Accountable Digital Identity | ADI Association

NEXT-GENERATION IDENTITY & AUTHENTICATION STANDARDS

By:
James M. Routh
Former CISO Mass Mutual, CVS / Aetna, KPMG, DTCC, and American Express
ADI Association Board Member

Contents

Executive Summary

Establishing and managing identity securely is an essential requirement for the digital world. Unfortunately, most digital services continue to rely on passwords as their primary form of authentication. However, new technologies enable enterprises to finally move away from passwords and establish a single, lifetime digital identity for each person, with accountability as a key pillar.

This paper describes next-generation authentication methods and standards, including the emerging Accountable Digital Identity (ADI) standard from the nonprofit ADI Association.

Introduction

Organizations of all sizes need a successful digital presence to meet customer requirements and support their business objectives. To achieve this, they must onboard digital customers securely without creating friction in the user experience. Today, these experiences still rely on legacy, password-based solutions for onboarding, even though these solutions are ineffective against identity fraud.

Compromised credentials are at the root of most cyber security attacks. The average digital consumer has 150 digital accounts requiring passwords. This is unmanageable, so consumers re-use their passwords. Threat actors can then easily compromise those credentials to commit large-scale fraud. While adding multi-factor authentication (MFA) to combat fraud can provide limited credentials protection, it increases user friction.

Fortunately, authentication techniques are advancing, promising a future with a vastly reduced reliance on passwords and dramatically lower fraud rates. The core technologies needed to establish this new identity layer are becoming available but need a set of standards and a framework in which to operate.

Role of ADI Association

The next generation of federated identity standards should support the issuance of a lifetime digital identity that a consumer can use across the digital services of their choice. It should eliminate passwords and protect personal data.

The World Wide Web Consortium (W3C) has been developing standards for verifiable credentials and decentralized identifiers. Established technology standards like FIDO add strong authentication to eliminate reliance on passwords. These developments, combined with maturing distributed ledger technologies, pave the way for a new set of federated standards for digital identity.

The Accountable Digital Identity (ADI) Association is developing an open standard, based on decentralized identity, for bootstrapping individual identities online. The work will give identity providers and relying parties a framework to establish secure exchanges of identity-based services for

their consumers, customers, employees, and partners. The ADI Association is following a model like the FIDO Alliance, which focuses on standards that enhance the digital consumer experience while improving cyber security at the same time.

The ADI Association published the first version of its technical specification in August 2021. The ADI Specification empowers users with a lifetime identity they can use to prove who they are, protect their personal data, and provide consent to share that data when necessary.

Privacy-preserving accountability is a key pillar of digital identity in the ADI Specification. Accountability begins with proper identity vetting to bind users and their devices to their claimed identity. Proper identity vetting reduces fraud risk, which is why it is becoming a cornerstone of many regulations, such as Know Your Customer (KYC). Traditional knowledge-based account creation and recovery methods are vulnerable because any reliance on "something you know" can safely be assumed as weak and susceptible to social hacking by determined adversaries.

ADI Association is a nonprofit, and membership is open to any organization that wishes to contribute to the evolution of digital identity standards. This is an excellent opportunity for commercial software providers and device manufacturers to participate in the move toward federated decentralized identity.

Beginnings of Digital Authentication

In 1961, Fernando Corbató created the first password for accessing files on a timesharing service at MIT. The original authentication systems were binary systems ("access approved" or "access denied"). Over the next several decades, the username and password combination served enterprise security needs relatively well, and it is still the predominant method of authentication for web apps, mobile apps, and internal applications within an enterprise. In the last two decades, the use of passwords has ballooned, with the average digital user having to remember passwords for 150 different digital services (forty-six mobile apps and over a hundred web applications on average). This is extremely challenging. As a result, most users re-use their passwords across services and are highly vulnerable to identity fraud.

Credential stuffing is an automated technique for entering stolen username and password pairs into website login forms to find a match and gain improper access to accounts. This technique now represents a significant amount of traffic to popular websites. Cybercriminals have learned that using compromised credentials on a digital service is more effective for fraudulent activities than exploiting system vulnerabilities. This is because an end user who enters the correct credentials and passes the required binary authenticator is trusted entirely in most applications and networks. Criminals using those same credentials can now exfiltrate account data, move laterally within the network, or monetize data by selling it to other criminals.

