We appreciate your interest in the FIDO Alliance and are pleased to share with you this FIDO Alliance Reference Architecture Document.

The membership agreement of the FIDO Alliance includes a commitment by participants to not assert their patent claims which are required to implement FIDO Alliance Requirements, Architectures and Specifications. We need assurance that your review of FIDO Alliance materials and discussions with the FIDO Alliance are consistent with those terms.
You acknowledge by receipt and use of this document that you have no rights to reproduce, prepare derivative works of, publicly display, publicly perform, sublicense, and distribute this FIDO Alliance Reference Architecture Document and that you receive no license of or agreement to not assert any patent claims in any way related to this FIDO Alliance Reference Architecture Document.
You additionally agree that if this FIDO Alliance Reference Architecture Document is marked "Confidential" or "Confidential Information" that you agree that unless and until this document is made available to the public, you will use the same degree of care and discretion that you normally use to avoid disclosure of your own confidential information to not disclose this FIDO Alliance Reference Architecture Document to any entity or person who is not a FIDO Member engaged in the activities for which this document was provided.

You are not required to provide any comments or input ("Comments"), verbally or in writing, on this document, but any Comments you do provide may be incorporated into these or other FIDO Alliance documents such as a FIDO Alliance Specification, Requirements or Architecture document.

By submitting Comments to the FIDO Alliance, you (on behalf of yourself if you are an individual and your company if you are providing Comments on behalf of the company) grant to FIDO Alliance and the authors of the FIDO Alliance Specifications or Requirements ("Authors") a perpetual (for the duration of the applicable copyright), worldwide, non-exclusive, no-charge, royalty-free, copyright license, without any obligation for accounting, to reproduce, prepare derivative works of, publicly display, publicly perform, sublicense, and distribute any Comments you provide. Likewise, if incorporation of your Comments into any of the FIDO Alliance Specifications or Requirements would cause an implementation of any of such FIDO Alliance Specifications or Requirements to infringe patent claims that you control, you agree to not assert that patent claim against any party making, using, selling, offering for sale, importing or distributing any implementation of the FIDO Alliance Specification or Requirement, 1) only to the extent it implements the FIDO Alliance Specification or Requirement and 2) so long as all required portions of the FIDO Alliance Specification or Requirement are implemented, where such FIDO Alliance Specification or Requirement describes the functionality causing the infringement in detail and does not merely reference the functionality causing the infringement.

You warrant that (a) to the best of your knowledge you have rights to provide these Comments, and if you are providing Comments on behalf of a company, you have the rights to provide Comments on behalf of your company; (b) the Comments are not confidential to you or to another party; and (c) to the best of your knowledge use of the Comments would not cause an implementation of any of the FIDO Alliance Specifications or Requirements to infringe any third-party patent or patent application known to you. You also acknowledge that FIDO Alliance and the Authors are not required to incorporate your Comments into any version of any of the specifications or Registry.


# Fast IDentity Online Alliance

**www.FIDOAlliance.org**

**Draft Reference Architecture [Confidential]**

**Feburary 2013**

# Executive Summary: The FIDO Alliance

This document presents the FIDO Alliance's initial reference architecture, as envisioned by FIDO member companies. It is intended to communicate the FIDO Alliance's vision, goals, and overall architecture to decision makers, technical architects, and IT managers/architects who wish to deploy strong authentication solutions, as well as to inform relevant standards development organizations.

The FIDO Alliance is a consortium composed of security vendors/integrators, computing device manufacturers, authentication token providers, and websites (i.e., *Relying Parties*). FIDO's overall goal is to enable websites, whether on the open Internet or within enterprises, to transparently leverage native security features of end-users' computing devices for the purpose of strong authentication. It will accomplish this by addressing the present lack of interoperability among strong authentication solutions – i.e., two-factor authentication (2FA) – as well as addressing the problems users face with creating and remembering multiple usernames and passwords. These issues can be summarized as:

**Proprietary** – Many existing 2FA products are proprietary solutions. It is difficult for organizations to switch solutions or to add additional complementary options that meet different needs.

**Expensive** – Many 2FA solutions are unnecessarily expensive. These costs include proprietary hardware, software and management that only apply to a single vendor. The cost of current authentication solutions limit the scalability for large website

**Deployment** – It is not feasible for large internet sites to deploy strong authentication solutions to all their users. The distribution and management of authentication tokens to millions of users is a logistic nightmare that few sites would contemplate. Smaller websites generally do not have the resources or will to adopt current authentication tokens.

**Convenience** – Today, most authentication tokens are inconvenient for users. Many sites that have deployed security tokens have unique devices for their site. This gives the user the "Token Necklace" problem in which they must carry a unique token for each site they access.

To address these issues the FIDO Alliance intends to develop technical specifications enabling:

**Broad Token Support –** FIDO is a non-proprietary approach. Any authentication token that conforms to the FIDO specifications will be usable within the ecosystem. This lowers costs for all, allows token vendors to participate in the ecosystem without

needing to maintain entire proprietary software stacks, and allows integrators to easily qualify and enable a broad range of options for their customers. Relying Parties are not locked into a single vendor and can offer appropriate security tokens to users according to their needs. End Users can select the security options that best meet their needs and can have a single secure token for all their accounts.

