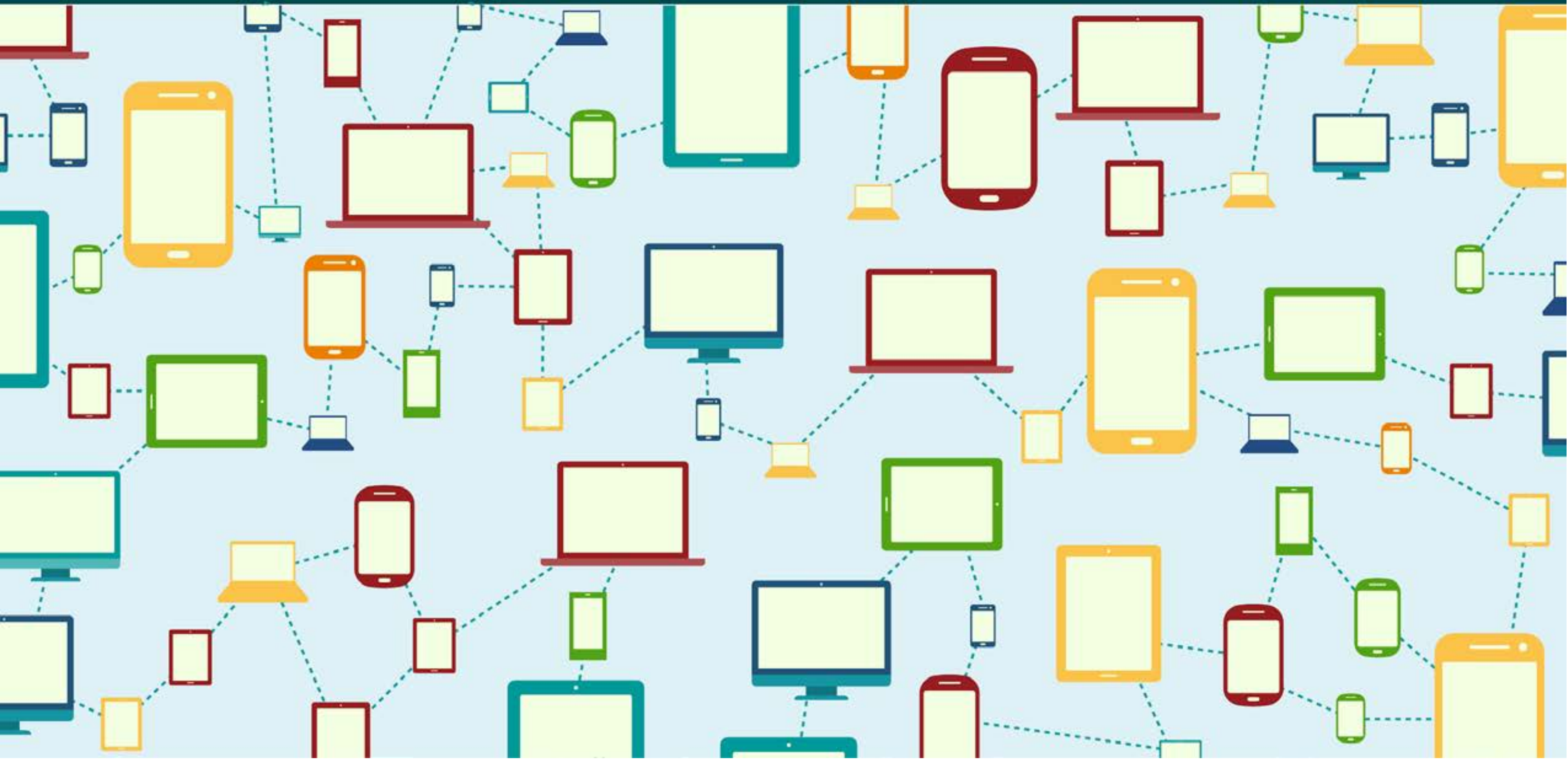
fido ALLIANCE simpler stronger authentication



FIDO Authentication and the General Data Protection Regulation (GDPR)

May 2018

Executive Summary

The General Data Protection Regulation (GDPR) takes effect on May 25, 2018 – impacting firms not just in the European Union (EU), but across the globe. Any organization that does business with EU residents will be required to comply with the regulation.

