fido™ alliance | simpler stronger authentication

FIDO 1.0 Final Specifications Have Arrived

Abstract

The FIDO Alliance has published the final 1.0 specifications. This whitepaper explores the background of FIDO authentication: the needs, benefits, and early deployments.

The Need for a New Authentication Model

During 2014, 783 data breaches occurred and 86 million personal records were stolen; during 2005 through 2014, a total of 4,794 breaches led to a staggering 641 million stolen personal records![1] Clearly, the situation is out of control. Cybercriminals are getting increasingly more sophisticated and are managing to stay ahead of new security technologies, products and services.

There are several fundamental issues with today's authentication infrastructure. Password based authentication relies on centralized stores of user passwords, and a single database breach often results in tens of thousands of stolen credentials. As strong passwords are difficult to remember, most people use weak passwords and/or use the same password at multiple sites - practices that result in security vulnerabilities. In addition, password authentication was developed before mobile devices entered the computing scene, and it is poorly suited for mobile devices, especially from the usability perspective. As a result, many mobile users disable passwords whenever they can, and when forced to use passwords they choose short simple ones (which are also easy to break).

A number of technologies have been implemented to strengthen passwords. Each of them has its own limitations. Hardware tokens provide strong security, and they have been broadly deployed in large enterprises. They have not taken hold with consumers or small businesses, primarily due to high deployment, replacement and support costs of such devices. Another major issue with hardware tokens is that they are very difficult to use with mobile devices. Software tokens are less expensive than hardware tokens but still carry substantial support costs. They are also less secure and have the same usability problem for mobile devices.

One Time Password (OTP) authentication has become popular, especially with the proliferation of mobile devices. A typical use case is to send a one time passcode to a mobile device that the user then enters as a secondary authentication when logging on via a PC. Unfortunately, this technology is ill suited to support authentication from a mobile device as there is typically no additional device where OTB passcodes can be directed.

A common but flawed assumption is that easy-to-use authentication is weak, and strong authentication has to be difficult to use. This model assumes a trade-off curve between usability and security strength (see Figure 1). As a result, strong authentication has been implemented mostly in environments where security is required (or even mandated) such as financials, government, and healthcare. Most other environments are relying on weak password schemes. This situation is leading to a growing number of data breaches and other security disasters. Clearly, something needs to change.

[1] IRTC Data Breach Reports, December 2, 2014

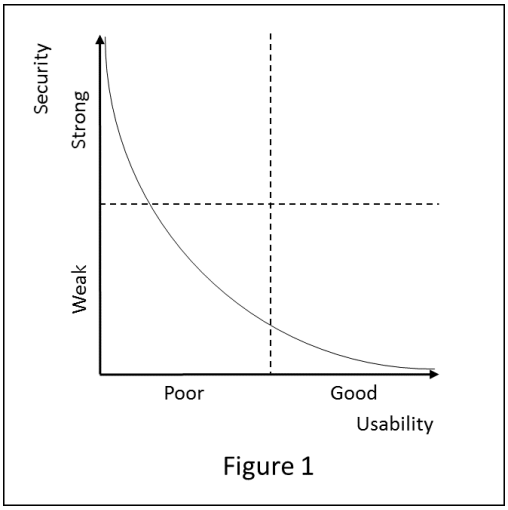

Figure 1

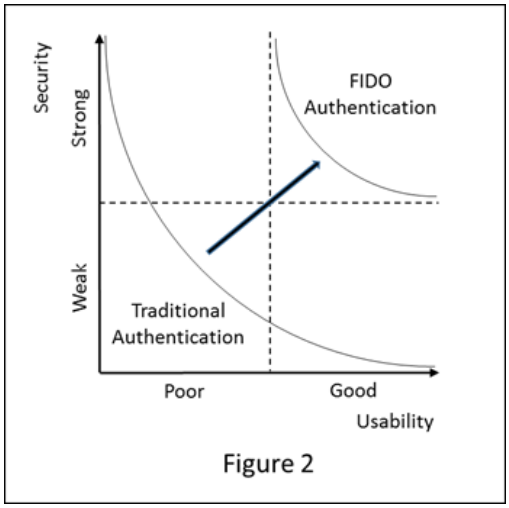

Figure 2

FIDO Authentication Model

The FIDO (Fast IDentity Online) Alliance was formed to create open standards for strong and secure authentication that is also easy to use. It is developing specifications for technologies that will reduce the reliance on passwords, eventually replacing them with other authenticators such as biometrics.