**Dynamic Token Discovery –** Relying Parties will be able to dynamically discover a user's new token(s) and suggest that the user bind their token to their Relying Party account. Users will be able to acquire whatever token they wish rather than having one necessarily assigned by the Relying Party. Dynamic discovery of user-provided tokens enables user choice and ameliorates the token deployment and cost problems for large internet sites.

**Third Party Token Attestation –** Dynamic discovery requires validation of newly found tokens. The FIDO specifications will enable the validation of tokens through a third party – using either locally-cached data or online services. Token vendors will insert a unique value into each token when it is made and share information to decode the secret with validation services. Relying Parties can use these validation services that will attest to the authenticity of the token.

The principles of the FIDO Alliance are:

**Standards Principles:**

- Develop and publish open, unencumbered technical specifications leveraging and complementing existing standards as appropriate.

**Business Principles:**

- Enable genuine user choice with strong authentication.
- Reduce development time and costs when deploying new solutions.

**Technical Principles:**

- Leverage existing standards as much as possible while meeting FIDO's goals.
- Align with existing authentication and federated identity management approaches and initiatives, e.g., OAuth, OATH, OpenID, PSKC, DSKPP, etc.

**Security and Privacy Principles:**

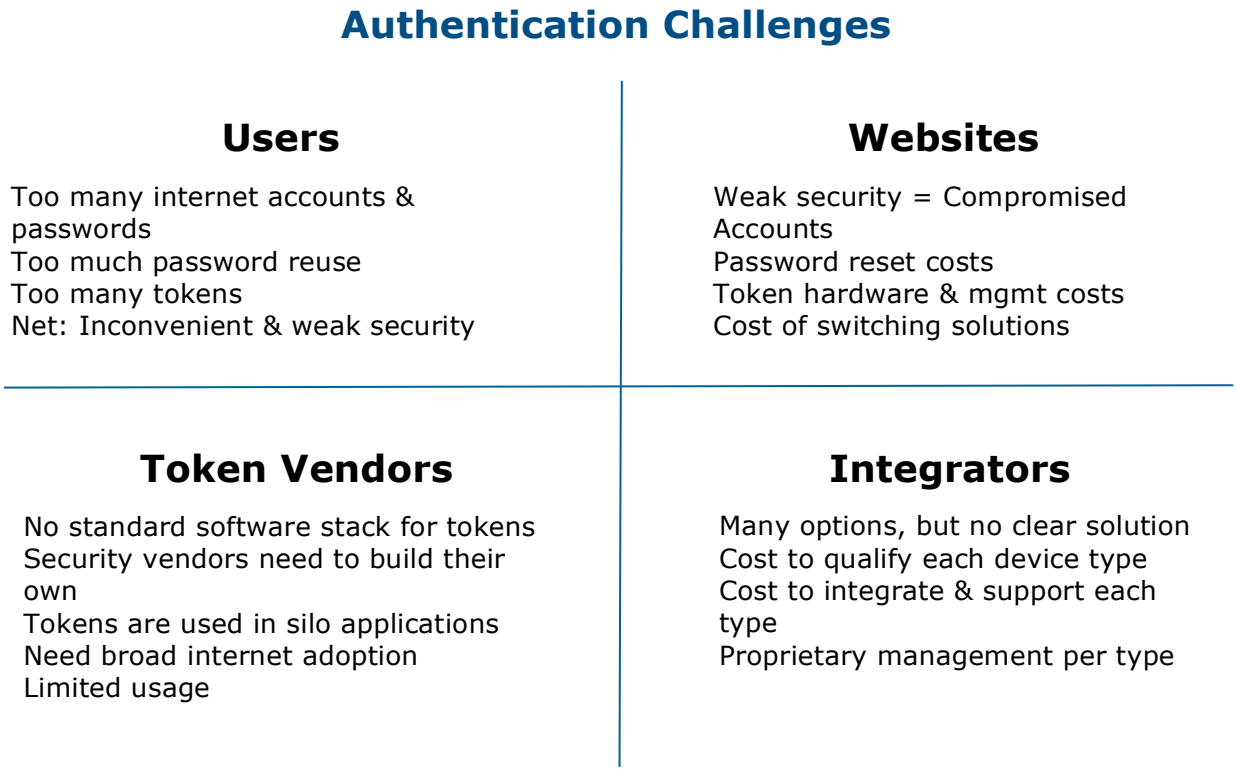
- Design with consideration for the security and privacy of users and providers.

The FIDO Alliance open reference architecture, presented in the document below, will establish an ecosystem fostering innovation and competition among its participants. Consequently, this will lower the costs and complexities of deploying ubiquitous strong authentication.

