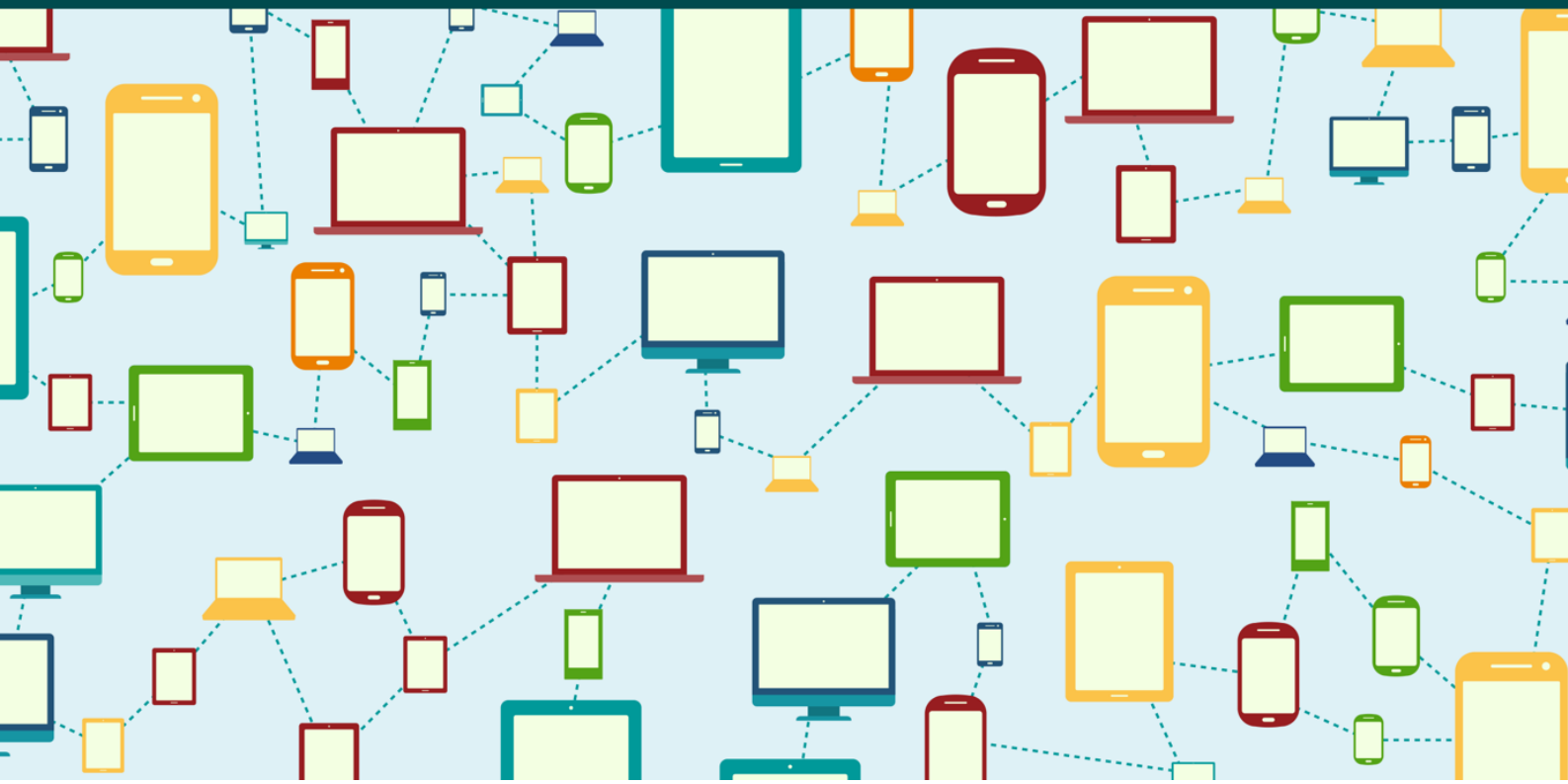
fido alliance | simpler stronger authentication



Response to the European Banking Authority (EBA) Discussion Paper on Future Draft Regulatory Technical Standards on Strong Customer Authentication and Secure Communication Under the Revised Payment Services Directive (PSD2)

The Fast Identity Online (FIDO) Alliance welcomes the opportunity to comment on the European Banking Authority (EBA) *Discussion Paper on future Draft Regulatory Technical Standards on Strong Customer Authentication and Secure Communication* ("Discussion Paper") under the revised Payment Services Directive (PSD2).

We recognize and applaud EBA's inclusive approach as articulated in the Discussion Paper as it embarks on its mandate to lead the development of regulatory requirements for strong customer authentication under PSD2. As a not-for-profit, multi-stakeholder, global industry consortium of more than 250 organizations – many of whom are regulated payment service providers and/or financial institutions – we appreciate how European banks' experiences with previously available authentication solutions have shaped some of the thinking that has gone into the Discussion Paper; likewise, we acutely understand the challenges industry and government face in addressing strong consumer demand for easy-to-use solutions, particularly when transacting from a mobile device.

The approach fostered by the FIDO Alliance – and reflected in the large variety of businesses and governments that support it – builds on Europe's successes to date in driving a high standard for strong authentication. At its core, FIDO takes the best elements of the public-key cryptographic-based security models, widely used throughout Europe for point-of-sale payments, and addresses further concerns about interoperability online, ease of use, consumer choice, privacy and mobility, much of which is highlighted by EBA in the Discussion Paper.

As we detail in this response, the FIDO specifications – and the array of companies and governments supporting them – represent a recent advance in authentication that is fundamentally transforming the landscape, enabling better security, usability and privacy without the tradeoffs that have accompanied these three elements in the past.

Some of the questions raised in the Discussion Paper stem from concerns about the limits of technologies that have been implemented in the past. As we detail in our response, these concerns are being addressed in an innovative way today by the dozens of FIDO-compliant solutions that implement FIDO specifications. We believe that FIDO-compliant implementations that follow security best practices are ideal examples of what the EBA regulations for "strong customer authentication" under PSD2 are striving to foster; simpler, stronger authentication capabilities that merchants and consumers will adopt at scale. This adoption will reduce online fraud rates and accelerate overall online payment volume, especially in mobile commerce.

