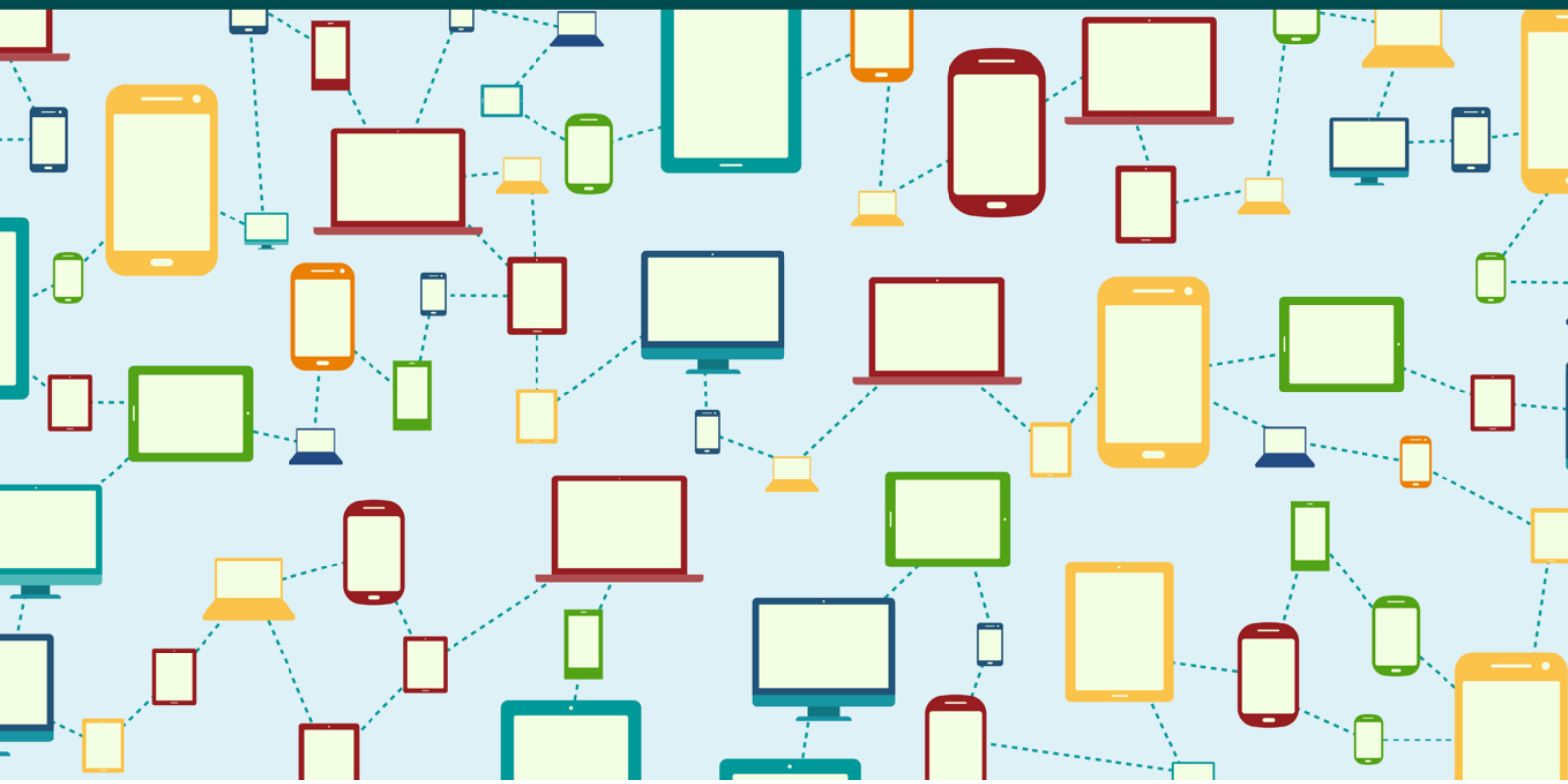
fido alliance | simpler stronger authentication



FIDO Privacy
FIDO Alliance White Paper

19 January 2016

Abstract

This document is a brief explanation of how Authentication using FIDO v1.0 protects Users' privacy.

