FIDO vs MPC

A perspective on the differences between FIDO Authentication and Multi-Party Computation, and how FIDO became the preferred standard for password-less authentication.

Has FIDO Won the Enterprise?

The IAM industry is experiencing a paradigm shift as a wide range of new and old methodologies compete for the budgets and attention of enterprises worldwide. User authentication is transitiong from the age of shared secrets, centralized passwords and OTP tokens - to an era of password-less security powered by decentralized authentication, biometrics and PKI.

There have been a number of different approaches to solving "the password problem." This paper focuses on two such protocols - **FIDO Authentication and Multi-Party Computation** - that are often compared and have been evaluated extensively across the IAM landscape. This is a rare and unique competition of 2 very different cryptographic protocols that have been pitted against one another in proving they are the right approach to next-gen user authentication.

Having been deployed at scale, FIDO standards so far appear to be winning in terms of enterprise adoption, applicability, interoperability, and ecosystem. MPC has been around much longer with a wide variety of use cases but has not yet proven successful for passwordless authentication. How did FIDO win over the hearts and minds of enterprises? This paper explores the differences between the two and aims to help companies evaluating FIDO and MPC understand why the former became the gold standard for passwordless and strong authentication.

fido™ VS MPC

FIDO AUTHENTICATION

FIDO (Fast Identity Online) is an open-source specification for strong password-less authentication. FIDO architecture enables a service provider to replace passwords with public key cryptography techniques (PKI). Proponents who have adopted FIDO standards aim to achieve a state of "password-less security."

MULTI-PARTY COMPUTATION

Multiparty Computation (MPC) is a concept that gives different parties to a relationship the ability to compute data and arrive at a mutually desired result, but without requiring parties to the transaction to divulge their private data. Examples such as Shamir's Key Sharing Algorithm have been used in problems requiring zero-knowledge proofs.More recently attempts have been made to leverage MPC for strong authentication.

FAST IDENTITY ONLINE

A Simplified Approach to Solving a Complex Problem

The idea for Fast Identity Online (FIDO) dates back to late 2009, followed by the public launch of the FIDO Alliance in February 2013. December 9, 2014 saw the publishing of the completed v1.0 specification of its password-less protocol (UAF) and was followed by a number of production deployments. Subsequent activities included the launch of a rigorous FIDO® Certified testing program for ensuring security, conformance, and interoperability across an emerging ecosystem of solution providers.

FIDO authentication has been deployed in both consumer and employee-facing applications, allowing a user to enroll and authenticate to mobile, web and desktop services by leveraging a variety of authenticators such as biometrics or PINs stored on their personal devices.

FIDO protocols leverage public key cryptography to enable secure password-less authentication. When registering with an online service, a user's client device generates a public-private key pair. The private key is retained on the device and the public key is registered with the online service.

During authentication, the user signs a challenge using the private key stored on their client device. FIDO architecture ensures that the private key is stored on a personal mobile device or second-factor token and can be protected with additional layers such as biometrics or Trusted Execution Environments.

FIDO ARCHITECTURE ELEMENTS

FIDO Mobile Client
iOS, Android

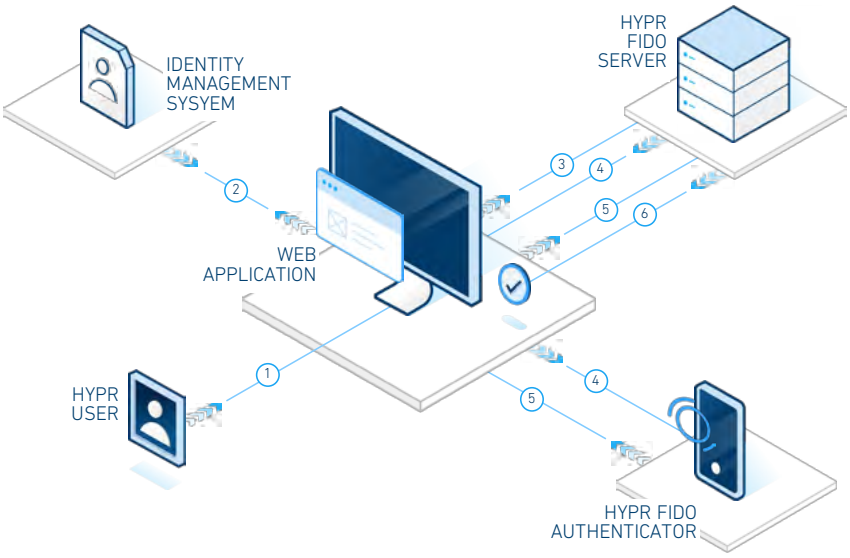
FIDO Desktop Agent
Windows 7, Windows 10, MacOS

