Universal 2nd Factor

From Wikipedia, the free encyclopedia

[Jump to navigation](https://en.wikipedia.org/wiki/Universal_2nd_Factor#mw-head)[Jump to search](https://en.wikipedia.org/wiki/Universal_2nd_Factor#searchInput)

[](https://en.wikipedia.org/wiki/File:U2F.USB-Token.jpg)

A U2F Security Key by Yubico

[](https://en.wikipedia.org/wiki/File:KEY-ID_FIDO.gif)

FIDO certified U2F identity credential with USB interface

**Universal 2nd Factor** (**U2F**) is an [open standard](https://en.wikipedia.org/wiki/Open_standard) that strengthens and simplifies [two-factor authentication](https://en.wikipedia.org/wiki/Two-factor_authentication) (2FA) using specialized [Universal Serial Bus](https://en.wikipedia.org/wiki/Universal_Serial_Bus) (USB) or [near-field communication](https://en.wikipedia.org/wiki/Near-field_communication) (NFC) devices based on similar security technology found in [smart cards](https://en.wikipedia.org/wiki/Smart_card).[[1]](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_note-Google_security_keys-1)[[2]](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_note-Using_Security_Key-2)[[3]](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_note-USB_key_drive_could_remove_the_hassles-3)[[4]](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_note-FIDO_Universal_2nd_Factor-4)[[5]](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_note-Google_Wants_To_Make_Passwords_Obsolete-5)

While initially developed by [Google](https://en.wikipedia.org/wiki/Google) and [Yubico](https://en.wikipedia.org/wiki/YubiKey), with contribution from [NXP Semiconductors](https://en.wikipedia.org/wiki/NXP_Semiconductors), the standard is now hosted by the [FIDO Alliance](https://en.wikipedia.org/wiki/FIDO_Alliance).[[6]](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_note-FIDO_Alliance_standards-6)[[7]](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_note-Google_Accounts_Now_Support_Security_Keys-7)



**Contents**

* [1Design](https://en.wikipedia.org/wiki/Universal_2nd_Factor#Design)
* [2Support and use](https://en.wikipedia.org/wiki/Universal_2nd_Factor#Support_and_use)
* [3Specifications](https://en.wikipedia.org/wiki/Universal_2nd_Factor#Specifications)
* [4References](https://en.wikipedia.org/wiki/Universal_2nd_Factor#References)

Design[[edit](https://en.wikipedia.org/w/index.php?title=Universal_2nd_Factor&action=edit&section=1)]

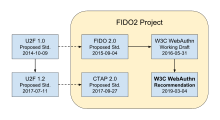
The USB devices communicate with the host computer using the [human interface device](https://en.wikipedia.org/wiki/Human_interface_device) (HID) protocol, essentially mimicking a keyboard.[[8]](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_note-Auto58-16-8) This avoids the need for the user to install special hardware driver software in the host computer, and permits application software (such as a browser) to directly access the security features of the device without user effort other than possessing and inserting the device. Once communication is established, the application exercises a [challenge–response authentication](https://en.wikipedia.org/wiki/Challenge%E2%80%93response_authentication) with the device using [public-key cryptography](https://en.wikipedia.org/wiki/Public-key_cryptography) methods and a secret unique device key manufactured into the device.[[9]](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_note-Auto58-17-9) The device key is vulnerable to [malicious manufacturer duplication](https://en.wikipedia.org/wiki/ID-based_encryption), and logically secured against reverse-engineering or counterfeiting by the robustness of the encryption and physical possession.

