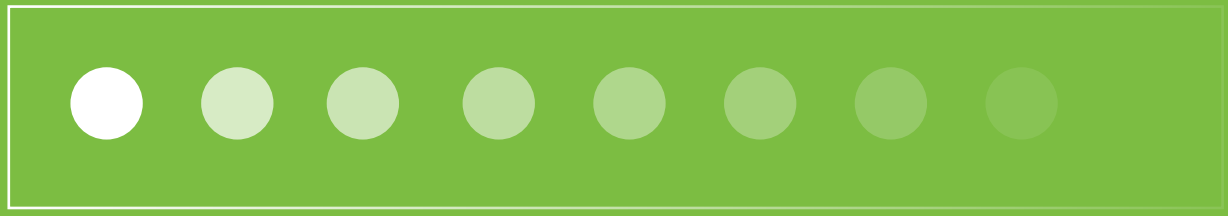
yubico

DOCUMENTACIÓN DE YUBICO
OCTUBRE 2020

Olvídese de las contraseñas

con FIDO2 y WebAuthn



Índice

Resumen ejecutivo 3
Tiempo y coste de las contraseñas 4
Solucionar el problema de las contraseñas con FIDO2 6
Introducción a la autenticación sin contraseña 7
  Opciones de autenticación FIDO2/WebAuthn 8
Ventajas de no usar contraseñas 9
  Usabilidad mejorada 9
  Seguridad mejorada 10
  Eficiencia mejorada 11
  Tan práctico como una tarjeta de débito 12
  FIDO2, WebAuthn y FIDO U2F 13
Nuevos casos de uso con inicio de sesión sin contraseña 14
  Empleados 14
  Venta minorista 14
  Finanzas 15
  Fabricación 15
  Sector de la salud 15
  Redes de proveedores y distribuidores 16
Conclusión 17
Recomendaciones 18
Referencias 19

Resumen ejecutivo

Imagine un mundo en el que los usuarios ya no necesiten establecer, restablecer, olvidar y volver a restablecer varias contraseñas. Las contraseñas son conocidas como el eslabón más débil de la seguridad de la empresa y son un obstáculo para la simplificación de la experiencia de uso de los clientes y los procesos internos. El mundo está a punto de cambiar con la introducción de la autenticación sin contraseña. En una estudio mundial del Ponemon Institute a 2.507 profesionales de la seguridad de TI y 563 usuarios individuales, se descubrió que el 49% de los profesionales de TI encuestados y el 51% de los individuos comparten sus contraseñas con sus colegas para acceder a las cuentas de la empresa. Esto ilustra las malas prácticas que agravan los problemas de seguridad que pueden crear las contraseñas.[1]

Los nuevos estándares de autenticación FIDO2/WebAuthn ofrecen a las organizaciones la oportunidad de resolver los problemas inherentes a la seguridad basada en contraseñas. FIDO2 es un estándar abierto, desarrollado conjuntamente por Yubico, Microsoft y otros miembros de la FIDO Alliance, que permite ampliar las opciones de autenticación segura, incluida la flexibilidad de ofrecer a los usuarios una autenticación segura de factor único o multifactor sin contraseña, además de respaldar la autenticación de dos factores actual.

La autenticación sin contraseña ofrece la oportunidad de transformar la seguridad de la empresa y las experiencias de los usuarios en todos los sectores, incluidos los de la atención sanitaria, la fabricación y el comercio minorista, así como para los trabajadores de oficina, asociados y proveedores. Puede simplificar la incorporación del usuario y, dado que el restablecimiento de contraseñas representa actualmente el mayor coste de asistencia técnica, el inicio de sesión sin contraseña promete reducir significativamente las cargas de trabajo en los centros de llamadas de TI donde los agentes emplean actualmente un tiempo considerable configurando y restableciendo las contraseñas de los usuarios.

¿Cómo se podría simplificar la experiencia de uso de los clientes y del personal con un inicio de sesión sin contraseña? ¿Cuáles son las posibilidades de los nuevos productos y servicios cuando ya no se requieren contraseñas? Estas son las preguntas que los líderes de negocio y de TI con visión de futuro deberían hacerse.

Este documento técnico desarrolla los antecedentes de la autenticación sin contraseña y las consideraciones para su implementación a nivel empresarial.

Tiempo y coste de las contraseñas

Hoy en día, las empresas buscan formas de aprovechar la tecnología móvil y de la nube para ofrecer productos y servicios mejorados de forma más rápida y eficiente. Sin embargo, las empresas que persiguen planes ambiciosos para agilizar la experiencia de uso de sus clientes y empleados, a menudo se encuentran con problemas de seguridad.

Las tecnologías y los controles de seguridad se ponen en marcha para proteger la empresa, pero esos mismos controles de seguridad pueden frustrar a los usuarios. Las contraseñas se perciben como el control de seguridad más incómodo e irritante.

Desde los años 50, las contraseñas han sido ineludibles para los usuarios empresariales y los consumidores por igual. Casi todas las experiencias digitales requieren una contraseña, desde las redes sociales como Facebook, a los bancos y comercios minoristas como H&M y Zara, e incluso las aplicaciones empresariales como Salesforce y QuickBooks Online.

