At Yubico, we are often asked why we are so dedicated to bringing the FIDO U2F open authentication standard  to life when our YubiKeys already support the OATH OTP standard. Our quick answer is that we will always provide multiple authentication options to address multiple use cases. Regarding U2F and OTP, we think both have unique qualities.

**OTP**

The one-time password (OTP) is a very smart concept. It provides a strong level of protection to hundreds of millions of accounts, and has been implemented for decades. Its popularity comes from its simplicity. On top of a static user name/password credential, a user adds another authentication factor — one that is dynamically generated. By definition, this OTP credential is valid for only one login before it becomes obsolete.

OTPs are delivered in many ways, usually via an object the user carries with him, such as his mobile phone (using SMS or an app), a token with an LCD-display, or a YubiKey. OTP technology is compatible with all major platforms (desktop, laptop, mobile) and legacy environments, making it a very popular choice among second-factor protocols.

As good as it is, traditional OTP has limitations.

* Users need  to type codes during their login process.
* Manufacturers often possess the seed value of the tokens.
* Administrative overhead resulting from having to set up and provision devices for users.
* The technology requires the storage of secrets on servers, providing a single point of attack.

Yubico’s OTP implementation solves some of those issues.

* The user never has to type a code instead he just touches a button.
* Enterprises can configure their own encryption secrets on a YubiKey, which means no one else ever sees those secrets.
* OTPs generated by a YubiKey are significantly longer than those requiring user input (32 characters vs 6 or 8 characters), which means a higher level of security.
* YubiKeys allow enrollment by the user, which reduces administrative overhead.
* It is easy to implement with any existing website with no client software needed.
* For the OATH standard, Yubico uniquely offers a token prefix that can be used for identity, simplifying enrollment and user experience.

The remaining issues, however, are phishing and man-in-the-middle attacks, the most  infamous assaults that defeat OTP technology. The theory is quite simple: the hacker sets up a fake website designed to trick visitors into submitting their credentials. When a user falls into the trap and enters his information (user name, password, and even his one-time password), it is immediately intercepted by the hacker and used to access the victim’s account.

It is difficult to pull off, especially against security-aware users who may notice the strange behavior of the fake site, yet it is can be done and is, nowadays, one of the more popular attacks.

**FIDO U2F**

The increasing sophistication of attacks against OTP schemes was a motivating factor in the development of the FIDO U2F protocol.

The U2F protocol involves the client in the authentication process (for example, when logging in to a web application, the web browser is the client). When a user registers a U2F device with an online service, a public/private key pair is generated.

After registration, when the user attempts to log in, the service provider sends a challenge to the client. The client compiles information about the source of the challenge, among other information. This is signed by the U2F device (using the private key) and sent back to the server (service provider).

Real-time challenge-response schemes like U2F address OTP vulnerabilities such as phishing and various forms of man-in-the-middle attacks. As the legitimate server is issuing the challenge, if a rogue site or middle-man manipulates the flow, the server will detect an abnormality in the response and deny the transaction.

Advantages of U2F include:

* Strong security from public key cryptography.
* Easy to use with no codes to re-type and no drivers to install.
* High privacy so that no personal information is associated with a key.
* Unlimited usage in that an unlimited number of accounts can be protected by one single device.

With all of these great benefits, why isn’t FIDO U2F implemented in more large scale services beyond Google, Dropbox, and GitHub? One reason is that the Chrome browser is the only available client. We expect Mozilla Firefox support during the Spring and within two more browsers later this year, which will make U2F available to the vast majority of internet users. Also, it takes time to drive new global standards and U2F’s technical specifications were made available just a year ago.

If you are thinking about improving strong authentication for your service, OTP is a good start, but FIDO U2F should definitely be on your radar. Here are a few useful links:

* [Protocol details from Yubico’s developer’s website](https://developers.yubico.com/U2F/Protocol_details/)
* [U2F Webinar: From Concept to Implementation (from Yubico)](https://www.yubico.com/2015/10/u2f-webinar-from-concept-to-implementation-2/)
* [Contactless, tokenless, passwordless mobile authentication (Yubico blog)](https://www.yubico.com/2016/01/fido-u2f-now-offers-contactless-tokenless-passwordless-mobile-authentication/)