There are three things every organization should know about GDPR when it comes to authentication:

1. GDPR requires firms to implement data protection safeguards. Strong, multi-factor authentication is a fundamental building block of cybersecurity and data protection. Last year, 81% of all breaches were due to attacks that exploited weak or stolen passwords[1] - which means that any approach to data protection that does not include the use of multi-factor authentication (MFA) is incomplete. Moreover, some forms of MFA are better than others – with older, first-generation MFA technologies less effective now that attackers have learned how to get past them.

2. GDPR requires firms to respond to requests from individuals to view, change, delete, or transfer their data. It also requires firms to demonstrate they obtained the consent of individuals to the processing of their data and, specifically, *explicit consent* if this data is deemed sensitive. A key element of delivering these capabilities securely is to ensure that the identity of individuals making these requests or providing their consent are authenticated - organizations need to demonstrate that an individual actually consented or requested that their information be changed.

3. Biometrics are one of the most promising technologies to deliver strong authentication – offering not just enhanced security, but also excellent convenience and a great user experience. However, the GDPR highlights biometric data as a "sensitive" category of personal information warranting robust protection, and setting out specific restrictions on the use of biometrics. Thus, any entity implementing biometric authentication needs to ensure that its use of biometrics does not run afoul of the GDPR.

FIDO Alliance standards were designed from the start with a “privacy by design” approach – to ensure that the FIDO standards minimize any potential privacy or security harms that might arise from authentication technologies. FIDO delivers authentication with no third-party in the protocol, and no link-ability or tracking between accounts and services.

This “privacy by design” approach extends to FIDO’s use of biometrics. That means that FIDO standards:

1) Prohibit biometrics from being stored or matched in servers, and

2) FIDO-certified devices (i.e., smartphones, laptops or tokens) must not allow for any biometric captured by that device for a FIDO solution to be transferred to a server. With FIDO, biometrics can <u>only</u> be stored and matched on a consumer’s device.

[1] See http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

While biometrics are not required in FIDO implementations, many FIDO solutions use biometrics as one authentication factor. Here, FIDO offers a standards-based approach for GDPR-compliant biometric authentication.

FIDO standards are backed by a certification program designed to measure compliance and ensure interoperability among products and services that support FIDO specifications.

With more than 425 FIDO® Certified products in the market, FIDO authentication represents the best way for organizations to implement simpler, stronger authentication that meets GDPR's rigorous requirements – and enhances the user experience.

About GDPR

The GDPR[2] is the most significant change to European data protection law in twenty years. This new regulation will have global impact on a variety of industries that collect and process information from EU citizens, including those that process and use biometric data for the purpose of uniquely identifying a natural person.

Unlike current EU data protection laws, the GDPR may apply to any processing of personal data of an EU resident (i.e., "data subject") if a firm offers goods or services to an EU data subject. Firms may be covered by the GDPR even if they do not have an office or employees in the EU.

The potential fines are significant. The GDPR allows EU Data Protection Authorities (DPAs) to levy hefty fines for non-compliance. Fines for fundamental violations of the GDPR could be up to €20 million or up to 4% of global turnover (i.e., revenue), whichever is higher. Fines for secondary violations, related to obligations such as privacy by design and children's consent, could be €10 million or up to 2% of global turnover, whichever is higher.

There will be a supervisory authority established in every EU Member State to enforce GDPR – meaning that firms doing business in Europe may have to deal with 28 different supervisory authorities once the GDPR takes effect on May 25, 2018.

How GDPR Impacts Authentication

Within GDPR there are several Articles that specifically impact authentication. These Articles can be grouped into three categories: Data Security, Consent and Individual Rights, and Biometrics.

1. **Data Security**
    - Article 5 lays out core principles relating to processing of personal data, including that personal data shall be:

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC.

  - Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')
  - Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
  - Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')

- Article 25 calls for data protection by design and by default. More specifically, GDPR states that entities should
  - Implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimization
  - Implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed
- Article 32 defines requirements for data security. Specifically, the GDPR directs entities to implement technical and organisational measures to ensure appropriate security relative to state of the art, cost of implementation and risks. Specific elements[3] called out include:
  - Measures to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
  - Measures commensurate to the risk
  - Measures to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
  - A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing
- Articles 33 and 34 lay out requirements for data breach notification. These include:
  - Organizations must report breaches to their supervisory authority within 72 hours - unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons
  - Notification must outline numbers of people impacted, as well as the nature of records breached, likely consequences, and measures to be taken to address it
  - If a breach is likely to result in a “high risk to the rights and freedoms” of someone, it must be reported to them “without undue delay”

Impact: Strong, multi-factor authentication is a fundamental building block of cybersecurity and data protection. Last year, 81% of all breaches were due to attacks that exploited weak or

[3] Article 32 ¶1.a-d.

stolen passwords[4] - which means that any approach to data protection that does not include the use of multi-factor authentication (MFA) to prevent password-based attacks is incomplete.

Moreover, some forms of MFA are better than others. SMS-based authentication is generally considered a weaker form of authentication, due to several reasons, such as vulnerabilities in the SS7 protocol and the ability of mobile malware to intercept SMS messages arriving at a mobile phone. As a result NIST has deemed its use as "restricted", meaning organizations would be taking a risk using SMS.[5] One-time passwords (OTPs), while they provide stronger protection than SMS, can also be susceptible to phishing attacks[6]. Thus, to truly enhance the security of accounts, it is important that organizations use "high assurance strong authentication" – where at least one factor leverages public key cryptography.

FIDO authentication offers organizations a simpler, standards-based approach to delivering high-assurance strong authentication.

2. Consent and Individual Rights

- Article 7 requires that *"the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data."*
- Articles 16-20 lay out a variety of rights for an individual, including:
  - A right to rectification - allowing an individual to correct inaccurate personal data concerning him or her.
  - A right to erasure – aka a "right to be forgotten" – allowing an individual to request that an entity delete all his or her personal data
  - A right to data portability – allowing an individual to request a copy of his or her data, as well as transmitted to another entity.

Impact: A key element of delivering these capabilities securely is to ensure that the identity of individuals making these requests are authenticated - organizations need to demonstrate that an individual actually requested that their information be changed. Failure to do so could trigger violations of other aspects of the GDPR.

3. Biometrics

- Article 4 defines Biometric Data as *"personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of*

[4] See http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

[5] See https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf

[6] The vulnerabilities of OTP have been documented by firms like Google, who publicly flagged the extent of the problem in 2015 at the Cloud Identity Summit, noting that these days, a "phisher can pretty successfully phish for an OTP just about as easily as they can a password" and noted their shift to hardware-based solutions using the FIDO Alliance specifications as the way to stop these targeted phishing attacks. (See https://www.youtube.com/watch?v=UBjEfpfZ8w0) Note that Google had previously tried to drive two-factor login by offering OTP through both SMS and a free OTP app based on the OATH protocol; these comments reflect their experience with this technology.

a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data."

It also lists biometrics in the definition of "sensitive personal data."[7]

- Article 9 states that "*Processing of…biometric data…shall be prohibited."* – but then lays out a number of conditions where this prohibition might be lifted.
- Recital 91 states that when data controllers and processors look to process biometric information, they are required to perform a data protection impact assessment ("DPIA") prior to the processing activity occurring. A DPIA will need to include a description of the processing taking place, an assessment of the necessity of the processing, an assessment of the risks to the rights and freedoms of data subjects, and what measures will be taken to mitigate those risks including any safeguards.

Of note, GDPR states that biometrics are a special type of data where any of the 28 EU Member States "may maintain or introduce further conditions, including limitations, with regard to the processing of…biometric data." This means that companies using biometrics may have to comply with different rules in different parts of the EU.