De media, el consumidor estadounidense intenta llevar un registro de más de 70 contraseñas diferentes, que utiliza en todas sus páginas web y servicios en línea[2], mientras que se estima que los usuarios empresariales deben memorizar y utilizar un número aún mayor de contraseñas, hasta 191[3]. Dado que los millennials constituyen una parte cada vez mayor de la fuerza laboral, los resultados de un estudio de IBM muestran que son menos pacientes con la memorización de todos estos secretos. Es más probable que reutilicen las contraseñas, ya que suelen memorizar no más de ocho, lo que pone en riesgo la seguridad en aras de la conveniencia.[4]

El hartazgo de las contraseñas conduce a filtraciones de datos

Los usuarios se cansan de crear nuevas contraseñas para diferentes servicios y de tener que cambiarlas cada pocos meses según los requisitos de las políticas de seguridad. Para reducir la memorización, muchos usuarios terminan confiando en contraseñas simplistas que son fáciles de descifrar o son reutilizadas en varias páginas, donde la vulneración de un servicio y la filtración de las credenciales puede abrir la puerta a muchas más.

El 80% de las brechas de seguridad todavía implican credenciales comprometidas y débiles, según el informe de investigación de vulneraciones de datos (DBIR) de Verizon de 2019.[5] Increíblemente, después de años de brechas de datos muy publicitadas, la mayoría aún implican una contraseña débil. El análisis de brechas de seguridad de NCSC 2019 Cyber Survey del Reino Unido encontró que 23,2 millones de cuentas de víctimas en todo el mundo usaban “123456” como contraseña.[6]

Las contraseñas olvidadas provocan altos costes de asistencia técnica

Cuando los usuarios olvidan sus contraseñas, normalmente terminan llamando a los centros de ayuda o asistencia, lo que consume un tiempo valioso. Las consultas de restablecimiento de contraseña representan hasta el 6 % de las actividades de los centros de llamadas, lo que supone un coste para las grandes empresas de entre 5 y 20 millones de dólares anuales.

El 80 % de las brechas de seguridad aún implican credenciales comprometidas y débiles.[5]

Estudio de Verizon Data Breach sobre filtraciones de datos

A medida que las compañías continúan añadiendo aplicaciones de negocio, el costo de las contraseñas sólo sube. De hecho, las empresas dedican entre el 30 y el 60 por ciento de sus llamadas al servicio de asistencia técnica al restablecimiento de las contraseñas.

El equipo de TI de Microsoft cambió a la autenticación sin contraseña y ahora el 90 % de los empleados de Microsoft inician sesión sin introducir una contraseña. Como resultado, los costos de soporte técnico se redujeron en un 87 %. A medida que las compañías continúan añadiendo aplicaciones empresariales a sus carteras, el costo de las contraseñas no hace más que aumentar. De hecho, las empresas dedican entre el 30 y el 60 por ciento de sus llamadas al servicio de asistencia técnica a reiniciar las contraseñas.[7]

Los ataques de phishing tienen como objetivo el robo de credenciales

El phishing sigue siendo un problema de seguridad masivo, ya que las técnicas de ataque siguen evolucionando. Los mensajes de correo electrónico falsos que instan a los usuarios a volver a introducir sus credenciales pueden utilizarse para recopilar credenciales que se utilizarán seguidamente para la suplantación de cuentas. Alrededor del 30 % de los correos electrónicos de phishing son abiertos por sus destinatarios y a más del 7 % de los destinatarios se les persuade para abrir un archivo adjunto o hacer clic en un enlace, que normalmente es un enlace de inicio de sesión. La mayoría de los ataques de phishing provocan la instalación de malware que se aprovecha para perpetrar una vulneración.[8] Incluso si los usuarios establecen contraseñas complejas, los hackers pueden acceder a ellas a través de ataques de phishing y penetrar en las cuentas de los usuarios.

Venta de listas de credenciales robadas

Cuando los hackers entran en una organización y roban credenciales, obtienen acceso no solo a las cuentas de esa organización sino también a las cuentas de otras organizaciones en las que los consumidores han utilizado el mismo par de nombre de usuario y contraseña. Por ejemplo, cuando los hackers robaron 1000 millones de credenciales de inicio de sesión de Yahoo! en 2016, obtuvieron acceso a todas las demás cuentas a las que se podía acceder con los mismos pares de dirección de correo electrónico y contraseña. En la dark web se pueden encontrar miles de millones de credenciales robadas y los ciberdelincuentes tratan de acceder de manera automatizada a este tesoro de contraseñas robadas. Hoy en día, nueve de cada diez intentos de inicio de sesión en páginas populares de comercio y banca son en realidad ataques dirigidos por bots.[9]

Mientras la TI de la empresa tenga que depender de las contraseñas para la autenticación, los costosos requisitos de asistencia, la falta de seguridad y las experiencias frustrantes de los clientes son inevitables. Las contraseñas olvidadas y robadas degradan la experiencia de los clientes, reducen la fidelidad a la marca y contribuyen a la pérdida de ingresos.

Solucionar el problema de las contraseñas con FIDO2

Imagine ofrecer servicios rápidos, cómodos y seguros de todo tipo a los usuarios, ya sean clientes o empleados, sin requerir contraseñas y sin incurrir en los gastos operativos de la gestión de contraseñas. Imagine que los clientes, asociados y empleados que utilizan equipos de sobremesa y dispositivos móviles pudieran acceder instantáneamente al contenido y los servicios que desean sin tener que recordar contraseñas o llamar al servicio de asistencia técnica para pedir ayuda. Imagine los nuevos servicios que podrían ofrecerse si la autenticación fuera instantánea y fácil. Imagine que las organizaciones de TI se liberaran del trabajo y los gastos diarios de la gestión y el restablecimiento de las contraseñas.

