POINT OF VIEW

Financial Services
Secure Banking

Banks Seek to Stop Fraud in its Tracks with Simpler, Stronger Authentication

Banks can thwart malicious attacks and increase consumer confidence in online banking transactions with Fast IDentity Online* (FIDO*) coupled with Intel® Online Connect

Executive Summary

In today's competitive marketplace, banks must use every means available to attract and retain customers. Online banking services can be a differentiator, with customers choosing banks that offer the most convenience and flexibility. However, increasingly sophisticated cyberattacks can make customers wary—they want assurance that their online transactions are protected. Banks that deploy advanced cyber protection can gain a definitive competitive edge.

The Fast IDentity Online* (FIDO*) Alliance addresses banks' need for stronger authentication methods that don't rely on multiple usernames and passwords. Instead, FIDO uses a locally stored private key. The private key is used to sign a "challenge," which is then verified on the bank's backend server using a corresponding public key. With Intel® Online Connect the local private key, including any biometric templates and data processing, is not available to the OS—it is stored on the client device in a trusted execution environment—protecting against both man-in-the middle (MitM) and man-in-the-browser (MitB) attacks.

Banks can combine FIDO with Intel Online Connect to create simple yet strong security for online transactions. Intel Online Connect is a PC-based FIDO client and authenticator implementation. Third-party solution providers can use Intel Online Connect either as a silent authenticator (without any user interaction) to provide platform-bound second authentication factor capabilities, or coupled with a biometric factor.

The hardware-based security provided by FIDO protocols and Intel Online Connect provide protection that banks—and their customers—can rely on to help protect the user's ID while providing an easier authentication process.

Authors

Bruno Domingues
CTO Financial Services Industry
Intel, Industry Solutions Group

Guy Itzhaki
Intel Cyber Technologies Enablement
Platform Security Division

"The world has a password crisis that can only be solved with an alternative authentication capability that is more user friendly, more secure, and ubiquitously interoperable across all Internet-enabled devices and applications."

- Brett McDowell,
Executive Director, FIDO Alliance

Solution Benefits

- Better protection against cyberattacks
- Fewer losses due to online banking fraud
- Strong yet simple multifactor authentication using a private/public key pair approach
- Higher customer confidence

State of the Industry: Fraud on the Rise but More Passwords Are Not the Answer

The convergence of explosive growth in mobile and online banking services, increasing regulations, more sophisticated cyberattack techniques, and the "password crisis" has created a perfect storm: banks are working to find stronger, more innovative secure authentication methods to help protect themselves and their customers (Figure 1).

Online banking is cost efficient for banks and convenient for customers. Banks have already invested billions of dollars to create effective online fraud-prevention systems that include features like multifactor authentication.[1] But more security is needed. Cyberattacks are getting more frequent and more sophisticated, making it harder for banks and consumers to detect.

According to the 2015 Identity Fraud Study, USD 16 billion was stolen from 12.7 million consumers in the United Sates in 2014, resulting in a new identity fraud victim every two seconds. The Identity Theft Resource Center reports that over 175 million records were breached so far in 2015.[2] Not just a problem in the United States, banking fraud also plagues financial institutions across the globe. For example, in the United Kingdom, financial fraud losses across payment cards, remote banking, and checks totaled £755 million in 2015, an increase of 26 percent compared to 2014; remote banking accounted for 22 percent of the 2015 fraud total.[3]

In spite of banks' efforts to stem fraud, two specific types of attacks still pose significant threats to online banking transactions:

- **Man-in-the-middle (MitM) attacks** are characterized by an attacker who secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other. For example, the attacker can intercept and alter the configuration of the TCP connection, while the user is unaware of the attack. The attacker is then able to read, insert, and modify the data in the intercepted communication—such as capturing a session cookie or changing the amount of a monetary transaction.
- **Man-in-the-browser (MitB) attacks** are similar to MitM attacks, but feature a proxy Trojan horse which, after being installed on the user's computer, acts between the browser and the browser's security mechanism. The Trojan horse sniffs or modifies transactions as they are formed on the browser, but still displays the user's intended transaction. The Trojan horse can also covertly modify web pages or insert additional transactions, unknown to both the user and the host web application.

Creating more passwords is not the answer to the fraud issue. The average person has up to 27 passwords,[4] at least 90 online accounts, and has to reset a forgotten password for at least 37 accounts each year.[5] Strong password rules may make passwords hard for hackers to decipher, but they also make it hard for users to remember them. Several studies indicate that the human memory simply is not equipped to support strong passwords[6] —leading to insecure practices such as writing passwords down, creating weak passwords that are easier to remember, or using the same password for multiple accounts.

"We are excited to collaborate with other industry leaders in the FIDO Alliance to develop simpler and more secure solutions to authenticate users and to eliminate the need for passwords over time,"

- Mark Hocking,
Vice President and General Manager of Safe Identity,
Intel Security

Figure 1. To protect themselves and customers, banks are seeking additional secure authentication methods.