We would welcome the opportunity to engage directly with the EBA, both to demonstrate how FIDO solutions are being used in the marketplace today, as well as to answer any questions. Our executive director, Brett McDowell, can be reached at brett@fidoalliance.org.

As a prelude to our response, we highlight: that FIDO has gained rapid support from a wide array of stakeholders worldwide; that its specifications are backed by certification; that more than 100 million devices are FIDO-certified in the market today and; that the specifications were specifically designed to support EU privacy requirements. More information about the Alliance and FIDO-compliant implementations can be found as an appendix to this paper, following our answers to the EBA questionnaire.

FIDO Alliance Responses to EBA Questions

Chapter 4.1: Requirements on strong consumer authentication

1. *With respect to Article 97(1) (c), are there any additional examples of transactions or actions implying a risk of payment fraud or other abuses that would need to be considered for the RTS? If so, please give details and explain the risks involved.*

The FIDO Alliance does not have any additional examples to suggest here.

2. *Which examples of possession elements do you consider as appropriate to be used in the context of strong customer authentication, must these have a physical form or can they be data? If so, can you provide details on how it can be ensured that these data can only be controlled by the PSU?*

At the core of FIDO specifications is the generation of a public/private key pair on a FIDO Authenticator[1] device where the private key is contained within, and protected by, the FIDO Authenticator. Proof-of-possession of this private key is the basis for FIDO Authenticators' capability to fulfill the possession requirements for strong customer authentication. We note that there are a range of technologies available for FIDO Authenticators to use to protect the private key from being exported from the user's device.

The degree to which a FIDO Authenticator protects the FIDO authentication private key from theft or tampering is implementation-specific, but can be tested. It is for this type of testing, presumably performed by 3rd-party security labs, that FIDO Alliance is currently defining requirements; the Alliance will be launching a formal FIDO Security Certification Program later in 2016.

A well-protected private key cannot be exported from the device; nor can an attacker duplicate or spoof that key. Thus, any authentication ceremony which uses that key, subject to the service provider's required level of assurance, proves possession of the device on which it was generated.

Because only the FIDO Authenticator itself contains the private key, the only practical way to attack that key is to attack the user's personal device. When the FIDO Authenticator leverages modern technology for the protection of the private key, such as secure elements, Trusted Execution Environments (TEE) or TPM chips (which is the trend with consumer electronics today, especially mobile devices), the attacker must actually gain physical possession of that user's device to even attempt an exploit. This type of attack does not scale and is quickly detectable as mobile devices are highly personal and quickly missed by the owner. Such an attack is therefore not economical from a cyber-crime perspective.

Even if an individual's device is captured, the only way an attacker can unlock that key is through a second factor – in the case of FIDO UAF[2] this would typically require the attacker to also have a spoof of the genuine user's biometrics (though other options are available such as PIN codes), and in the case of FIDO U2F this would typically require the attacker to also have the first-factor credentials for the user's account such as their username and password. Simply having possession of a FIDO Authenticator does not grant access to any account protected by that FIDO Authenticator, which is why all FIDO Authenticators are inherently multi-factor authenticators. When an adversary must steal someone's device before launching an attack on their Authenticator, it materially changes the risk model.

Many FIDO-compliant solutions are further bolstered by the presence of a hardware-backed Attestation Key, present in every FIDO Authenticator of that make and model, that attests to the particulars of the device itself. This Attestation Key can be used by an online service provider (Relying Party) to understand what kind

[1] An Authenticator is a logical component that may be contained in a device, such as in a physically secure execution environment (i.e., a Trusted Execution Environment (TEE) or Secure Element) in a smartphone or Trusted Platform Module (TPM) of a computer, or may reside in a separate physical device (e.g., a USB token with a Secure Element that can be attached to a laptop, or a smartwatch that is connected via Bluetooth Smart with another device).

[2] Note that version 1.0 of FIDO specifications includes two types of protocols: the Universal 2nd Factor (U2F) and Universal Authentication Framework (UAF); these protocols support two different use cases that will both be supported in the new FIDO 2.0 specifications, whose web browser and web server components have been submitted for formal standardization to the W3C. We discuss the two specifications in more detail in our Appendix.

of technology (e.g., biometric type, hardware security element, etc.) is being used in that particular device. This Attestation Key provides an additional role in the chain of trust.

Some FIDO Authenticators go a step further and take advantage of the FIDO Metadata Service which is a mechanism for online services to reference a local cache of authenticator-manufacturer-provided metadata about the authenticator itself. This is a public service operated by the FIDO Alliance, optional for online services and authenticator vendors, that if used may help facilitate the exchange of relevant information that online service providers can use to make informed trust decisions when presented with a previously unknown FIDO Authenticator requesting registration.

3. *Do you consider that in the context of "inherence" elements, behavior-based characteristics are appropriate to be used in the context of strong customer authentication? If so, can you specify under which conditions?*

The FIDO Alliance does not assert that there is any single "silver bullet" solution for authentication that is capable of supplanting all other authentication technology currently in operation. The FIDO specifications and associated testing programs enable a new solution that does provide a much stronger "first signal" of strong, reliable authentication to any given online service's authentication infrastructure that is not phishable, privacy-respecting, and cryptographically reliable. But most modern authentication systems will also incorporate what is typically referred to as "risk-based authentication" that will look at behavior-based characteristics in addition to the authentication credentials themselves. The FIDO Alliance recognizes the value of these systems but we do not produce requirements or guidance on how such systems should be used.

We note that there is an emerging array of biometric solutions in the market that rely on measurements of behavior, rather than "traditional" biometrics that focus on measuring the unique aspects of a person's biometric sample (fingerprint, iris, etc.). As with all other forms of biometric authentication, some of these behavior-based biometrics are more reliable than others. The key distinguisher is whether that behavior-based biometric is able to measure a trait that has a high enough level of uniqueness.

All biometrics – behavior-based and otherwise – are not equal; the FIDO Alliance is researching the feasibility of launching a biometric testing program to validate that biometrics proposed for use in FIDO Authenticators meet thresholds for accuracy and robustness.

Note that FIDO specifications also ensure that privacy of biometrics is protected by requiring that biometrics never leave the device; under no circumstances are biometrics to be shared with or stored by online service providers. The FIDO Security Certification Program mentioned earlier as a way of testing how well a FIDO Authenticator protects the private keys, will also test how well that FIDO Authenticator, if biometric are used, protects the user's biometric information from unauthorized access to the locally stored biometric templates.

