Fuente:
Wired

Las passkeys se crearon para permitir un futuro sin contraseñas. Te explicamos qué son y cómo puedes empezar a utilizarlas.

Las contraseñas son un asco. Son difíciles de recordar, pero peor aún es jugar a adivinar los códigos de tus cuentas más importantes. Ahí es donde entran en juego las passkeys. En los últimos dos años, la llamada "guerra contra las contraseñas" ha despegado contra titanes como Google, Microsoft y Apple impulsando un futuro sin contraseñas que la Alianza FIDO, un consorcio creado para "ayudar a reducir la excesiva dependencia mundial de las contraseñas", lleva más de una década intentando hacer realidad.

Te guste o no, en algún momento se te pedirá que crees una passkey, y es probable que ya lo hayas hecho. Eso es bueno, ya que las claves de acceso no solo son mucho más fáciles de usar que una contraseña tradicional, sino que también son mucho más seguras. Aquí tienes todo lo que necesitas saber sobre su uso.

¿Qué es una contraseña?

Las passkeys ofrecen una forma de confirmar que eres quien dices ser sin tener que recordar una contraseña larga y complicada, y de una manera que es resistente a los ataques comunes a las contraseñas como el phishing y los ataques de diccionario. "Las passkeys están pensadas para sustituir por completo a las contraseñas y a las formas obsoletas de autenticación de dos factores", explica a WIRED Andrew Shikiar, director ejecutivo y CEO de la Alianza FIDO. Representan un avance poco habitual en ciberseguridad; no solo son más fáciles de usar que los métodos anteriores, sino también más seguras.

Conceptualmente, las passkeys pueden adoptar muchas formas, pero lo más habitual es que interactúes con ellas en un dispositivo propio. Por ejemplo, imagina que quieres acceder a tu cuenta de Google en un dispositivo nuevo. En lugar de introducir una contraseña, una clave de acceso te permite acceder a tu cuenta con un dispositivo que ya hayas verificado. Puedes utilizar tu teléfono como passkey, lo que te permitirá acceder a tu cuenta de Google de forma instantánea sin tener que introducir nunca una contraseña. Las mejores implementaciones de passkeys ni siquiera necesitan un nombre de usuario.

Las passkeys resultan más seguras y prácticas que las contraseñas porque funcionan de una forma fundamentalmente distinta. En el mundo de la ciberseguridad, las contraseñas son lo que se llama un "secreto compartido". Tú conoces el secreto y el servicio al que te conectas también. El problema es que tienes que recordar ese secreto y no lo controlas totalmente, ya que tienes que compartirlo con el servicio que estés utilizando. Una filtración de datos y un poco de tiempo de descifrado es todo lo que se necesita para acabar con una cuenta comprometida, y ni siquiera has hecho nada malo.

Las passkeys utilizan criptografía de clave pública. En lugar de hacer coincidir un secreto compartido, la criptografía de clave pública funciona haciendo coincidir un par de claves: una clave pública que cualquiera puede ver y una clave privada a la que solo tú tienes acceso. Es más segura porque solo tú tienes acceso a tu clave privada, y es más fácil porque esa clave está vinculada a algún dispositivo de tu propiedad y suele estar protegida con datos biométricos.

¿Las passkeys son seguras?

Las passkeys son seguras, incluso más que una contraseña larga y aleatoria. Cuando inicias sesión con una contraseña, envías un puñado de información al servicio al que te estás conectando, incluida tu clave pública, que se almacena como una representación de ti como usuario. Esta información por sí sola no hace nada.

En el dispositivo donde creaste la passkey, tendrás que participar en un "desafío" para desbloquear tu clave privada, normalmente alguna forma de autenticación biométrica. Si tienes éxito, se firma y se envía de vuelta al servicio al que intentas acceder. A continuación, se coteja con la clave pública y, si coincide, se te da acceso. Lo más importante es que esta autenticación se realiza en tu dispositivo, no en un servidor lejano.