# Table of Contents

# 1 Problem Definition

Current approaches to online authentication are failing to deliver sufficient security and usability to meet the needs of end users and the organizations that serve them. Users are undermining their security by choosing weak passwords or reusing passwords across sites to cope with the growing number of passwords they must manage. This simply renders them more vulnerable to broad compromise through various attacks such as phishing. Meanwhile, organizations serving those users are struggling to protect systems against unauthorized access without adversely impacting these same users, as well as struggling with compliance requirements. Unfortunately, current alternatives to passwords are costly to deploy across large populations of heterogeneous platforms with complex use cases. These challenges are illustrated in the following diagram:




This situation has various ramifications, such as:

- **Elevated risk of data breach or fraud:** Relying on static, reusable – i.e., “phishable" – passwords increases the risk of unauthorized access to sensitive data or infrastructure, or unauthorized transactions.

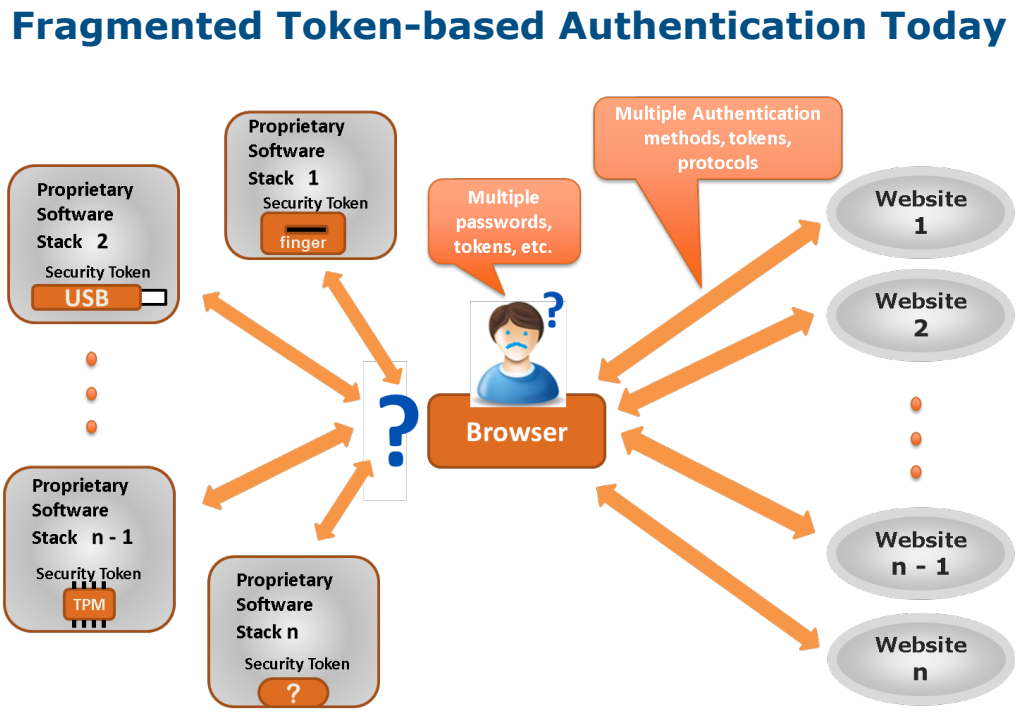
- **Increased IT and compliance costs:** Alternatives to passwords are expensive, requiring specialized hardware or software to be procured and deployed to end users.
- **Redundant authentication silos:** Organizations must deploy and maintain multiple authentication solutions to support diverse platform and use case requirements. End users are obliged to manage credentials for each separate web application, and often fall back to reusing the same password on multiple sites.
- **Lack of flexibility:** Organizations can't easily evolve their use of authentication to support new use cases, pursue new opportunities, or counter emerging online threats.

*Strong authentication* is commonly perceived as a means to resolve some of the issues. By definition, strong authentication mechanisms are cryptographically based and have the properties of not being trivially susceptible to common attack techniques such as credential theft and replay (i.e., *phishing*), and credential forgery (e.g., password guessing). Strong authentication mechanisms are implemented in various fashions. They involve at least protocol support and may leverage physical *authenticators* implemented as platform hardware features, or discrete security tokens, for example: Trusted Platform Module (TPM), biometric sensors, One-Time-Password (OTP) generators, etc.

However, on their own strong authentication protocols and authenticators address only the first issue above -- the use of weak, reusable, and phishable passwords -- and do not, on their own, address the latter issues of cost, authentication silos, and lack of flexibility. This is due to:

- Authenticator-based strong authentication systems are typically vendor-specific and proprietary in part or whole, and support various subsets of available platforms.
- There are a multitude of available authenticators, as well as a multitude of authentication protocols, both open and proprietary.
- There are various open standard authenticator attestation and provisioning protocols, but they each only address the needs of a subset of authenticators. None address authenticator discovery.
- There is a lack of a uniform, open, and cross-platform authenticator API.
- There is a lack of a standardized means for Relying Parties to assess whether a given user device, such as a computer or smartphone, features any employable authenticators and supports a mutually implemented strong authentication protocol.