One of FIDO's main design principles is to achieve a satisfactory user experience. In order for authentication to be broadly deployed among consumers and enterprise users, it must be easy to use while providing strong security. This is breaking new ground for authentication, as illustrated in Figure 2.

One of the ways to achieve ease of use in FIDO is to use the same authentication factor (a U2F token or a biometric sensor, for example) seamlessly across multiple services, once initial registration with each service is complete.

Another key design principle is that authentication must protect user privacy. For example, the user's biometric data should never leave the user's device, and any personal data collected during a FIDO operation can only be used for FIDO authentication. Any identification of the user outside of FIDO operations must be prevented. For an in-depth discussion of FIDO privacy principles, please see "The FIDO Alliance: Privacy Principles Whitepaper"[2].

Currently, there are two FIDO protocols – Universal 2nd Factor (U2F) and Universal Authentication Framework (UAF). Both protocols share common FIDO design principles around ease of use and privacy. While U2F and UAF have been developed in parallel and

[2] FIDO Privacy Principles, February 2014

are separate and distinct within the final 1.0 specification, we can expect the two protocols to further develop and harmonize in the future.

Let's take a look at the user experience for U2F and UAF.

U2F strengthens password authentication by adding a physical token. In a typical U2F deployment, a user inserts a U2F token (usually a USB device) into the computer when signing into an online service and taps it when prompted by the browser. The same U2F token may be used to sign in to multiple services (Figure 3).

UAF provides strong authentication without passwords, by using biometrics and other modalities to authenticate users to their local devices, then enabling the devices to authenticate to online services by using cryptography. In a typical UAF deployment, a person simply swipes a finger (or speaks a phrase, or looks at a camera) on a mobile device to login, pay for an item or use another service (Figure 4). Since biometrics and private cryptographic keys are stored on local devices (as a best practice, in hardware tokens or trusted execution environments) and never communicated to the cloud, what's stored on the service provider site is only public cryptographic keys. Even if the service provider site gets hacked, there are no user credentials to be exposed, eliminating the possibility of scalable data breaches.

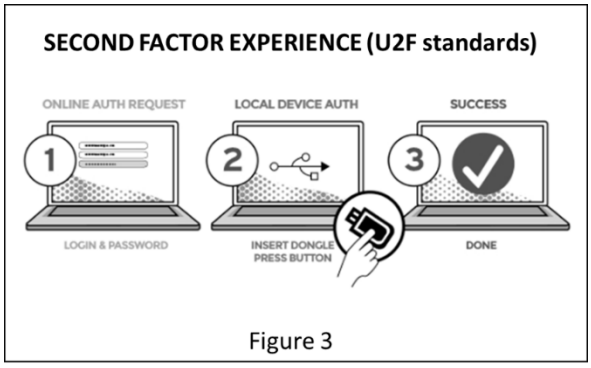

Figure 3

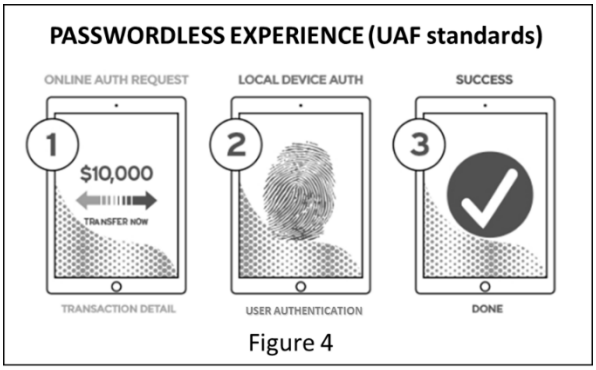

Figure 4

Benefits of FIDO Authentication

FIDO authentication provides a number of powerful benefits to each of its constituencies – consumers, online service providers, and enterprises.

For consumers, FIDO provides strong security with a superior user experience, all while protecting their privacy. It relieves a major pain by eliminating the need to remember many passwords while providing a higher level of security. It has the potential to enable

the use of many mobile applications that are currently hampered by lack of sufficient security.

Consider mobile banking, a use case where a bank acts as an online service provider. According to the Federal Reserve, "concerns about the security of the technology were a common reason for not using mobile banking or mobile payments (69 percent and 63 percent, respectively, of non-users)" [3]. With the FIDO authentication model, authentication from mobile devices is secured with low added cost or complexity.