You can test the above assertion about the scale of credential stuffing by using your favorite Internet search engine:

1. Enter the words "Sentry MBA YouTube" and click to search.

2. You will see thousands of search results for YouTube videos teaching how to use this specific tool to crack accounts using compromised credentials.

3. Now, search instead for "Sentry MBA download" to see tens of thousands of listings for free download sites to get this hacking tool.

Remember, these are just the search results for ONE tool, and there are many other such tools available. The scale of credential stuffing attacks is massive, demonstrating that passwords are obsolete as a security mechanism.

History of FIDO Standard

The deficiencies of passwords shifted industry attention to biometric authentication. The Fast Identity Online (FIDO) standard was developed to support this evolution.

The development of FIDO began when biometric sensors became prominent in the PC market, initially for unlocking the PC. That evolved into a password manager using biometric unlock. Protocols for Zero-Knowledge Proof and challenge-response were already well-defined, and many network equipment solutions used these frameworks. These two well-tested technologies and the lessons learned from the failure of large-scale PKI projects gave birth to the FIDO protocol.

FIDO introduced biometric technology bound to a specific user. It also leveraged challenge-response protocols to show proof to a service provider without using a shared secret. With these building blocks, FIDO brought biometrics into mainstream use through industry-wide adoption of the standard by service providers.

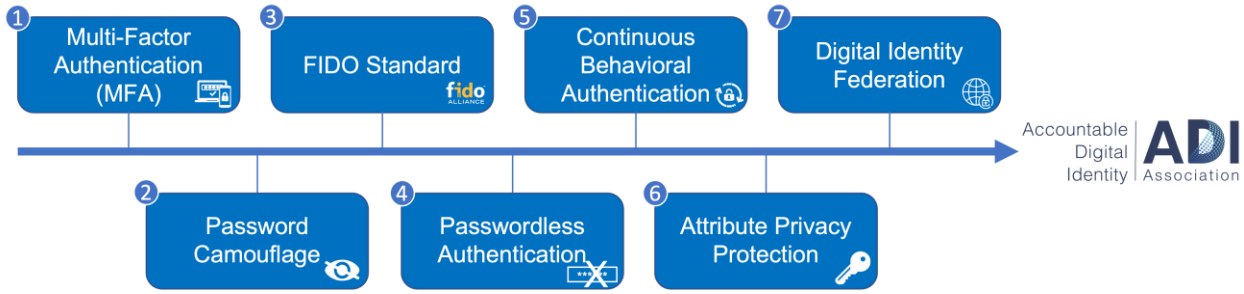
While the FIDO Alliance was announcing the first FIDO protocol, Nok Nok Labs was piloting the first FIDO reference implementation with Samsung and PayPal. Samsung had included the client FIDO stack in their Galaxy mobile product line, and PayPal was a design partner to Nok Nok Labs for an early pilot use case.

As the market changed from a PC-centric to a mobile-centric economy, the adoption of subscription services increased. As a result, password management became an unavoidable problem because of the proliferation of account takeover attacks and the complexity of account recovery and device migration.

These market forces provided a tailwind for FIDO. At the time, there were also other efforts to eliminate passwords, but they all eventually joined with FIDO, which made it the natural choice for any organization standardizing its authentication infrastructure.

Advanced Authentication Spectrum Framework

The Advanced Authentication Spectrum framework shown below represents several options for an organization to improve its authentication. This framework is not a product market analysis; instead, it shows how the sector is evolving to help organizations replace passwords as the primary authenticator. Each item on the spectrum is a category of authentication capabilities with common attributes or features. These categories capture the choices available for organizations and provide a path toward more advanced and effective authentication options.



1. Multi-Factor Authentication (MFA)

Digital services that store sensitive information often implement MFA. Many security standards have incorporated MFA, and it has become pervasive across digital services. However, the end user must tolerate a level of friction to use MFA. Before gaining access to a digital service, they must enter their username and password and then enter an additional one-time password sent via an alternate channel.

Unfortunately, even with MFA, the foundation of authentication continues to be the password. This shared secret is becoming less secret every day, given the tens of billions of compromised passwords available on the dark web.

2. Password Camouflage

End users want to access their digital services without having to remember all their credentials.