The following diagram illustrates the complicated, fragmented status-quo:




# 2 Comparison to Other Technologies

## *2.1 OpenID, SAML, and OAuth*

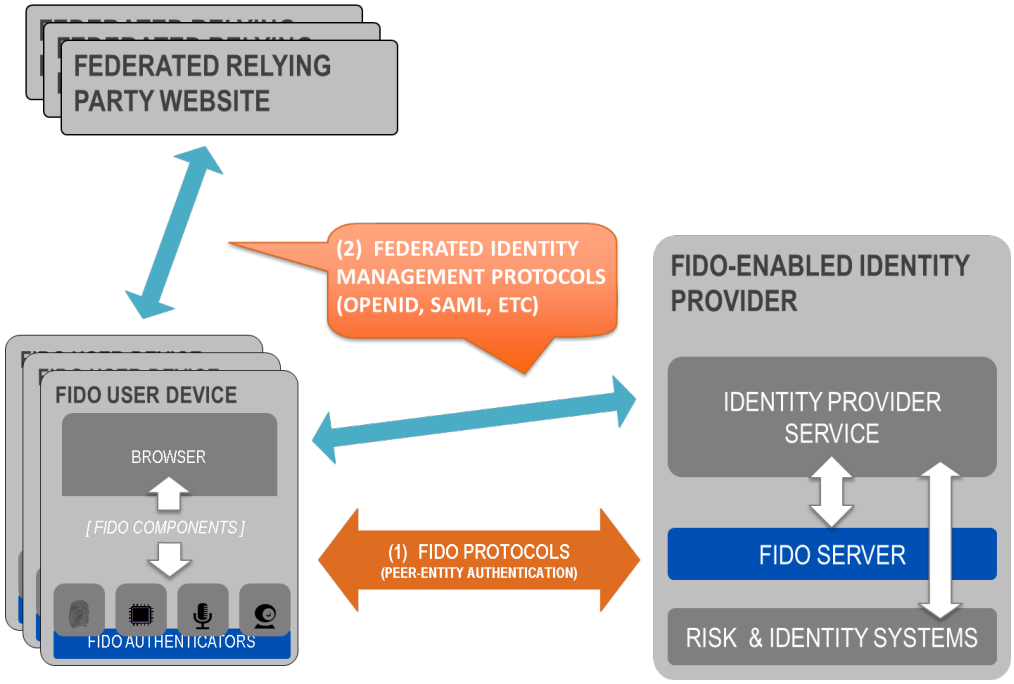
FIDO complements Federated Identity Management (FIM) frameworks, such as OpenID and SAML, as well as web authorization protocols, such as OAuth. These protocols facilitate leveraging an initial authentication event by a set of relying parties (RPs). However, OpenID and SAML do not specify particular mechanisms for direct user authentication, for example, at the Identity Provider (IdP).

FIDO focuses on closing this gap by providing trusted authentication from the start. If such a FIDO authentication event occurs with an Identity Provider (IdP), then the IdP can subsequently leverage the attributes of the FIDO authentication with its Relying Parties via the FIM and authorization protocols it supports.

The following diagram illustrates this relationship. FIDO-based authentication (1) would occur logically first, and then FIM protocols would leverage that authentication event into single sign-on events between the Identity Provider and other federated relying parties (2).[1]

[1] FIM protocols typically convey IdP <-> RP interactions through the browser via HTTP redirects.

## Relationship Between FIDO and Federated Identity Management Frameworks




## 2.2 OATH, TCG, PKCS#11, and ISO 24727

These are either initiatives (OATH, Trusted Computing Group (TCG)), or are standards (PKCS#11, ISO 24727).They all share an underlying focus on hardware authenticators.

PKCS#11 and ISO 24727 define smart-card-based authenticator abstractions.

TCG produces specifications for the Trusted Platform Module, as well as networked trusted computing.

OATH, the "Initiative for Open AuTHentication", focuses on defining symmetric key provisioning protocols and authentication algorithms for hardware One-Time Password (OTP) authenticators.

The FIDO framework shares several core notions with the foregoing efforts, such as an authentication abstraction interface, authenticator attestation, key provisioning, and authentication algorithms. FIDO's work will leverage and extend some of these specifications.

Specifically, FIDO will complement them by addressing:

- Authenticator discovery

- User experience
- Harmonization of various authenticator types, such as biometric, OTP, simple presence, smart card, TPM, etc.

# 3 FIDO Vision and Goals

In order to resolve today's high-friction situation and develop a smoothly-functioning low-friction ecosystem benefitting everyone, we need an overall, open, multi-vendor solution architecture encompassing:

- User devices and their deployment environments, whether home, small office, or enterprise
- Authenticators[2]
- Relying party applications and their deployment environments
- Meeting the needs of both end users and Relying Parties
- Strong focus on both browser- and native-app-based end-user experience

This architecture must feature:

- Authenticator discovery, attestation, and provisioning
- Cross-platform strong authentication protocols leveraging authenticators
- Uniform cross-platform authenticator API

Accordingly, the FIDO alliance envisions an open, multi-vendor, cross-platform reference architecture with these goals:

- **Support strong, multi-factor authentication**: Protect Relying Parties against unauthorized access by supporting end user authentication using two or more strong authentication factors (“something you know”, “something you have”, “something you are”).
- **Build on, but not require, existing device capabilities**: Facilitate user authentication using built-in platform authenticators or capabilities (fingerprint sensors, cameras, microphones, embedded TPM hardware), but do not preclude the use of discrete additional authenticators.

