Passkeys and WebAuthn

Revolutionizing Authentication with the Passwordless Technology

Edited by **C.J. ANTONY**

In today's digital era, securing online identities is more critical than ever. Traditional password-based authentication systems are increasingly vulnerable to cyber threats such as phishing, credential stuffing, and brute-force attacks. In this context, Passkeys and WebAuthn represent transformative advancements poised to redefine authentication paradigms.

What is WebAuthn?

Web Authentication (WebAuthn) is a core component of the FIDO2 (Fast IDentity Online) standard, developed by the FIDO Alliance and the World Wide Web Consortium (W3C). WebAuthn eliminates the reliance on passwords by leveraging public key cryptography. It allows users to authenticate using more secure methods, such as biometrics (fingerprint or facial recognition) or hardware security keys.

At its core, WebAuthn works by:

- Generating a unique key pair (public and private keys) for every service or application.
- Storing the private key securely on the user's device.
- Sending the public key to the server for authentication.

The server never has access to the private key, reducing the risk of credential theft during breaches.

The Rise of Passkeys

Passkeys build upon the WebAuthn standard to create a seamless, user-friendly authentication experience. A passkey is a passwordless credential tied to a device and secured through biometric or PIN-based verification. It eliminates the need for users to remember complex passwords while maintaining robust security.

Passkeys work by synchronizing between devices via cloud storage—like Apple's iCloud Keychain or Google Password Manager—ensuring accessibility across platforms while maintaining strong encryption and privacy controls.

Passkeys and WebAuthn are revolutionizing digital authentication by eliminating passwords and enhancing security. WebAuthn, a FIDO2 standard, uses public key cryptography for secure authentication, storing private keys on devices and preventing phishing and credential theft. In Kerala's Entebhoomi Integrated Land Information Management System (ILIMS) project, passkeys are integrated into the Single Sign-On (SSO) system to ensure secure access to land-related services. With stringent measures like single-passkey registration per user and OTP-based verification, the system balances usability and robust security. As global adoption grows, these technologies promise a safer, passwordless future for digital interactions.

Why Passkeys and WebAuthn?

Enhanced Security

- **Protection Against Phishing:** Passkeys and WebAuthn are resistant to phishing attacks because they rely on domain-bound credentials that cannot be reused on malicious websites.
- **Elimination of Passwords:** By removing passwords entirely, these technologies mitigate risks from weak, reused, or compromised credentials.

Improved User Experience

- **Ease of Use:** Users no longer need to create or remember passwords. Authentication becomes as simple as scanning a fingerprint or using facial recognition.
- **Cross-Platform Support:** Passkeys work seamlessly across devices, making the user experience consistent and hassle-free.

Compliance and Privacy

- WebAuthn is designed to comply with global data protection regulations. User credentials are stored locally on devices, ensuring privacy and reducing centralized storage risks.

Devices Compatible with Passkeys

Passkeys are compatible with a wide range of modern devices equipped to handle FIDO2/WebAuthn standards. Smartphones, particularly Android and iOS devices, are highly feasible due to their robust security features, including secure hardware like Android's Secure Element and iOS's Secure Enclave for storing cryptographic keys. These devices also feature built-in biometric authentication, such as fingerprint or facial recognition, enabling seamless, secure, and user-friendly passwordless authentication. In addition to smartphones, tablets and laptops with secure hardware (e.g., Secure Enclave, TPM) and biometric capabilities are common choices. Dedicated physical options like hardware security keys (e.g., YubiKey, Google Titan) provide enhanced security for sensitive environments. Furthermore, desktops with compatible biometric devices and cloud-based platforms like iCloud Keychain and Google Password Manager extend passkey functionality, offering cross-platform synchronization and accessibility for modern digital interactions.

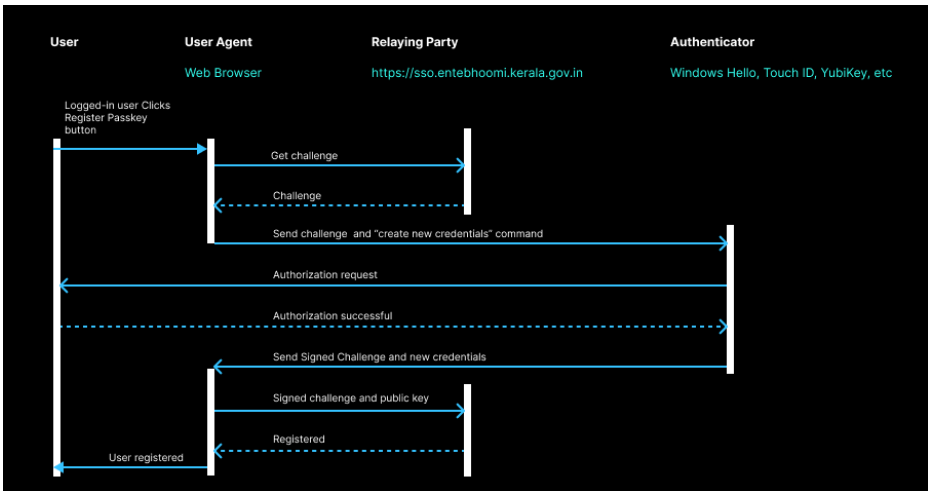
Syamkrishna B.G.
Scientist-C
syam.krishna@nic.in

Amiya Manayath
Scientist-B
amiya.m51@nic.in

Key Components in Passkey Authentication

Passkey authentication involves four critical components working seamlessly together: the user, user agent, relying party, and authenticator.

