VIEW POINT

LOOKING BEYOND THE PASSWORD

Infosys®
Navigate your next

Overview

The World Economic Forum indicates that cybercrime is set to cost the global economy $2.9 million every minute in 2020 and approximately 80% of these attacks are password related. In 2019, it was estimated that the average cost of a data breach was $8.19 million. In the long run, it is not just the absolute cost of a data breach, but also the loss of customers' trust that hugely impacts businesses.

To protect the customer's interest and loyalty, businesses invest significant resources in securing "passwords" that can become a single point of failure for enterprises and a favorite vulnerability for malicious hackers. Despite fortifying authentication data (passwords), users still fall prey to various attacks such as phishing, account take over, credential stuffing, password spraying etc. Studies suggest that corporate clients see up to 90% of their login attempts done through malicious attacks. This leads to a 2-fold problem – handling continuous pressure to protect the crown jewels from cyber-attacks and maintaining additional infrastructure capacity to sustain the barrage of spiked authentication requests. The overall cost of password management is on the rise while the cost for adversaries to find the areas of compromise is shrinking.

Although enterprises have deployed complex authentication solutions, they continue to struggle with persistent password related attacks. This has probed the users to think beyond the ubiquitous password. The existing authentication paradigm needs to be disrupted. Be it the seminal need of businesses to transform in-line with Darwin's evolutionary theory of survival of the fittest or the need to provide a remedial solution for the weakest link in the authentication chain, it's important that in the cyber transformational journey, new models of authentication protect digital infrastructure.

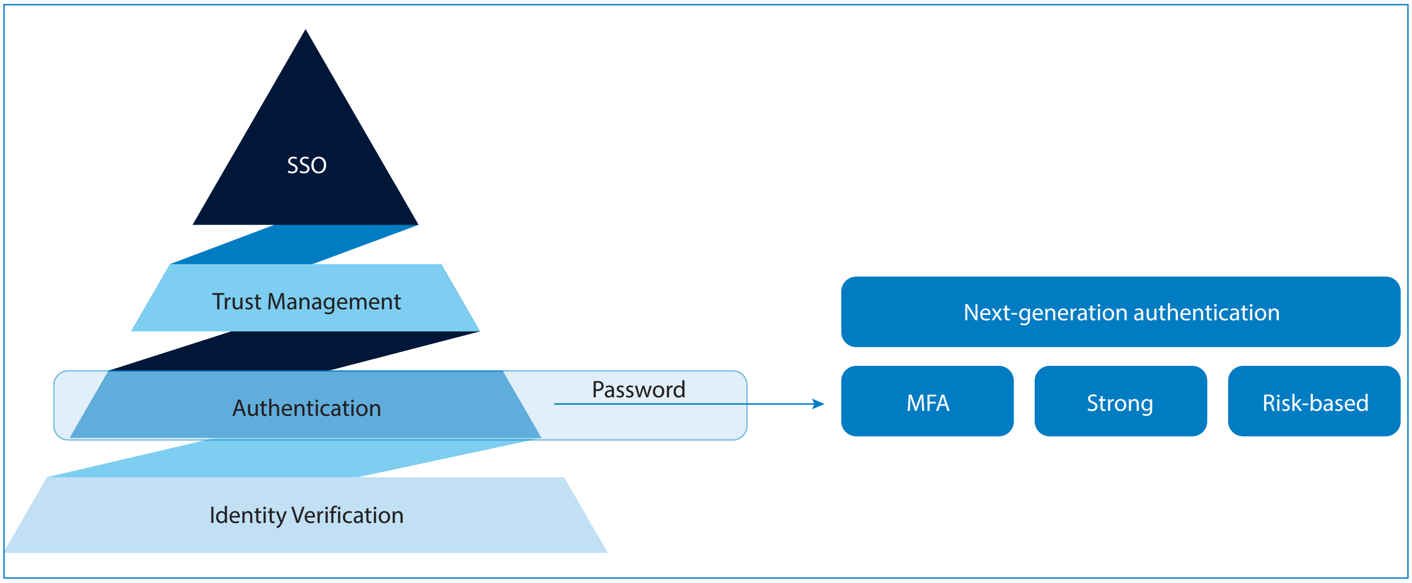


Figure 1: Pyramid of authentication

Current framework for authentication

Authentication has always been an integral part of biological life. Human beings relate to each other by way of proving they are who they claim to be. In the digital world too, a similar concept applies wherein the digital identity proves to an authenticator that it is the same entity as it claims. The following steps are constituent for the overall process of authentication

