Trust your login

The strength of the FIDO authentication protocol with NXP secure elements

Make username and passwords a thing of the past by upgrading your login to support strong authentication with easier-to-use NXP secure elements.

The average person uses dozens of online services, accessing everything from email and social media to banking, shopping, personal health, home automation, and more. New services are coming online every day, and each requires its own login, involving a username and password. Having to keep track of all those username/password combinations can be frustrating, and, despite warnings about the importance of security, there are still millions of people using weak passwords that are easy to hack.

At the same time, news headlines are a daily reminder that cyber attacks, aimed at stealing usernames, passwords, and other private information, are growing in frequency and scale. The Identity Theft Resource Center (ITRC), a consumer advocacy group, reports that, in 2014 alone, there were 783 data breaches in the US, with 86 million personal records stolen. That's an average of more than two data breaches a day, with roughly one in every four Americans having their identities compromised.

As the risks continue to grow — the ITRC says identity theft is increasing at an annual rate of more than 25% — it becomes even clearer that we need a more secure way to log in. Many people think that stronger security is, by definition, harder to use, but that's not the case. A new approach to logins, based on FIDO authentication with secure elements, proves that security can be both simple and strong, intuitive yet trustworthy and private.

fido™ alliance | simpler stronger authentication

What is FIDO authentication?

The Fast IDentity Online (FIDO) specification defines a way to access online services without having to type in a username or password. FIDO is strong authentication, which means it increases security by going beyond the simple combination of a username and password. It uses a dedicated security key or a biometric, like a fingerprint, to perform a more rigorous kind of authentication.

The FIDO specification is developed and guided by the FIDO Alliance, a member-driven organization that includes some of the biggest names in online services, component and service design, and software development. The specification was finalized in 2014, and is quickly gaining momentum. FIDO keys are already available from several retailers, including Amazon and many major online players, including Google, PayPal, and Alibaba, already support FIDO authentication. Samsung has released FIDO-enabled smartphones, and Microsoft has announced that FIDO will be part of Windows 10.

How does FIDO work?

FIDO can be implemented in one of two ways: in a standalone authentication device, called a security

NXP

key, or embedded in the system itself. Standalone security keys use the Universal 2nd Factor (U2F) protocol, while embedded systems use the Universal Authentication Framework (UAF) protocol. Either way, the authentication process is seamless, secure, and simple to use. It's also protected from phishing, man-in-the-middle (MITM), man-in-the-browser (MITB), and other kinds of attacks.

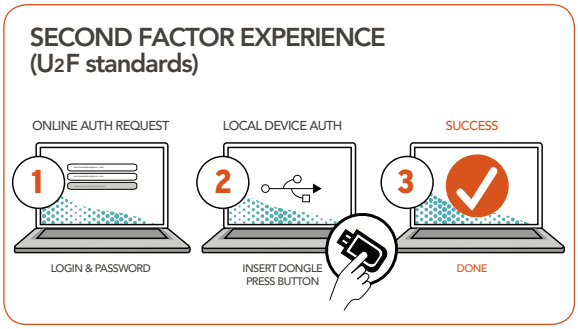


Figure 1. Second factor experience (U2F standards)

With a standalone U2F security key, deployment is remarkably easy. All you do is get a security key (or use one supplied by your service provider), register it with your existing web service, and then start using the enrolled device for authentication. No personal data is collected and stored on the U2F security key. To ensure privacy, the U2F security key is only used for FIDO authentication, and the only information it contains is the unique private key used with the authentication process. To reduce risk further, the private key remains on the U2F security key, and is not stored on servers maintained by the online service or a third party. Similarly, the backend FIDO server only stores login information that has been encrypted.

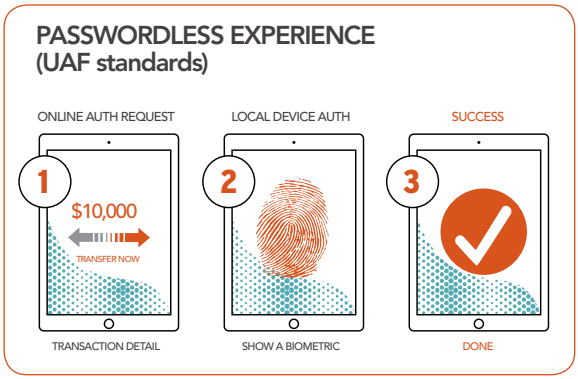


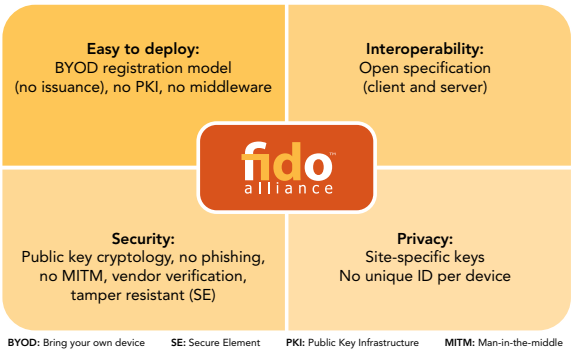
Figure 2. Passwordless experience (UAF standards)

Get it, register it, use it. It's that simple.