- **User:** The individual who initiates the authentication process by interacting with a service or application. The user provides a biometric input (e.g., fingerprint or facial recognition) or a PIN to verify their identity.
- **User Agent:** This is typically the web browser or application acting as an intermediary between the user and the service. Popular user agents include browsers such as Google Chrome, Microsoft Edge, Mozilla Firefox, and Apple Safari. The user agent handles communication with the relying party and interacts with the authenticator to facilitate secure authentication. These web browsers provide built-in support for WebAuthn through JavaScript APIs. These APIs enable seamless integration of passwordless authentication into web applications, allowing developers to securely register and authenticate users using Passkeys.
- **Relying Party:** The service or application requesting authentication (e.g., a government portal like Entebhoomi). The relying party stores the public key generated during passkey registration and uses it to verify the user's authentication response.
- **Authenticator:** The device or system that securely generates and stores cryptographic keys. Examples include:
  - **Built-in Authenticators:** Modern devices such as iPhones, Android smartphones, Windows laptops (with Windows Hello), and macOS devices (with Apple Secure Enclave) that securely handle authentication.
  - **External Authenticators:** Hardware security keys like YubiKey, Google Titan Key, or Feitian keys that connect via USB, NFC, or Bluetooth.
  - **Cloud-based Authenticators:** Services like Apple's iCloud Keychain, Google Password Manager, and Microsoft Authenticator that enable synchronized Passkeys across multiple devices.



▲ Fig 11.1: Diagram illustrating the Passkey Registration process

These components, supported by industry leaders like Apple, Google, and Microsoft, work together to deliver a seamless, secure, and passwordless authentication experience. This ensures robust security while maintaining ease of use for end users in modern digital interactions.

Use Case: Passkeys in the Entebhoomi, the Integrated Land Information Management System Project

The Ente Bhoomi Project, spearheaded by the Government of Kerala, aims to modernize and digitize land-related services across the state. As a part of the Integrated Land Information Management System (ILIMS), it integrates and streamlines services from the Survey, Registration, and Revenue Departments. Leveraging advanced technologies, the project provides citizens with seamless access to land records, digital survey services, and real-time updates on land activities.

A key innovation in the Entebhoomi Project is its integration of passkeys to enhance both security and user experience. The project employs an in-house developed Single Sign-On (SSO) system, connecting the Survey, Registration, and Revenue Departments. This SSO facilitates secure user authentication using passkeys.

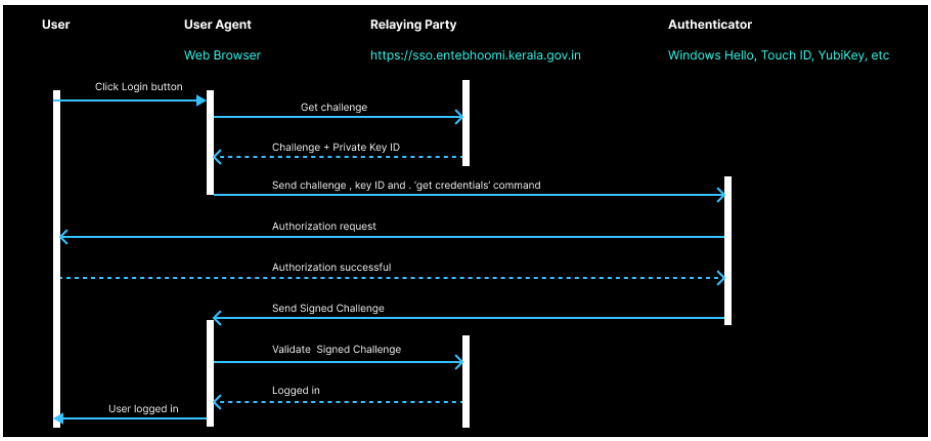
To address the critical security needs of government applications, the implementation of passkeys adheres to strict measures. Authentication is restricted to the specific passkey registered for the user within the application. The registration process is further secured through OTP verification, ensuring that only the rightful user can complete it. These comprehensive safeguards establish a robust framework for secure and efficient access to digital services.

Conclusion

The transition to Passkeys and WebAuthn in eGovernance systems marks a paradigm shift, promising a future where citizens can interact with public services securely and effortlessly. These technologies offer governments the ability to safeguard sensitive data, enhance user trust, and reduce operational costs, making them a vital component of modern digital strategies.

As governments and organizations increasingly embrace passwordless authentication, they pave the way for a secure, transparent, and citizen-centric digital ecosystem. Passkeys and WebAuthn are not just technological advancements but strategic investments that ensure resilience in an interconnected and threat-prone world. By adopting these solutions today, eGovernance systems can position themselves at the forefront of the digital revolution, delivering unparalleled value to citizens and stakeholders alike.

▼ Fig 11.2: Diagram illustrating the Passkey based authentication process



Contact for more details

Manoj P. A.
Sr. Technical Director
NIC Kerala State Centre
CDAC Building, Vellayambalam
Thiruvananthapuram, Kerala - 695033
Email: manoj.pa@nic.in, Phone: 0471-2724529