4. *Which challenges do you identify for fulfilling the objectives of strong customer authentication with respect to the independence of the authentication* ***elements*** *used (e.g. for mobile devices)?*

The independence of authentication elements is an essential question when considering strong customer authentication – particularly when all authentication factors rely upon the traditional "shared secrets" model of credentials, such as passwords and one-time passcodes.

Given the risks associated with payments, it is understandable that the authors of this requirement would insist on the independence of the authentication elements. In an architecture when both the first and second factor are "shared secrets," one would want to ensure that if the first channel (i.e., a web browser), were compromised by an attack that the second "secret" not be provided through that same compromised browser but instead be provided through an independent channel, such as a phone.

The proliferation of mobile devices – where consumers expect to engage in secure commerce without carrying anything other than their device – has presented significant new challenges to the model of having two distinct authentication elements. This challenge has been exacerbated by an increasing array of successful attacks on "shared secrets" credentials (phishing, man-in-the-middle), including ones supporting independent, multiple factors – meaning that even if the practical challenges of requiring consumers to carry two separate elements could be overcome, the security risks would still be significant.

Fortunately for all parties considered, the state-of-the-art solution for online authentication is no longer dependent solely on the "shared secrets" model of passwords and one-time-passcodes. The state-of-the-art solution leverages architectures such as FIDO, where we use asymmetric cryptography for

authentication, and do so in a way that is designed to address both modern security and mobility challenges, as well as consumer expectations.

The FIDO architecture is widely used today, with more than 100 million FIDO Certified devices already in market, and several firms using these devices to protect financial transactions. This points to a deployment pattern that meets (a) increased demand from users for transaction convenience and (b) the original security purpose of this independence requirement, albeit in an innovative way that facilitates market acceptance and delivers even greater security than what was likely envisioned by the authors of this requirement at the time it was drafted.

In the FIDO architecture the "secret" is never shared, only a cryptographic proof-of-possession of the secret is shared. In addition, the FIDO architecture takes advantage of Channel ID / Token Binding capabilities to mediate the risk of man-in-the-middle attacks. Given the market's embrace advancement of a new, more secure authentication model, the original analysis of how to mediate attacks on payment services credentials, which drove the creation of this requirement, should be revisited..

We suggest the FIDO architecture (or other similar architectures) offers a truly "best of both worlds" solution to the problems that drove the creation of this requirement.

- With biometric solutions being used for "user verification" (a "what you are" authentication factor) we address increased market demand for greater user **convenience** than anything we have used for online payments before.
- With the FIDO **privacy** requirements, we ensure biometric data is never shared, addressing requirements by data protection authorities and consumer concerns about sharing biometric information online.
- With asymmetric cryptography at the heart of the security model, we address the **security** requirement designed to mitigate theft of payment service credentials by all known attacks that successfully harvest "shared secret" credentials, the same techniques that are behind 95% of all web app attacks that lead to data breach (per Verizon's 2015 Data Breach Investigations Report, http://www.verizonenterprise.com/DBIR/2015/).

The result of this combination is a single-gesture, multi-factor authentication event ("what you are" – the on-device biometric user verification step plus "what you have" – the cryptographic proof-of-possession of the private key) packaged for consumers in a very simple user experience they are already familiar with since they likely use this same user experience to unlock their device several times per day.

We assert this is a far better outcome for all parties involved than explicit channel separation of "shared secret" credentials, as the requirement seems to anticipate. That being said, FIDO Authenticators often offer additional independence of authentication elements above-and-beyond what has been described above. We detail these Factors of Independence in the appendix attached to our response.

Note that the EBA is not alone in considering whether "traditional" multi-factor authentication solutions require a physically distinct, rather than merely logically separate, token. The U.S. government went through a similar process this past year, when it considered how to enable its agencies to extend the trust model of its Personal Identity Verification (PIV) smart cards to mobile devices. First launched in 2004, the PIV was designed for an era dominated by desktops, where the notion of an employee having to bring a separate physical token to log in made sense. Desktops themselves had little built-in security; the PIV smart card enabled users to bring strong security with them. The White House issued two policy memoranda for Federal agencies (OMB memoranda M-06-16 and M-07-16) that called for two-factor authentication solutions where "one of the two factors to be provided by a device that is separate from the device accessing the remote resource."

However, with the move toward mobile devices – most of which were not practical to use with the ISO 7816 smart card form factor – the U.S. National Institute of Standards and Technology (NIST) issued new guidance in December, 2014 to agencies (Special Publication 800-157, "Guidelines for Derived Personal Identity Verification (PIV) Credentials" http://csrc.nist.gov/publications/nistbul/itlbul2014_12.pdf), to provide the technical details for a system by which mobile devices such as smartphones and tablets are provisioned with strong credentials, allowing these credentials to take the place of the smart card for remote authentication to federal systems. As part of this, NIST and the White House made clear that these two OMB memoranda would have to be written to remove the requirement that one factor be separate from the device accessing the resource, noting that "guidance will be updated by OMB to provide an alternative to current remote authentication policy." The evolution of mobile devices - in particular the increased use of hardware architectures that offer highly robust and isolated execution environments (such as TEE, SE and TPM) - which has allowed these devices to achieve PIV-grade security without the need for a physically distinct token – prompted the U.S. government to rethink its requirements in this area.

5. *Which challenges do you identify for fulfilling the objectives of strong customer authentication with respect to dynamic linking?*

One of the biggest challenges for Financial Institutions (FIs) who operate with a global footprint is interpreting and complying with the various mandated standards presented by the various governing bodies across multiple regions. Finding solutions to comply with these mandates can be a time consuming and costly effort for participating FIs to implement.

Several preeminent FIs are FIDO Alliance Board Members, and are providing proactive requirements to address concerns specific to the financial community. FIDO would help drive out a standard that could be easily adopted and implemented by the various FIs. By adopting FIDO within the EBA technical standards to define the model for authentication, FIs would be able to quickly react to changing regulations and reduce the costs associated with implementing those solutions. By leveraging FIDO Alliance specifications; the EBA could help establish a common pragmatic standard that all participating FIs could easily adopt.