Fast IDentity Online* (FIDO*) Offers Better Security

In response to the need for additional secure authentication methods, the Fast IDentity Online (FIDO) Alliance was formed in 2012. The Alliance's mission: address the lack of interoperability among strong authentication devices and solve the problems users face with remembering multiple usernames and passwords. (See the sidebar, "A Closer Look at the FIDO* Alliance" for more information.)

FIDO protocols offer several advantages over previous authentication approaches:

- No third party is involved in the protocol.
- No secrets are stored on the server side—biometric data (if used) never leaves the client device.
- No links exist between services or accounts.

With FIDO, users do not use credentials known by the online service to authenticate directly to the online service (as is done today with passwords). Instead, FIDO uses a challenge/response approach. The challenge is sent to the device, and the user unlocks the private key to sign the challenge. The private key used to sign the challenge resides on the device and is unlocked with locally stored multifactor authentication credentials. This can include something the user knows (a PIN), something user has (a mobile device) and/or something the user is (biometrics, such as a fingerprint, voice pattern, or iris picture). The FIDO authenticator locally verifies the user on his or her device and then authorizes the signing of the server-issued challenge. The signed challenge (response) is verified on the server using the corresponding public key.

FIDO provides two user experiences (Figure 2) to address a wide range of use cases and deployment scenarios. Both FIDO approaches to authentication are more secure than passwords.

- **Passwordless user experience.** This user experience is supported by the Universal Authentication Framework (UAF) protocol. The user carries a client device (such as a laptop or tablet) on which the UAF stack is installed. The user presents a local biometric to answer the authentication challenge. The UAF protocol allows experiences that combine multiple authentication mechanisms such as fingerprint and PIN.
- **Second-factor user experience.** This user experience is supported by the Universal Second Factor (U2F) protocol. The user logs in with a username and password, but also has access to a U2F device that verifies user presence and provides the FIDO assertion.

Keeping biometric templates and data processing confined to a trusted execution environment on the client device prevents biometric data from being sent over the wire. In this way, FIDO protects against both MitM and MitB attacks. The public/private key pair approach mitigates against scalable cyberattacks since there is no shared secret that resides on the device and on the server.

A Closer Look at the FIDO* Alliance

Since its founding in 2012, the membership of the Fast IDentity Online Alliance has grown to over 250 organizations, spanning payment, financial, service provider, and device manufacturer firms. More than150 products are now FIDO-certified. Intel joined the FIDO Alliance Board of Directors in 2015. Other notable financial services members include Bank of America*, ING Bank*, Chase*, E*Trade*, Wells Fargo*, and the China Financial Certification Authority*. Bank of America was the first bank to deploy FIDO authentication. VASCO Data Security International, Inc.*, a leading provider of authentication solutions to financial institutions, is also a FIDO Alliance member. Microsoft Windows* 10 OS is also FIDO-compliant, with embedded user and website multifactor authentication.

The FIDO Alliance defines standard protocols for stronger authentication using public key cryptography and certifies interoperable products for stronger, simpler online authentication. The information security industry is embracing the FIDO Alliance's mission. For example, Yahoo* Tech recently reported that Lenovo* has announced that upcoming laptops will include a biometric authentication system backed by FIDO authentication to protect users' identities online.[7] Digital Transactions* said it is looking into replacing passwords with a more secure solution, and has reached the conclusion that FIDO standards are a promising option.[8]

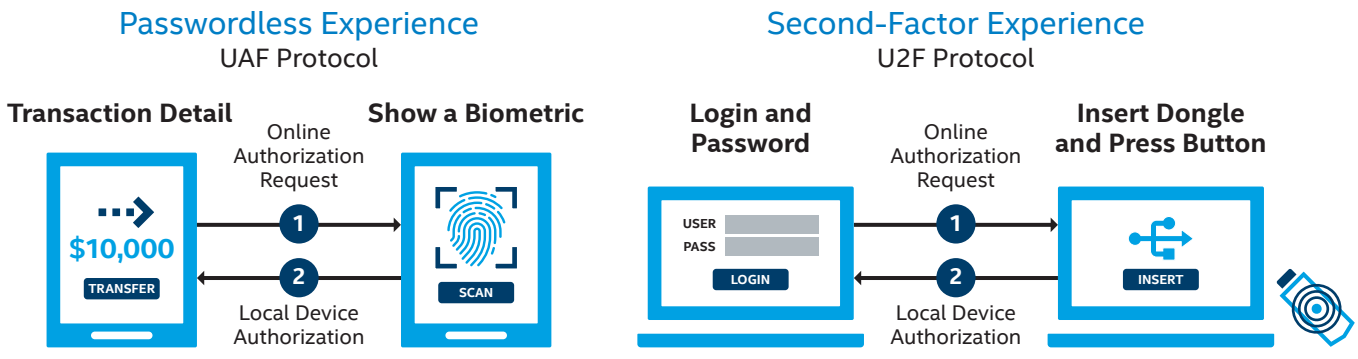

Figure 2. FIDO*-based solutions reduce reliance on passwords while providing a superior and trusted authentication experience.