1. **Identity Proofing:** Identifying and establishing the digital persona of an entity. This is done by verification and validation of attributes like name, nationality, date of birth, biometric scans etc
2. **Authentication Credentials:** After identity proofing is complete, the identity is issued with a set of credential(s) that need to be presented to the digital platform for establishing a claim and proving it is the rightful owner of the requested service. This step comprises of multiple factors such as the following out of which one or all can be leveraged by the authentication framework
   a. **Something you know:** Such as password, passphrase or PIN
   b. **Something you have:** Such as a hard token, smart card or mobile phone
   c. **Something you are:** Biometrics such as facial scan, iris scan or fingerprints

Passwords in recent years have been made more advanced by leveraging one or more of the above enumerated authentication factors. To make it contextual and to ensure that run-time identity of the user is established against the prevalent risk factors, additional factors with stronger authentication such as behavior-based access patterns, time of access, geolocation of access, trustworthiness of the network used to access etc. are being leveraged. An aspect of interest in the authentication process is that validation does not have to be absolute, but rather should be sufficient to establish the identity with reasonable trust. Having 100% deterministic evaluation in authentication system will be very expensive as compared to establishing an authentication system with, about, 95% accuracy. This is because, an authentication framework will not always return 100% match and will have a certain degree of false positives associated with it.

One common feature across the existing authentication factors is that they rely heavily on 'shared-secrets'. Shared secrets, like passwords, passphrases and one-time passwords (OTPs), represent digital keys which can be possessed by both the user and a centralized database. Because of this, they have become a common source of data breaches, leading to attacks such as credential reuse, account take over, phishing attacks etc. Thus, there is a need to move away from the concept of shared secrets as they have the strong potential to render businesses vulnerable to frauds, contribute in loss of reputation and high cost yielding breaches.

Need to look beyond a password linked authentication solution

While businesses have moved swiftly to embrace multiple factors of authentication, there are a few underlying problems with legacy multi-factor authentication (MFA) solutions that rely heavily on shared secrets and the use of passwords

a. **MFA for desktops is not prevalent:** While MFA is adopted for accessing applications through remote login or VPN based access, the existing MFA solutions do not considerably address the weak authentication issues linked with desktops. Enterprises are also of the view that enforcing the use of complex passwords along with MFA can cause delay in login (productivity loss) and result in poor user experiences. Procurement of hardware tokens such as smart cards or token generators etc. result in additional costs for the enterprises.

b. **Evolving regulatory standards:** Some regulatory standards such as PSD2 directive for open banking mandate the use of Strong Customer Authentication (SCA) for payment related transactions. While this improves the embracement of MFA in financial services industry, it leaves the ground open for adoption in other segments of the industry.

c. **User experiences:** Users, inherently, want to access digital service quickly with minimum verification. Thus, having multiple factors of authentication can impact user experience.

d. **Online Vs offline:** Many mechanisms of MFA require users to have an active phone number (receive short message over the phone) or active internet connection (push notifications). This can have a bearing on users who may not have access to mobile devices or internet due to work or travel reason(s).

e. **Cost of password management:** Over the years, the cost of password management through helpdesk calls, the complexity of password self-service, sharing of credentials with unauthorized recipients unknowingly, the weaknesses associated with short message service (SMS) delivery etc. has led to an exponential increase in costs of managing password led solutions.

f. **Reuse of password:** Dedicated attacks focused on password based data breaches has led to a situation where the dark web holds a massive repository of account passwords. The tendency of users to use a common password across personal and business accounts leads to a situation where password spraying and account take-over presents a massive challenge to the enterprises.