[2] Also known as: authentication tokens, security tokens, etc.

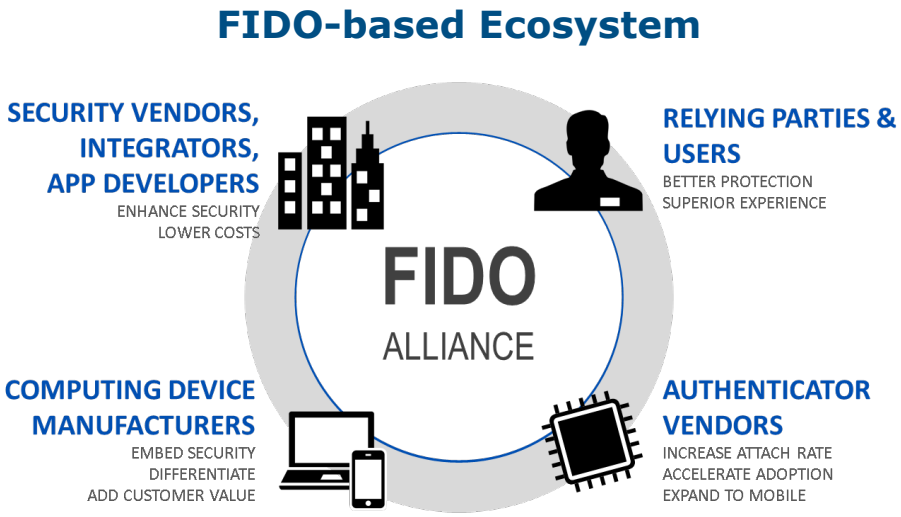
- **Enable Selection of the authentication mechanism**: Facilitate Relying Party choice amongst supported authentication mechanisms in order to mitigate risks for their particular use cases.
- **Simplify integration of new authentication capabilities**: Enable organizations to expand their use of strong authentication to address new use cases, leverage new device's capabilities, and address new risks with a single authentication approach.
- **Incorporate extensibility for future refinements and innovations**: Design extensible protocols and APIs in order to support the future emergence of additional types of authenticators, authentication methods, and authentication protocols, while maintaining reasonable backwards compatibility.
- **Leverage existing open standards where possible, openly innovate and extend where not**: An open, standardized, royalty-free specification suite will enable the establishment of a virtuous-circle ecosystem, and decrease the risk, complexity, and costs associated with deploying strong authentication. Existing gaps – notably uniform authenticator provisioning and attestation, a uniform cross-platform authenticator API, as well as a flexible strong authentication challenge-response protocol leveraging the user's authenticators – will be addressed..
- **Complement existing single sign-on, federation initiatives:** While industry initiatives (such as OpenID, OAuth, SAML, and others) have created mechanisms to reduce the reliance on passwords through single sign-on or federation technologies, they do not directly address the need for an initial strong authentication interaction between end users and relying parties.
- **Preserve the privacy of the end user:** Provide the user control over the sharing of device capabilities information with Relying Parties, and mitigate the potential for collusion amongst Relying Parties.
- **Unify end-User Experience:** Create easy, fun, and unified end-user experiences across all platforms and across similar Authenticators.

A FIDO-based ecosystem will yield the following benefits to adopters:

- **Reduce the risk of compromised accounts:** By displacing static, re-usable passwords as the primary authentication mechanism, FIDO will strengthen the protection of online accounts against attacks enabled by phishing, malware, and poor password management practices.

- **Streamline the user experience:** Allowing users to authenticate across FIDO-enabled applications using their fingerprint, voice, face, TPM, or other security features will reduce the risk of compromise due to a lost or stolen authentication password.
- **Match authentication strength to risk:** Selecting the appropriate authentication method available on the FIDO user device will provide the appropriate level of assurance for interacting with the Relying Party, while minimizing the impact on the end user experience.
- **Respond flexibly to new threats and opportunities:** Incorporating support for new authentication approaches in the future–without undertaking additional integration effort–will defend against emerging online threats or address new use cases.

The following diagram illustrates a FIDO-based ecosystem:



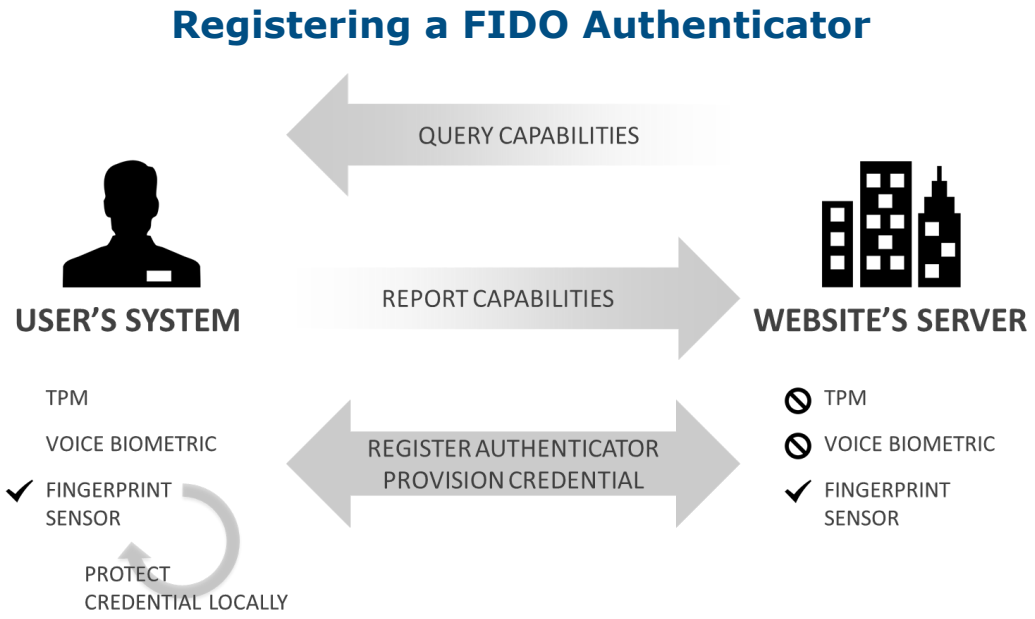

# 4 Use Cases

Ever growing amounts of personal and business value – both reputational and financial – are now represented online, thus the risks associated with credential compromise are only rising. Therefore, all typical cases where users must authenticate themselves online can benefit from strong authentication.

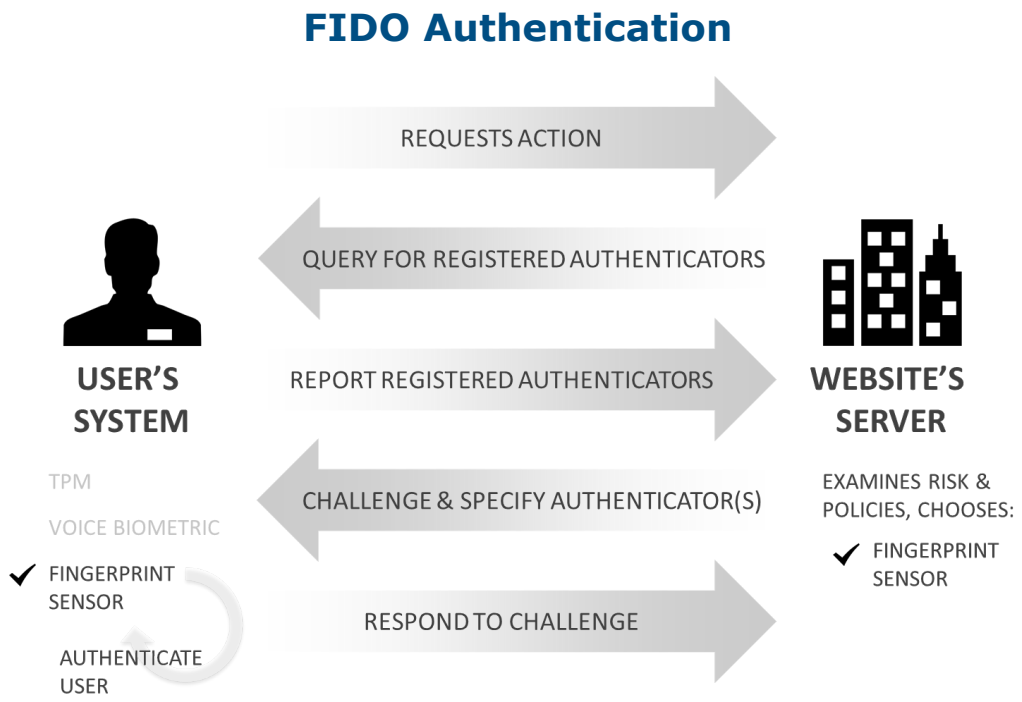
Although the FIDO architecture can ultimately support arbitrary peer-entity authentication interactions – e.g. network access login, end system login – the initial focus is on website login, which we will describe here.

## 4.1 FIDO-enabled Website Login

Users will acquire FIDO authenticators in various ways: they purchase a new system that comes with embedded FIDO authenticator capability; they purchase a device such as a USB drive with an embedded FIDO authenticator, or they are given a FIDO authenticator by their employer or some other institution such as their bank. After receiving a FIDO authenticator – whether separately or as part of a system or device – the user will go through a authenticator-specific *enrollment* process. For example, in the case of a fingerprint sensing authenticator, the user will register their fingerprint(s) with the authenticator. Once enrollment is accomplished, the FIDO authenticator is *initialized* and ready for *registration* with FIDO-enabled websites.




Given the FIDO architecture, websites (also known as Relying Parties) will be able to transparently detect when a user begins interacting with them while possessing an initialized FIDO authenticator. In this initial introduction phase, the website will prompt the user regarding any detected FIDO authenticator(s), giving the user options regarding registering it with the website or not. Upon registration, the FIDO authenticator will be subsequently employed whenever the user authenticates with the website (and the authenticator is present). The website can implement various fallback strategies for those occasions when the FIDO authenticator is not present. These might range from allowing conventional login with diminished privileges to disallowing login.