The UAF scheme uses FIDO technology embedded in the end-user device itself. Since the manufacturer has already equipped the device with FIDO functionality, using UAF is even more convenient, because there's no separate device to keep track of.

On a UAF-enabled smartphone with a fingerprint sensor, for example, you might want to log in to your bank and make a transfer. As part of the transaction, you would press your thumb against the phone's fingerprint reader to perform authentication. The biometric data stays private on the phone, and is never sent over the network, where it might be vulnerable to attack. If the smartphone doesn't have a biometric sensor, but is equipped with a secure element that provides a cryptographic token, then a simple four-digit PIN can confirm the transaction. There's no need for a complex username/password combination.

FIDO value proposition



What does a FIDO-enabled device look like?

Since the UAF protocol can be embedded into just about any system — laptop, tablet, smartphone, watch, fitness bracelet, headset or home appliance — FIDO can be a seamless part of system operation. When FIDO is designed into a standalone security key, using the U2F protocol, the key can take on many forms. USB sticks are popular, as are keys that use some form of wireless connectivity, such as Near Field Communication (NFC) or Bluetooth Low

Energy (BLE). FIDO's high degree of flexibility means designers can choose just about any format they want for their application, since any "FIDO-ready" device can provide authentication to any online service equipped to support FIDO.

How does FIDO protect private information?

Several features make FIDO a stronger authentication method that protects sensitive data. The protocol uses strong public-key or asymmetric cryptography, based on elliptic curves, which uses two separate keys, one public and one private, to safeguard data. The public key is shared with the web service, but the private key remains hidden and protected, and is only used during the login process. This provides the highest level of security and privacy.

No data is collected during a FIDO operation, and any U2F security key registered to a particular website can only be used for login by that website. This protects against phishing, since user accounts can't be linked between online services. U2F security keys are produced in batches that use a single serial number to refer to more than 10,000 keys, so keys are essentially untraceable. Also, any biometric data, such as a finger- or voiceprint, collected by the FIDO authenticator, remains on the device; it's never exposed to the network.

The U2F and UAF schemes also support use of an attestation key. Injected at manufacturing, the attestation key is used to verify that the FIDO-enabled device or security key is, in fact, a FIDO-ready device produced by an authorized manufacturer that the web service accepts onto their network.

Secure elements

One of the strongest security features of FIDO, though, is the fact that the U2F and UAF FIDO protocols can work with a specialized, tamper-resistant microcontroller, called a secure element, which performs cryptographic processing, generates random numbers, and stores the authentication and attestation keys. The secure element hides authentication data, prevents information from leaking onto the network, and protects data from a wide range of attacks. The secure element is like a vault that protects the unique private key, adding an extra level of protection simply not possible with a software-only approach.