Support and use[[edit](https://en.wikipedia.org/w/index.php?title=Universal_2nd_Factor&action=edit&section=2)]

U2F security keys are supported by [Google Chrome](https://en.wikipedia.org/wiki/Google_Chrome) since version 38[[2]](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_note-Using_Security_Key-2) and [Opera](https://en.wikipedia.org/wiki/Opera_(web_browser)) since version 40. U2F security keys can be used as an additional method of two-step verification on online services that support the U2F protocol, including Google,[[2]](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_note-Using_Security_Key-2) [Dropbox](https://en.wikipedia.org/wiki/Dropbox_(service)),[[10]](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_note-Auto58-1-10) [GitHub](https://en.wikipedia.org/wiki/GitHub),[[11]](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_note-Auto58-2-11) [GitLab](https://en.wikipedia.org/wiki/GitLab),[[12]](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_note-Auto58-3-12) [Bitbucket](https://en.wikipedia.org/wiki/Bitbucket),[[13]](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_note-Auto58-4-13) [Nextcloud](https://en.wikipedia.org/wiki/Nextcloud),[[14]](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_note-Auto58-5-14) [Facebook](https://en.wikipedia.org/wiki/Facebook),[[15]](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_note-Auto58-6-15) and others.[[16]](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_note-Auto58-7-16)

Chrome, [Firefox](https://en.wikipedia.org/wiki/Firefox), and Opera were, as of 2015, the only browsers supporting U2F natively. [Microsoft](https://en.wikipedia.org/wiki/Microsoft) has enabled FIDO 2.0 support for [Windows 10](https://en.wikipedia.org/wiki/Windows_10)'s [Windows Hello](https://en.wikipedia.org/wiki/Windows_10#System_security) login platform.[[17]](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_note-Auto58-8-17) Microsoft [Edge](https://en.wikipedia.org/wiki/Microsoft_Edge)[[18]](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_note-Auto58-9-18) browser gained support for U2F in the October 2018 Windows Update. [Microsoft accounts](https://en.wikipedia.org/wiki/Microsoft_account), including [Office 365](https://en.wikipedia.org/wiki/Office_365), [OneDrive](https://en.wikipedia.org/wiki/OneDrive), and other Microsoft services, do not yet have U2F support. [Mozilla](https://en.wikipedia.org/wiki/Mozilla) has integrated it into Firefox 57, and enabled it by default in Firefox 60[[19]](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_note-Auto58-10-19)[[20]](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_note-Auto58-11-20)[[21]](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_note-Auto58-12-21)[[22]](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_note-Auto58-13-22) and [Thunderbird](https://en.wikipedia.org/wiki/Mozilla_Thunderbird) 60.[[23]](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_note-Auto58-14-23) Microsoft Edge starting from build 17723 support FIDO2.[[24]](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_note-Auto58-15-24). As of iOS and iPadOS 13.3 Apple now supports U2F in the Safari browser on those platforms.

Specifications[[edit](https://en.wikipedia.org/w/index.php?title=Universal_2nd_Factor&action=edit&section=3)]

[](https://en.wikipedia.org/wiki/File:Evolution_of_FIDO2-WebAuthn.svg)

The evolution of the U2F protocol standard

The U2F standard has undergone two major revisions:

* U2F 1.0 Proposed Standard (October 9, 2014)[[25]](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_note-Auto58-18-25)
* U2F 1.2 Proposed Standard (April 11, 2017)[[26]](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_note-Auto58-19-26)

Additional specification documents may be obtained from the FIDO web site.[[27]](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_note-Auto58-20-27)

The U2F 1.0 Proposed Standard (October 9, 2014) was the starting point for a short-lived specification known as the FIDO 2.0 Proposed Standard (September 4, 2015). The latter was formally submitted to the [World Wide Web Consortium](https://en.wikipedia.org/wiki/World_Wide_Web_Consortium) (W3C) on November 12, 2015.[[28]](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_note-FIDO_submission_to_W3C-28) Subsequently, the first Working Draft of the W3C Web Authentication ([WebAuthn](https://en.wikipedia.org/wiki/WebAuthn)) standard was published on May 31, 2016. The WebAuthn standard has been revised numerous times since then, becoming a W3C Recommendation on March 4, 2019.