With regards to "dynamic linking", the FIDO UAF specification provides a feature called transaction confirmation. The use case for this feature is as follows: imagine a situation in which an online service wants the user to confirm a transaction (e.g., such as a payment) so that any tampering of a transaction message during its route to the end device display and back can be detected. If a FIDO UAF Authenticator is equipped with a transaction confirmation display, the FIDO UAF architecture makes sure that the system supports What You See is What You Sign mode (WYSIWYS). More details can be found in the UAF specifications available for download at https://fidoalliance.org/specifications/download/. As long as a financial services provider can associate the authentication operation with an account holder, then dynamic linking may be enabled through transaction confirmation.

6. *In your view, which solutions for mobile devices fulfil both the objective of independence and dynamic linking already today?*

See response to item #5 where we discuss "dynamic linking" and the potential relationship to transaction confirmation available in FIDO UAF specifications.

See response to item #4 where we explain how FIDO-compliant implementations fulfill, and improve upon, the security requirements that drove the creation of the independence requirements.

Chapter 4.2: The exemptions to the application of strong customer authentication

7. *Do you consider the clarifications suggested regarding the potential exemptions to strong customer authentication, to be useful?*

8. *Are there any other factors the EBA should consider when deciding on the exemptions applicable to the forthcoming regulatory technical standards?*

9. *Are there any other criteria or circumstances which the EBA should consider with respect to transaction risks analysis as a complement or alternative to the criteria identified in paragraph 45?*

Note we respond to all three questions around exemptions here:

The FIDO Alliance does not have views on particular exemptions to requirements for strong authentication.

The FIDO Alliance has approached this issue from a different angle: it is our goal to make strong authentication cheaper, simpler and easier to use – not only when compared to other approaches to strong authentication, but also when compared to passwords alone – therefore reducing the market pressure for exemptions in a FIDO-enabled ecosystem. Usability was the guiding design principle of FIDO, with a focus on enabling very strong, asymmetric public key cryptography alongside a user experience that surpasses any other authentication approach. FIDO specifications provide an open standard way to vastly improve the security and usability of authentication. For example, the user need only touch something (fingerprint sensor or present a "security key" device), look at something (iris or facial recognition), or say something (voice authentication), which is a vast improvement over the usability of typing passwords or one-time-passcodes.

The practical impact of FIDO-enabled solutions in the marketplace is that all parties can benefit from strong authentication without costs or burdens – which should significantly reduce the demand for exemptions.

Chapter 4.3: The protection of the payment service users' personalized security credentials

10. *Do you consider the clarification suggested regarding the protection of users personalized security credentials to be useful?*

At a high level, the clarifications address important issues. We do note that the clarifications seem to focus on specific types of solutions; for those credential solutions that work differently, these clarifications may be less applicable.

From the FIDO Alliance's perspective, to protect the user's personalized security credentials four steps are necessary:

1. As a first step, the security goals and assumptions of the authentication protocol need to be documented to build the foundation for a solid design. For the FIDO U2F specification the documentation can be found at https://fidoalliance.org/specs/fido-u2f-v1.0-nfc-bt-amendment-20150514/fido-security-ref.html l and the respective text for FIDO UAF can be found at https://fidoalliance.org/specs/fido-uaf-v1.0-ps-20141208/fido-security-ref-v1.0-ps-20141208.htm.
2. Since the design of the authentication protocol impacts which parties have access to personalized security credentials the members of the FIDO Alliance have designed the FIDO authentication protocols in such a way that they use public key cryptography and separate user verification from the cryptographic authentication protocol itself. The use of public key cryptography allows sensitive cryptographic keys to only be stored at the user's device rather than on payment service providers or relying parties in general. Additionally, privacy has been taken into account from the beginning in the design and therefore ensures that users cannot be tracked across online services. For a more detailed discussion about the privacy properties please see https://fidoalliance.org/resources/FIDO__Privacy_White_Paper_Jan_2016.pdf. FIDO protocols rely on widely deployed Internet security protocols and cryptographic algorithms.
3. Third, implementations need to comply to the technical specifications. This compliance is accomplished in FIDO with the certification program described at https://fidoalliance.org/certification/.
4. As a last step, products may voluntarily choose to go through a third-party security certification. The development of such a program is currently ongoing in the FIDO Alliance and is expected to be launched in 2016.

11. *What other risks with regard to the protection of users' personalized security credentials do you identify?*

As the use of multi-factor authentication has spread, so have attacks on some of the most popular methods. Some types of one-time password technologies, for example, have been shown to be vulnerable to malware, phishing attacks and man-in-the-middle attacks.

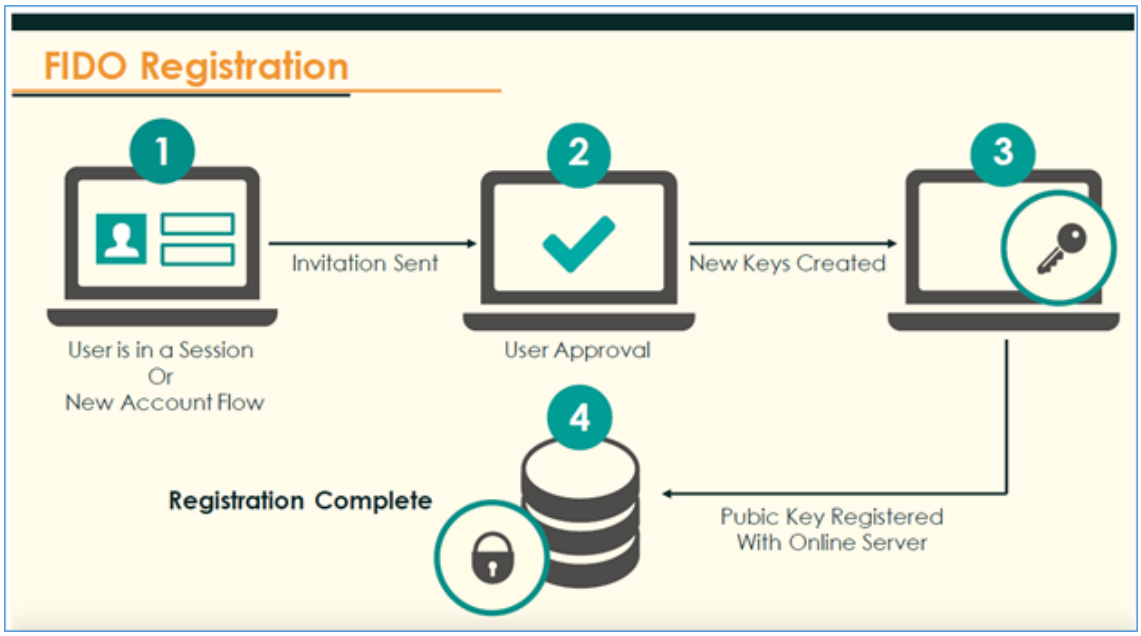
Google (a FIDO Alliance member) discussed the extent of the problem last summer, noting that these days, a "phisher can pretty successfully phish for an OTP just about as easily as they can a password" (see https://www.youtube.com/watch?v=UBjEfpfZ8w0) and noted their shift to FIDO hardware-based solutions as the way to stop these targeted phishing attacks.[3]