For enterprise users, single sign-on (SSO) solutions enable access to multiple applications using one enterprise network login. Tokens or keys are passed to the applications so that, as long as their device or digital identity is recognized, enterprise users can avoid having to enter their credentials again. Another enterprise option is Identity-as-a-Service (IDaaS). These proxy services allow users to authenticate at the network layer and then use an authenticator to replace the password with a push notification or text message requiring acknowledgment.

For consumers, password managers enable access to multiple applications without requiring the user to remember their passwords. The password manager automatically generates, stores, and manages

complex passwords for all websites and mobile applications used by the consumer. It camouflages those passwords, so the consumer must remember only the one password that accesses the password manager itself. In the password manager, the user can view all the passwords for their various digital accounts, but they do not have to remember them.

Password camouflage options improve the user experience and enhance password complexity to reduce fraud. However, these options are still vulnerable to credential theft. When an enterprise network credential gets compromised, the threat actor can get immediate access to multiple applications because of SSO. When a consumer password manager gets compromised, the threat actor can harvest all the passwords the consumer uses.

3. FIDO Standard

Device and software providers across the industry now support the FIDO standard. With FIDO, a user configures their biometric authentication once. Authentication then takes place at the application layer without requiring any user action to exchange keys and authenticators.

FIDO is limited to a single domain and one FIDO token per device. This limit eliminates man-in-the-middle, server-side, and phishing attacks while maintaining privacy between domains. However, this limit does increase implementation costs for enterprises with more than one domain.

4. Passwordless Authentication

An enterprise authenticator replaces password usage. There are several approaches: Cryptographic keys generated from a smartphone can act as authenticators; device attributes and browser configurations can be captured and used as authenticators; and biometric options on smartphones are also good authenticators, as demonstrated by the FIDO standard.

Passwordless authentication options improve user experience and reduce fraud, but threat actors can still defeat binary authenticators. Adding multiple authenticators can make it more difficult for threat actors to use techniques like replay attacks or spoofing text messages at scale.

5. Continuous Behavioral Authentication

This category highlights the evolution from binary to continuous authentication. Binary authentication has only two results: successful authentication with access to the application or unsuccessful authentication with no access to the application. An alternative approach is to check identity signals continuously during application usage.

Continuous behavioral authentication uses a risk engine to capture certain behavioral attributes of a user and compare them to a fuzzy template established from patterns of prior use. This produces a deviation score. If the score is low, the user's identity is considered confirmed. If the score is high, an automated workflow is triggered to authenticate the user through an email message, one-time

password, text message, or similar method. If the score is high enough, the enterprise automatically revokes access and initiates a security event.

Continuous behavioral authentication offers near real-time authentication decisions with a positive user experience and the ability to trigger immediate prevention steps to stop account takeover and fraud. Using machine learning models to match attributes to patterns while the application is in use, continuous behavioral authentication can operate in milliseconds and remain transparent to the user. This approach can be added to other authentication methods or potentially replace them.

6. **Attribute Privacy Protection**

Advances in complex cryptography can allow attributes for digital identity to be protected using a technique called a "lattice." A lattice ensures that the attributes are not accessible by the issuing enterprise or anyone else. This method offers the highest protection of authentication attributes.

7. Digital Identity Federation

Digital consumers should each have a digital identity that is issued once and then accepted by all the digital services they use. This concept would eliminate the multitude of digital identities users have today, all of which vary in strength. Achieving this requires a decentralized identity trust framework. In this framework, user identifiers such as email addresses would be replaced with standards-based, self-owned, interoperable identifiers that can exchange data.

Gaining the full benefit of this approach requires mass adoption, which requires interoperability to avoid burdening users with multiple wallets and identities. Interoperability requires establishing standards to support transferable digital identities between issuers and service providers

Fortunately, the latest standards from W3C, ToIP, DIF, and ADI Association, coupled with maturing distributed ledger technology (DLT) for security, support the development of a workable decentralized identity trust framework.

Conclusion: The Future of Digital Identity

Consumers and service providers recognize that identity is central to the digital experience. That is also why identity is the primary target of threat actors. Unfortunately, today's identity approaches are highly vulnerable to fraud through compromised credentials.

The call to action of this paper is to establish and adopt a new standard that gives individuals the freedom to use one digital identity across all digital services, without the risk of fraud. The interoperability requirements necessitate the establishment of a set of global standards. The members of ADI Association are committed to the challenging work of creating enduring standards to advance authentication capabilities on behalf of the consumer. ADI Association is seeking support from enterprises to participate in the development process by joining as members.

