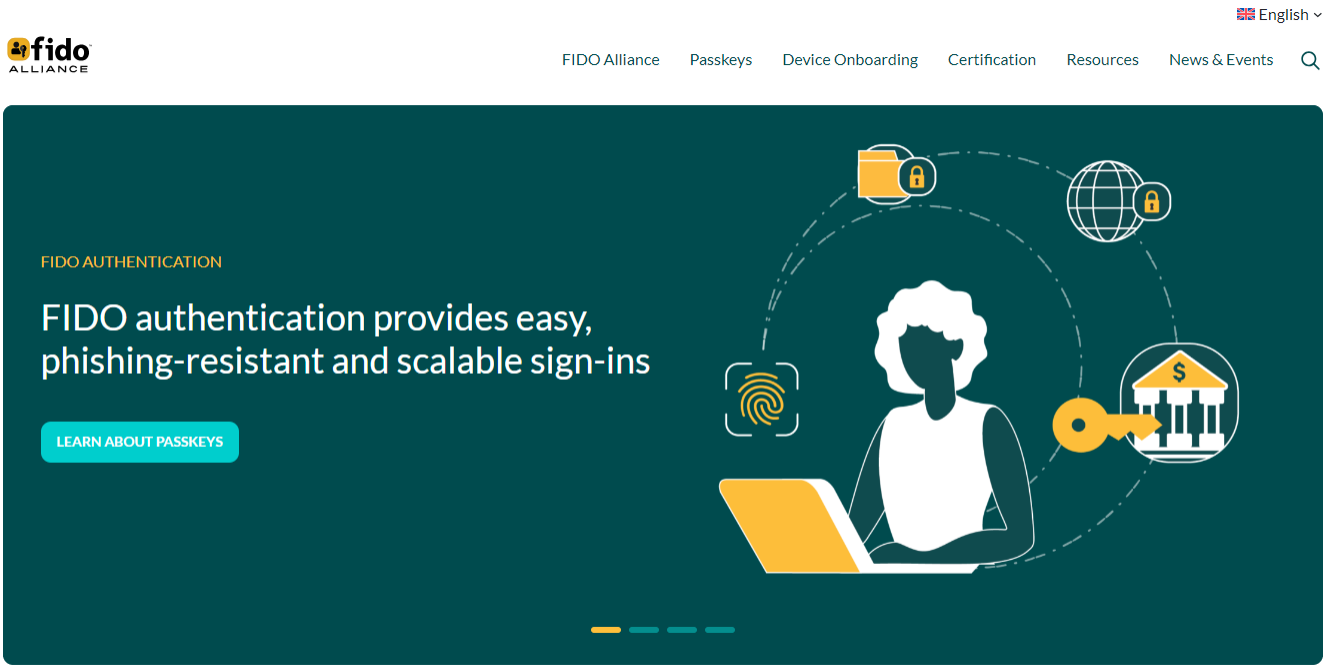

.

.

El nuevo estándar FIDO (Fast Identity Online) refuerza la seguridad de los sistemas de autentificación de la identidad ‘online’ en dispositivos móviles y aplicaciones web. Su objetivo es reemplazar el uso exclusivo de contraseñas por mecanismos de autenticación biométricos más seguros protegidos por sistemas de encriptación.

La Alianza FIDO (Fast Identity Online), creada por algunas de las compañías tecnológicas líderes en el mundo, tiene como propósito cambiar la forma de autenticación ‘online’ para hacerla más segura y cómoda.

En la actualidad **el método más habitual de autenticación ‘online’ es el uso de contraseñas,** un sistema que puede generar problemas ya que, para que sean seguras han de ser complejas, y si son complejas, resultan difíciles de recordar. Más aún si se tiene en cuenta que los usuarios tienen de media en torno a 90 cuentas ‘online’, según la Alianza FIDO.

Con el objetivo de mejorar esta situación y hacer más segura la autenticación de la identidad ‘online’, la Alianza FIDO ha creado una serie de estándares técnicos interoperables que facilitan la creación de experiencias de inicio de sesión seguras y rápidas en sitios web y aplicaciones. Esto facilita la identificación de los usuarios a través

de **sistemas biométricos** como la huella dactilar o el reconocimiento facial; así como mediante la **autenticación de doble factor o factor múltiple**, que consiste en comprobar varias veces mediante diferentes mecanismos que la persona es quien dice ser.

El uso de estándares FIDO **facilita la integración segura de estas alternativas** de autenticación en los dispositivos móviles y navegadores web y se basa en el uso de técnicas criptográficas de llave pública, lo que ofrece un método de identificación más robusto y cómodo, frente al uso de las contraseñas como único sistema de protección.

¿Cómo funciona?

Cuando un usuario se registra en un servicio ‘online’ que emplea el estándar FIDO, el sistema genera una pareja de **claves criptográficas**, de forma que **la clave privada se conserva en el ‘hardware’ del dispositivo y la clave pública se guarda en el servicio ‘online’**. Para realizar la autenticación, el dispositivo del cliente debe demostrar al servicio ‘online’ que dispone de la clave privada realizando una verificación matemática. Además, la clave privada del cliente únicamente se podrá utilizar una vez que el usuario la haya desbloqueado de forma local en el dispositivo. Este desbloqueo puede realizarse mediante una acción segura y fácil como por ejemplo introduciendo su huella dactilar, utilizando su voz o introduciendo un PIN.

De esta forma se consigue **proteger la privacidad del usuario y sus credenciales de acceso**, consiguiendo que los usuarios no se vean obligados a elegir entre mejor seguridad o mejor experiencia de usuario, sino que pueden disponer de ambas.

Julio Pari (IT Architect BIAN)

Especialista BIAN Semantic API | Gobierno de Integración | IBM Integration CP4I | IBM API Connect 10 | IBM ACE | IBM DataPower | OpenShift | Azure | AWS. Cualquier consulta envíame un mensaje a: info@arquitecturabank.com o sino a través de Linkedin: https://www.linkedin.com/in/juliopari/