yubico

Introducing WebAuthn: The W3C Standard for Multi-Factor and Passwordless Authentication

With the introduction of WebAuthn, Yubico and the members of the W3C have helped advance a standardized approach to strong authentication for web and mobile applications and services.

The current use of password and SMS-based authentication creates a poor user experience and a heavy support load due to helpdesk calls, resulting in lost productivity and high IT costs. While two-factor and multi-factor authentication have been demonstrated to be effective in protecting users from account takeover, the lack of a global standard across browsers and operating systems has hampered widespread adoption of strong authentication to date.

Web Authentication, or WebAuthn, is a new global standard introduced by the World Wide Web Consortium (W3C) and FIDO Alliance for secure authentication on the Web. WebAuthn is compatible with FIDO2 and Universal 2nd Factor (U2F) security keys like the YubiKey. Users are able to use existing U2F and newer FIDO2 YubiKeys for a strong authentication-based login across web browsers, services, and applications that have upgraded to WebAuthn.

WebAuthn defines a standard API that enables web and mobile applications to easily invoke strong authentication via support built-in to all leading browsers and web platforms. Microsoft, Google, and Mozilla have committed to the WebAuthn standard, and rolled out support in their web platforms and browsers.[1] WebAuthn support is also currently on the developer preview version of Apple Safari. Works with YubiKey members 1Password, Daon, ForgeRock, Isosec, Microsoft, OneLogin, Ping Identity, Singular Key, StrongKey and Thycotic have integrated support for WebAuthn.

WebAuthn Authenticator	Example
Platform Authenticators Built-in to the computer or mobile device	Biometrics with TPM or TEE/ secure enclave • Fingerprint Reader • Face/Iris/Voice Recognition • PIN/pattern/passphrase with TPM or TEE/secure enclave
Roaming Authenticators Security Keys	USB (USB-A, USB-C) NFC (Near Field Communication) BLE (Bluetooth Low Energy)

Ease of use and greater choice for users

With WebAuthn, service providers can now provide users a choice of strong cryptographically backed authentication using a choice of security keys or built-in authenticators such as a biometric touchpad or camera on a laptop.

Best Practices

A best practice for service providers is to have users first register an external authenticator like the YubiKey and then register an internal authenticator.

[1] https://www.scip.ch/en/?labs.20180424

If the device with the internal authenticator gets lost, stolen, or compromised in any way, the external authenticator can be used as a portable root of trust to effortlessly gain access to the web service, disable the previously registered internal authenticator, and register a new internal authenticator on the new device.

Once the external authenticator is used to grant access to the service on the device, the internal authenticator can then be added as an additional mode of authentication. From that point on, the user can choose to use either the internal or external authenticator whenever they authenticate to the service.

Previously, methods such as passwords or SMS were often used as the method to bootstrap or recover a device, however this approach creates a less than ideal user experience and weak security methods.

Going beyond passwords for stronger security

WebAuthn uses asymmetric (public-key) cryptography and origin (relying party) bound key validation instead of passwords or SMS for registering and authenticating with websites. This resolves significant security vulnerabilities, such as phishing, phone number porting scams and similar attacks that could potentially lead to data breaches.

Easy to implement strong authentication

WebAuthn greatly simplifies and standardizes the integration of advanced authentication options for web and mobile applications using external and internal authenticators. WebAuthn makes it easy for developers to create secure applications and enable strong authentication to effectively protect user accounts from phishing and other forms of account takeovers.

The Yubico Developer Program provides resources to enable rapid implementation of strong authentication. Resources include workshops, documentation, implementation guides, APIs, and SDKs. Sign up to receive updates and access to resources for implementing WebAuthn: yubico.com/for-developers.

Resources

- About WebAuthn: www.yubico.com/webauthn
- "The YubiKey as the WebAuthn Root of Trust" blog post: www.yubico.com/the-yubikey-as-the-webauthn-root-of-trust/
- WebAuthn demo site: demo.yubico.com/webauthn
- Yubico Developer Site: developers.yubico.com

Works with YubiKey Partners with WebAuthn Support

1Password · Daon · FORGEROCK · isosec · Microsoft · onelogin · PingIdentity · SingularKey · STRONGKEY · thycotic

About Yubico Yubico sets new global standards for easy and secure access to computers, servers, and Internet accounts. Founded in 2007, Yubico is privately held with offices in Australia, Germany, Singapore, Sweden, UK, and USA. Learn why nine of the top 10 internet brands and millions of users in more than 160 countries use our technology at www.yubico.com.

Yubico AB
Olof Palmes gata 11
6th floor
SE-111 37 Stockholm
Sweden

Yubico Inc.
530 Lytton Avenue, Suite 301
Palo Alto, CA 94301 USA
844-205-6787 (toll free)
650-285-0088