Valuable data needs to be protected by a strong, secure fence — a perimeter that lets authorized users in while keeping bad actors out. For years, this has meant passwords. Unfortunately, passwords are not always the answer because they’re rarely both secure and easy for the user to remember. Since the average internet user has to maintain over 90 passwords, they tend to reuse the same ones or make them too simple. It’s no wonder passwords are often easily guessed or open to theft. In fact, Google research estimates that from March 2016 – March 2017, 1.9 billion usernames and passwords were exposed. In addition, 81% of data breaches are caused by compromised, weak and reused passwords.

Stronger solutions, like multi-factor authentication (MFA) and sophisticated cryptography, have helped to combat these password vulnerabilities, requiring users to present multiple forms of identification before achieving access. These solutions are less prone to compromise, but the infrastructure required is often complex. In addition, some of them require user credentials like biometric fingerprints to be stored in the cloud. Cybersecurity professionals have long searched for a simpler and more secure way to control access to data.

Enter FIDO.

Origins and Evolution of the FIDO Alliance

FIDO, which stands for Fast Identity Online, began with a group of leading tech companies banding together to make authentication easier and more secure. The FIDO Alliance is comprised of some of the biggest and most respected names in tech, many of them competitors. To create the Alliance, however, they banded together to establish a framework and standards that can be built directly into almost any device — as opposed to proprietary, device-specific security.

In its first iteration, FIDO allowed:

- Users to easily register a device (e.g. computer) to a service leveraging public/private key technology (UAF)
- A private key, unique to each service, to be stored on the device
- Local device log-in options like a password, fingerprint, face recognition and/or smart card
- The increased security of a second factor authenticator (U2F)

The most recent update, FIDO2, offers the same features as the original as well as a few browser benefits, such as:

- FIDO security for the entire web
- Browser-based FIDO technology, rather than software installed on the device
- FIDO client integration into the browser ensuring that any browser (Firefox, Chrome, etc.) supporting it will be secure
Increased Security + Improved User Experience

FIDO essentially works like a lock and key. First, a user registers a device and chooses any authentication option provided locally by this device (either a biometric, like a fingerprint, or password or smart card). During this registration, a public/private key pair is created. The private key stays on the local device and is used to authenticate the device to the service. Access to this key is protected by the local authentication chosen. In addition, a second authentication factor can be registered (like a FIDO token or a smart card supporting FIDO U2F specification).

When the user needs to access the service, they confirm their identity on their device with their authenticator. That information is sent to the service. Essentially, the device acts as a translator between the authenticator’s security and the service’s security. This combination of layered protocols provides extremely robust access control.

Authenticators: Something You Are or Something You Have

The FIDO Alliance certifies two categories of authenticators: biometrics and security keys. Both offer increased security, which can further be strengthened with simple four-digit PINs. The authenticators are certified through a standard process where developers thoroughly test, prove the testing by submitting lab results, then apply for certification from the alliance. Both subcomponents and authenticators must go through this certification process.

With biometric authentication, the user doesn’t have to remember or carry a form of identification — it’s inherent in who they are. Biometric options include:

- **Fingerprint** — Many smart phones already use fingerprint authentication to unlock the device, so users are familiar with the process and technology. Here, the device serves as the key, and the identification data is stored locally. This is also the least expensive key option.

- **Facial Recognition** — Facial recognition is similar to fingerprint, with the added bonus of no-contact authentication — a growing concern on devices with multiple users. It does not, however, prove identity as definitively as fingerprints.

- **Voice Recognition** — Voice is another no-contact technology but may not be as secure — especially in crowded spaces, where clearly and audibly stating passwords is not ideal.

Security keys are comprised of two components:

- Contactless card readers, like HID’s OMNIKEY®, which are connected over USB to or embedded in the device.

- NFC smart cards, which may only serve as FIDO authenticators or may be multifunctional. Cards like HID Crescendo® can be used in combination with an integrated RFID antenna for building access, cashless payment, elevator access or secure printing. With their integrated crypto-processor, they offer FIDO U2F functionality as well as digital signature and data encryption.

These keys are inserted into a reader that connects directly to the device, most often a computer. They may also unlock more than websites. Just like this one card can access many different physical locations while denying entry to others, it can be used to access individual websites without sharing security data, since a unique public/private key combination is created for each online location.
Enabling a Passwordless Future

We hope this executive brief has illuminated how FIDO works and its capacity to make user authentication seamless and secure. In a FIDO-enabled world, people can forget about memorizing complicated passwords and keep their data private. Organizations can reduce the financial and reputation hit of all-too-common security breaches caused by weak or exposed passwords.

To learn more about HID Global’s broad portfolio of FIDO-certified readers and authenticators visit https://www.hidglobal.com/products/readers/omikey.