FOR IMMEDIATE RELEASE

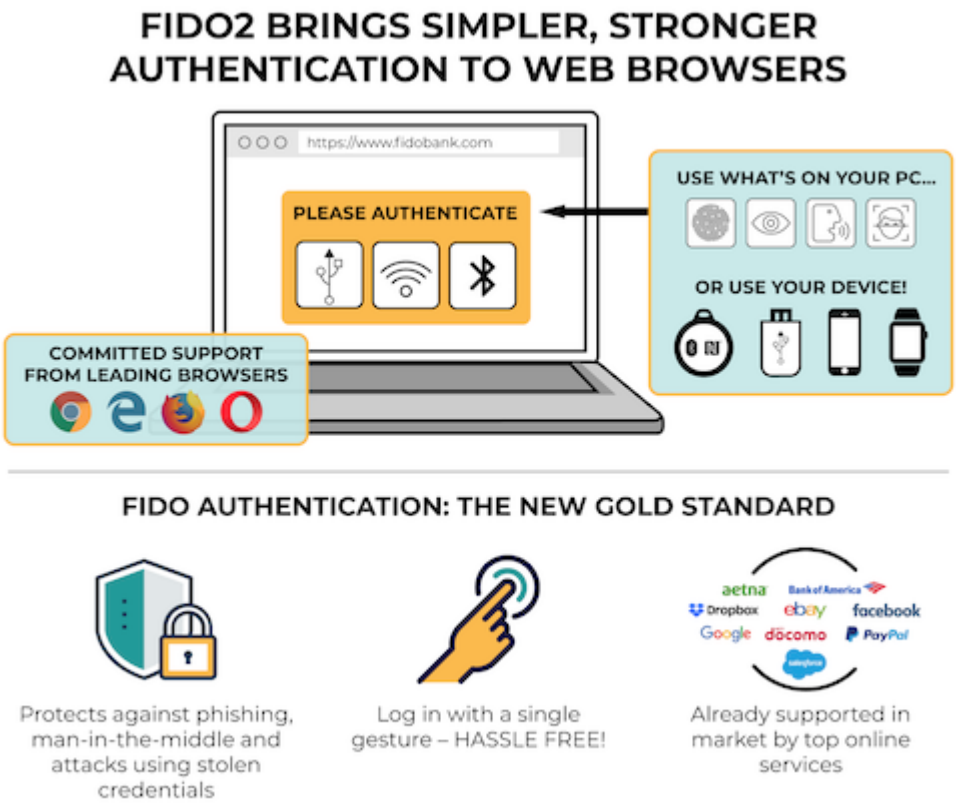
FIDO Alliance and W3C Achieve Major Standards Milestone in Global Effort Towards Simpler, Stronger Authentication on the Web

With support from Google Chrome, Microsoft Edge and Mozilla Firefox, FIDO2 Project opens new era of ubiquitous, phishing-resistant, strong authentication to protect web users worldwide

---

Read [testimonials from W3C Members]

Translations | W3C Press Release Archive



https://www.w3.org/ and Mountain View, Calif. — 10 April 2018 — The

FIDO Alliance and the World Wide Web Consortium (W3C) have achieved a major standards milestone in the global effort to bring simpler yet stronger web authentication to users around the world. The W3C has advanced Web Authentication (WebAuthn), a collaborative effort based on Web API specifications submitted by FIDO to the W3C, to the Candidate Recommendation (CR) stage. The CR is the product of the Web Authentication Working Group, which is comprised of representatives from over 30 member organizations. CR is a precursor to final approval of a web standard, and the W3C has invited online services and web app developers to implement WebAuthn.

WebAuthn defines a standard web API that can be incorporated into browsers and related web platform infrastructure which gives users new methods to securely authenticate on the web, in the browser and across sites and devices. WebAuthn has been developed in coordination with FIDO Alliance and is a core component of the FIDO2 Project along with FIDO's Client to Authenticator Protocol (CTAP) specification. CTAP enables an external authenticator, such as a security key or a mobile phone, to communicate strong authentication credentials locally over USB, Bluetooth or NFC to the user's internet access device (PC or mobile phone). The FIDO2 specifications collectively enable users to authenticate easily to online services with desktop or mobile devices with phishing-resistant security.

"*With the new FIDO2 specifications and leading web browser support announced today, we are taking a big step forward towards making FIDO Authentication ubiquitous across all platforms and devices,*" said Brett McDowell, executive director of the FIDO Alliance. "*After years of increasingly severe data breaches and password credential theft, now is the time for service providers to end their dependency on vulnerable passwords and one-time-passcodes and adopt phishing-resistant FIDO Authentication for all websites and applications.*"

Google, Microsoft, and Mozilla have committed to supporting the WebAuthn standard in their flagship browsers and have started implementation for Windows, Mac, Linux, Chrome OS and Android platforms. Both the WebAuthn and CTAP specifications are available today, enabling developers and vendors to get a jumpstart on building support for the next generation of FIDO Authentication into their products and services.

"*Security on the web has long been a problem which has interfered with the many positive contributions the web makes to society. While there are many web security problems and we can't fix them all, relying on passwords is one of the weakest links. With WebAuthn's multi-factor solutions we are eliminating this weak link,*" stated W3C CEO Jeff Jaffe. "*WebAuthn will change the way that people access the Web.*"

The completion of the FIDO2 standardization efforts, promotion of WebAuthn along the W3C standards track, and the commitment of leading browser vendors to implementation opens a new era of ubiquitous, hardware-backed FIDO Authentication protection for everyone using the internet.