FIDO Web Plugin
Edge, Safari, Chrome, FireFox, Opera
W3C Native Browser Support

FIDO Authentication Server
Red Hat, Windows Server
AWS or Azure

FIDO Management Console
Policy Management & Orchestration

FIDO Identity Extensions
PingIdentity, Okta, ForgeRock, ADFS, Shibboleth, CA, Oracle Access Manager



FIDO WEB AUTHENTICATION

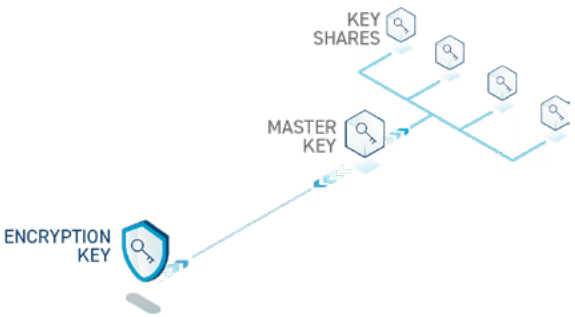
User Request
User Validity Check
Authentication Initiation
Authentication Challenge
FIDO Signed Response
Authentication Complete

MULTI-PARTY COMPUTATION

Complicated Cryptography for Complex Problems

Multi-Party Computation refers to a field of cryptography with the goal of enabling multiple parties to jointly compute a function over their inputs while maintaining the privacy of those inputs. If that doesn't sound simple enough its because it isn't. MPC is in fact a complex and non-trivial field with signficant implications for solving zero-trust situations. But how has it been applied to authentication?

There are many different MPC methodologies that have be applied to problems involving trust-less systems in many different ways (e.g. secret sharing), with popular implementations such as Shamir's Secret Sharing algorithm. More recently, attempts have been made to develop proprietary solutions that novelly apply MPC by leveraging Shamir's Key Sharing for password-less user authentication.



According to Wikipedia, Shamir's Key Sharing "is a form of secret sharing, where a secret is divided into parts, giving each participant its own unique part. To reconstruct the original secret, a minimum number of parts is required."

Shamir's Key Sharing Algorithm

Is used to secure a secret in a distributed way, most often to secure other encryption keys. The secret is split into multiple parts, called shares. These shares are used to reconstruct the original secret and authenticate the user.

At its core, a password is a shared secret - and MPC authentication providers aim to bolster the security of shared secrets. These passwords, or "secrets" are distributed or divided between a user's mobile device and a key validation server, with the user authenticating with device biometrics, PIN, or PUSH.

The mobile application communicates with the validation server to conduct an exchange that, once securely tallied, approves the authentication. The end result is a password-less user experience combined with a complex cryptographic scheme. Although the user no longer has to enter a password, the service provider still relies on "shared secrets." This has led to debates about wether or not MPC is really password-less.

FIDO - 10 YEARS OF **RESULTS**

Since 2010 FIDO has matured as a technology and as an ecosystem, backed by an industry consortium accelerating development and adoption of authentication standards. The FIDO Alliance consists of 250+ members and boasts the support of industry leaders across the globe. The standard has been widely adopted and deployed at scale by enterprises such as Google, Microsoft, Samsung, Bank of America, Mastercard, and many more. Participation from such a large ecosystem has further evolved platform, browser, and infrastructure support and, as of 2018, the vendor ecosystem consists of more than 200 certified products - all of which adhere to interoperability requirements set forth by the FIDO Alliance.

3B

Through large-scale deployments, FIDO has been made available to over 3 billion users worldwide.

Notable platform integrations include the addition of FIDO as a native capability in Windows 10 devices, Samsung smartphones, and even web browsers. In mid-2018 the FIDO Alliance and W3C web standards organization announced that the new Web Authentication standard would be supported by all major web browsers. This major development would bring strong authentication to browsers such as Chrome, Safari and FireFox and enables large companies to standardize password-less security across the web experience.

MPC - 40 YEARS OF **RESEARCH**

To date, there have been few notable examples of multi-party computation technology being deployed at scale for password-less authentication.

Multi Party Computation originated long before FIDO and work in the field has been ongoing since the 1970s, with the protocol being considered "a mathematical answer or response to the longstanding challenge of trusted third parties no longer being trustworthy." MPC has a strong following in academia while practical use cases for multi-party computation have primarily remained in the field of applied cryptography.

Internet searches on real-world use cases for MPC yield numerous white papers, proposals and discussions on applicability of practical uses such as key distribution, secret sharing, and problems involving zero-knowledge proofs.

A noteworthy real-world application of MPC occurred 10 years ago in the Danish sugar beet market. In this example farmers bid for contracts at auction without having to reveal the price they were willing to sell for, or their economic position. New America notes that, "The past few years have seen the most significant advances in making MPC's use more wide-scale. Since 2015, MPC has been used to evaluate gender pay disparities in Boston, detect tax fraud in Estonia, and prevent satellite collisions."