El estándar de autenticación FIDO2 ofrece la opción de autenticación sin contraseña.

Ventajas de la autenticación sin contraseña

Usabilidad mejorada

La autenticación sin contraseña libera a los usuarios de tener que recordar y escribir las contraseñas.

Seguridad mejorada

La autenticación sin contraseña elimina los riesgos de seguridad asociados con las contraseñas robadas y los ataques de fuerza bruta contra las páginas de inicio de sesión.

Eficiencia mejorada

La autenticación sin contraseña elimina la necesidad de que los departamentos de TI gestionen las contraseñas.

Estas ventajas de la autenticación sin contraseña pueden lograrse con los estándares de autenticación abiertos de FIDO2/WebAuthn.

Introducción a la autenticación sin contraseña

El estándar de autenticación FIDO2, de la que son coautores Yubico, Microsoft y los miembros de la FIDO Alliance, junto con el World Wide Web Consortium (W3C), soporta múltiples escenarios y experiencias de uso.

FIDO2 está compuesto por dos componentes estandarizados, una API web (WebAuthn) y un protocolo de autenticación del cliente (CTAP). Ambos funcionan de forma conjunta y son necesarios para lograr una experiencia sin contraseña en el inicio de sesión. WebAuthn define una API web estándar que puede integrarse en los navegadores y en la infraestructura de la plataforma web para ofrecer a los usuarios nuevos métodos para autenticarse de forma segura en la web. CTAP permite que un autenticador externo, como una llave de seguridad, comunique credenciales de autenticación segura a nivel local a través de USB, NFC o Bluetooth al PC o teléfono móvil del usuario.

Ecosistema FIDO2

FIDO2 se basa en un par asimétrico (público/privado) de claves criptográficas para autenticar a los usuarios. La clave pública se almacena en cualquier servicio o dispositivo informático que sea compatible con la autenticación FIDO2, mientras que la clave privada la conserva el usuario y está protegida por una llave de seguridad física, como la serie YubiKey 5 y la serie Security Key de Yubico. La autenticación en sí es rápida y sencilla: con solo insertar o tocar la llave de seguridad se ejecuta la autenticación y se inicia sesión de manera inmediata.

Con FIDO2, la llave de seguridad puede utilizarse por si sola o junto con un PIN o un gesto de usuario para proporcionar una autenticación segura sin contraseña, y además también admite la autenticación de dos factores con contraseña.

FIDO2 es respaldado por World Wide Web Consortium (W3C)

La especificación de la API de autenticación web (WebAuthn) ofrece a los usuarios de navegadores nuevos métodos para autenticarse de forma segura en la web basados en la especificación FIDO2. Los navegadores Microsoft Edge, Google Chrome y Mozilla son compatibles con la especificación API de WebAuthn.

Opciones de autenticación FIDO2/WebAuthn

Factor único (sin contraseña)

El uso de la llave de seguridad como primer factor robusto de autenticación, que requiere únicamente la posesión del dispositivo, permite una experiencia de «tap and go»

Dos factores (contraseña + autenticador)

Uso de la llave de seguridad como segundo factor en una solución de autenticación de dos factores

Multifactor (sin contraseña + PIN o datos biométricos)

El uso de la llave de seguridad para la autenticación multifactor, que requiere la posesión del dispositivo en conjunción con un PIN o datos biométricos, permite cumplir con requisitos exigentes en materia de seguridad

FIDO2 es compatible con la última versión de los dispositivos de Windows 10, tanto de escritorio como móviles. Esto hace que FIDO2 esté disponible en más de 700 millones de dispositivos en todo el mundo y en miles de millones de cuentas de Azure AD.

Ventajas de no usar contraseñas

Usabilidad mejorada

El inicio de sesión sin contraseña FIDO2 hace que la autenticación sea rápida y fácil, lo que elimina la necesidad de utilizar contraseñas.

El inicio de sesión sin contraseña FIDO2 hace que la autenticación sea rápida y fácil, lo que elimina la necesidad de utilizar contraseñas. Con FIDO2, se puede utilizar un único autenticador de hardware, como YubiKey, para autenticar todos los servicios con los que interactúa un usuario, incluidas las aplicaciones y servicios empresariales en el trabajo, redes sociales y otras aplicaciones de consumo en el hogar, sin secretos compartidos.

Al mismo tiempo, FIDO2 puede utilizarse para que un mismo usuario se autentique con varias identidades. La misma YubiKey puede utilizarse para el acceso a aplicaciones, páginas web, servicios, servidores y dispositivos tanto empresariales como de consumo, desde edificios hasta vehículos diseñados para ser compatibles con FIDO2.

Con la autenticación sin contraseña, trabajadores que viajan en avión o metro sin acceso a wifi o internet móvil pueden seguir autenticándose en sus portátiles y trabajar de forma productiva y segura, incluso si la falta de acceso a la red les impide recibir credenciales SMS u OTP para la autenticación de usuarios.

FIDO2 elimina la necesidad de acceso a la red (ya sea móvil o de datos) para recibir claves de segundo factor. Además de reforzar la seguridad de TI, FIDO2 facilita a los usuarios el acceso a los dispositivos que necesitan para trabajar en cualquier momento y lugar.