Introduction

The FIDO Alliance 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 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. This document is not a technical explanation of how FIDO Authentication operates.

An introduction to how FIDO Authentication operates and the FIDO Privacy Principles can be found on the FIDO Alliance website[1]. A glossary of FIDO privacy-related terms can be found in this document's appendix.

What is the FIDO Alliance?

The FIDO Alliance is an industry body open to companies, governments, as well as individual experts who are interested in co-operating to develop technical specifications. 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[2]. This task is left to the members of the FIDO Alliance, such as software and hardware vendors, or non-members. The ability to produce FIDO products, such as FIDO Authenticators, does not depend on being a member of the FIDO Alliance. Hence, standards specifications are made accessible to all for implementation and deployment.

User Privacy

Accessing online services often requires Users to authenticate themselves to the Relying Party in order to offer services tailored to a specific User. Use of the service by the User may mean sharing personal information: banking details, health records or other information which the User would expect to be kept secure and not be open for view and use by others. At the moment most Relying Parties use a combination of username and password to prevent unauthorized access. However, this form of authentication is vulnerable to attacks and places User privacy at risk.

How FIDO Authentication Protects Users

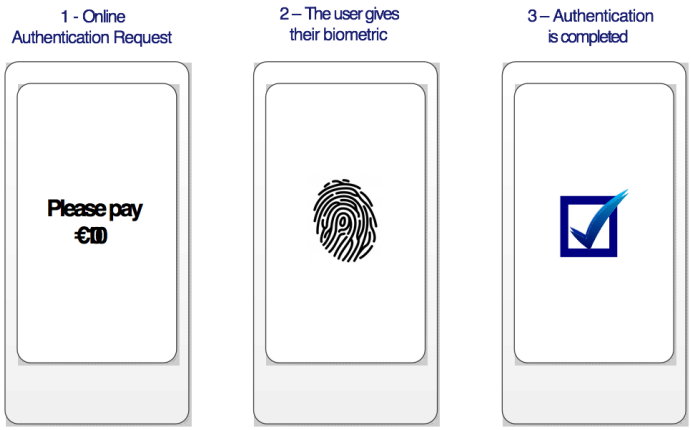
How FIDO Authentication is used

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 fingerprint sensor.

[1] http://fidoalliance.org/wp-content/uploads/2014/12/FIDO_Alliance_Whitepaper_Privacy_Principles.pdf

[2] The FIDO Alliance offers software for the purpose of interoperability testing used as part of the certification program, see https://fidoalliance.org/certification/

Figure 1 - User Authentication.



1. The Relying Party asks the User to authenticate themselves.
2. The User unlocks cryptographic credentials stored on that phone using their fingerprint.
3. The mobile phone verifies the user's fingerprint and executes the FIDO authentication protocol to authenticate the user to the Relying Party.
4. The Relying Party verifies the authentication result and authorizes the payment transaction. Biometric information never leaves the User's device and the user is authenticated based on the strong FIDO authentication protocol.

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

- User verification is performed locally by the User's device. Any Personal Data that could identify a User, such as a fingerprint pattern, is not shared with the 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 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.
- FIDO Authenticators are subject to voluntary certification. A record of its features protected by a cryptographic mechanism is stored on the FIDO Authenticator itself. Meta-data related to it is submitted to the FIDO Alliance. A Relying Party can use the meta-data 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 in the clear3.

[3] The FIDO U2F specification allows an Authenticator to store the private key at the Relying Party but requires the key to be encrypted with a key known only to 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 FIDO Alliance developed a certification program; details can be found at https://fidoalliance.org/certification/. This program ensures that different FIDO components interoperate with other vendors' on a technical level and that the technical specifications are followed. Participation in these certification programs is voluntary but a pre-requisite for obtaining a FIDO Certified™ logo. Future extensions of the certification program will also include third party certification.