Phishing is rendered moot by FIDO's use of long-proven asymmetric public key cryptography, where the private key is the only "secret," and it is stored on the user's Authenticator device. Only the public key is ever shared with the online service, resulting in no credential secrets ever being shared with servers, which renders the threat of credential theft from a data breach at the website or even phishing attack moot. The only way to attack a FIDO credential/private key is to attack the user's personal device and particularly the Authenticator.

[3] 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.

12. *Have you identified innovative solutions for the enrolment process that the EBA should consider which guarantee the confidentiality, integrity and secure transmission (e.g. physical or electronic delivery) of the users' personalized security credentials?*

"Enrollment" in the FIDO sense involves the process by which a security credential is first created on a device. We refer to this as the "registration" process. Here, FIDO Authenticators generate a public-private key pair directly on the device. One benefit of this approach is that it reduces the attack surface of the authentication solution; there is no need to generate a credential remotely, and thus, no issues associated with secure transmission or delivery of the credential.



Note that one FIDO Authenticator can generate multiple key pairs; FIDO specifications call for the Authenticator to create a new key pair specifically for each online application that invites the user to register FIDO credentials. This ensures that there is no information provided by the FIDO Authenticator or the FIDO protocols that could be used by different service providers to track the use of an authenticator across applications, websites, etc.

Note, however, that FIDO specifications do not describe or mandate what other application-specific data needs to be provided by the user during the initial registration phase since this varies heavily from use case to use case. We discuss one option for this in more detail in our response to question 19, exploring the way that identity proofing processes associated with eID cards might be leveraged for this purpose.

13. *Can you identify alternatives to certification or evaluation by third parties of technical components or devices hosting payment solutions, to ensure that communication channels and technical components hosting, providing access to or transmitting the personalized security credential are sufficiently resistant to tampering and unauthorized access?*

The FIDO Alliance believes that certification is vital, yet optional to the interoperability, security and privacy of solutions using the FIDO protocols. We have established an initial certification program that is entirely voluntary and has been utilized by more than 100 products from over 50 companies in just the first 9 months of operation; details are at https://fidoalliance.org/certification/

Our current certification program is focused on ensuring compliance with the technical specifications with the help of self-operated conformance test tools and proctored interoperability testing. To address third-party security certification, the FIDO Alliance is currently in the process of developing a new security certification program.

The only alternative we have seen proposed in the marketplace to certification is self-assessment, which we have observed leads to some level of abuse in some cases, either intentionally or unintentionally, by vendors advertising FIDO implementations that turn out to be non-compliant upon inspection.

14. *Can you indicate the segment of the payment chain in which risks to the confidentiality, integrity of users' personalized security credentials are most likely to occur at present and in the foreseeable future?*

While other authentication solutions might offer a potential attack at various segments of the payment chain, FIDO specifically designed our specifications so that the only potential attack vector in the user-credential-authentication step is to steal the user's device and then attempt to break the second factor. No credential secrets are ever shared with servers, which renders the threat of credential theft from a data breach moot. Thus, the only segment of the chain that offers an attack vector is the segment where use of a strong credential is first initiated. That said, FIDO specifications do not apply to other steps in the chain after authentication of the user's credentials to the appropriate account with the payment service provider.

Chapter 4.4: Considerations prior to developing the requirements on common and secure open standards of communication

15. *For each of the topics identified under paragraph 63 above (a to f), do you consider the clarifications provided to be comprehensive and suitable? If not, why not?*

The FIDO technical specifications are created based on building blocks developed primarily by other recognized standards developing organizations, such as the Internet Engineering Task Force (IETF) and the World Wide Web Consortium (W3C). The standardization process in the FIDO Alliance, as well as the process in the IETF and the W3C, follow the principles of open standards development.

The standards process is open to all interested and informed parties who choose to join the FIDO Alliance, participate through our Liaison Program, attend FIDO Alliance public events and webinars, participate in our free open developer forum, or provide written comment on our published specifications through our public website. Finalized specifications are published on the FIDO Alliance website at https://fidoalliance.org/specifications/download/ and these documents are available for download at no cost. Furthermore, membership at the FIDO Alliance is not a prerequisite for deployment of FIDO implementations. Some of the FIDO Alliance members have also published their FIDO protocol implementations as open source and we expect more open source projects around FIDO specifications in the future.

We cannot provide feedback on the term 'common' since it is less well defined.

16. *For each agreed clarification suggested above on which you agree, what should they contain in your view in order to achieve an appropriate balance between harmonization, innovation while preventing too divergent practical implementations by ASPSPs of the future requirements?*

The FIDO Alliance does not have any comment here.

17. *In your opinion, is there any standards (existing or in development) outlining aspects that could be common and open, which would be especially suitable for the purpose of ensuring secure communications as well as for the appropriate identification of PSPs taking into consideration the privacy dimension?*

The FIDO Alliance does not have any comment here.

18. *How would these requirement for common and open standards need to be designed and maintained to ensure that these are able to securely integrate other innovative business models than the one explicitly mentioned under article 66 and 67 (e.g. issuing of own credentials by the AIS/PIS)?*

The FIDO Alliance does not have any comment here.