France's Data Protection Authority has already proposed additional rules[8] for biometric authentication and other countries may soon follow.

Impact:

As this paper details in the sections that follow, the "privacy by design" approach of the FIDO standards provides the best way for an organization to address GDPR rules around use of biometrics in authentication.

Collectively, these requirements make three things clear:

1. Organizations need to implement MFA as part of their approach in order to be compliant with the requirements of data protection under GDPR
2. Organizations need to authenticate individuals who are providing consent to their sensitive data being captured or are asking for their data to be erased, corrected, or transmitted to another party.
3. For organizations using biometrics as part of their authentication solution, they must ensure that the biometrics application does not run afoul of GDPR.

[7] Article 4 ¶14; Article 9 ¶1.

[8] See "Biometrics in private smartphones: how does the law on computers and freedoms apply?" March 8, 2017 at https://www.cnil.fr/fr/biometrie-dans-les-smartphones-loi-informatique-et-libertes-exemption-ou-autorisation

FIDO Standards are Optimised for GDPR Compliance

With more than 425 FIDO-certified products in the market, FIDO authentication represents the best way for organizations to implement simpler, stronger authentication that meets GDPR's rigorous requirements – by at the same time enhancing the user experience.

FIDO Alliance standards were designed from the start with a "privacy by design" approach[9] – to ensure that the FIDO standards minimize any potential privacy or security harms that might arise from authentication technologies. FIDO delivers authentication with no third-party in the protocol, and no link-ability or tracking between accounts and services.

This approach also extends to FIDO's use of biometrics. Where biometrics are involved, FIDO minimizes risk by ensuring that entities can leverage biometric authentication without having to collect, control or process biometric data themselves.

That means that FIDO standards:

1) Prohibit biometrics from being stored or matched in servers, and
2) FIDO Certified devices (i.e., smartphones, laptops or tokens) must not allow for any biometric captured by that device for a FIDO solution to be transferred to a server. With FIDO, biometrics can only be stored and matched on a consumer's device.

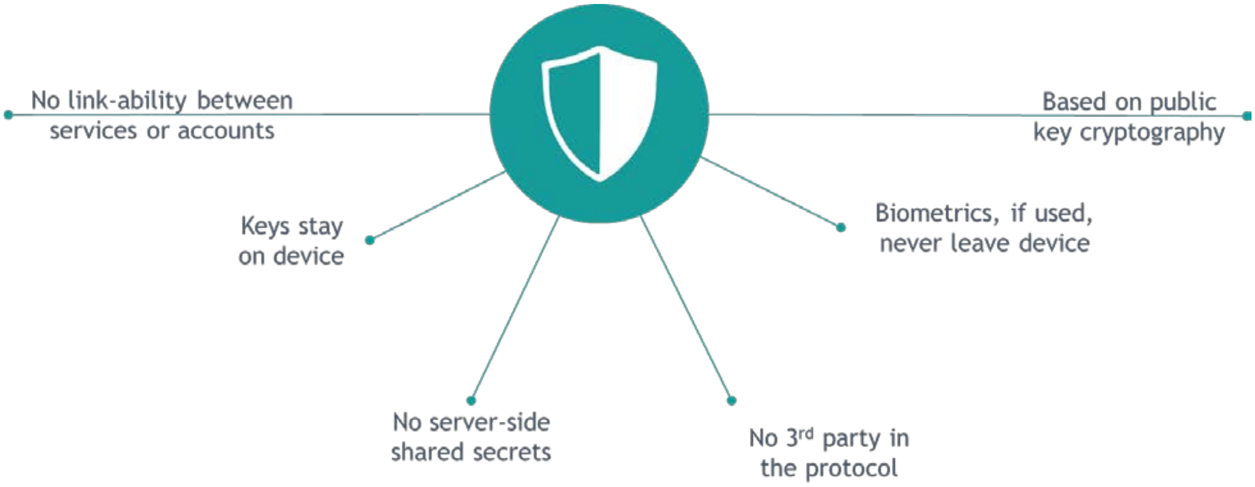

No link-ability between services or accounts
Based on public key cryptography
Keys stay on device
Biometrics, if used, never leave device
No server-side shared secrets
No 3rd party in the protocol