Enterprises and online service providers looking to protect themselves and their customers from the risks associated with passwords — including phishing, man-in-the-middle attacks and the abuse of stolen

credentials — can soon deploy standards-based strong authentication that works through the browser or via an external authenticator. Deploying FIDO Authentication enables online services to provide choice to users from an interoperable ecosystem of devices people use every day like mobile phones and security keys.

The standardization of the new FIDO2 specifications in browsers and operating systems will further expand the reach of FIDO Authentication, which is referenced by regulators and standards-setting bodies worldwide and is already available on hundreds of millions of devices and offered to more than 3.5 billion user accounts worldwide through services from companies such as Google, Facebook, NTT DOCOMO, Bank of America and many more. The new specifications complement existing passwordless FIDO UAF and second-factor FIDO U2F use cases, and expand the availability of FIDO Authentication. FIDO2 web browsers and online services are fully backwards compatible with all previously certified FIDO Security Keys.

FIDO will soon launch interoperability testing and will issue certifications for servers, clients and authenticators adhering to FIDO2 specifications. The conformance test tools are available on FIDO's website. Additionally, FIDO will introduce a new Universal Server certification for servers that interoperate with all FIDO authenticator types (FIDO UAF, FIDO U2F, WebAuthn, CTAP).

WebAuthn and FIDO2 Project Benefits

W3C's WebAuthn API, a standard web API that can be incorporated into browsers and related web platform infrastructure, enables strong, unique, public key-based credentials for each site, eliminating the risk that a password stolen from one site can be used on another. A web application running in a browser loaded on a device with a FIDO Authenticator can easily call to a public API to enable simpler, stronger FIDO Authentication of users with cryptographic operations in place of, or in addition to password exchange, delivering many advantages to service providers and users alike:

- **Simpler authentication**: users simply log in with a single gesture using:
  - Internal or built-in authenticators (such as fingerprint or facial biometrics) in PCs, laptops and/or mobile devices
  - Convenient external authenticators, such as security keys and mobile devices, for device-to-device authentication using CTAP, a protocol for external authenticators developed by the FIDO Alliance that complements WebAuthn
- **Stronger authentication**: FIDO Authentication is much stronger than relying only on passwords and related forms of authentication, and has these advantages:
  - User credentials and biometric templates never leave the user's device and are never stored on servers
  - Accounts are protected from phishing, man-in-the-middle and replay attacks that use stolen passwords
- **Developers** can get started on creating apps and services that leverage FIDO Authentication on FIDO's new developer resources page.

About the FIDO Alliance

The FIDO (Fast IDentity Online) Alliance, www.fidoalliance.org, was formed in July 2012 to address the lack of interoperability among strong authentication technologies, and remedy the problems users face with creating and remembering multiple usernames and passwords. The FIDO Alliance is changing the nature of authentication with standards for simpler, stronger authentication that define an open, scalable, interoperable set of mechanisms that reduce reliance on passwords. FIDO authentication is stronger, private, and easier to use when authenticating to online services.

About the World Wide Web Consortium

The mission of the World Wide Web Consortium (W3C), www.w3.org, is to lead the Web to its full potential by creating technical standards and guidelines to ensure that the Web remains open, accessible, and interoperable for everyone around the globe. W3C develops well known specifications such as HTML5, CSS, and the Open Web Platform as well as work on security and privacy, all created in the open and provided for free and under the unique W3C Patent Policy. For its work to make online videos more accessible with captions and subtitles, W3C received a 2016 Emmy Award.

W3C's vision for "One Web" brings together thousands of dedicated technologists representing more than 400 Member organizations and dozens of industry sectors. W3C is jointly hosted by the MIT Computer Science and Artificial Intelligence Laboratory (MIT CSAIL) in the United States, the European Research Consortium for Informatics and Mathematics (ERCIM) headquartered in France, Keio University in Japan and Beihang University in China. For more information see https://www.w3.org/.

End Press Release

FIDO Alliance PR Contacts

Mike Smith or Adrian Loth, Montner Tech PR <fidopr@montner.com>
+1.203.226.9290 (US, Eastern Time)

W3C PR Contact

Amy van der Hiel, W3C Media Relations Coordinator <w3t-pr@w3.org>
+1.617.253.5628 (US, Eastern Time)

Testimonials from W3C members

-

Google Inc. • Microsoft Corp. • Mozilla

Google "Google Chrome is dedicated to building a better

Inc. web, and allowing developers to interact with secure keystores in a structured way helps us continue this mission. As a founding member of the U2F and FIDO2 working groups within FIDO, we're excited for the launch of these standards and look forward to our continued collaboration."

Sam Srinivas, Management Director, Google Cloud Security Product

Microsoft "Providing a password alternative that works across devices, apps, browsers, and websites delivers on our commitment to a future without passwords. We are excited to announce that we will add support for WebAuthn API, currently in the approval process stage, and W3C, in Microsoft Edge thanks to our work with the FIDO Alliance."

Dave Bossio, Group Program Manager, Operating System Security, Microsoft

Mozilla "With Web Authentication, we're giving people using Firefox the opportunity to add another layer of security to their browsing experience. Giving people greater control over how they manage their security online and making the internet safer is central to Mozilla's mission to keep the web open and accessible to all."

Selena Deckelmann, Senior Director of Engineering, Firefox Runtime, Mozilla

---

Translations | W3C Press Release Archive