FIDO: Fast Identity Online Alliance Privacy Principles Policy

FIDO Privacy Principles

Introduction

The FIDO Alliance is a non-profit 501(c)6 organization founded to address both the lack of interoperability among strong authentication devices, as well as the problems users face with creating and remembering multiple usernames and passwords.

The success of the FIDO Alliance ecosystem is predicated upon user trust, with the goal of preserving users' privacy while providing strong authentication to online services.

This paper describes the privacy-preserving principles that are a core part of the FIDO Alliance's technologies, and explains how they reinforce the FIDO Alliance's approach to strong authentication.

Privacy

Privacy means many different things to many different people the world over: even its formal definitions differ across cultural, linguistic, and legislative borders. In the FIDO Alliance context, we use the terms "user verification" to refer to how a device locally interacts with or identifies the user, and "authentication" to refer to how the user is identified to a remote system over the network using FIDO cryptographic protocols.

Privacy in the context of FIDO is intrinsically challenging, since a strong user verification system must be able to identify the legitimate account holder, which in turn requires persistently retaining information about that user. The FIDO Alliance's approach to privacy revolves around well-defined collection and use of data that pertains to a specific user. We will refer to this data throughout this document as personal data.

Moreover, any use of this data *must not* be surprising to the user. This also means that user verification information should not be easily combinable with data from other sources, as that would allow persistent identification outside the scope of a FIDO-based user verification process.

The Flow of FIDO Registration and User Verification

There are two main tasks that a user wants to perform using FIDO technology: initial registration with a given online service, and subsequent authentication with that service. The user needs a FIDO Authenticator for any of this to work. Such an Authenticator provides the user verification mechanism used. It can be a standalone hardware device, a fingerprint sensor and its firmware that are integrated into a device, or one of many other options. A FIDO Client is also part of the user's environment, and handles communications between the Authenticator and a FIDO Server. The server is part of the online service provider's infrastructure.

This service provider is also known in FIDO parlance as the Relying Party, since it's the entity that needs to rely on the authentication.

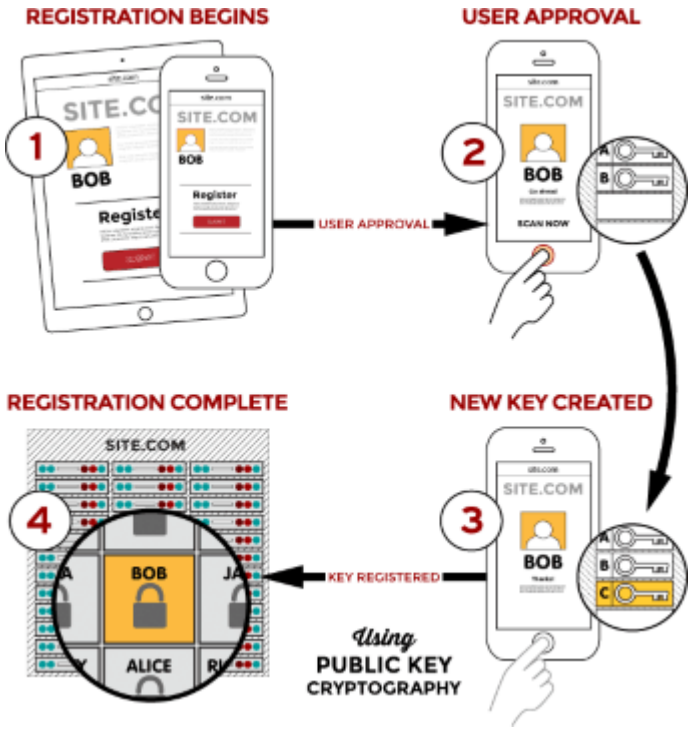

Figure 1: Registration

At the end of the registration process, the Relying Party has the public key that was created by the Authenticator, and the Authenticator recognizes that this public key can only be legitimately used by the domain belonging to the Relying Party.

When it's time to use this information to authenticate the user to the service, all the same pieces are involved.

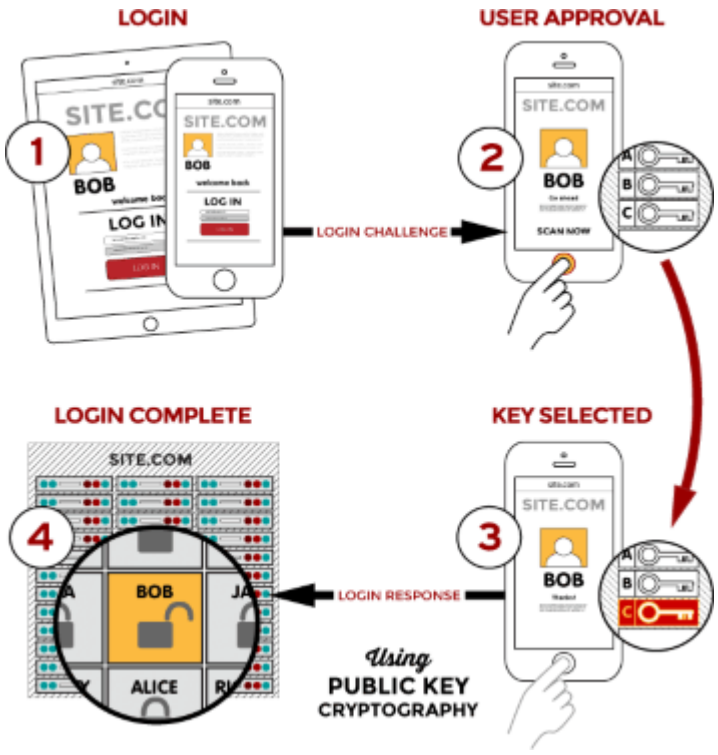

Figure 2: Authentication

Privacy and security requirements both share the same goal: that only the correct user is authenticated, and only when the user wants it.