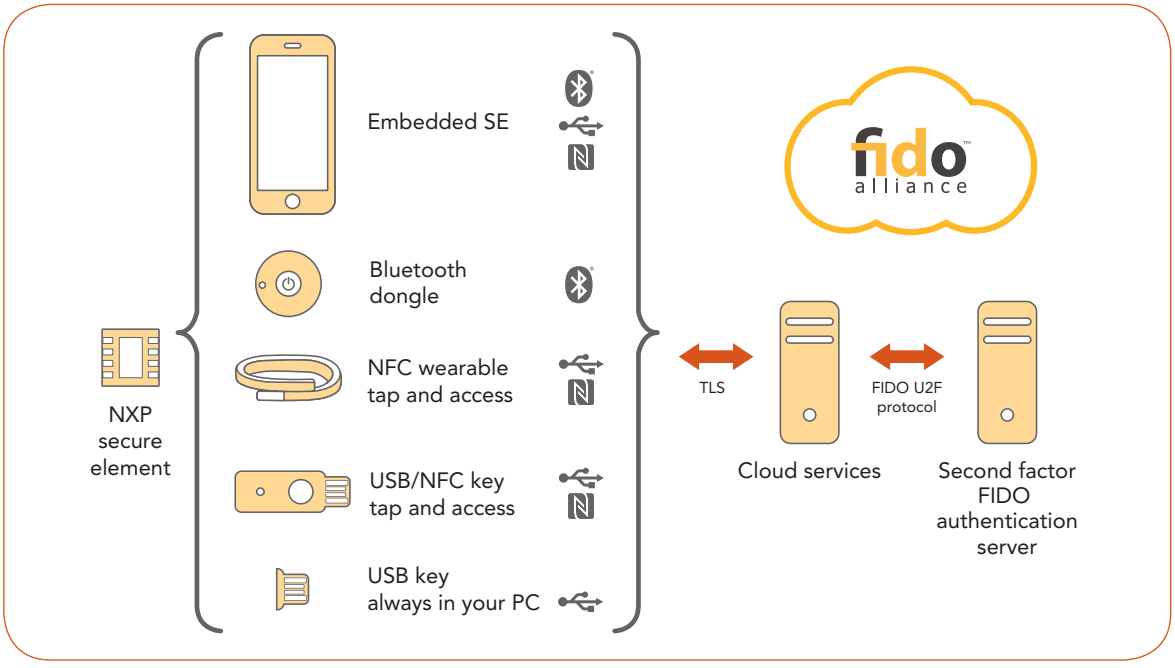
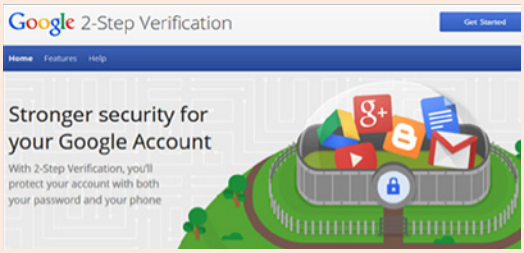


Figure 3. The secure element acts as a vault, adding an extra level of protection simply not possible with a software-only approach

The secure element is like a vault that protects the unique private key.

How does FIDO operate within an online service?
The FIDO specification defines a dedicated authentication server for use with cloud-based services. The provider of the online service, referred to by the FIDO Alliance as the relying party, deploys a FIDO authentication server that runs the FIDO U2F/UAF protocol.

If, for example, you're using a FIDO security key with a FIDO-enabled browser, like Google Chrome, the relying party uses a FIDO server to authenticate the FIDO security key. The process uses an authentication scheme based on challenge-signature response. The FIDO server sends a unique, random challenge to the FIDO security key. The FIDO security key digitally signs the challenge, using the private key, and sends it back to the server.



In October 2014, Google, in combination with the Google Chrome browser, became the first web service to support the open FIDO U2F protocol. To authenticate at login, users insert their Security Key into their computer's USB port and tap it when prompted by the Google Chrome browser. The setup works with any USB device supplied by a tested and approved "FIDO Ready" U2F supplier. There's no need for drivers, client software, or middleware, and the authentication process can't be phished, since the security key won't provide its cryptographic signature if a fake site attempts to impersonate a Google sign-in page.

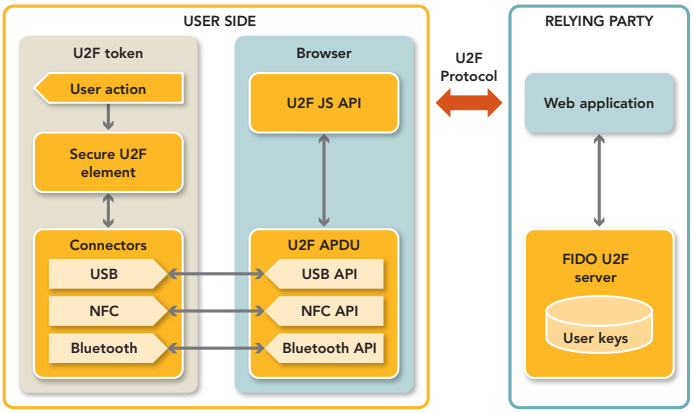


Figure 4. Using a FIDO U2F security key with a FIDO-enabled browser

The FIDO server then verifies the challenge and its signature, using the public key, to authenticate the user.

The concept is the same if you're using a UAF-enabled device.