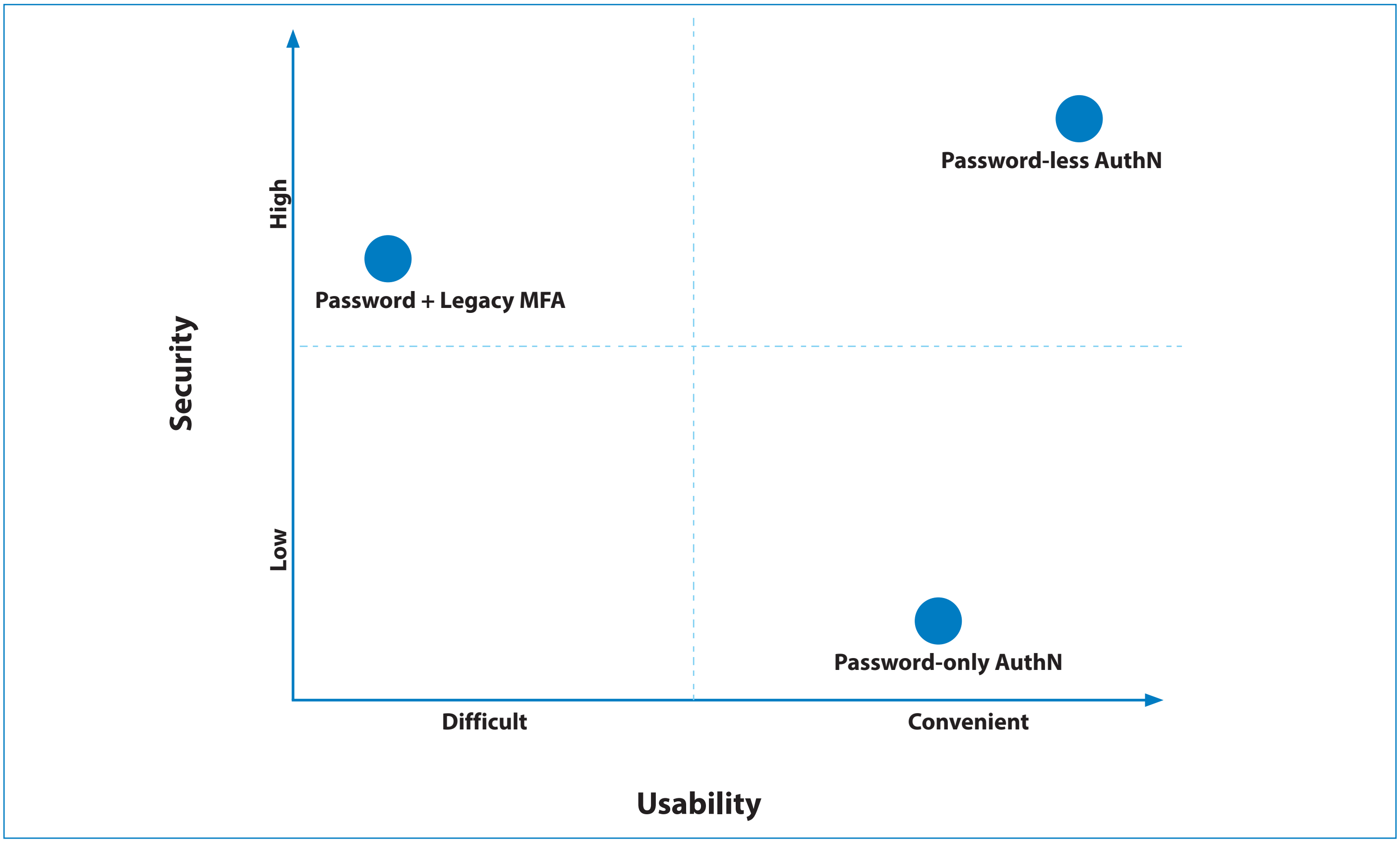


Figure 2: Password-less authentication- Scoring high on security and usability

Characteristics of a next-generation authentication framework

As discussed earlier, there are credible challenges associated with the traditional shared-secret based authentication framework. It is, thus, important to have a robust authentication framework which can address the needs of verification in the future. The authentication framework must be designed keeping in mind that cyber attackers are highly skilled at finding vulnerabilities within the authentication construct. Thus, careful deliberation needs to be applied while building a secure and scalable next-generation authentication framework.

