fidoalliance.org

History of FIDO Alliance - FIDO Alliance

7-9 minutes

2009 – Validity Sensors and PayPal discuss using biometrics for identification of online users instead of passwords. The meeting inspired the idea to work on an industry standard designed around public key cryptography, enabling a passwordless log-in backed purely by local authentication.

July 2012 – The FIDO Alliance was founded by PayPal, Lenovo, Nok Nok Labs, Validity Sensors, Infineon, and Agnitio, and work on a passwordless authentication protocol began.

February 2013 – The Alliance was launched publicly.

April 2013 – Google , Yubico and NXP joined the Alliance and brought with them the idea of an open, second factor authentication protocol. Such second-factor devices were successfully deployed to Google employees as a precursor to publicly publishing the second-factor protocol.

February 2014 – Paypal and Samsung collaborate for the first deployment of FIDO authentication that enabled Samsung Galaxy S5 users to login and shop with the swipe of a finger in online, mobile and in-store payments wherever PayPal is accepted.

December 2014 – The completed v1.0 passwordless protocol (called FIDO Universal Authentication Framework - FIDO UAF) and the second-factor protocol (called FIDO Universal 2nd Factor - FIDO U2F) were completed and published simultaneously. Production deployments of fully compliant v1.0 devices and servers began.

February 2015 – Microsoft announced that it would support FIDO authentication in Windows 10, based on its contributions to new FIDO specifications.

May 2015 – The Alliance introduced the FIDO® Certified testing program, and the first FIDO Certified testing sessions were conducted.

May 2015 – NTT DOCOMO became the first mobile network operator to deploy FIDO Authentication, enabling a passwordless future for 65 million users in Japan.

June 2015 – The Alliance introduced the government membership program that attracted government agencies from the United States, United Kingdom, Germany and Australia.

October 2015 – The Alliance added the FIDO Cooperation and Liaison Program, which invites industry associations worldwide to collaborate on the influence development or implementation of FIDO standards.

June 2015 – The Alliance announces support in FIDO 1.0 specifications for contactless transport over Bluetooth and Near Field Communication (NFC).

November 2015 -The first FIDO Certified iOS products are announced as well as a line-up of smartphones from the

world's leading OEMs.

January 2016 – The Alliance launched the FIDO China Working Group (FCWG).

February 2016 – The World Wide Web Consortium (W3C) launched a new standards effort in Web Authentication based on the FIDO2 2.0 Web APIs submitted by the Alliance. The FIDO Alliance's intent with this work, called FIDO2, was to work with the W3C to standardize FIDO strong authentication across all web browsers and related web platform infrastructure.

September 2016 – Intel, Lenovo, PayPal and Synaptics, all FIDO Alliance board members, announced a collaboration to use FIDO standards to web-enable biometric authentication on the desktop.

December 2016 – The FIDO Japan Working Group (FJWG) was formed.

December 2016 – Over the course of 2016, Aetna, BcCard and Feitian joined the lineup of FIDO services on the FIDO Board.

January 2017 – Facebook announced support for FIDO Authentication. This announcement brought the number of user account that could can leverage FIDO to improve their account security to more than 3 billion.

March 2017 – The Alliance announced the Authenticator Certification Program, which introduces security requirements for authenticators going through FIDO Certification, with two levels: Level 1 (L1) Authenticator and FIDO Certified Level 2 (L2) Authenticator.

May 2017 – The Alliance launched a working group in India to further drive global FIDO standards adoption.

November 2017 – The FIDO Europe Working Group (FEWG) was formed.

December 2017 – The FIDO Korea Working Group (FKWG) was formed.

December 2017 – The Alliance announced updates to the specifications including FIDO UAF 1.1, making FIDO Authentication backed by hardware key attestation openly available on any Android 8.0 or later device without customization by the OEM.

January 2018 – Amazon joins the FIDO Board.

April 2018 – The W3C Web Authentication standard reached candidate recommendation and FIDO2 was officially launched. FIDO2 is comprised of the Web Authentication JavaScript API standard and FIDO's corresponding Client-to-Authenticator Protocol (CTAP). Leading major web browsers including Google Chrome, Mozilla Firefox and Microsoft Edge have implemented the standards; Android, Windows 10 and related Microsoft technologies pledge to have built-in support for FIDO Authentication soon.

September 2018 – The FIDO Alliance announced its Biometric Component Certification Program – the first such program for the industry at large. The program utilizes accredited independent labs to certify that biometric subcomponents meet globally recognized performance standards for biometric recognition performance and Presentation Attack Detection (PAD) and are fit for commercial use.

September 2018 – The FIDO Alliance announced the expansion of the Authenticator Certification Program, launching Level 3 (L3) and Level 3+ (L3+) testing and certification.

September 2018 – FIDO2 browser support and first certified products were made available to reduce password use on the web. With this, any website can leverage FIDO2 strong authentication protocols from the W3C and FIDO Alliance to replace passwords with cryptographically secure logins using convenient alternatives like on-device biometrics and FIDO Security Keys.

December 2018 – Two FIDO specifications – FIDO UAF 1.1 and CTAP – were recognized as international standards by the International Telecommunication Union's Telecommunication Standardization Sector (ITU-T). This milestone established FIDO UAF 1.1 and CTAP as official ITU standards (ITU-T Recommendations) for the global infrastructure of information and communication technologies (ICT).

February 2019 – The FIDO Alliance announced the Samsung Galaxy S10 and S10+ smartphones as the first to achieve certification from the FIDO Alliance's new Biometric Component Certification Program.

February 2019 – Android earned FIDO2 Certification, enabling simpler, stronger authentication for over a billion devices running on the platform. This gave users the ability to leverage their device's built-in fingerprint sensor and/or FIDO security keys for secure passwordless access to websites and native applications that support the FIDO2 protocols.

March 2019 – W3C's Web Authentication (WebAuthn) recommendation – a core component of the FIDO Alliance's FIDO2 set of specifications – became an official web standard, signaling a major step forward in making the web more secure and usable for users around the world.

May 2019 – Windows Hello earned FIDO2 Certification,enabling Windows 10 users to move beyond centrally-stored passwords and leverage Windows Hello biometrics or PINs to access their devices, apps, online services and networks with FIDO Certified security.