Con una contraseña, un atacante tiene muchas posibilidades de robarla. Las filtraciones de datos pueden sacar a la luz tu contraseña, e incluso si está encriptada, puede ser descifrada. Los esquemas de phishing son un vector de ataque fácil para los hackers que buscan robar contraseñas. Además, si utilizas un servicio con prácticas de seguridad poco seguras, tu contraseña podría quedar expuesta como texto plano en una brecha; hay docenas y docenas de ejemplos de que esto ya ha ocurrido antes.

Claves de acceso frente a 2FA y MFA

Las passkeys son complicadas porque van en contra de las convenciones de seguridad que existen desde hace años, es decir, la autenticación de dos factores (2FA) o la autenticación multifactor (MFA). Aunque no es necesario introducir un código de texto o copiar algo de una aplicación de autenticación, las passkeys utilizan intrínsecamente la autenticación multifactor. Simplemente ocurre tan rápido que es fácil pasarlo por alto.

MFA consiste en añadir capas adicionales de protección más allá de tu contraseña. En lugar de tu contraseña,

necesitas esta y un código que te envíen por SMS. Las passkeys ya funcionan así. Tienes que hacer coincidir el par de claves pública-privada, pero también tienes que autenticar que tienes acceso a esa passkey, normalmente con datos biométricos. No se trata de "algo que sabes y algo que posees", como suele describirse la 2FA, pero siguen siendo dos capas de autenticación.

Así lo describe Shikiar: "Cuando inicias sesión, el servicio emite un desafío criptográfico al que solo se puede responder con la clave privada de tu teléfono o laptop y, a menudo, por algo muy tuyo, como un dato biométrico. El resultado es un inicio de sesión resistente al phishing sin credenciales reutilizables que robar".

Dispositivos y navegadores compatibles con passkeys

Las passkeys están ampliamente integradas en los sistemas operativos. Si utilizas un sistema operativo que no admite de forma nativa las contraseñas, como Linux, pueden serte útiles. Sin embargo, tendrás que utilizar otro dispositivo, como tu smartphone, para escanear un código QR y autenticarte, o un gestor de contraseñas de terceros.

Estos son los sistemas operativos totalmente compatibles con passkeys:

- Android 9 o posterior
- iOS 16 o posterior
- macOS 13 (Ventura) o posterior
- Windows 10/11 23H2 o posterior

Cada uno de estos sistemas operativos soporta passkeys para apps nativas, así como en su navegador. Chromium también las soporta, lo que cubre la gran mayoría de navegadores disponibles, incluyendo Brave, Opera, Vivaldi y Google Chrome. Igualmente funcionan con el principal navegador que no es Chromium, Mozilla Firefox, en la versión 122 o superior.

Cómo crear y almacenar passkeys

Para utilizar passkeys, es necesario almacenarlas en algún lugar. Los principales sistemas operativos que las admiten incluyen una forma de almacenarlas, pero no se crean por igual.

Windows 10 y Windows 11

Debe configurar Windows Hello para utilizar las passkeys en Windows 10 o Windows 11. Es posible que lo hayas configurado durante la instalación, pero si no es así, puedes habilitarlo en la aplicación Configuración haciendo clic en Cuentas > Opciones de inicio de sesión. Siempre que quieras utilizar una clave de acceso, tendrás que autenticarte con Windows Hello, ya sea con tu cara, huella dactilar o PIN.

Windows 10 u 11, versión 23H2 o posterior, te pedirá que utilices una passkey siempre que intentes iniciar sesión en un servicio compatible en un navegador compatible, o a través de una aplicación nativa de Windows. A diferencia de otros sistemas operativos, estas claves de acceso no se sincronizan entre dispositivos. Solo funcionan en tu dispositivo Windows.

macOS

Tanto macOS como iOS almacenan las passkeys en tu llavero de iCloud, por lo que tendrás que activar tu llavero si aún no está activado. Puedes activarlo en la app Configuración siguiendo ID de Apple > iCloud > Contraseñas y llavero. Tendrás que activar 2FA para tu ID de Apple para poder utilizar el Llavero de iCloud.