Some of the common characteristics of such authentication framework include:

Characteristic	Key design considerations
Security	• Effectiveness of authentication solution against the known vulnerabilities (shared-secret compromise, phishing etc.) • Ability to cause reduction in risk and fraud management • Capability to integrate with existing SSO/ access management solutions and provide a secure user experience • Avoid account compromises at all lifecycle stages, including continuous authentication after initial authorization • Risks of compromise introduced by the proposed solution • Integration with existing identity and access management solutions • Decentralization of user credentials to minimize the risk of stolen secrets
User experience	• Impact on user experience, including, user access journey, transparent user access management, ease of user experiences • Omni-channel user access and disruption to existing user access patterns • Complexity of installation, administration of solution and user enrollment • Ease of resetting forgotten or lost credentials • Uniformity in user experience without compulsion of being online throughout • Ability to manage false positives
Performance	• Ability to scale the solution for growing customer and workforce requirements without adverse impact on performance • Provision to integrate with open standards of access management (SAML, OAuth, OpenID Connect etc.) • Transition journey from existing authentication solution • Support for web based, mobile native and desktop thick client applications • Options for high-availability and disaster recovery • Scalability for cloud-based and on-premise based solution • Identification and remediation of single points of failure • Ease of integration with existing AI/ ML solutions
Privacy	• Alignment of solution with applicable privacy regulations (e.g. CCPA, GDPR, Australian DPA etc.) • Ability to demonstrate compliance with privacy stipulations across lifecycle stages of identity proofing, consent management, validation & authentication, managing lost/ forgotten credentials etc. • Forward looking capabilities for privacy including delegation control to users for data sharing, improved privacy through data governance, management across different classes of users like VIPs/ admin users etc. • Integration with SOC for security posture monitoring without compromise of user privacy • Sharing information that can be used to collaborate and track a user across different protected applications
Costs	• Justifiable return on investments to balance between enhanced security and user experience • Compatibility with legacy solutions and extent of customizations required for modernization • Ability to manage costs for reputation management of business and reduction in fraud indices • Additional costs to be borne by enterprises, including, external authenticators, authentication server, refactoring of applications etc. • Training and enablement costs across users and administrators for enterprise infrastructure • Ubiquity of solution for interoperability with open standards and on-premise vs cloud applications

The above enumerated dimensions of next generation authentication solution must be tested periodically to ascertain their relevance and acceptability with regards to continuous security posture improvement and addressing business concerns.

Password-less Security –Its working and anatomy

Next generation authentication frameworks are expected to remediate the single largest vulnerability related to data breaches - use of stolen or compromised passwords. This can be achieved by incrementally embracing a 'password-less security' paradigm. Customers, globally, have started to move towards password-less authentication using techniques such as biometrics and public-private key cryptography. FIDO alliance has been spearheading the movement to help move towards a password-free era. Standards developed by FIDO alliance, in conjunction with WebAuthN (adopted by W3C) and CTAP protocol are enabling password-less authentication across enterprise platforms.

Password-less authentication offers to establish an authentication framework that aligns with key characteristics of next-generation validation and verification systems.