According to a 2014 study by Axil Partners[4], 60 percent of smartphone or tablet owners who switched primary banks reported mobile banking capabilities as "important" or "extremely important" in their decision to switch, up from 48 percent in a similar survey in the first half of 2013. Clearly, new services such as mobile banking provide one of the largest potentials for differentiation and growth in the banking industry. Yet there are currently no good solutions that can be effectively implemented to enable secure consumer authentication from mobile devices. For banks and others providing high value mobile services, FIDO represents a major opportunity for differentiation and growth. FIDO has the potential to provide similar benefits for service providers in payments, consumer web services, and other industries.

Enterprises also stand to benefit from FIDO protocols. While strong authentication has been deployed by many large enterprises, it is typically implemented via hardware tokens that carry high acquisition costs. According to Gartner[5], average enterprise authentication implementation for a large enterprise in 2014 was priced at $189,000. In addition, a 2014 survey found that companies lose $420 of productivity annually per employee due to struggling with passwords.[6] FIDO can significantly reduce these costs while improving security.

The FIDO Alliance and FIDO Deployments

The growth of internet technologies and mobile devices have made strong online authentication an increasingly important requirement. Yet, as described earlier in this paper, strong authentication solutions have been complex, expensive and difficult to use. The FIDO Alliance was conceived to transform the nature of online authentication by creating a new model of stronger and simpler authentication. Back in 2009, Ramesh Kesanupalli (then CTO of Validity Sensors) had a conversation with Michael Barrett (then CISO of PayPal). Ramesh proposed to "fingerprint enable" PayPal, and while Michael was intrigued with the idea he expressed the need for such solution to be vendor agnostic and

[3] Consumers and Mobile Financial Services 2014, Board of Governors of the Federal Reserve System, March 2014
[4] AlixPartners Mobile Financial Services Tracking Study, March 12, 2014
[5] Gartner Magic Quadrant for User Authentication, 1 December 2014
[6] Survey by Widmeyer sponsored by Centrify Corporation, 2014

standards based. The conversations progressed on from there, more experts got involved, and eventually the FIDO Alliance with six founding members was formed in the summer of 2012 and publicly launched in February 2013.

As the vision of transforming online authentication appealed to many industry players, the Alliance experienced explosive growth, adding around 10 members per month to grow to over 150 members strong. Leading online service providers, financial institutions and technology companies joined the Alliance and contributed to the development of FIDO specifications. In February 2014, the Alliance issued draft specifications for public review, and in December 2014, final 1.0 specifications were made available.

In parallel with the specifications work, several mass-scale FIDO deployments were launched in the market during 2014. At the Mobile World Congress event in February 2014, PayPal and Samsung announced[7] the first FIDO deployment, a collaboration that enables Samsung Galaxy S5 users to login and shop with the swipe of a finger wherever PayPal is accepted. The Samsung Galaxy S5 device is equipped with a fingerprint sensor from Synaptics. PayPal and Samsung selected[8] the Nok Nok Labs S3 Authentication Suite to enable the new payment system. The new service became available in April 2014. In September 2014, Alipay also selected[9] Nok Nok Labs to enable secure online payments via the fingerprint sensor on the Samsung Galaxy S5.

In October 2014, Google launched[10] support for the U2F protocol in its Chrome browser, which set the stage for the world's first deployment of FIDO U2F authentication. With this deployment, Google Chrome became the first browser to implement FIDO standards. In this use case, when signing into a Google Account, the user simply inserts a Security Key into their computer's USB port and taps it when prompted. Users can buy a compatible Security Key from any tested and approved FIDO Ready™ U2F vendor (currently, Yubico and Plug-up).

With the final 1.0 FIDO specifications available and with multiple mass-scale FIDO deployments launched, it is clear that the FIDO Alliance is picking up steam. More important, the new authentication model is changing the world – protecting consumers, reducing the cost of exposure to breaches for online service providers, and lowering infrastructure cost and complexity for enterprises.

[7] The FIDO Alliance Announces First FIDO Authentication Deployment, February 24, 2014
[8] Samsung and PayPal select Nok Nok Labs to power the first FIDO Ready Authentication Ecosystem, April 22, 2014
[9] Alipay Selects Nok Nok Labs to Power First FIDO Ready™ Authentication Ecosystem in China, September 17, 2014
[10] Google Launches Security Key, World's First Deployment of Fast Identity Online Universal Second Factor (FIDO U2F) Authentication, October 21, 2014