FIDO2 es compatible con la última versión de los dispositivos de Windows 10, tanto de escritorio como móviles. Windows 10 tiene más de 1.000 millones de usuarios en todo el mundo, lo que hace que aproximadamente 700 millones de dispositivos sean compatibles con FIDO2.[10]

Dado que FIDO2 se ha desarrollado como un estándar abierto del sector y está siendo ampliamente promovido por Microsoft y el World Wide Web Consortium (W3C) con el apoyo de Google y Mozilla, su adopción no depende de una sola entidad. FIDO2 ahorra a las empresas el gasto de tener que invertir en el desarrollo y mantenimiento de modelos de seguridad personalizados para resolver los problemas de las contraseñas. Ahora las empresas de todos los sectores pueden aprovechar un estándar abierto de autenticación industrial avalado por los líderes del sector.

Cumplimiento de las normas de autenticación del NIST

FIDO2 puede ser un token criptográfico de un solo factor o un token criptográfico de varios factores. Según la publicación especial 800-63 del NIST, el token criptográfico multifactor está clasificado en el nivel 3 de garantía de autenticación, que es el nivel de garantía más alto establecido por esa norma. Por lo tanto, el uso de FIDO2 con un PIN cumple con los más altos requisitos de autenticación en mercados regulados donde el cumplimiento NIST SP800-63 es obligatorio.[11]

Seguridad mejorada

FIDO2 mejora notablemente la seguridad de la autenticación de usuarios y la gestión del acceso.

FIDO2 mejora notablemente la seguridad de la autenticación de usuarios y la gestión del acceso.

Con el inicio de sesión sin contraseña, se evita el riesgo de que se engañe a los usuarios para que divulguen sus contraseñas inadvertidamente, ya que las contraseñas ya no son necesarias. Los usuarios se autentican con un autenticador de hardware como una YubiKey, que a grandes rasgos funciona de la siguiente manera:

- La YubiKey crea y gestiona la credencial FIDO2 (un par de claves públicas/privadas) incluida la vinculación de la credencial al servicio específico, conocido como origen. La vinculación del origen evita los ataques de intermediarios, también conocidos como hombre en el medio (MiTM).
- Cuando un servicio como Azure AD presenta un desafío de autenticación, la clave privada se utiliza para firmar la respuesta, que se envía a través de la red y es verificada por el servicio en línea utilizando la clave pública.

La credencial FIDO2, que se almacena en un chip seguro dentro de la YubiKey y que nunca sale del dispositivo, está diseñada para evitar que los hackers suplanten a los usuarios que acceden a las páginas web.

FIDO2 reduce los riesgos en aplicaciones, páginas web, servicios, servidores y dispositivos al eliminar el almacenamiento y la gestión centralizados de las credenciales confidenciales. Las cuentas FIDO2 no necesitan una contraseña, por lo que ya no existe ese tesoro de contraseñas que se pueda robar. Las páginas web y otros servicios solo almacenan las claves públicas que los usuarios han registrado, por lo que el secreto (clave privada) se mantiene de forma segura en el autenticador de hardware, y nunca se envía a través de la red como una contraseña tradicional. Esas claves públicas pueden validar las firmas generadas por las claves privadas, pero no se pueden utilizar para iniciar sesión en otros recursos. Solo un usuario final con la llave privada FIDO2 puede autenticarse en un servicio. De esta manera se mejora la seguridad, al mismo tiempo que se consigue que el inicio de sesión sea más rápido, fácil y fiable para los usuarios finales.

Los privilegios de autenticación pueden concederse en conformidad con las políticas de seguridad específicas de la organización o según los requisitos de las normativas del sector como GLBA y HIPAA, o las normativas gubernamentales como NIST SP800-63. Al cumplir con la norma NIST SP800-63, FIDO2 asegura el cumplimiento de una amplia gama de otras normativas que se basan en las normas NIST. Los administradores de TI y los responsables de regulación pueden estar seguros de que los usuarios no eluden los controles de autenticación compartiendo las contraseñas en notas adhesivas o por correo electrónico. Cada usuario recibe una clave única que lo autentica en los servicios y aplicaciones registrados.

«FIDO2 no requiere un entorno de PKI complejo para gestionar los certificados»

Eficiencia mejorada

FIDO2 libera a los departamentos de TI, incluidos los centros de servicio y de llamadas, de tener que crear, almacenar, modificar y restablecer las contraseñas.

El inicio de sesión sin contraseña ofrece la oportunidad de que los empleados y contratistas se incorporen sin problemas, al eliminar los costes de asistencia en la creación y gestión de contraseñas. En lugar de crear contraseñas temporales para los nuevos empleados y contratistas que deben cambiarse inmediatamente y luego volverse a cambiar en un calendario prescrito, con la autenticación FIDO2 se crea una clave de seguridad FIDO2 para cada usuario y este puede especificar un PIN opcional. Los privilegios de autenticación FIDO2 pueden revocarse fácilmente cuando un empleado o un contratista termina su servicio para la empresa.

Con la clave de seguridad FIDO2, los usuarios pueden autenticarse en un servicio central como Azure AD y crear así su identificador para poder registrar nuevos dispositivos como, por ejemplo, un smartphone. En las organizaciones en las que se comparten dispositivos informáticos, cada usuario puede autenticarse de forma rápida y sencilla sin tener que recordar e introducir contraseñas. Simplemente con insertar una YubiKey, o con tocarla si es compatible con NFC, los usuarios pueden desbloquear sus dispositivos y acceder a sus cuentas.