Al igual que en Windows, se te pedirá que crees una passkey cada vez que crees una nueva cuenta con un servicio que admita contraseñas. Si quieres añadir una passkey a una cuenta ya creada, tendrás que hacerlo a través de la configuración de esa aplicación. A diferencia de Windows, estas passkeys funcionan en todos los dispositivos, siempre que tengas acceso a tu llavero de iCloud.

En las versiones más recientes de macOS (versión 15 y posteriores), es mucho más fácil crear y gestionar passkeys a través de la aplicación dedicada Contraseñas.

iOS

iOS sigue los mismos principios que macOS en lo que respecta a las passkeys. Se almacenan en tu llavero de iCloud y se sincronizan en todos tus dispositivos. En iOS 18 y versiones posteriores, puedes gestionar las passkeys en la app dedicada Contraseñas, y en versiones anteriores, puedes encontrarlas en tu configuración.

Android

Android 9 y las versiones más recientes admiten passkeys, pero de formas diferentes. De forma predeterminada, las passkeys en Android utilizan el Administrador de contraseñas de Google, que está vinculado a tu cuenta de Google y se sincroniza con todos tus dispositivos. En Android 14 y versiones más recientes, puedes optar por almacenar tus passkeys en otro lugar, como en un gestor de contraseñas de terceros.

Claves de acceso en un gestor de contraseñas

Si quieres tener todas tus passkeys en todos tus dispositivos, sin importar el sistema operativo, necesitas un gestor de contraseñas. La mayoría admiten passkeys, lo que te permite almacenarlas y sincronizarlas en casi cualquier dispositivo. Personalmente, utilizo 1Password, pero servicios como NordPass, Bitwarden y Dashlane también admiten contraseñas. Puedes crear y almacenar claves de acceso con un gestor de contraseñas en Android e iOS.

Aplicaciones que admiten passkeys

Solo hay unos pocos lugares donde puedes almacenar y sincronizar passkeys, pero muchos servicios las admiten para iniciar sesión. Los sospechosos habituales incluyen Microsoft, Adobe, Amazon, Google y Apple, pero todavía hay muchos sitios web y aplicaciones que no admiten passkeys.

Puedes encontrar un puñado de directorios que afirman tener una lista completa de aplicaciones que admiten passkeys con una rápida búsqueda en Google. 1Password mantiene un directorio, al igual que un par de servicios B2B, incluyendo un directorio de Hanko y otro de OwnID. No son listas completas. Por ejemplo, las aplicaciones de Meta, como Facebook e Instagram, no están en la lista, a pesar de haber añadido soporte para passkeys en junio de 2025.

El mejor directorio que he encontrado es el de una organización sin fines de lucro llamada 2factorauth, de Suecia. Está alojado en GitHub, se actualiza constantemente y, lo que es más importante, lo mantiene la comunidad. Es el más actualizado que he encontrado, y las aplicaciones incluso están organizadas en categorías para que puedas, por ejemplo, elegir un servicio VPN que admita passkeys.

Las passkeys sustituirán (con el tiempo) a las contraseñas

Las passkeys se crearon para sustituir a las contraseñas, pero estamos en medio de una larga y ardua transición para conseguirlo. Requiere que todas las aplicaciones, dispositivos y sistemas operativos adopten un nuevo estándar de autenticación y abandonen un modelo que hemos estado utilizando durante décadas a lo largo de toda nuestra vida digital.

Sin embargo, el punto de inflexión ya está en marcha. Con los principales servicios adoptando passkeys, es posible utilizarlas en tus cuentas más importantes. Aunque solo sea por eso, vale la pena utilizarlas en cuentas conectadas a otras, como las de Google o Facebook, si utilizas las funciones de inicio de sesión social.

A pesar de ofrecer claras ventajas de seguridad, las passkeys no son una solución para mejorar la seguridad. En palabras de Shikiar, "protegen la puerta de entrada, pero las organizaciones siguen necesitando reforzar todo el recorrido de la identidad, desde la incorporación y la recuperación hasta la gestión de la sesión".

Disponible en:

https://es.wired.com/articulos/como-funcionan-las-passkeys-y-como-utiliz... [1]

Links
[1] https://es.wired.com/articulos/como-funcionan-las-passkeys-y-como-utilizarlas