Chapter 4.5: Possible synergies with the regulation on electronic identification and trust services for electronic transactions in the internal market (e-IDAS)

19. *Do you agree that the e-IDAS regulation could be considered as a possible solution for facilitating the strong customer authentication, protecting the confidentiality and the integrity of the payment service users' personalized security credentials as well as for common and secure open standards of communication for the purpose of identification, authentication, notification, and information? If yes, please explain how. If no, please explain why.*

The FIDO Alliance is familiar with the e-IDAS initiative; the government of both Germany and the United Kingdom are members of FIDO Alliance, and many of our members are involved in supplying key components of national eID programs in countries across Europe.

Accordingly, we recognize that e-IDAS may play a role in supporting strong authentication requirement for PSD2. The ability for European consumers to choose to leverage a strong credential they already have makes inherent sense.

"Choice" is, in our view, the essential issue here. While some consumers may wish to use a national ID solution for payments authentication, others may find that solution burdensome or simply prefer to use a different credential or credential service. Given that market acceptance of strong authentication is directly tied to reducing the burden placed on consumers to use the technology, letting them choose from a variety of different types of strong authentication solutions that meet EBA requirements offers the most logical path forward. Open standards and specifications maximize the opportunity for user choice in any market.

As governments consider ways to extend the functionality and trust model of traditional national ID cards, FIDO specifications offer a logical path to expand the e-IDAS ecosystem – particularly for entities interested in using a country's eID to "derive" a trusted public-private key pair from a national eID, using that eID as a root of trust.

One challenge that eIDAS may have, in common with many public sector schemes, is gaining the level of visibility and "brand recognition" across the EU. It has taken many decades for currently recognised commercial brands to be accepted as effective "trust marks" in transactions and eIDAS will face similar challenges. One advantage of the FIDO ecosystem is that it leverages the existing trust relationships between the highly recognized brands that are implementing FIDO solutions, thus accelerating market acceptance of these new capabilities without any prerequisite branding campaign.

Cooperation between e-IDAS and FIDO Alliance would be mutually beneficial in advancing the goals of both initiatives.

20. *Do you think in particular that the use of "qualified trust services" under e-IDAS regulation could address the risks related to the confidentiality, integrity and availability of PSCs between AIS, PIS providers and ASPSPs? If yes, please identify which services and explain how. If no, please explain why.*

Please see our response to question 19.

APPENDIX: ABOUT THE FIDO ALLIANCE AND FIDO SPECIFICATIONS

Introduction to the FIDO Alliance

The FIDO Alliance's mission is to change the nature of online strong authentication by:

- Developing technical specifications defining open, scalable, interoperable mechanisms that supplant reliance on passwords to securely authenticate users of online services.
- Operating industry programs to help ensure successful worldwide adoption of the specifications.
- Submitting mature technical specifications to recognized standards development organization(s) for formal standardization.

The FIDO Alliance was launched in 2013 to improve online authentication by developing open, interoperable industry specifications that leverage proven public key cryptography for stronger security and device-based user verification for better usability. FIDO Alliance was created to specifically solve the authentication problem in the larger context of identity and access management, without duplicating effort or reinventing the wheel. FIDO specifications are therefore complementary to other industry efforts in this area.

The core ideas driving the FIDO Alliance's efforts are ease of use, privacy and security, and interoperability. The primary objective is to enable online services and websites, whether on the open Internet or within enterprises, to leverage native security features of end-user computing devices for strong user authentication, and to reduce the problems associated with creating and remembering passwords.

FIDO was founded on a simple premise: to address the common but flawed assumption that easy-to-use authentication must be weak, and strong authentication must be difficult to use. For years, the uptake of strong authentication solutions has been inhibited by this assumption (as noted in Figure 1, with solutions in the marketplace falling on one end of the curve or the other).

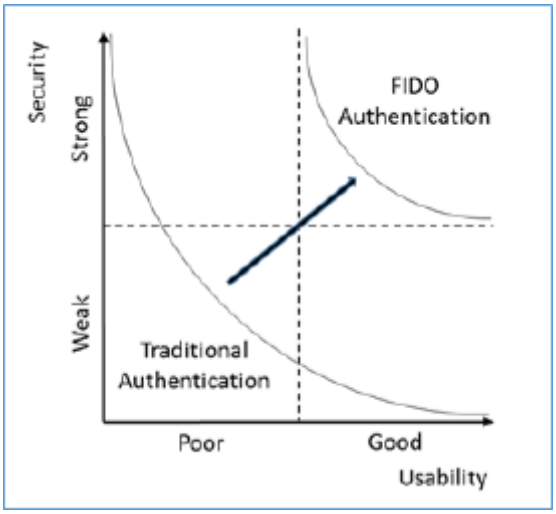


Figure 1: FIDO Authentication changes the paradigm – enabling excellent security and usability

Too many times, products have been engineered to prioritize security over usability, with the assumption that individuals would use the solution; the reality, however, has been that consumers have rejected using solutions that are hard to use – leading to a growing number of data breaches and other security exploits. In order for authentication to be broadly accepted by both online service providers and their users, it must be affordable to deploy and easy to use while providing improved security.

FIDO has gained rapid support from an array of major stakeholders across the globe

Since its launch in 2013, the FIDO Alliance has attracted strong support from Europe and around the world. European government entities including the UK Cabinet Office and the Bundesamt fuer Sicherheit in der

Informationstechnik (BSI) in Germany have joined the FIDO Alliance, as have more than 250 corporate members.

Bundesamt für Sicherheit in der Informationstechnik

Cabinet Office

Our board members, listed below, comprise key players across services, apps, devices, platforms, and vendors from across the globe.