FIDO and its Application to Privacy

FIDO Authentication is a means of supporting authentication online. However, it is useful to be able to show what the FIDO specification covers. The analysis shows how the use of FIDO Authentication supports some privacy principles by offering better security than a username and password.

This analysis is solely for the FIDO v1.0 specifications themselves. It is up to the implementers of the overall authentication system, and specifically of the FIDO components therein, to meet the specifications and satisfy the FIDO Privacy Principles.

Privacy in the European Economic Area

The following table shows how FIDO v1.0 conforms to the privacy principles outlined in the European Directive 95/46/EC[4].

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 computation5. 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 fingerprint, 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.

[4] The European Data Protection Directive can be found at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

[5] The FIDO UAF specification also allows vendors to build a "Silent Authenticators", which do not perform user verification. The 'Security and Privacy Guidelines' section of the FIDO UAF Authenticator-Specific Module API specification, see https://fidoalliance.org/specs/fido-uaf-v1.0-ps-20141208/fido-uaf-asm-api-v1.0-ps-20141208.html, places requirements on vendors implementing silent authenticators to prevent tracking, and to get the users consent during registration.

EU Privacy Principle	FIDO Implementation of EU Privacy Principle
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.
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 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.

EU Privacy Principle	FIDO Implementation of EU Privacy Principle
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.

Privacy in the US: Mapping FIDO and IDESG Privacy Requirements[6]

The Identity Ecosystem Steering Group (IDESG) is a public-private partnership lead by the National Institute of Science and Technology (NIST). NSTIC aims to help individuals and organizations utilize secure, efficient, easy-to-use and interoperable identity credentials to access online services in a manner that promotes confidence, privacy, choice and innovation.

Table 2 shows how FIDO privacy principles are related to the IDESG privacy requirements[7]. The principles listed in Table 2 are described in Table 3.

Table 2 - FIDO Privacy Principles mapped to IDESG Requirements.

FIDO Privacy Principle	IDESG Privacy requirements
Require explicit, Informed consent for any operation using personal data	PRIVACY-6. USAGE NOTICE PRIVACY-8. THIRD PARTY LIMITATIONS PRIVACY-9. USER NOTICE OF CHANGES PRIVACY-10. USER OPTION TO DECLINE PRIVACY-11. OPTIONAL INFORMATION
Provide clear context to the user for any FIDO operations	PRIVACY-6. USAGE NOTICE PRIVACY-8. THIRD PARTY LIMITATIONS PRIVACY-9. USER NOTICE OF CHANGES PRIVACY-10. USER OPTION TO DECLINE PRIVACY-11. OPTIONAL INFORMATION

[6] Full current version of the Identity Ecosystem Framework, its requirements, and supplemental guidance, can be found at https://www.idesg.org/The-ID-Ecosystem/Identity-Ecosystem-Framework/IDEF-Core-Documents

[7] Note that Table 1 and Table 2 use a different format for comparison. While Table 1 interprets the EU privacy principles with respect to the FIDO specification Table 2 matches the FIDO privacy principles against the IESG privacy requirements.