Figure 1 - FIDO Embraces Privacy-by-Design

[9] See FIDO Alliance's Privacy Principles at https://fidoalliance.org/wp-content/uploads/2014/12/FIDO_Alliance_Whitepaper_Privacy_Principles.pdf

How FIDO Authentication Works

At the heart of FIDO is an authentication solution based on long-proven asymmetric Public Key Cryptography, where the private key is the only "secret," and it is stored on the user's device. Only the public key is shared with the online service, resulting in no credential secrets ever being shared with servers; this renders the threat of credential theft from a data breach moot.

In a typical deployment of FIDO standards, a user swipes a finger, speaks a phrase, or looks at a camera on a device to login, pay for an item, or use another service. Behind the scenes on that device, the biometric is used as an initial factor of verifying the user to the device to then unlock a second, more secure factor: a private cryptographic key. The private key is used "behind the scenes" to authenticate the user to the service. Since biometrics and cryptographic keys are stored on local devices and never sent across the network – eliminating shared secrets – user credentials are secure even if service providers get hacked, thereby eliminating the possibility of scalable data breaches.

FIDO solutions can also be deployed via standalone "security key" tokens. They are based on tamper resistant chips similar to the secure element embedded in devices. With the security key architecture, a user can use a single token across several different devices, leveraging common interfaces such as USB, NFC and Bluetooth.

In terms of the user experience with biometrics, a user wishing to access an online service goes through three steps. In the example below, the user is making a payment on a mobile phone equipped with a FIDO-compliant fingerprint sensor, though FIDO specifications support the use of multiple biometric modalities, in addition to modalities that don't require biometrics.

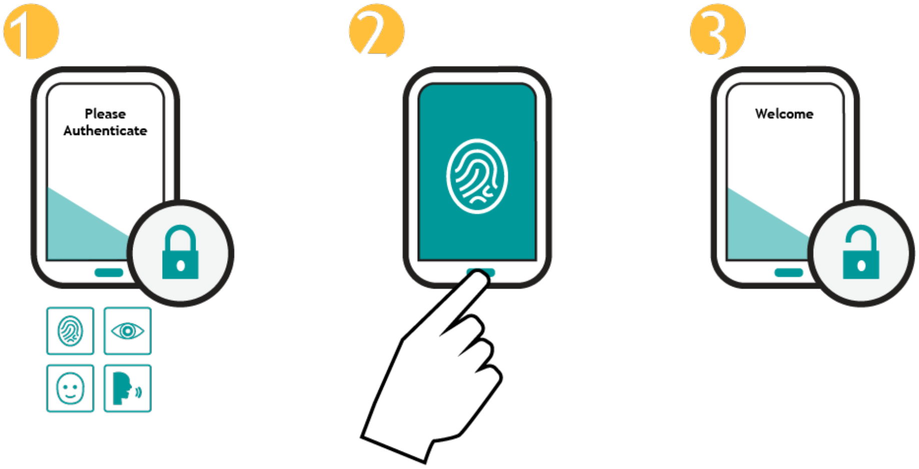


Figure 2 - User Authentication

1. The online service provider asks the user with a previously registered device to authenticate themselves.

2. The user unlocks cryptographic credentials stored on that phone by means of successfully presenting their fingerprint to the FIDO-compliant fingerprint sensor they previously enrolled their fingerprint with.

   The mobile phone locally (offline) verifies the user's fingerprint by performing a "local match" against the previously stored biometric template for that user and executes the FIDO authentication protocol to sign the FIDO-compliant authentication challenge and send that signed challenge online to the service provider.

   Note that biometrics never leave the device: FIDO's "privacy-by-design" approach means that biometrics can only be matched and stored on device.
   - Biometric matches against a database are prohibited
   - Biometrics cannot be exported off device

3. The online service provider verifies the signature on the authentication challenge using the public key that was previously registered for that user's account from that phone when it was first registered by that user with this online service. The result is a highly secure, very easy to use authentication that protects biometric information.