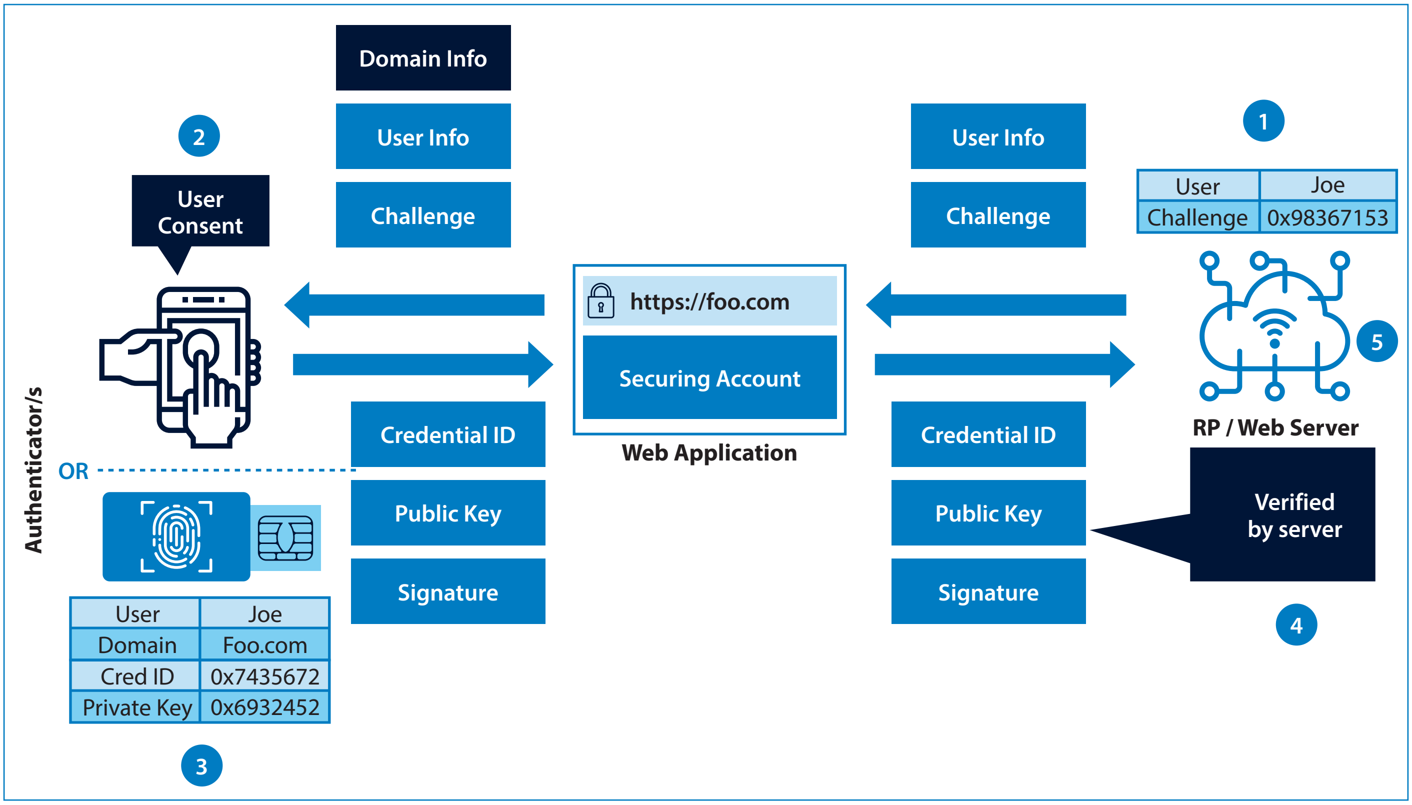
The FIDO standard supports authentication leveraged by public-key cryptography. The public key is shared with service accessed by user, while the private key is held securely within the device or authenticator used by the user. Thus, the private key never leaves the device. Users can authenticate an application supporting FIDO by performing challenge-response to prove possession of the private key. The private keys held by users' device can be accessed only after they are unlocked locally on the storing device, by the user. This local unlock can be done by one of these methods - swiping, entering pin, local biometrics scan, inserting a key etc.

Password-less authentication inherently implements multi-factor authentication, comprising of the following two factors:

1. Something you have- The authenticator is linked to a particular device which is in custody of the user
2. Something you are- A biometric scan used to unlock the device and link private key with the authenticator

The 2 steps involved in enabling users to access password-less enabled service include:

a. User registration:



User	Joe
Challenge	0x98367153

User	Joe
Domain	Foo.com
Cred ID	0x7435672
Private Key	0x6932452

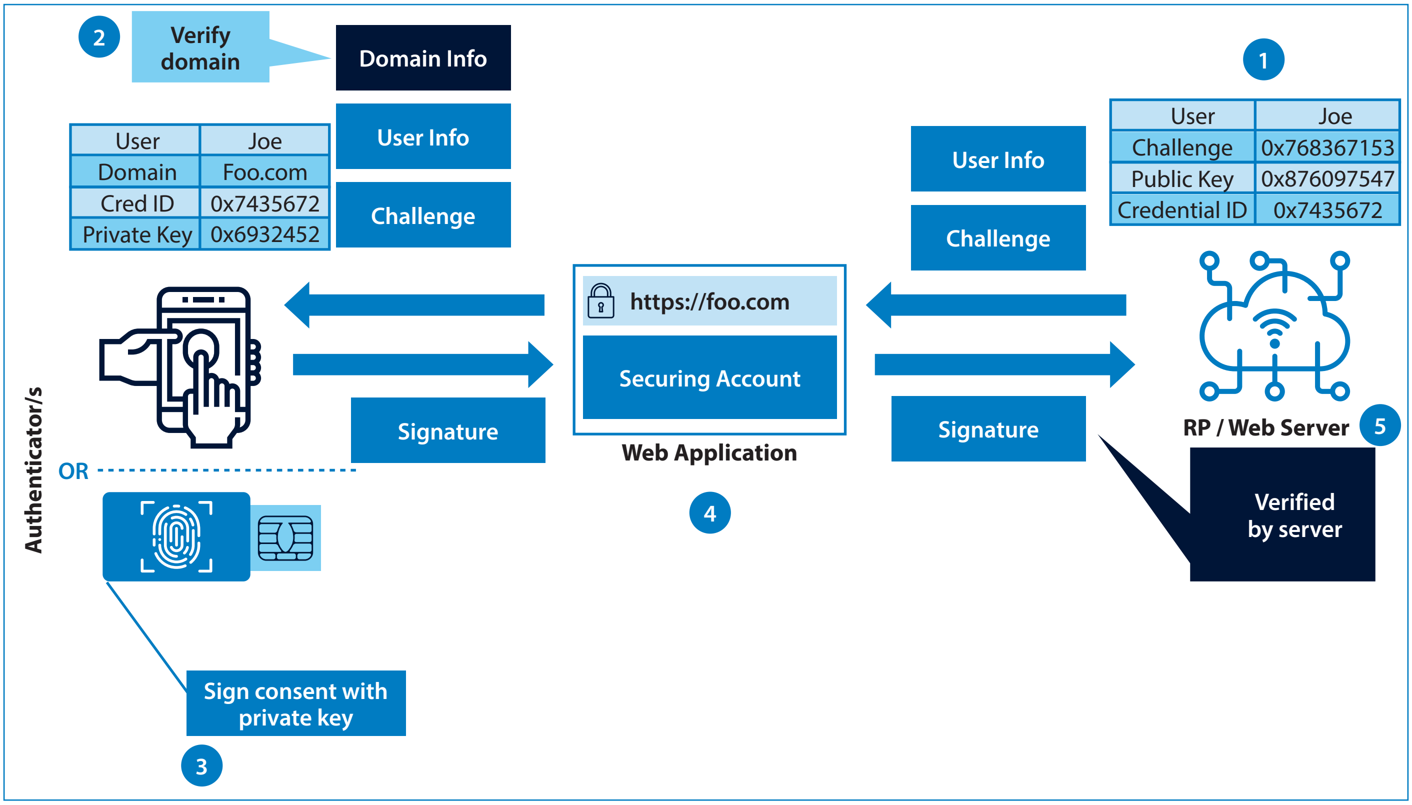
Figure 3: User registration flow

When a user registers credential to a website (referred to by WebAuthN as the "Relying Party"):

1. It obtains the public key. The WebAuthN Relying Party initiates a WebAuthN registration flow – it sends the very basic public user information along with a onetime challenge
2. Upon receiving the registration request, authenticator (External or platform based (Fido2)) now signs an attestation statement with its attestation private key – this is also called trusting the service with user consent
3. The signed attestation statement contains a copy of the public key that the WebAuthN Relying Party ultimately uses to verify a signed authentication assertion, credential id mapped for user account and signature calculated over the given challenge
4. The WebApp then forwards this information to the Relying Party server
5. RP digitally verifies the signature and stores the public key and associated credential id for the user account in the server

It may be noted that since authentication keys are now held locally on user's device, attackers tend to shift their focus on the device ecosystem. Thus, it is essential to store the private keys in a trusted area of the device. For example, in mobile trust zone such as iOS Secure Enclave (SE) or Android's Trusted Execution Environment (TEE).

b. User authentication:



User	Joe
Domain	Foo.com
Cred ID	0x7435672
Private Key	0x6932452

User	Joe
Challenge	0x768367153
Public Key	0x876097547
Credential ID	0x7435672

Figure 4: User authentication process

When a website needs to obtain proof that it is interacting with the correct user,

1. The Relying Party generates a challenge and supplies the browser with a list of credentials that are registered to the user. It can also indicate where to look for the credential, e.g., on a local built-in authenticator, or on an external one over USB, BLE, etc.
2. The browser asks the authenticator to sign the challenge, with verification of domain from where the request is coming
3. If the authenticator contains one of the given credentials, associated domain, the authenticator returns a signed assertion to the web app after receiving user consent
4. The web app then forwards a signed assertion to the server for the Relying Party to verify
5. Once verified by the server, the authentication flow is considered successful, and the challenge gets invalidated

The interoperability standards supported by FIDO allow service providers to integrate applications with public APIs and eliminate dependency on passwords. WebAuthN is the FIDO2 standard which enables the web application to communicate with authentication server for password-less authentication.