Además, FIDO2 no requiere un entorno PKI complejo para gestionar los certificados. El departamento de TI puede emplear su tiempo y esfuerzos en tareas más estratégicas y productivas.

Cumplimiento de los requisitos empresariales para la autenticación de usuarios

FIDO2 cumple con todos los requisitos fundamentales para la autenticación de usuarios:

- **Proporciona credenciales que no pueden piratearse o falsificarse**
- **Proporciona un método de autenticación que evita el phishing**
- **Proporciona una mejor experiencia para el usuario final que las contraseñas**
- **Proporciona una autenticación y una autorización de tal modo que la autenticación no puede transferirse entre máquinas**
- **Es compatible con diferentes niveles de autenticación segura**
- **Es compatible con varias credenciales**
- **Solo requiere un único gesto del usuario, como un toque o pasar el dedo para conceder el acceso**

La facilidad del inicio de sesión aumenta el uso de los servicios digitales en un 10 - 20 %

Fuente: encuesta de McKinsey ClickFox[13]

Tan práctico como una tarjeta de débito

Para comprender la comodidad de un inicio de sesión sin contraseña con una YubiKey, piense por un momento en lo práctico que le resulta usar su tarjeta de débito. Es probable que lleve su tarjeta de débito a todas partes. La protege, no la deja expuesta en público. Para utilizarla en un cajero automático, introduce un PIN corto. El PIN se cambia con muy poca frecuencia, si es que se cambia, no necesita recordar ninguna contraseña ni nombre de usuario, y sin embargo su acceso al cajero automático es muy seguro.

Una YubiKey sin contraseña es similar. La lleva a todas partes. Para desbloquear un dispositivo, ya sea un ordenador de sobremesa, un smartphone, un sistema de control de fabricación, un portal de salud o cualquier otro dispositivo, solo tiene que conectar la YubiKey en un puerto USB o colocar la llave cerca de un sensor NFC. A continuación, cuando se le solicite, toque la llave y, de forma opcional, puede introducir un PIN o usar un control biométrico, en función de la aplicación o servicio.

Al igual que el PIN de su tarjeta de débito, el PIN de FIDO2 garantiza su acceso al mecanismo de la clave de seguridad. El PIN desbloquea su clave de seguridad FIDO2 y le permite iniciar un intercambio de claves con lo que puede autenticarse en un dispositivo local, un servicio de directorio remoto, una página web, una red social o algún otro servicio de TI.

De forma opcional, se pueden configurar servicios para autenticar a los usuarios sin tener que usar PIN o gestos. Por ejemplo, con el fin de proporcionar el servicio más rápido posible a los clientes, se podría permitir que un empleado de ventas al por menor se autentique colocando su llave en un teclado NFC, lo que desbloquearía al instante un sistema informático. Si el sistema informático está configurado con una almohadilla de presión que detecta la presencia del usuario, el sistema puede cerrar automáticamente la sesión del usuario cuando el empleado de ventas autenticado se aleja.[12] Dado que FIDO2 altera radicalmente el proceso de autenticación de los usuarios, las empresas pueden permitirse las medidas de autenticación adicionales, ya que las experiencias de los usuarios de FIDO2 son tan sencillas y rápidas, lo que mejora la productividad y reduce al mismo tiempo los gastos de asistencia.

En todos estos escenarios, el inicio de sesión sin contraseña FIDO2 proporciona una experiencia más rápida y segura que los nombres de usuario y las contraseñas. El inicio de sesión sin contraseña transforma la experiencia del usuario de acceder a aplicaciones, páginas web, servicios, servidores y dispositivos, y la equipara a la comodidad habitual de un cajero automático.

El inicio de sesión sin contraseña requiere el uso de un autenticador certificado FIDO2, como los de la serie YubiKey 5.

FIDO2, WebAuthn y FIDO U2F

¿Cómo funcionan FIDO2 y WebAuthn con FIDO U2F?

U2F es un estándar de autenticación abierto que permite a los autenticadores de hardware, teléfonos móviles y otros dispositivos acceder de forma segura a cualquier número de servicios basados en la web, de forma instantánea y sin necesidad de controladores o software de cliente. U2F ha sido creado por Google y Yubico, con la contribución de NXP, y actualmente está gestionado por el consorcio de la industria de la autenticación abierta, la FIDO Alliance.

U2F es una solución de autenticación segura, pero es una solución de dos factores, que se basa en los nombres de usuario y las contraseñas como primer factor. De hecho, 2F significa dos factores.

FIDO2 es la segunda generación de U2F. FIDO2 se basa en U2F al que se añaden los elementos necesarios para que un usuario pueda ser identificado y autenticado sin necesidad de una contraseña. La autenticación FIDO2 permite una autenticación segura de un solo factor, de dos factores y multifactor.

Esto significa que todas las llaves de seguridad FIDO U2F previamente certificadas, incluidas las YubiKeys, seguirán funcionando como autenticación de segundo factor con navegadores web y servicios en línea que soportan WebAuthn.

Nuevos casos de uso con inicio de sesión sin contraseña

Empleados

Cuando se incorporan nuevos empleados, las empresas ya no necesitan crear contraseñas temporales o de ningún otro tipo. En su lugar, pueden usar un autenticador de hardware, como YubiKey. Con YubiKey, el usuario puede autenticarse en Azure AD o en otros servicios con o sin un PIN corto, en función de la aplicación. YubiKey también puede utilizarse para registrar dispositivos adicionales, como smartphones o portátiles, para que también sirvan como autenticadores.