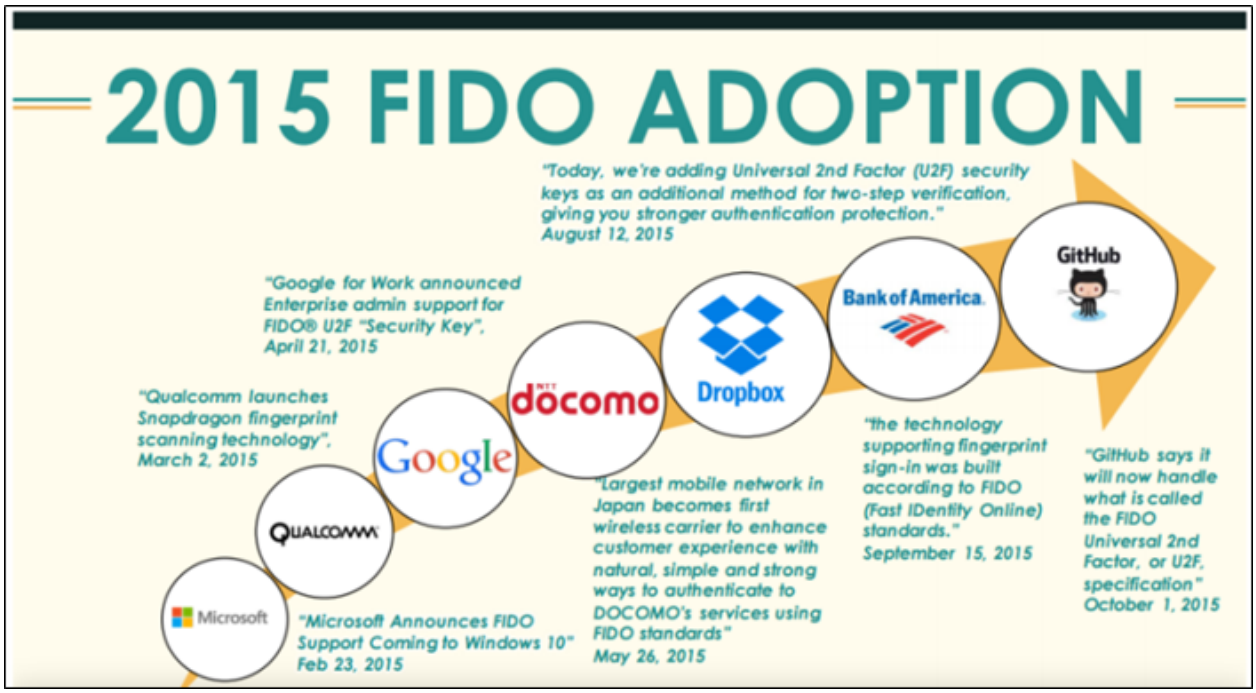
Alibaba Group, American Express, Bank of America, BCcard, ING, MasterCard, PayPal, USAA, VISA, Google, Microsoft, NTT docomo, Lenovo, Samsung, CrucialTec, Daon, egis Technology, Infineon, intel, ARM, Nok Nok Labs, NXP, oberthur Technologies, Qualcomm, RSA, Synaptics, VASCO, yubico, aetna

Note that this list of companies are not just members; many are leading the development of the FIDO ecosystem by being early adopters of the technology and deploying FIDO solutions to their customers at scale. For example:

- Google launched support for FIDO 2-factor authentication in 2014 and extended this to its Google for Work customers in 2015
- Microsoft has pledged to build support for FIDO into Windows 10
- PayPal in 2014 launched a partnership with Samsung allowing PayPal customers to use FIDO specifications to securely and easily authenticate for payments with the swipe of a finger wherever PayPal is accepted
- Bank of America deployed FIDO-enabled fingerprint authentication for its mobile banking app across both iOS and Android, enabling millions of customers to add a very secure, easy-to-use authentication capability to improve the security of payments and mobile banking transactions

- In Japan, NTT DOCOMO – Japan's largest Mobile Network Operator (MNO) – deployed FIDO-enabled strong authentication across its network by introducing 10 FIDO(R) Certified mobile phones, enabling millions of customer to have a streamlined, secure log-in solution for a variety of NTT DOCOMO applications, including banking and payment applications. A video demonstrating the user experience is at https://vimeo.com/130950213

Additional implementations and deployments of FIDO specifications were launched in 2015 by firms such as Qualcomm, Dropbox and Github; 2016 should produce an even wider array of deployments.



The superior security, usability and privacy offered by FIDO specifications represents a fundamental paradigm shift in the world's approach to strong authentication; the rapid embrace of FIDO by so many of the world's leading firms and governments reinforces the credibility of the security behind the FIDO specifications and the compelling value FIDO-compliant solutions offer when compared to alternative authentication approaches.

The FIDO Alliance is an industry consortium with a membership policy open to companies, governments, academics, and not-for-profit organizations who are interested in cooperating to develop technical specifications and industry best practices for simpler, stronger authentication technology. The specifications describe how a user may be authenticated when accessing an online service.

The FIDO Alliance itself does not develop any devices, software, or services. This task is left to the implementers of FIDO specifications, such as software and hardware vendors, device manufacturers, platform providers, and online service providers.

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 ever 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.

A user wishing to access an online service goes through three steps. In this example, 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 to approve a payments transaction.
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.
3. 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.
4. 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 authorization of the payment transaction. Biometric information never leaves the user's device, i.e. the biometric information is never shared with the online service provider and never stored on a server.

Note that version 1.0 of FIDO specifications includes two types of protocols: the Universal 2nd Factor (U2F) and Universal Authentication Framework (UAF); these protocols support two different use cases that will both be supported in the new FIDO 2.0 specifications, whose web browser and web server components have been submitted for formal standardization to the W3C. The illustration above depicts FIDO UAF.

FIDO U2F differs from FIDO UAF in that it uses a FIDO Authenticator as a second factor of authentication, only invoked after a password or other method is first presented. FIDO UAF, in contrast, offers a way to replace passwords entirely with a two-factor authentication solution. While the user experience differs between the two, the fundamental concept is the same: both solutions are rooted in public key cryptography, as noted in Figure 3. The fact that FIDO U2F and FIDO UAF are closely aligned allows both user experiences to be supported in the new FIDO 2.0 specifications.