This overall scenario will vary slightly depending upon the type of FIDO authenticator being employed. Some authenticators will sample some biometric data such as a face image, fingerprint, or voice print. Others will require a PIN or local authenticator-specific passphrase entry. Still others may simply be a hardware bearer authenticator.

## 4.2 Step-up authentication

Step-up authentication is an embellishment to the basic website login use case. Often, websites allow unauthenticated, and/or only nominally authenticated use – for informational browsing, for example. However, once users request more valuable interactions, such as entering a members-only area, for example, the website may request further higher-assurance authentication. This could proceed in several steps, for example if the user then wishes to purchase something, with higher-assurance steps with increasing transaction value.

FIDO will smoothly facilitate this interaction style since the website will be able to discover which FIDO authenticators are available on FIDO-wielding users' systems, and select incorporation of zero to all of them (or subsets thereof) in any particular authentication interaction. Thus websites will be able to dynamically tailor initial, as well as step-up authentication interactions according to what the user is able to wield and the needed inputs to website's risk analysis engine given the interaction the user has requested.

### 4.3 Adoption of New Types of FIDO Authenticators

Authenticators will evolve and new types are expected to appear in the future. Their adoption on the part of both users and relying parties is facilitated by the FIDO architecture. In order to support a new FIDO authenticator type, relying parties need only to add a new entry to their configuration describing the new authenticator, along with its FIDO attestation certificate. Afterwards, end users will be able to use the new FIDO authenticator type with those relying parties.

### 4.4 Secure Transactions

There are various innovative use cases possible given FIDO-enabled relying parties with end-users wielding FIDO authenticators. Website login and step-up authentication are relatively simple examples. A somewhat more advanced use case is secure transaction processing.

Imagine a situation in which a relying party wants the end-user to confirm a transaction (e.g. financial operation, privileged operation, etc) so that any tampering of a transaction message during its route to the end device display and back can be detected. FIDO architecture has a concept of “secure transaction” which provides this capability. Basically if a FIDO authenticator has a secure display capability, FIDO architecture makes sure that the system supports **What You See is What You Sign** mode (WYSIWYS).

a number of different use cases can derive from this capability – mainly related to authorization of transactions (send money, perform a context specific privileged action, confirmation of email/address, etc).

# 5 Terminology

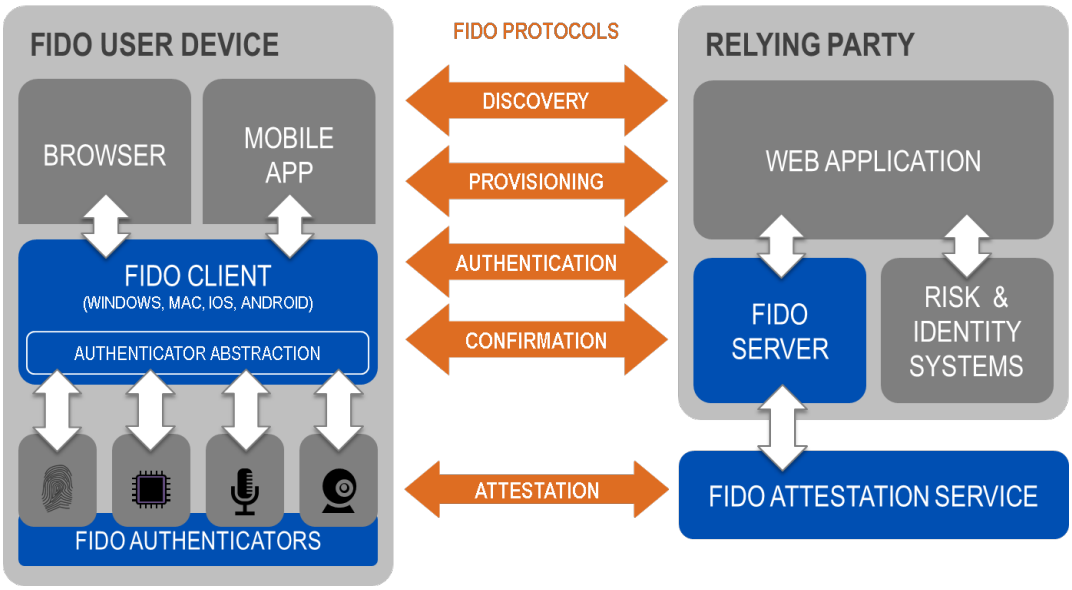
| | |
|---|---|
| FIDO Attestation Service | The Attestation service provides cryptographic proof of the provenance of FIDO Authenticators. |
| FIDO Client | The FIDO-compliant client-side software component which runs on the FIDO User Device. |
| FIDO-compliant | An authenticator, server or client that has demonstrated compliance to the requirements defined by the FIDO Alliance. |
| FIDO User Device | FIDO-enabled user device or system (e.g. PC, Tablet, Smartphone, etc.) which incorporates a FIDO Authenticator and hosts a FIDO Client.<br>Not to be confused with the FIDO Client, or FIDO Authenticator. |

| | |
|---|---|
| FIDO Server | The FIDO-compliant on-premises server component. |
| FIDO Authenticator | The authentication or identification token, e.g. fingerprint sensor, TPM or software implementation of a authenticator.<br>Not to be confused with the FIDO user device or the FIDO client.. |

# 6 FIDO Reference Architecture

The FIDO reference architecture is designed to meet the FIDO goals and yield the desired ecosystem benefits. It accomplishes this by filling in the status-quo's gaps using standardized protocols and APIs.