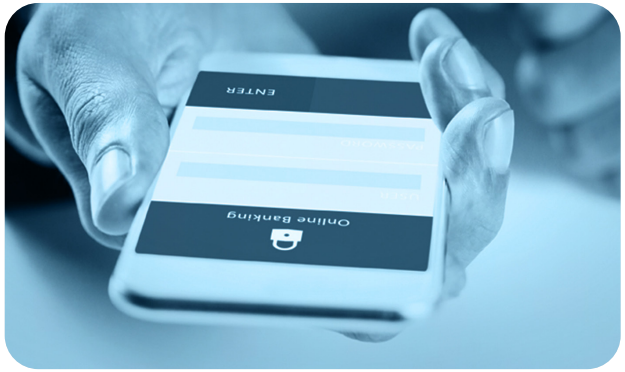
El proceso de autenticación puede llegar a ser especialmente rápido y fácil. Por ejemplo, en lugar de sentarse e introducir un nombre de usuario y una contraseña, un empleado de oficina puede simplemente sentarse, tocar la YubiKey y comenzar su día de trabajo en cuestión de segundos.

Comercio minorista

Los empleados de ventas, los jefes de planta, los jefes de equipo, los cajeros y otros empleados del comercio minorista necesitan un acceso rápido y fácil a los sistemas de TI. Los inicios de sesión sin contraseña agilizan la incorporación y el acceso a la vez que proporcionan una autenticación segura como protección contra el fraude.

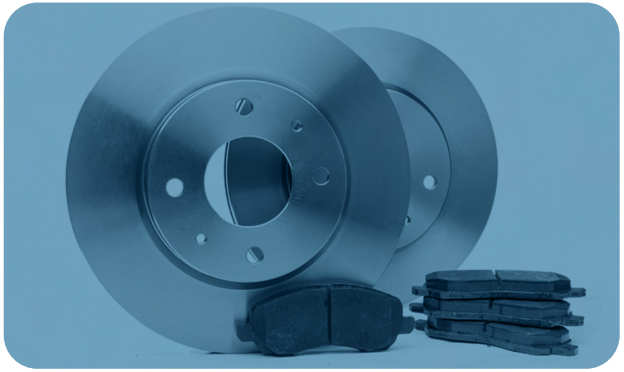
Los minoristas suelen contratar personal de temporada. Por ejemplo, un conocido minorista norteamericano suele contratar a unos 30 000 trabajadores temporales para la temporada de fiestas navideñas. Tradicionalmente todos esos trabajadores habrían tenido que usar nombres de usuario y contraseñas. Gracias a FIDO2, solo se les tiene que dar una llave de seguridad. Los servicios autorizados pueden desactivarse de forma centralizada a través de un servicio de directorio como Azure AD cuando finaliza la actividad estacional.

FIDO2 ahorra al departamento de TI el problema de crear, restablecer y rescindir contraseñas. Si se contrata de nuevo a determinados empleados, simplemente se puede reactivar y reasignar sus claves de seguridad para el acceso a los servicios de la tienda.



Finanzas

Ofrecer una autenticación rápida y sin complicaciones, mejora la experiencia de la marca, agiliza el comercio electrónico y las interacciones de asistencia al cliente, e incluso ayuda a la creación de nuevos productos y servicios. Un banco, cooperativa de crédito u otra institución financiera que ofrece a los clientes llaves de seguridad y autenticación sin contraseña, reduce el riesgo de la suplantación de cuentas a la vez que simplifica la vida de los titulares.



Fabricación

Al igual que los minoristas, los fabricantes tienen varios turnos de trabajadores. FIDO2 simplifica la gestión del acceso para esta plantilla en constante cambio. Dado que los trabajadores no tienen que introducir contraseñas pero pueden autenticarse de manera exclusiva, FIDO2 agiliza el acceso a los sistemas de TI al mismo tiempo que respalda las políticas internas de seguridad y de gestión de la identidad. Al mismo tiempo, elimina el riesgo de que las políticas de gestión de contraseñas (como la actualización periódica de contraseñas) generen retrasos u otros problemas en las operaciones.

El Departamento de seguridad nacional de Estados Unidos ha advertido que el sector de la fabricación sigue siendo un objetivo destacado de los ataques de phishing, en parte porque los hackers están interesados en robar la propiedad intelectual.[14] Al sustituir las contraseñas que pueden ser objeto de phishing por las llaves de seguridad FIDO2, los fabricantes pueden ayudar a evitar este tipo de ataque, al ofrecer una autenticación segura que protege contra el phishing.

Sector de la salud

Las organizaciones del sector de la salud son vulnerables a filtraciones de datos de varios tipos. La información sobre la salud del paciente, incluido el historial del paciente y la información del pagador, es diez veces más valiosa en el mercado negro que los datos de tarjetas de crédito.[15] ¿Por qué? Porque el fraude médico, como la presentación de denuncias falsas al seguro, genera muchos beneficios.

Estas organizaciones también son susceptibles a ataques de ransomware, muchos de los cuales se lanzan a través de phishing. Al sustituir las contraseñas por llaves de seguridad, las organizaciones del sector de la salud y sus socios comerciales pueden reducir en gran medida su vulnerabilidad a este tipo de ataques.