Meanwhile the U2F 1.2 Proposed Standard (April 11, 2017) became the starting point for the [Client to Authenticator Protocol](https://en.wikipedia.org/wiki/Client_to_Authenticator_Protocol) (CTAP) Proposed Standard, which was published on September 27, 2017. FIDO CTAP complements W3C WebAuthn, both of which are in scope for the [FIDO2 Project](https://en.wikipedia.org/wiki/FIDO2_Project).

WebAuthn and CTAP provide a complete replacement for U2F, which has been renamed "CTAP1" in the latest version of the FIDO2 standard.[[29]](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_note-Auto58-23-29) The WebAuthn protocol is backward-compatible (via the AppID extension) with U2F-only [security keys](https://en.wikipedia.org/wiki/Security_key)[[30]](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_note-W3C-WebAuthn-Level-1-30) but the U2F protocol is not compatible with a WebAuthn-only [authenticator](https://en.wikipedia.org/wiki/Authenticator).[[31]](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_note-Auto58-21-31)[[32]](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_note-Auto58-22-32)[[29]](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_note-Auto58-23-29) Some authenticators support both U2F and WebAuthn while some WebAuthn clients support keys created via the legacy U2F API.[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)]

References[[edit](https://en.wikipedia.org/w/index.php?title=Universal_2nd_Factor&action=edit&section=4)]