FIDO Privacy Principle	IDESG Privacy requirements
Limit collection of personal data to FIDO-related purposes	PRIVACY-1. DATA MINIMIZATION PRIVACY-2. PURPOSE LIMITATION PRIVACY-3. ATTRIBUTE MINIMIZATION PRIVACY-5. DATA AGGREGATION RISK PRIVACY-8. THIRD PARTY LIMITATIONS PRIVACY-12. ANONYMITY PRIVACY-13. CONTROLS PROPORTIONATE TO RISK
Use personal data only for FIDO operations	PRIVACY-1. DATA MINIMIZATION PRIVACY-2. PURPOSE LIMITATION PRIVACY-5. DATA AGGREGATION RISK PRIVACY-8. THIRD PARTY LIMITATIONS
Prevent identification of a user outside of FIDO operations	PRIVACY-1. DATA MINIMIZATION PRIVACY-2. PURPOSE LIMITATION PRIVACY-3. ATTRIBUTE MINIMIZATION PRIVACY-5. DATA AGGREGATION RISK PRIVACY-8. THIRD PARTY LIMITATIONS PRIVACY-12. ANONYMITY
Biometric data must never leave the user's personal computing environment	PRIVACY-1. DATA MINIMIZATION PRIVACY-2. PURPOSE LIMITATION PRIVACY-3. ATTRIBUTE MINIMIZATION PRIVACY-4. CREDENTIAL LIMITATION PRIVACY-8. THIRD PARTY LIMITATIONS PRIVACY-15 ATTRIBUTE SEGREGATION
Protect FIDO-related data from unauthorized access or disclosure	Covered by IDESG Security Requirements PRIVACY-14. DATA RETENTION
Allow users to easily view and manage their FIDO Authenticators	PRIVACY-7. USER DATA CONTROL PRIVACY-8. THIRD PARTY LIMITATIONS PRIVACY-14. DATA RETENTION

Table 3 - IDESG Privacy Requirements.

IDESG Privacy requirement	Description
PRIVACY-1. DATA MINIMIZATION	Entities MUST limit the collection, use, transmission and storage of personal information to the minimum necessary to fulfill that transaction's purpose and related legal requirements. Entities providing claims or attributes MUST NOT provide any more personal information than what is requested. Where feasible, IDENTITY-PROVIDERS MUST provide technical mechanisms to accommodate information requests of variable granularity, to support data minimization.
PRIVACY-2. PURPOSE LIMITATION	Entities MUST limit the use of personal information that is collected, used, transmitted, or stored to the specified purposes of that transaction. Persistent records of contracts, assurances, consent, or legal authority MUST be established by entities collecting, generating, using, transmitting, or storing personal information, so that the information, consistently is used in the same manner originally specified and permitted.
PRIVACY-3. ATTRIBUTE MINIMIZATION	Entities requesting attributes MUST evaluate the need to collect specific attributes in a transaction, as opposed to claims regarding those attributes. Wherever feasible, entities MUST collect, generate, use, transmit, and store claims about USERS rather than attributes. Wherever feasible, attributes MUST be transmitted as claims, and transmitted credentials and identities MUST be bound to claims instead of actual attribute values.
PRIVACY-4. CREDENTIAL LIMITATION	Entities MUST NOT request USERS' credentials unless necessary for the transaction and then only as appropriate to the risk associated with the transaction or to the risks to the parties associated with the transaction.
PRIVACY-5. DATA AGGREGATION RISK	Entities MUST assess the privacy risk of aggregating personal information, in systems and processes where it is collected, generated, used, transmitted, or stored, and wherever feasible, MUST design and operate their systems and processes to minimize that risk. Entities MUST assess and limit linkages of personal information across multiple transactions without the USER's explicit consent.
PRIVACY-6. USAGE NOTICE	Entities MUST provide concise, meaningful, and timely communication to USERS describing how they collect, generate, use, transmit, and store personal information.