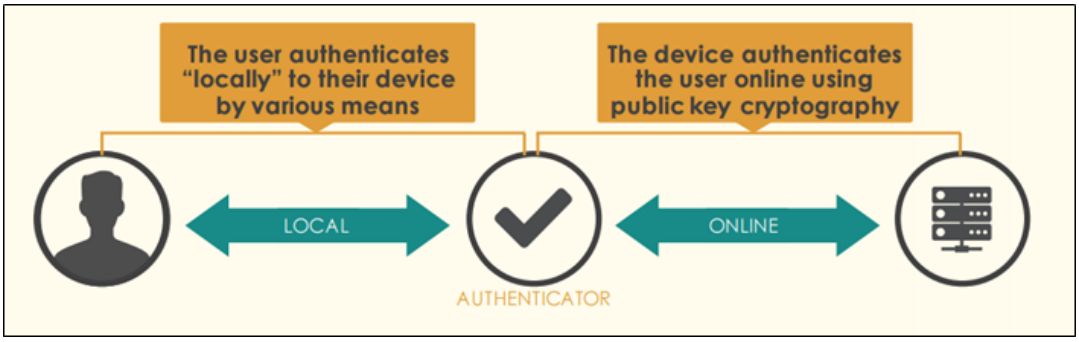


Figure 3: Both FIDO UAF and FIDO U2F specifications support authentication through the same core approach

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 smart phone 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. As noted earlier, this is not an attack model that is easy to execute, nor is it scalable to a large number of devices. It is also worth noting that this is a far more secure system than one that relied upon share secret credentials, even when full channel separation was adhered to because the second factor would still be vulnerable to a scalable attack whereas a well-implemented FIDO Authenticator is not.

Specifications backed by certification

In support of building confidence in the FIDO ecosytem, 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 are a prerequisite for obtaining rights to use a FIDO Certified™ logo. Future extensions of the certification program will also include third party security lab certification and security assurance verification, in addition to this "function testing" currently offered by the FIDO Alliance directly.

There have been over 100 products tested and certified under this program since it was launched in May of 2015. Over 50 different companies have certified their FIDO implementations through this program, including leading OEMs such as Samsung, Huawei, Lenovo, Sony and LG. A detailed list of these products can be found at https://fidoalliance.org/certification/fido-certified/.

FIDO is specifically designed to support EU Privacy requirements

The FIDO architecture defines several techniques to help ensure the security of the authentication process and, in turn, support user privacy.

- User verification is performed locally by the user's personal device. Any Personal Data that could identify a user, such as a fingerprint pattern, is not shared with the online service provider ("Relying Party").
- When a user registers a FIDO Authenticator for use with a Relying Party, a unique pair of cryptographic keys is produced by the FIDO Authenticator for use solely with that Relying Party. As a result a User has a different credential for each Relying Party. This means that Relying Parties cannot use any information provided by the FIDO protocols to collude to track a user's activity online.

- The private data for FIDO — biometrics and private cryptographic keys — are stored on the user's local devices and are not accessible to the Relying Party. Hence, a data breach at a Relying Party cannot leak cryptographic keys nor biometric information.
- Vendors developing FIDO Authenticators are subject to voluntary certification. A record of its features protected by a digital signature, i.e. the Attestation Key, is stored on the FIDO Authenticator itself. Metadata related to it may be submitted to the FIDO Alliance for inclusion in a public utility metadata service that is operated by the FIDO Alliance as a service to the community. A Relying Party can use the metadata about FIDO Authenticators and their characteristics to make policy decisions about which of those are suitable for a given deployment or use case. Revocation of a compromised FIDO Authenticator can also be accomplished using the same mechanism.

In summary, User privacy is protected by having designed the FIDO technical requirements in such a way that they offer the following properties:

- The FIDO authentication operation happens between the Relying Party and the FIDO Authenticator. There is no reliance on a separate, or third party, system to authenticate the User.
- No User identifiable information is stored by the Relying Party as part of the FIDO operation.
- Private keys are generated by the Authenticator and never leave the Authenticator.
- Biometric data used for User Verification never leaves the user's device as part of the FIDO operations.
- Transactions of a user are not linkable between Relying Parties.

The following table shows how FIDO v1.0 conforms to the privacy principles outlined in the European Directive 95/46/EC.

Table 1 - FIDO Implementation of EU Privacy Principles.

EU Privacy Principle	FIDO Implementation of EU Privacy Principle
Personal data must be processed fairly and lawfully	For a User to access a Relying Party's services through FIDO Authentication, the User must first agree to register with that Relying Party. When the User wishes to access the online service, they must execute the User Verification step, e.g. touching a sensor, entering a passcode, or providing their fingerprint, in order to execute the cryptographic computation.. This ensures that malware installed on the User's device is unable to autonomously perform FIDO operations.
Personal data can only be processed for one or more specified lawful purpose(s)	The Personal Data required to access an online service, such as a biometric, can only be accessed by the FIDO Authenticator which is part of the User's device. The FIDO Authenticator can only access such data when it is required to perform an Authentication. The FIDO protocol requires a minimum amount of data stored by the Relying Party, for which the user is required to provide consent.
Personal data must be adequate, relevant, and not excessive in relation to the purposes for which it is being used	The data needed to perform an Authentication is collected by the Relying Party when the User registers with it. This data is: • A public key: This allows the Relying Party to verify that the FIDO Authenticator being used is the one previously registered by the User. • Authenticator Attestation ID (AAID): This is a reference that allows the Relying Party to look-up the characteristics of the used FIDO Authenticator. • Key Handle: An identifier created by a FIDO Authenticator, potentially containing an encrypted private key, to refer to a specific key maintained the FIDO Authenticator.

EU Privacy Principle	FIDO Implementation of EU Privacy Principle
Personal data must be accurate and up to date	The data used for FIDO Authentication, such as the registered public key, must be accurate since cryptographic verification fails otherwise. If the data becomes corrupted for any reason, the User needs to re-register with the Relying Party. Re-registration changes the registered public key.
Personal data must not be kept for longer than necessary to fulfil the purposes for which it was collected	The User may de-register from a Relying Party at any time. Once de-registration has taken place, the private key is removed from the user device and the Public key held by the Relying Party is of no further use.
Personal data must be kept secure	Allowing users to authenticate using FIDO Authentication provides a greater level of security around accessing personal data than passwords alone. Data required for local User Verification is stored locally on the FIDO Authenticator. FIDO-related data stored at the Relying Party is not confidential by itself. The FIDO Authenticator is required to protect data required for User Verification and FIDO-related data, such as cryptographic keys, against unauthorized access by third parties.
Personal data must be processed in accordance with rights of data subjects	Personal data used to authenticate a User can only be accessed by that User when the User wishes to be authenticated.
Personal data cannot be transferred outside a given geographical area, such as the EEA, without specific circumstances being in place.	Personal data held in a FIDO Authenticator will be protected by the same mechanisms irrespective of the device's location and the device can only leave the EEA if the owner wishes it to do so. The FIDO Server used by the Relying Party does not contain personal data.