FIDO2 también puede ayudar a las empresas del sector sanitario a garantizar que la información médica protegida (PHI, por sus siglas en inglés) solo sea accesible para usuarios autorizados de conformidad con las normativas de la HIPAA. Los resultados de una encuesta publicada en Healthcare Informatics Research informaron de que el 73 % de los encuestados dijeron haber reutilizado las credenciales de otro funcionario para acceder a historiales médicos electrónicos.[16] La simplificación de los procesos de inicio de sesión anima a los medicos a utilizar solo sus propias credenciales para acceder a PHI y a otros datos y servicios protegidos, y a dejar de compartir las credenciales. Como mínimo, los limita a compartir el acceso solo con otras personas que están físicamente presentes. Por el contrario, las contraseñas compartidas permiten el acceso desde cualquier ubicación.

FIDO2 ofrece otra importante ventaja para el sector sanitario: una autenticación rápida y sencilla. Los médicos y las enfermeras tienen que iniciar sesión docenas de veces al día mientras pasan de un paciente a otro, de una habitación a otra y de un dispositivo a otro. Ahora el acceso puede ser inmediato y más seguro con inicios de sesión sin contraseña. Los cuidadores pueden concentrarse en el cuidado de los pacientes en lugar de tener que lidiar con engorrosos procedimientos de inicio de sesión.

Redes de proveedores y distribuidores

El número de brechas de seguridad relacionadas con proveedores de terceros ha aumentado en un 22 % por ciento desde 2015.[17]

El fortalecimiento en la autenticación a los portales de asociados con claves de seguridad FIDO2 agiliza el acceso de los socios y elimina la posibilidad de que se utilicen contraseñas robadas para infiltrarse en la empresa.

Además, FIDO2 no requiere que una empresa gestione todas las identidades de sus proveedores, sino que una empresa puede simplemente adoptar una política «sin contraseñas» y exigir a los proveedores que se autentiquen con una llave de seguridad. Los proveedores pueden adquirir fácilmente las llaves de seguridad FIDO2 por su cuenta. Este tipo de federación no era posible anteriormente con otras tecnologías de autenticación, lo que hacía que la seguridad de las redes de proveedores fuera económicamente prohibitiva.

Conclusión

Las contraseñas han sido un obstáculo para los usuarios finales, los equipos de seguridad y los equipos de TI durante demasiado tiempo. Al permitir una seguridad sin contraseñas, FIDO2 abre una nueva era en la TI de la empresa, el servicio al cliente y las interacciones hombre-máquina.

Mediante el inicio de sesión sin contraseña FIDO2, las empresas pueden reforzar la seguridad de la red, reducir los gastos de TI, mejorar la productividad y crear una nueva clase de servicios rentables gracias a una confianza generalizada, rápida y cómoda. El inicio de sesión sin contraseña ofrece las siguientes ventajas:

- **Usabilidad mejorada:** con el inicio de sesión sin contraseña, los usuarios nunca tienen que detenerse para introducir las contraseñas o tratar de recordarlas. El acceso es rápido y fácil.
- **Seguridad mejorada:** el hecho de no necesitar contraseña elimina las vulnerabilidades de seguridad de las contraseñas robadas, las contraseñas obtenidas mediante phishing y los ataques de fuerza bruta a las contraseñas simples.
- **Eficiencia mejorada:** un mundo sin contraseñas libera a los administradores de TI de tener que generar decenas o cientos de miles de contraseñas. La carga de asistencia del departamento de TI disminuye mientras la seguridad y la usabilidad mejoran.

FIDO2 es una solución que ya está disponible para cientos de millones de dispositivos de Windows 10 con una actualización a la última versión de Windows 10. Es una solución con la que los proveedores de TI y los departamentos de TI de las empresas pueden empezar a trabajar para abordar no solo las necesidades de seguridad de TI internas, sino también las de los clientes.

¿Cómo se podrían simplificar los casos de uso de los clientes con un inicio de sesión sin contraseña? ¿Cómo se pueden reimaginar las experiencias de los usuarios sin necesidad de contraseñas? ¿Qué pasaría si el acceso a las aplicaciones y servicios pudiera ser rápido, fácil y seguro en todas partes?

¿Cuáles son las posibilidades de mejora de los nuevos productos y servicios cuando ya no se requieren contraseñas, cuando los dispositivos móviles y de escritorio remotos se pueden utilizar fácilmente y son fiables, y cuando los riesgos de filtración de datos y fraude, al fin, disminuyen sustancialmente?

Estas son las preguntas que los líderes de negocio y de TI con visión de futuro deberían hacerse.

El inicio de sesión sin contraseña FIDO2 hace que estas preguntas no sean objeto de especulación, sino más bien una pregunta práctica, incluso una pregunta apremiante, para los responsables de seguridad de la información, jefes de producto, diseñadores de UX, profesionales del marketing y otros profesionales dedicados a ofrecer los mejores productos, servicios y experiencias posibles, al tiempo que garantizan que la autenticación sea siempre segura.

Recomendaciones

¿Cómo deberían prepararse los líderes empresariales, los directores de información, los directores técnicos y otros líderes de TI para un mundo sin contraseñas? Yubico ofrece las siguientes recomendaciones.