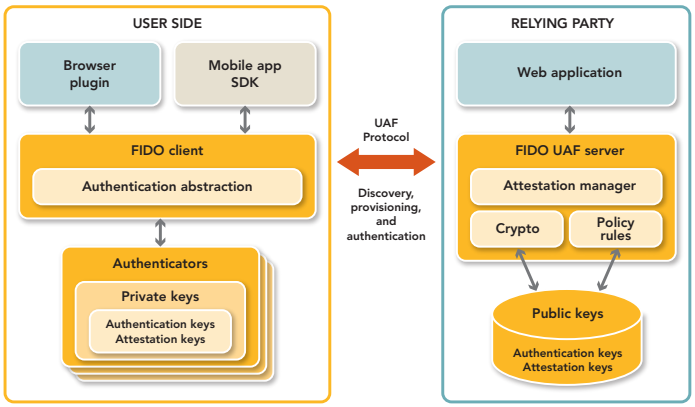


Figure 5. Using a UAF-enbaled device with a FIDO server

In either case, FIDO is a highly secure method of authentication. It is for this reason that relying parties of all kinds, including the world's most prominent payment companies, are such strong supporters of FIDO.

FIDO, secure elements, and the enterprise

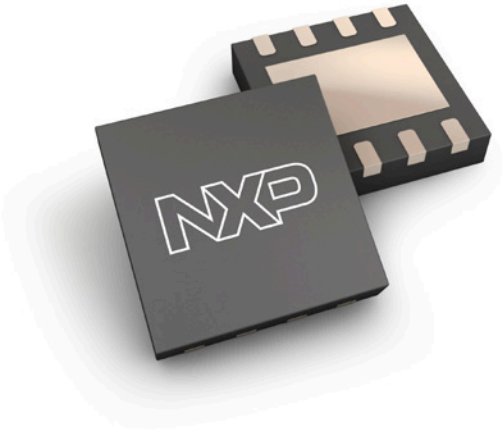
FIDO can help workers the same way it helps consumers. Many enterprise security applications — including Windows logon, VPN, email and hard-drive encryption, digital signature, and physical access — already use smartcards or USB keys that rely on secure elements to protect encryption keys and related information. FIDO is an easy add-on that can extend enterprise applications to the cloud, providing high-level security for cloud logins. Employee badges can become multi-purpose devices for physical and virtual access, and there's no middleware deployment for authentication. What's more, the IT department can support a heterogeneous computing environment, with support for tablets, mobile devices, and even BYOD scenarios, while replacing complicated token-issuance schemes with simple, user-based registration.

NXP and FIDO

NXP co-authored the original version of the U2F specification and became a FIDO Alliance member early on. We bring decades of bank- and government-grade security experience and technology leadership to FIDO and the computing industry, and are committed to the widespread use of FIDO authentication.

Billions of units shipped

For more than 15 years, NXP has been a leader in the use of secure elements for multi-factor authentication schemes. Our security technology has already seen extensive global deployment, with billions of units shipped to support mobile payment, bank cards, physical access, transit, and ePassport applications. We now bring all that expertise to FIDO, by providing the secure elements that are at the heart of the FIDO authentication protocol, and by offering complete hardware and software support for FIDO implementations.



NXP A7 Series secure element ICs

NXP supports the FIDO U2F and UAF protocols with secure elements based on our proven SmartMX architecture. The A7 Series runs a secure OS, supports state-of-the-art cryptography, and has earned EAL 5+ certification for hardware and software implementations. The A7 Series uses special manufacturing techniques to prevent reverse engineering. The IC architecture, including the memory, is laid out in a random format, and the metal wires are placed on different layers, so they're inaccessible. Shielding hides circuitry from view and prevents access to data if the IC package is opened, and on-chip sensors, which track light, voltage, and temperature, reset the IC if readings are out of range. These and many other features make the A7 Series resistant to a wide range of threats, including side-channel attacks.

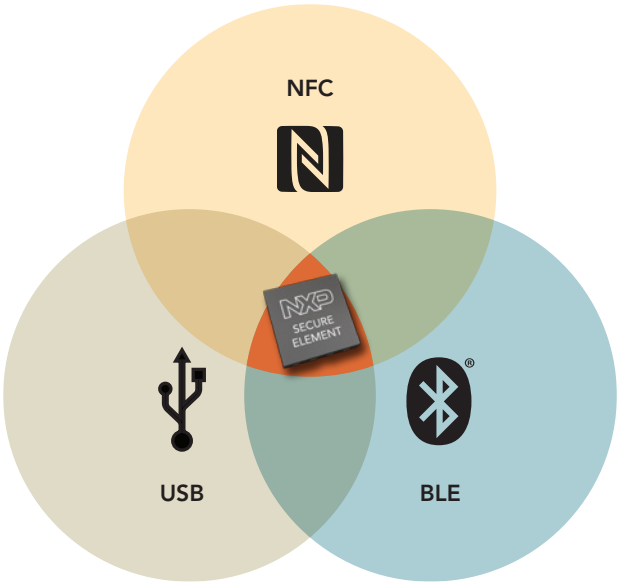
Trusted security with the A7 Series

- SmartMX secure MCU core
- CC EAL 5+ certified
- Tamper and attack resistance
- Trust provisioning and key management
- Secure multi-application software platform (Java Card)
- Verified interoperability