FIDO Authentication is Embraced by Leading Firms Across the Globe

FIDO standards are currently being used to enable simpler, stronger authentication in offerings from Google, PayPal, Mastercard, Bank of America, NTT DOCOMO, BC Card (Korea), Microsoft, Dropbox, GitHub, eBay, Samsung, Facebook, and other leading firms. In each of these deployments, end-users do not have to know how the authentication works or why it's more secure – they are getting login experiences that are easier to use, with state-of-the-art security baked in behind the scenes.

Added Security: FIDO Protocols Deliver Several Independent Authentication Factors

FIDO Alliance specifications were specifically designed to address challenges posed by security and usability concerns involved with traditional "shared secrets" approaches to authentication, enabling strong authentication through two independent factors.

This is particularly highlighted by the separation of local user verification and the cryptographic protocol. Independence is achieved on several levels:

1. In a typical smartphone FIDO solution, the biometric (the first factor) is on the user and the private cryptographic key (the second factor) is stored on the device. The biometric is presented to the device and matched locally; after a successful match, the device then uses the private key in a cryptographic protocol to respond to an authentication challenge issued by the service provider. The combination of the user verification through biometrics and the private key makes phishing attacks irrelevant.

2. The independence of these FIDO authentication factors can be enhanced by the use of modern hardware-backed technologies present on an ever increasing percentage of consumer devices (mobile and desktop) such as Secure Elements, Trusted Execution Environments (TEE) or Trusted Platform Modules (TPM). These hardware solutions are an independent element in the device, specifically created to ensure isolation from the rest of the device (which is running complex mobile operating systems and numerous applications), and protect the device from malware and other attacks.

3. This model is further enhanced by the Attestation Key that allows the characteristics of a FIDO Authenticator to be bound to a particular device. The attestation key allows any online service provider to know what specific security elements are on the device and make a judgement as to whether to trust it; among other protections, this prevents attacks from an adversary looking to try to trick a service provider into appearing to have a FIDO-compliant device.

The net impact of this approach is that an attacker must steal someone's device in order to launch an attack - and would have to somehow find a way to compromise the second factor (for example, the biometric) before an individual realized her device had been stolen. This attack model is neither easy to execute, nor is it scalable to a large number of devices.

Specifications backed by certification

In support of building confidence in the FIDO ecosystem, the FIDO Alliance has developed a robust certification program; details can be found at https://fidoalliance.org/certification/. This program ensures that different FIDO implementations interoperate with each other on a technical level and that the technical specifications are adhered to. Participation in these certification programs is voluntary but is a prerequisite for obtaining rights to use a FIDO Certified logo.

Additionally, with the security lab certification and security assurance verification accomplished by an independent third party, the FIDO Alliance has launched a new extension of the certification program allowing users and Relying Parties a fast and easy judgement of the security level of FIDO authenticators in addition to the functional testing for interoperability currently offered by the FIDO Alliance directly. Details on the FIDO Authenticator Certification Levels program are at https://fidoalliance.org/certification/authenticator-certification-levels/.

The hundreds of FIDO Certified products demonstrate a mature, competitive, interoperable authentication ecosystem. Many of these products are smartphones and laptops with FIDO authentication being built in. Organisations implementing FIDO for strong MFA therefore can rely not only on a mature ecosystem, but also on an extensive choice of FIDO-Certified products already available today.

About the FIDO Alliance

The FIDO (Fast IDentity Online) Alliance, www.fidoalliance.org, was formed in July 2012 to address the lack of interoperability among strong authentication technologies, and remedy the problems users face with creating and remembering multiple usernames and passwords. The FIDO Alliance is changing the nature of authentication with standards for simpler, stronger authentication that define an open, scalable, interoperable set of mechanisms that reduce reliance on passwords. FIDO authentication is stronger, private, and easier to use when authenticating to online services.