IDESG Privacy requirement	Description
PRIVACY-7. USER DATA CONTROL	Entities MUST provide appropriate mechanisms to enable USERS to access, correct, and delete personal information.
PRIVACY-8. THIRD-PARTY LIMITATIONS	Wherever USERS make choices regarding the treatment of their personal information, those choices MUST be communicated effectively by that entity to any THIRD-PARTIES to which it transmits the personal information.
PRIVACY-9. USER NOTICE OF CHANGES	Entities MUST, upon any material changes to a service or process that affects the prior or ongoing collection, generation, use, transmission, or storage of USERS' personal information, notify those USERS, and provide them with compensating controls designed to mitigate privacy risks that may arise from those changes, which may include seeking express affirmative consent of USERS in accordance with relevant law or regulation.
PRIVACY-10. USER OPTION TO DECLINE	USERS MUST have the opportunity to decline registration; decline credential provisioning; decline the presentation of their credentials; and decline release of their attributes or claims.
PRIVACY-11. OPTIONAL INFORMATION	Entities MUST clearly indicate to USERS what personal information is mandatory and what information is optional prior to the transaction.
PRIVACY-12. ANONYMITY	Wherever feasible, entities MUST utilize identity systems and processes that enable transactions that are anonymous, anonymous with validated attributes, pseudonymous, or where appropriate, uniquely identified. Where applicable to such transactions, entities employing service providers or intermediaries MUST mitigate the risk of those THIRD-PARTIES collecting USER personal information.
PRIVACY-13. CONTROLS PROPORTIONATE TO RISK	Controls on the processing or use of USERS' personal information MUST be commensurate with the degree of risk of that processing or use. A privacy risk analysis MUST be conducted by entities who conduct digital identity management functions, to establish what risks those functions pose to USERS' privacy.

IDESG Privacy requirement	Description
PRIVACY-14. DATA RETENTION	Entities MUST limit the retention of personal information to the time necessary for providing and administering the functions and services to USERS for which the information was collected, except as otherwise required by law or regulation.
PRIVACY-15. ATTRIBUTE SEGREGATION	Wherever feasible, identifier data MUST be segregated from attribute data.

Conclusion

A core FIDO tenet is to reduce reliance on passwords on the Internet. To accomplish this goal a new cryptographic mechanism was developed. This new technique, described in the FIDO technical specifications and referred in this document as FIDO Authentication, does not require Personal Data to be shared with the Relying Party. The result is an increase in privacy protection and reduced risks for Relying Parties in case of a data breach since no confidential information is stored by Relying Parties.

Commonly Used Terms

There are some commonly used terms in FIDO documents:

Authentication – The process where the Relying Party and User Device interact to allow the Relying Party to verify that the User being verified is the same as the User who registered the Authenticator. In FIDO, the Relying Party does this by verifying that the authenticator on the consumer device is in possession of a cryptographic key registered to that Relying Party.

FIDO Authenticator – This is the device that is used by the User to authenticate themselves to the Relying Party. A FIDO Authenticator implements the FIDO Authentication mechanism, which utilizes public key cryptography. Some FIDO Authenticators also include the ability to perform User Verification while others may only check for user presence, for example using a push of a button.

Relying Party – A relying party is an entity, often an online service provider, that wishes to authenticate a User before providing access to their services. This term comes from the fact that the entity relies on the outcome of the authentication transaction. For example, a relying party might be a bank offering online banking services to a customer, a shopping website, a service that holds medical records, or an online identity service. In each case, the Relying Party always makes the final decision whether or not to provide access to the User to their services.

Online Service – The technical systems operated by a Relying Party that perform authentication. This may include a FIDO Server, risk-management services, and user account management.

Personal Data – Any information relating to a User who can be identified, directly or indirectly. Examples include username, address or a fingerprint pattern.

User – The individual that wishes to access and use an online service.

User Device – This the mobile phone, desktop PC, laptop, tablet computer or other device the User is using.

Registration – This is the step where the User registers a cryptographic key generated by the Authenticator with a Relying Party. This key is the public key of public key crypto system. The corresponding private key also generated by the FDIO Authenticator remains on the FIDO Authenticator. Once registered, the User may subsequently authenticate themselves to the Relying Party using the Authenticator.

User Verification – User Verification is always local to a User's device. User Verification may simply be to show a User is present via the push of a button, or it may capture a pattern, such as a fingerprint or passcode and compare it with a registered pattern held on the User's device. As well as capturing the pattern with a sensor, the User Device will also perform further processing to perform the match.

User Authentication – This is performed by the Relying Party. User Authentication takes the result of the User Verification and uses the FIDO Authentication to decide whether or not the User is granted access to the online service.