* 1. [**^**](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_ref-Google_security_keys_1-0) *Turner, Adam (November 5, 2014).*[*"Google security keys may offer extra layer of online protection"*](http://www.smh.com.au/digital-life/consumer-security/google-security-keys-may-offer-extra-layer-of-online-protection-20141105-11dmca.html)*. The Sydney Morning Herald. Fairfax Media. Retrieved November 28, 2014.*
  2. ^ [Jump up to:***a***](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_ref-Using_Security_Key_2-0) [***b***](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_ref-Using_Security_Key_2-1) [***c***](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_ref-Using_Security_Key_2-2) [*"What browsers support U2F?"*](https://web.archive.org/web/20170818004610/https:/www.yubico.com/support/knowledge-base/categories/articles/browsers-support-u2f/)*. Yubico. Archived from*[*the original*](https://www.yubico.com/support/knowledge-base/categories/articles/browsers-support-u2f/)*on August 18, 2017. Retrieved August 17, 2017.*
  3. [**^**](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_ref-USB_key_drive_could_remove_the_hassles_3-0) *Bradley, Tony (October 21, 2014).*[*"How a USB key drive could remove the hassles from two-factor authentication"*](http://www.pcworld.com/article/2836692/how-the-fido-alliances-u2f-could-simplify-two-factor-authentication.html#tk.rss_all)*. PCWorld. IDG Consumer & SMB. Retrieved November 28, 2014.*
  4. [**^**](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_ref-FIDO_Universal_2nd_Factor_4-0) [*"FIDO Universal 2nd Factor"*](https://www.yubico.com/applications/fido/)*. Yubico AB. Retrieved November 28, 2014.*
  5. [**^**](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_ref-Google_Wants_To_Make_Passwords_Obsolete_5-0) *Diallo, Amadou (November 30, 2013).*[*"Google Wants To Make Your Passwords Obsolete"*](https://www.forbes.com/sites/amadoudiallo/2013/11/30/google-wants-to-make-your-passwords-obsolete/)*. Forbes. Forbes.com LLC. Retrieved November 28, 2014.*
  6. [**^**](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_ref-FIDO_Alliance_standards_6-0) [*"FIDO Alliance – download specifications"*](https://fidoalliance.org/download/)*. FIDO Alliance. Retrieved October 19, 2017.*
  7. [**^**](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_ref-Google_Accounts_Now_Support_Security_Keys_7-0) *Krebs, Brian (October 14, 2014).*[*"Google Accounts Now Support Security Keys"*](http://krebsonsecurity.com/2014/10/google-accounts-now-support-security-keys/#more-28412)*. Krebs on Security. Retrieved November 28, 2014.*
  8. [**^**](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_ref-Auto58-16_8-0) [*"FIDO U2F HID Protocol Specification"*](https://fidoalliance.org/specs/fido-u2f-v1.0-ps-20141009/fido-u2f-hid-protocol-ps-20141009.html)*. FIDO Alliance. October 9, 2014. Retrieved July 24,2018.*
  9. [**^**](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_ref-Auto58-17_9-0) [*"Key generation"*](https://developers.yubico.com/U2F/Protocol_details/Key_generation.html)*. Yubico. Retrieved 31 July 2018.*
  10. [**^**](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_ref-Auto58-1_10-0) *Heim, Patrick; Patel, Jay (August 12, 2015).*[*"Introducing U2F support for secure authentication"*](https://blogs.dropbox.com/dropbox/2015/08/u2f-security-keys/)*. Dropbox Blog. Retrieved August 12, 2015.*
  11. [**^**](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_ref-Auto58-2_11-0) *Olsen, Risk (October 1, 2015).*[*"GitHub supports Universal 2nd Factor authentication"*](https://github.com/blog/2071-github-supports-universal-2nd-factor-authentication)*. github.com/blog.*[*GitHub*](https://en.wikipedia.org/wiki/GitHub)*. Retrieved October 1, 2015.*
  12. [**^**](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_ref-Auto58-3_12-0) *Nwaigwe, Amara (June 22, 2016).*[*"Support for Universal 2nd Factor Authentication"*](https://about.gitlab.com/2016/06/22/gitlab-adds-support-for-u2f/)*. GitLab Blog. Retrieved July 9, 2016.*
  13. [**^**](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_ref-Auto58-4_13-0) *Kells, TJ (June 22, 2016).*[*"Universal 2nd Factor (U2F) now supported in Bitbucket Cloud"*](https://blog.bitbucket.org/2016/06/22/universal-2nd-factor/)*. Bitbucket Blog. Retrieved June 22, 2016.*
  14. [**^**](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_ref-Auto58-5_14-0) [*"Nextcloud 11 sets new standard for security and scalability"*](https://nextcloud.com/blog/nextcloud-11-sets-new-standard-for-security-and-scalability)*. Nextcloud. Retrieved 23 December 2016.*
  15. [**^**](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_ref-Auto58-6_15-0) [*"Security Key for safer logins with a touch"*](https://www.facebook.com/notes/facebook-security/security-key-for-safer-logins-with-a-touch/10154125089265766)*. Facebook. Retrieved 27 January 2017.*
