inflict on your users. The FIDO Alliance believes that authentication can best be represented by a quadrant chart with ease of use on one axis and security on the other. The top right quadrant represents solutions that are simultaneously more secure and easier to use.



Today, it's estimated that there are more than 100 proprietary authentication vendors, a number that historically has increased at a rate of about a dozen a year for the last several years. While there are very strong solutions offered by those vendors, product adoption has been severely hampered by the lack of interoperability standards. In particular, Relying Party (RP) organizations are challenged by the risk in deploying these solutions, because the integration methods are unique to each vendor. Hence, if the chosen solution doesn't work exactly as expected, integration with another vendor can result in compounded costs and time. Given that integration tends to be expensive – potentially well over a million dollars (US) for a complex system - few RPs will take a gamble on a proprietary authentication vendor.

Open industry standards for strong, and easy-to-use authentication are the only possible approach. The FIDO Alliance (Fast Identity Online) was founded to develop open standards specifications to both

simplify authentication and simultaneously improve security and ensure user privacy. This has not been attempted broadly before the FIDO Alliance.

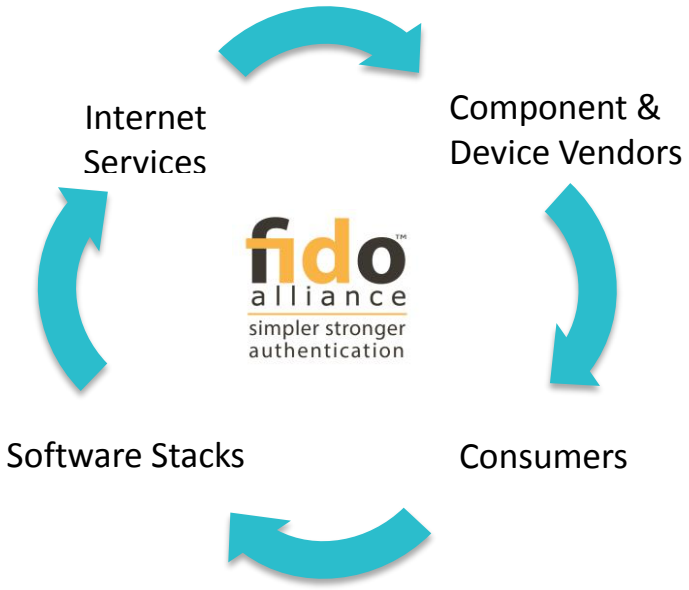
The FIDO Alliance was formed in July 2012 by a group of RPs and technology providers. It was publicly announced in February, 2013. However, the FIDO Alliance actually began its work to establish open authentication standards more than two years ago when industry leaders began collaborating and sharing IP to develop FIDO specifications. Today, the FIDO Alliance has working code and members have produced working prototypes; the alliance expects to publish and implement at least one FIDO specification in 2013 and a second in early 2014.

FIDO specifications provide a framework for authentication, by allowing a wide range of authentication types to fit within it. This makes authentication adaptable to future innovations and generations of technologies and products. FIDO specifications support a full range of authentication technologies, including biometrics, such as fingerprint scanners (FPS) and voice/facial/iris recognition, as well as existing solutions and communications standards, such as Trusted Platform Modules (TPM), USB Security Tokens, embedded Secure Elements (eSE), Near Field Communication (NFC), and many other proven and future technologies. The FIDO Alliance is embracing user controlled identity and bring your own authentication [BYOA] as well as traditional models.

The use of human factors in authentication is often criticized over the fear that biometric data could be vulnerable to egregious theft and beget new proportions of fraud. The FIDO Alliance specifications protect such human factors and all personal identifiers by the simple strategy of never sharing them, thus ensuring users of the utmost privacy. FIDO specifications require FIDO-enabled servers and FIDO-enabled devices to recognize and cooperate with each other, but they never share what they know about the authenticating user or the RP, even within the FIDO ecosystem.

Given the increasing toxicity of a password based Internet ecosystem, it's clear that the time for change is now. All of us, whether representing our employers, or just as consumers, have a need for better authentication technologies that are easier to use, private and stronger. The FIDO Alliance is the only open standards based initiative that is improving authentication for every Internet user in the world.

The FIDO Alliance Ecosystem



Benefits

For Internet Services	For Component & Device Vendors	For Users
• Greatly improved PKI-based security • Increased user engagement • User brings own device • Build server once: Leverage any authentication method	• Standardization ignites the market • Move past fragmented custom solutions	• Easy to use • No more worrying about passwords • Greater internet safety

Further information

For more information, please visit the FIDO Alliance online, to learn more about what the industry is doing to overcome password and PIN dependency:www.fidoalliance.org.

FIDO Alliance membership comprises global leaders: http://www.fidoalliance.org/members.html.

The FIDO Alliance specifications embrace all use cases, and personal user data or human factors/identifiers are never shared. You may see how FIDO works: http://www.fidoalliance.org/how-it-works.html

For recent FIDO Alliance news: http://www.fidoalliance.org/fidonews.html

You may view video demonstrations of FIDO-enabled authentication:
This video is of the Yubico key: http://vimeo.com/yubikey/fido-u2f The Yubico key, two-factor authentication, captured a lot of attention when Google posted their intention to use the Yubikey in Google applications.

Nok Nok Labs has many different types of FIDO-enabled product demos. Some demos can be found at: https://noknok.box.com/demo/
The password to access these videos is **nnlsecure** (note: it's not the number 1, it's a lower case "L")

To join the FIDO Alliance:
Melissa Bassignani, FIDO Alliance Membership Adminstrator
fidomembership@virtualmgmt.com