There Is No Privacy Without Security

FIDO technical specifications include several privacy-related requirements as part of the security mechanisms built into our standards. Indeed, in order to strongly authenticate a user, as is a core precept of FIDO technologies, a system must have enough information to do so. To that end, the FIDO Alliance has worked to find the delicate balance between having knowledge about the user, and making sure it collects only the information it needs to perform a FIDO-related operation.

Registration gives a Relying Party's website the ability to strongly authenticate an account holder, and is therefore a very high-value operation. As registration is the foundation of all subsequent FIDO operations related to that account, it must be taken particularly seriously. During the process of registration, the validity of a FIDO Authenticator is also verified to provide assurance of its integrity.

FIDO technical specifications state that a FIDO device must not have a global identifier visible *across* websites, which prevents unwanted and unexpected re-identification of a FIDO user. A user must not be identifiable by one entity because of a relationship with another Relying Party. Additionally, a FIDO Authenticator does not have a global identifier *within* a particular Relying Party. These are representative examples of the FIDO Alliance's overall technical approach and attitude toward actively building privacy protection into products.

An except is made for Enterprise Attestation enabled FIDO Authenticators which do have a global identifier within an Enterprise Attestation enabled Enterprise network or within the Enterprises' Relying Party, where an Enterprise is some form of organization, often a business entity. The Relying Parties of the Enterprises' Data Processors (as defined by the GDPR) are considered to be part of the Relying Party of the Enterprise. Enterprise Attestation enabled Authenticators are solely for use by the Enterprises' employees, contractors and defined members, not its customers.

Other technical safeguards within the FIDO specifications include that a key issued to a particular website can only be exercised in a web browser by that website, amplifying the strong boundary between different sites. This requirement renders useless the theft of a public key for the purposes of phishing from another origin, and also prevents multiple colluding sites from using an Authenticator to strongly verify and correlate a user's identity as he or she browses the Web.

Some of FIDO's privacy-related safeguards aren't exclusively technical; some are policy-based, and some focus on the user experience presented. For example, when creating a relationship between the FIDO Authenticator and the web site, notification is an important part of making sure this happens with the user's knowledge. It is critical to engender our users' trust; FIDO technologies must be transparent about their purpose.

FIDO Privacy Principles

The design and implementation of FIDO Authenticators, Clients, and Servers must adhere to the following principles in order to be considered fully compliant. Just as we seek to protect the integrity of users' accounts, we also ensure that FIDO technologies are not used to identify users when they don't want or expect it.

#1

Require explicit, informed user consent for any operation using personal data

This includes collection and use of personal, identifiable data during registration, user verification, and transaction confirmation. A user must not be identified without the user wanting, knowing, or expecting it.

#2

Provide clear context to the user for any FIDO operations

This includes, but is not limited to, explicitly specifying which user identity is being used for a FIDO-related operation and what the server identity is.

#3

Limit collection of personal data to FIDO-related purposes

Only collect FIDO-related personal information that is necessary for the FIDO operation between the user and the Relying Party.

FIDO-related personal information is data collected during registration (and potentially during user verification) that is necessary to perform the specific FIDO-related task. We distinguish it from other information that may be collected by a Relying Party at the same time, but that is not part of FIDO operations' scope.

At registration time, the Relying Party must disclose the information collected from the user. If any additional information is collected at user verification or transaction confirmation time, the collection must be disclosed to the user as well; if there is no further collection, no explicit further collection disclosure is required.

#4

Use personal data only for FIDO operations

The sole acceptable use of data collected during a FIDO operation is to perform identification— for example registration, user verification, or authorization.

#5

Prevent identification of a user outside of FIDO operations

FIDO-related data must not be used to identify a user other than during a FIDO operation, or a user-desired and user-expected identification operation such as a system login.

#6

Biometric data must never leave the user's personal computing environment

Biometric data, measurements and personally identifying derivations of such data must be protected against extraction from the authenticator, and never transmitted outside the user's personal computing environment.

#7

Protect FIDO-related data from unauthorized access or disclosure

Data related to FIDO operations must be protected appropriately. This will be verified as part of the FIDO Certification Working Group's guidelines.

#8

Allow users to easily view and manage their FIDO Authenticators

It should be easy for users to list the FIDO Authenticators associated with their account and perform standard tasks with this information, e.g. de-register an Authenticator in the event of its loss.

Conclusion

These Privacy Principles reflect the FIDO Alliance's unambiguously strong commitment to protecting our users' privacy. The comprehensive technical mechanisms that pervade FIDO's specifications provide the foundation that makes the FIDO standards as privacy-protecting as they are secure. For more details about the FIDO Alliance and its standardization efforts, please visit http://fidoalliance.org.