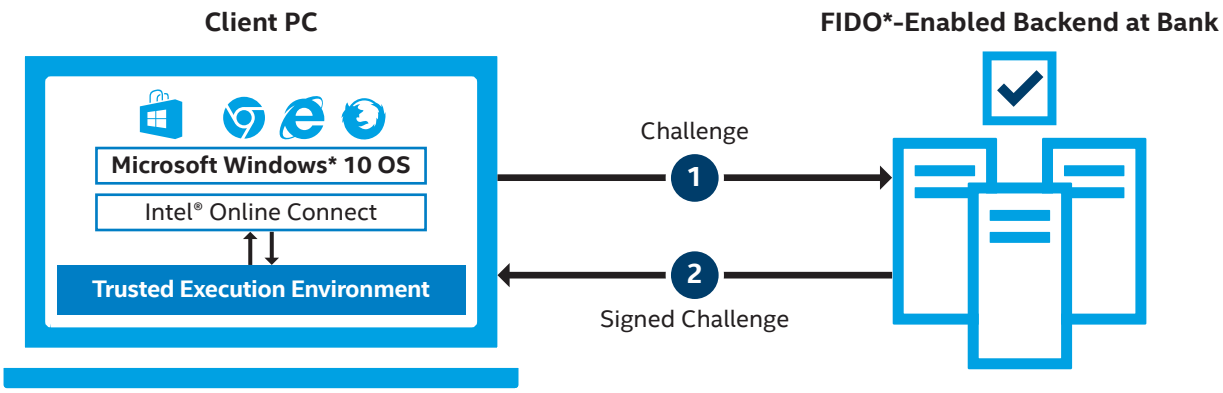

Figure 3. Intel® Online Connect, which uses hardware-based security, combines with Fast IDentity Online* (FIDO*) to better protect against attacks.

Intel® Technology Strengthens FIDO* Authentication

Intel has recently released Intel® Online Connect, a PC-based FIDO-compliant authenticator technology that uses a built-in trusted execution environment to generate and store a private key, which is used to authenticate the device to the FIDO backend. Having the FIDO keys stored in a trusted execution environment means that they are outside of the OS and out of reach to MitM and MitB attacks.

Intel Online Connect is FIDO-certified and it enables third-party solution providers to use it as a silent authenticator for second-factor authentication. It can be used without any user interaction to provide device ID capabilities, or coupled with a user-presence factor such as a biometric (integrated fingerprint identification). The biometric information is not exposed to the OS.

When using integrated fingerprint identification, users can authenticate using a fingerprint scan. A fingerprint match releases the signed FIDO challenge to the backend. Hardware-based security adds another layer of protection beyond FIDO itself (Figure 3). Intel® Software Guard Extensions (Intel® SGX) provides the trusted execution environment to protect the biometric authentication factor on the client device so that the biometric information is not exposed to the backend.

Intel Online Connect is easy to integrate into existing FIDO deployments. There are no extra steps required on the backend, and it can be activated on the PC with a single click. It supports all browsers and Windows* store apps.

Conclusion

The FIDO Alliance and Intel are moving forward with industry-leading collaboration to strengthen and also simplify authentication. The resulting hardware-based authentication that resides outside the OS enables stronger security compared to software-only solutions. By adopting FIDO and taking advantage of Intel Online Connect, the banking industry can protect its assets and reputation and provide customers with greater protection against malware and fraud.

Find the solution that is right for your organization. Contact your Intel representative or visit **intel.com/FSI**.

Solution Provided By:

fido® intel®

[1] "Banks Stop $11 Billion in Fraud Attempts in 2014," American Bankers Association.
[2] "5 Top Fraud Risks for Financial Institutions in 2016," Hagai Schaffe.
[3] "Bank fraud leaps by a quarter to £755m in just one year," Lee Boyce.
[4] "Survey Says: People Have Way Too Many Passwords To Remember," Joseph Bernstein.
[5] "Online Overload – It's Worse Than You Thought," Tom Le Bras.
[6] "The Memorability and Security of Passwords – Some Empirical Results," Jianxin Yan, Alan Blackwell, Ross Anderson, Alasdair Grant, Cambridge University Computer Laboratory.
[7] "Lenovo's Yoga 910 laptop will get touchy with customer security thanks to FIDO," Kevin Parrish.
[8] "The Password Is Passé," Peter Lucas.

0117/JWIL/KC/PDF ♻ Please Recycle 334994-001US