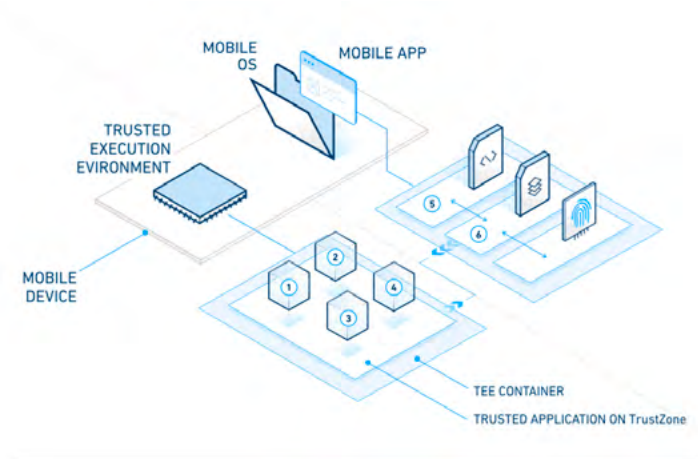
MOBILE SECURITY CHALLENGES FOR MPC

FIDO was designed to take advantage of advances in hardware-backed security by permitting developers to store private keys inside the most trusted area of a mobile device - the TrustZone. Most MPC implementations are unable to achieve this level of security in what is possibly MPC's biggest hurdle for enterprise adoption.

The rise of mobile biometrics and new modes of authentication have prompted device manufacturers to adopt ARM TrustZone technology, enhance device security and protect the storage of private keys. Innovations such as the iOS Secure Enclave (SE) and Android's Trusted Execution Environment (TEE) are now available on billions of mobile devices and have proven to be a powerful solution for securing private keys and biometric data.

Mobile trustzones serve as the foundation for password-less authentication and asymmetric cryptography leveraged by FIDO standards. Unfortunately they don't work for MPC solutions based on symmetric shared secrets.

ARM TRUSTZONE | iOS SECURE ENCLAVE | ANDROID TEE | INTEL SGX | SAMSUNG KNOX



MPC solutions built upon key-sharing and symmetric cryptography are unable to deliver an authentication flow that makes use of the mobile TrustZone. Not only is this a huge step back in security, it is especially critical for meeting PSD2 compliance for Strong Customer Authentication - which specifies that private keys must be stored in an isolated software layer.

By not leveraging these imperative layers of hardware-backed security, MPC implementations leave user credentials susceptible to malware or device-side attacks. This drawback has been a hurdle for security teams and business leaders deploying PSD2 compliant authentication.

> FIDO authentication is currently the best available solution to solve the password problem.
>
> - Abbie Barbir, Senior Security Advisor, Aetna

FIDO ENABLES A PASSWORD-LESS END-STATE. MPC RELIES ON PASSWORDS.

The point of going password-less is having to no longer store user authenticatioin keys inside the enterprise. FIDO's PKI-based approach has allowed companies to arrive at this desired end-state in which passwords and shared secrets no longer exist. Without shared secrets which can be stolen or phished by malicous hackers - the risk of phishing, credential stuffing and password reuse drops significantly. This has made FIDO an attractive approach for enterprises seeking to eliminate passwords.

MPC-based authentication relies on shared secrets which are complex and split up into different pieces. Although it increases the complexity and difficulty of an attack, MPC still relies on a shared secret - which is in essence, a password. It's in the name - "Secret Sharing." A secret which can be shared can also be stolen and re-used by a malicious third party. This approach has not been proven to be effective in deploying passwordless security as it fails to solve the underlying problem of credential reuse.

WHY FIDO WON THE ENTERPRISE

Interoperability

FIDO is less than 10 years old and has been successfully deployed to billions of users. Multi-Party Computation has been around much longer but has failed to solve "the password problem" and its use for large-scale user authentication remains in its infancy.

Usability

FIDO specifications are purpose-built for modern authentication and designed to leverage mobile advancements in mobile security. Like trying to fit a square peg into a round hole, MPC is being applied to a use case for which it wasn't originally intended. Companies have attempted to unsuccessfully shoehorn, retrofit, or restructure secret-sharing protocols to make the concept work for authentication.

Community

MPC-based authentication is an outgrowth of an existing community within the cryptosphere and is likely to continue growing. However, even with so much research, proprietary solutions built using key-sharing concepts have not benefitted from the community that evolves around a standards-based approach.

What Comes Next

MPC has proven to work for complex use cases and will continue to drive solutions for zero-trust problems. Usage of MPC for user authentication may continue in certain edge cases, but FIDO has proven to be the winner for scaling strong authentication across large user populations. FIDO standards, a long time in the making and under refinement, were designed for and developed by an ecosystem. The vision for interoperable, simple and secure authentication is shared across the community members - all of whom can contribute to the constantly-evolving standard.