  16. [**^**](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_ref-Auto58-7_16-0) [*"USB-Dongle Authentication"*](http://www.dongleauth.info/)*. Josh Davis. Retrieved 22 February 2017.*
  17. [**^**](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_ref-Auto58-8_17-0) *Ingalls, Dustin (February 13, 2015).*[*"Microsoft Announces FIDO Support Coming to Windows 10"*](https://blogs.windows.com/business/2015/02/13/microsoft-announces-fido-support-coming-to-windows-10/)*. Windows Blog. Retrieved October 3, 2015.*
  18. [**^**](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_ref-Auto58-9_18-0) [*"Microsoft Edge now supports passwordless sign-ins"*](https://www.engadget.com/2018/07/31/microsoft-edge-now-supports-passwordless-sign-ins/)*. Engadget. Retrieved 2018-10-04.*
  19. [**^**](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_ref-Auto58-10_19-0) [*"Firefox 57 has native support for U2F"*](https://addons.mozilla.org/en-GB/firefox/addon/u2f-support-add-on/reviews/920895/)*. Mozilla. Retrieved November 1, 2017.*
  20. [**^**](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_ref-Auto58-11_20-0) [*"U2F Support Addon"*](https://addons.mozilla.org/en-US/firefox/addon/u2f-support-add-on/)*. Retrieved May 8, 2016.*
  21. [**^**](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_ref-Auto58-12_21-0) [*"Firefox Nightly enables support for FIDO U2F Security Keys"*](https://www.yubico.com/2017/09/firefox-nightly-enables-support-fido-u2f-security-keys/)*. Yubico blog. 2017-09-22. Retrieved September 27, 2017.*
  22. [**^**](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_ref-Auto58-13_22-0) [*"Firefox 60.0 release notes"*](https://www.mozilla.org/en-US/firefox/60.0/releasenotes/)*. Retrieved May 11, 2018.*
  23. [**^**](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_ref-Auto58-14_23-0) [*"Thunderbird 60.0 release notes"*](https://www.thunderbird.net/en-US/thunderbird/60.0beta/releasenotes/)*. Retrieved June 22, 2018.*
  24. [**^**](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_ref-Auto58-15_24-0) [*"Introducing Web Authentication in Microsoft Edge — Microsoft Edge Dev BlogMicrosoft Edge Dev Blog"*](https://blogs.windows.com/msedgedev/2018/07/30/introducing-web-authentication-microsoft-edge/)*. blogs.windows.com. 2018-07-30. Retrieved 2018-08-03.*
  25. [**^**](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_ref-Auto58-18_25-0) [*"FIDO U2F V1.0 Proposed Standard 2014-10-09"*](https://fidoalliance.org/specs/fido-u2f-v1.0-ps-20141009/)*.*[*FIDO Alliance*](https://en.wikipedia.org/wiki/FIDO_Alliance)*. 9 October 2014. Retrieved 3 May 2019.*
  26. [**^**](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_ref-Auto58-19_26-0) [*"FIDO U2F V1.2 Proposed Standard 2017-04-11"*](https://fidoalliance.org/specs/fido-u2f-v1.2-ps-20170411/)*.*[*FIDO Alliance*](https://en.wikipedia.org/wiki/FIDO_Alliance)*. 11 April 2017. Retrieved 3 May 2019.*
  27. [**^**](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_ref-Auto58-20_27-0) [*"Download Specifications"*](https://fidoalliance.org/specifications/download/)*. FIDO Alliance. Retrieved 13 February 2019.*
  28. [**^**](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_ref-FIDO_submission_to_W3C_28-0) [*"Submission Request to W3C: FIDO 2.0 Platform Specifications 1.0"*](https://www.w3.org/Submission/2015/02/)*.*[*World Wide Web Consortium*](https://en.wikipedia.org/wiki/World_Wide_Web_Consortium)*(W3C). Retrieved 12 February 2019.*
  29. ^ [Jump up to:***a***](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_ref-Auto58-23_29-0) [***b***](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_ref-Auto58-23_29-1) *Chong, Jerrod (1 August 2018).*[*"10 Things You've Been Wondering About FIDO2, WebAuthn, and a Passwordless World"*](https://www.yubico.com/2018/08/10-things-youve-been-wondering-about-fido2-webauthn-and-a-passwordless-world/)*. Retrieved 1 May 2019.*
  30. [**^**](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_ref-W3C-WebAuthn-Level-1_30-0) *Balfanz, Dirk; Czeskis, Alexei; Hodges, Jeff; Jones, J.C.; Jones, Michael B.; Kumar, Akshay; Liao, Angelo; Lindemann, Rolf; Lundberg, Emil (eds.).*[*"Web Authentication: An API for accessing Public Key Credentials Level 1 (latest)"*](https://www.w3.org/TR/webauthn-1/)*.*[*World Wide Web Consortium*](https://en.wikipedia.org/wiki/World_Wide_Web_Consortium)*(W3C). Retrieved 4 March 2019.*
  31. [**^**](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_ref-Auto58-21_31-0) *Hakamine, Frederico (22 January 2019).*[*"Understanding FIDO Standards: Your Go-To Guide"*](https://www.okta.com/security-blog/2019/01/understanding-fido-standards-your-go-to-guide/)*. Retrieved 1 May 2019.*
  32. [**^**](https://en.wikipedia.org/wiki/Universal_2nd_Factor#cite_ref-Auto58-22_32-0) *Salam, Feroz (25 August 2018).*[*"Why you can't use Firefox to register a U2F key with Google"*](https://padlock.argh.in/2018/08/25/u2f-firefox-google.html)*. Retrieved 1 May 2019.*