TAL

How does Infosys help customers with adoption of password-less framework?

Infosys can help customers with the adoption of scalable open standards for password-less authentication, evaluation and implementation of additional processes such as assessment of password-less technology vendors, defining user journeys, building user experiences, aligning with stakeholders for ROI/ business case definition, execution of proof of concepts and creating strategic roadmap for migration to a password-less authentication framework.

Approach for transitioning to the password-less authentication framework

Infosys recommends a structured approach for customers to move to a password free era. This includes evaluation of a diverse set of technology solutions and outlining of processes to structure the transition approach aligned with the enterprise's landscape, application footprint, IT security priorities and business objective. The process involves:

1. Current state analysis

In this step, we gather data on:

- Enterprise's online access channels (web portals, mobile devices used etc.);
- Online services used (e.g. External facing portals, internal facing applications etc.);
- Total number of users accessing the services
- Number of users registered for external facing applications
- Existing pain points, including user experience journeys, password reset experience
- Feedback from focused groups (customer and enterprise workforce) on password-less authentication, including readiness to move to biometrics-based authentication, user experiences with existing user login flows etc.
- Applicability of regulatory standards vis-à-vis compliances and privacy management and existing work done for alignment with the same

2. Defining target state architecture

In this step, we work with enterprise security leaders to:

- Define the blueprint for password-less authentication framework
- Identify technology providers suitable for the enterprise strategic directions
- Identify the technology changes required for applications to transition to password-less framework
- Identify the touchpoints/ dependencies across enterprise for the transition and define plan for initiating discussions with the identified groups
- Identify a pilot application to perform proof of concept for migrating to password-less framework
- Define user stories and journey flows for user registration, migration and remediation of application to password-less framework

As a best practice, we recommend customers to migrate to password-less framework in a phased manner. It includes enabling the option for password-less sign-in in conjunction with the existing password-based authentication. This, however, is vulnerable to phishing attacks until migration is carried out to password-less authentication framework.

3. Comparative analysis of technology providers

In this step, we work with a selected set of technology providers to perform technology evaluation:

- Normative analysis of FIDO compliant technology providers vis-à-vis the determined characteristics of next generation authentication framework
- Identifying technology providers across open source and commercial vendors
- Identifying providers with native plugins available for standard access management solutions such as PingIdentity, Okta, MS Azure, OneLogin, IBM Security Access Manager etc.
- Determining ease of integration with existing identity lifecycle management framework and processes for management of lost credentials
- Weighted average score calculation for capabilities including, membership of FIDO alliance, SaaS offering, ability to host in private cloud, rollout timelines, existing product maturity, scalability for number of users, availability of product documentation, support available for integration with existing enterprise online applications, availability of SDK for customization and product capability extension, ease of integration with 3rd party applications including MS applications, SAP applications, Oracle applications etc.

4. Executing Proof of concept

Post completion of technology design and product analysis, Infosys recommends executing a proof of concept for an identified set of applications. The pilot proof of concept should be done with:

- Limited set of use cases that cover the key flows for user registration and login
- Demonstration of high availability and scalability
- Benchmarking against the commonly known password related vulnerabilities like phishing, account take over, credential stuffing etc.
- Identifying budgetary estimates for the strategic rollout

5. Strategic phase implementation

In this step, we execute project phases for setting up of password-less authentication framework, defining lifecycle management use cases and executing tasks for structured onboarding of applications onto the strategic solution defined for the enterprise.

Conclusion

Authentication solutions have predominantly been focused on the use of password as a primary factor of verification. However, this has resulted in many issues such as loss of customers, complex authentication approaches and data breaches caused by the inherent vulnerabilities associated with the passwords. This strengthens the logic that the need for a next-generation authentication framework is imperative and enterprises must look at leveraging password-less authentication framework as one of their near term objectives. While the newer technologies related to cloud adoption, federation, zero-trust framework, privacy regulations etc. will have a deciding bearing on the future of authentication paradigm, the need to move away from passwords is certainly the immediate mandate for a cyber-secure future.

Authors

Mohit Jain
Principal Technology Architect
Mohit_Jain01@infosys.com

Nitin Bajpai
Principal Consultant
nitin.bajpai@infosys.com

Rajinder Rathor
Principal Consultant
Rajinder_Rathor@infosys.com

For more information, contact askus@infosys.com

Infosys®
Navigate your next