Manténgase informado

Suscríbase a las actualizaciones de Yubico y visite www.yubico.com/go-passwordless

Únase al Programa de desarrolladores de Yubico

Los desarrolladores pueden unirse al Programa de desarrolladores de Yubico para tener acceso a los talleres, al software de código abierto y a la asistencia de desarrollo.

Actualice hoy mismo las opciones de autenticación de dos factores

Incluya compatibilidad con las llaves de seguridad FIDO2 y del primer paso para usar el inicio de sesión sin contraseña.

Desarrolle una estrategia para olvidarse de las contraseñas

Reúna a un equipo de líderes empresariales y de TI de su organización para evaluar cómo aprovechar la autenticación sin contraseñas. Para empezar, el equipo podría optar por:

- Desarrollar un modelo de costes para las contraseñas. ¿Cuántas solicitudes de asistencia técnica y de centros de llamadas están vinculadas a las contraseñas? ¿Cuánto tiempo se suele emplear en cada solicitud? ¿Cuánto tiempo tardan los administradores en asignar las contraseñas de los nuevos usuarios? ¿Cuánta productividad se pierde debido a los bloqueos de cuentas? Evalúe el tiempo y los gastos de sus prácticas de autenticación actuales para que pueda comprender el ahorro de costes.
- Identificar los proyectos piloto que permitirán a su equipo implementar el acceso sin contraseña a una comunidad de usuarios seleccionada. Céntrese en las áreas que requieren una autenticación segura, donde la optimización de la experiencia del usuario aportaría grandes beneficios. Realice un seguimiento del progreso de implementación y aplique las lecciones aprendidas en futuras implementaciones.

Referencias

1. ”2020 State of Password and Authentication Security Behaviors Report”. Ponemon Institute. https://pages.yubico.com/2020-password-and-authentication-report
2. “New Research: Most People Have 70-80 Passwords”. Newswire. https://www.newswire.com/news/new-research-most-people-have-70-80-passwords-21103705
3. “Average Business User Has 191 Passwords”. Security Magazine. https://www.securitymagazine.com/articles/88475-average-business-user-has-191-passwords
4. Kessem, Limor. “Millennial Habits May Bring An End To The Password Era | SC Media”. SC Media. https://www.scmagazine.com/millennialhabits-may-bring-an-end-to-the-password-era/article/746144/
5. “Data Breach Investigation Report”. Verizon Enterprise. https://enterprise.verizon.com/resources/reports/dbir/2019/introduction/
6. “Most hacked passwords revealed as UK cyber survey exposes gaps in online security”. National Cyber Security Center, 2019 Cyber Security Survey. https://www.ncsc.gov.uk/news/most-hacked-passwords-revealed-as-uk-cyber-survey-exposes-gaps-in-online-security
7. “Protect your accounts with smarter ways to sign in on World Passwordless Day”. Microsoft. https://www.microsoft.com/security/blog/2020/05/07/protect-accounts-smarter-ways-sign-in-world-passwordless-day/
8. Verizon, ibid.
9. Ward, Kelsey. “Credential stuffing rules the day as 90% of login attempts no longer made by humans”. Secureidnews.com. https://www.secureidnews.com/news-item/credential-stuffing-rules-the-day-as-90-of-login-attempts-no-longer-made-by-humans/
10. “Statistic: the total market share of Windows 10 version 1903/1909 edition reach 75.2%”. Meterpreter. https://meterpreter.org/statistic-the-total-market-share-of-windows-10-version-1903-1909-edition-reach-75-2/
11. “NIST SP 800-63 Digital Identity Guidelines”. Nist.Gov. https://www.nist.gov/itl/tig/projects/special-publication-800-63
12. “Pcprox® Mat | RF Ideas”. Rfideas.Com. https://www.rfideas.com/products/presence-detectors/pcprox-mat
13. “Is Cybersecurity Incompatible With Digital Convenience?” McKinsey & Company. https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/is-cybersecurity-incompatible-with-digital-convenience
14. “Energy Sector Tops List Of US Industries Under Cyber Attack, Says Homeland Security Report - Iot Now - How To Run An Iot Enabled Business”. Iot Now - How To Run An Iot Enabled Business. https://www.iot-now.com/2015/03/12/30962-energy-sector-stays-top-of-the-list-ofus-industries-under-cyber-attack-says-homeland-security-report
15. “Your Medical Record Is Worth More To Hackers Than Your Credit Card”. Reuters. https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924
16. “Survey Reveals Sharing EHR Passwords is Commonplace”. HIPAA Journal. https://www.hipaajournal.com/sharing-ehr-passwords-commonplace/
17. “Data trust pacesetters show how to create and protect value from data”. PwC. https://www.pwc.com/us/en/services/consulting/cybersecurity/data-trust-pacesetters.html

yubico

Acerca de Yubico Yubico establece nuevos estándares globales para el acceso fácil y seguro a ordenadores, servidores y cuentas de internet. Fundada en 2007, Yubico es una empresa privada con oficinas en Alemania, Australia, Estados Unidos, Reino Unido, Singapur y Suecia. Descubra por qué 9 de las 10 principales marcas de Internet y millones de usuarios en más de 160 países utilizan nuestra tecnología en **www.yubico.com**

Yubico AB
Kungsgatan 44
2 ° piso
SE-111 35 Estocolmo
Suecia

Yubico Inc.
530 Lytton Avenue, Suite 301
Palo Alto, CA 94301 EE. UU.
844-205-6787 (número gratuito)
650-285-0088