The following diagram summarizes the FIDO reference architecture:




The FIDO-specific components of the reference architecture are:

- **FIDO Protocols**
- **FIDO Client**
- **FIDO Authenticator Abstraction Layer**

- **FIDO Server**
- **FIDO Attestation Service**
- **FIDO User Device**
- **FIDO Authenticator**

These components are discussed further in turn below.

## 6.1 FIDO Protocols

The FIDO protocols are user device to relying party protocols addressing the given needs for:

- Authenticator Discovery, Attestation, and Provisioning:
  - Discovery – The FIDO protocols will enable Relying Party discovery of the FIDO authenticators available on a user's system or device. Discovery will convey authenticator attributes to the Relying Party thus enabling policy decisions.
  - Attestation – The FIDO protocols will allow a Relying Party to directly validate a newly discovered authenticator, or do so via a third party FIDO attestation service[3].
  - Provisioning – Once the authenticator has been validated, the Relying Party can provide a unique secure identifier that is specific to the Relying Party and the authenticator. This identifier can be used in future interactions between the pair {RP, Authenticator} and is not known to any other devices.
- User authentication – This is anticipated to be based on cryptographic challenge-response authentication protocols (also supporting various OTP algorithms), and will facilitate user choice regarding which FIDO authenticator(s) are employed in an authentication event.
- Secure Action Confirmation – The Relying Party can present the user with a secure message for confirmation. The message content is determined by the Relying Party and could be used in a variety of contexts such as confirming a financial transaction, a user agreement or releasing patient records.

[3] A design requirement for attestation is attestation information to be cacheable on-premises.

## 6.2 FIDO Client

The FIDO client implements the client side of the FIDO protocols, and interfaces with the FIDO Authenticator abstraction layer via the FIDO Authenticator API.

While the FIDO client software implementation will be platform-specific, the FIDO specifications will define the interactions and APIs between the protocol-handling code provided by any FIDO-specific browser extensions, the devices that handle the user authentication and provide the authenticators, and what the user experience should be, in order to ensure as consistent an experience as possible from platform to platform.

The FIDO architecture will be designed and specified so that the FIDO client software can be implemented across a range of operating systems, system types and Web browsers.

## 6.3 FIDO Authenticator Abstraction Layer

The FIDO authenticator abstraction layer provides a uniform API to upper layers enabling the utilization of authenticator-based cryptographic services. It provides a uniform lower-layer "authenticator plugin" API facilitating the employment of multi-vendor authenticators and their requisite drivers.

## 6.4 FIDO Server

The FIDO server component implements the server side of the FIDO protocols, and interfaces with the FIDO Attestation Service. The FIDO server is responsible for:

- Implementing the server portion of the FIDO protocols.
- Communicating with the FIDO Attestation Service to validate FIDO Authenticator attestations.
- Communicating with the FIDO Attestation Service to update FIDO Authenticator data.

The FIDO server is conceived as being deployable as an on-premise server by relying parties or as being outsourced to a FIDO-enabled third-party service provider.

## 6.5 FIDO Attestation Service

The FIDO Attestation Service closes the loop between the FIDO Authenticators and the FIDO service. It is an entity responsible for:

- Endorsing FIDO Authenticators. Endorsement provides a means for FIDO Authenticators to later attest as to their provenance.
- Providing means for validating FIDO Authenticator attestations.
- Maintaining an up to date list of endorsed FIDO Authenticators and their characteristics.
- Providing up to date revocation data to FIDO Servers.

The FIDO Attestation Service is conceived as being deployable as an on-premise server by relying parties or be outsourced to a FIDO-enabled third-party service provider.

## 6.6 FIDO User Device

FIDO-enabled user devices may consist of almost any sort of computing platform employed by end users:

- Web-focused user devices: e.g., tablets and media players
- PC-based notebooks and desktops
- Mobile devices: e.g. smartphones
- Smart TVs, game consoles, and other, consumer devices

## 6.7 FIDO Authenticator

A FIDO authenticator is a secure entity, attached to or housed within FIDO user devices, that is remotely provisionable with key material by relying parties, and is then capable of participating in cryptographic strong authentication protocols. For example, the FIDO authenticator will be capable of providing a cryptographic challenge response based on the key material thus authenticating itself.

In order to meet the goal of simplification of authentication capability integration, a FIDO authenticator will be able to attest to its particular type (e.g., biometric) and capabilities (e.g., supported crypto algorithms), as well as to its provenance. This provides the relying party with a high degree of confidance that the device and user being authenticated is indeed the same device and user that was originally provisioned.

# 7 Contributors

The following members of the FIDO Alliance Technical Working Group(TWG) have contributed to this document:

Infineon Technologies

Lenovo

Nok Nok Labs

PayPal

Validity Sensors