Complete solutions for FIDO authentication

As a recognized innovator in connectivity, NXP provides options that make it easy to combine A7 Series secure elements with USB, BLE, or NFC. We enable FIDO U2F authentication in a number of form

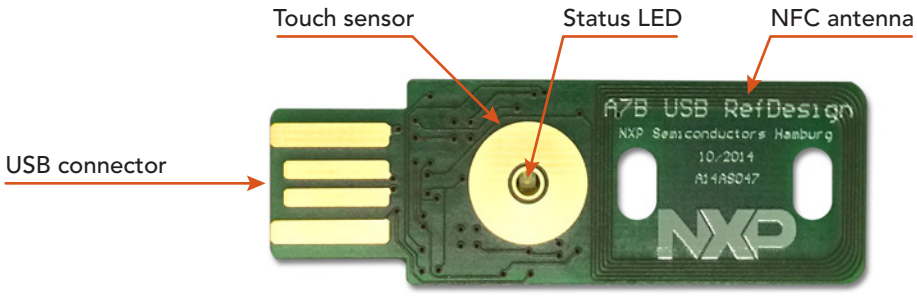
factors, from USB tokens to new options like key fobs, wearables, smart cards, and more. We supply everything needed for a complete application — including software and secure-key generation and insertion — all with proven interoperability.



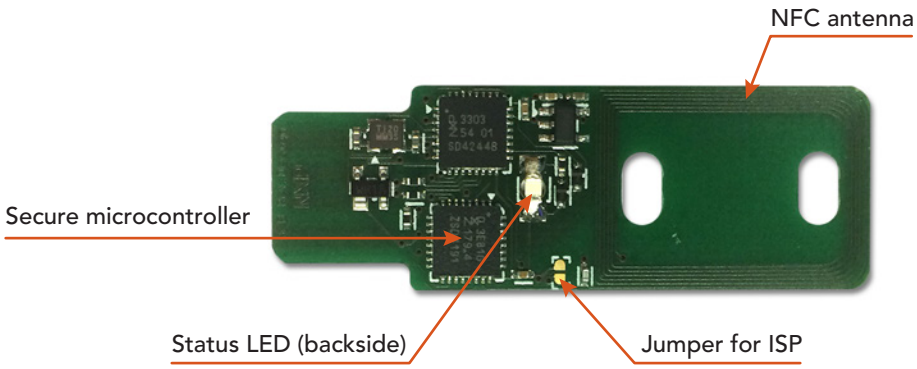
NXP delivers the complete package

- FIDO U2F secure elements
- NFC/BLE/USB connectivity
- Trust provisioning and key management
- Secure Java Card OS, crypto-library, FIDO application
- Tested interoperability
- Certified interfaces and drivers

USB reference design



Hardware top view — A7B USB reference design



Hardware bottom view — A7B USB reference design

The bottom line

Strong, trustworthy logins are the starting point for online security, but the login process still needs to be convenient and easy to use. FIDO authentication with secure elements makes this a reality, by performing multi-factor authentication in a simple, straightforward way. The result is a substantially better way to protect logins. FIDO promises an end to insecure login schemes that rely on hard-to-remember, difficult-to-type username/password combinations.

FIDO may be a recent entrant in the market, but it's already catching on in a very big way. FIDO-enabled logins are widely available and leading online services, including Google, PayPal, and others, already use them.

NXP, a global leader in semiconductors for security, helped shape the FIDO standard, and is committed to making FIDO the authentication method of choice for online access. Our proven A7 Series of secure elements provides tamper-resistant protection of private data, and we supply all the necessary ingredients, including connectivity ICs, software stacks, reference designs, and trust provisioning, to deliver interoperable FIDO solutions.

NXP and FIDO go together.

To learn more, visit www.nxp.com.

Useful links

FIDO Alliance
https://fidoalliance.org

NXP on cloud security
www.nxp.com/applications/cyber-security/cloud-security.html

www.nxp.com

Date of release: April 2015

Published in the USA