ePAPER

APCI FEDERAL CREDIT UNION

Passkeys

A new, more advanced way to authenticate

What is a Passkey?

A passkey is a modern form of multifactor authentication that combines public key cryptography with biometrics, such as fingerprint and facial recognition or a device PIN to verify a user's identity. They do this by securing a digital credential stored on a trusted device that allows users to sign in without a traditional password.

Passkeys are designed to replace traditional passwords with a more secure and streamlined authentication method.

Why Use a Passkey?

Before passkeys were introduced, most multifactor authentication (MFA) methods relied on passwords in combination with secondary verification tools, such as one-time codes sent through authentication apps or text messages. Passkeys eliminate the need for traditional passwords and add additional authentication steps by allowing users to securely sign in using a trusted device.

Unlike passwords, passkeys are unique to both the individual user and their device, making them significantly more difficult for cybercriminals to compromise. As a result, many organizations are transitioning from password-based authentication to passkeys to strengthen access control and improve overall cybersecurity.

Passkeys provide stronger security, support compliance requirements, and add an additional layer of protection through device-based verification. With phishing attacks and data breaches becoming increasingly common, passkeys represent a significant advancement in secure authentication technology.

How Does a Passkey Work?

Passkeys are built on public key cryptography, a technology that has long been used to secure websites and online communications.

Public key cryptography uses two separate keys:

- A public key used for encryption
- A private key used for decryption and authentication

This approach enables secure communication without requiring an exchange of sensitive credentials beforehand.

When used for authentication, a passkey confirms that the user's device contains the correct cryptographic key required to access the account. Biometrics or a device PIN verify that the authorized user is in possession of the device.

Passkey Compatibility and Integration

Passkeys are supported across a growing number of devices and operating systems. Major technology providers such as Microsoft, Google, and Apple have integrated passkey support into their platforms and services.

You can use passkeys to protect accounts across many devices, including:

- Windows devices
- iOS 16+ iPhones and iPads
- macOS 13+ computers
- Android devices

Passkeys can also be integrated into existing security infrastructures, allowing organizations to adopt stronger authentication methods without requiring major system changes.

Security Benefits of Passkeys

Even with strong password protections, passkeys provide important security advantages over traditional passwords. Below are a few benefits.

Physical Device Verification

Since passkeys are unique to both the user and device, they are extremely difficult for attackers to guess, steal, or replicate. Even if a passkey were somehow compromised, the attacker would still need physical access to the associated device to use it.

Enhanced Protection Against Phishing

Passkeys are highly resistant to phishing attacks because authentication relies on the possession of a trusted device rather than a password that can be entered anywhere.

Even if a user unknowingly interacts with a phishing attempt, an attacker cannot gain access without the physical device containing the passkey.

Therefore, passkeys can significantly strengthen login, email, and overall security.

Reduced Risk of Account Takeover

The combination of device-based authentication and biometric verification significantly reduces the risk of account takeover compared to traditional password-based methods.

Compliance With Security Standards

Passkeys often meet or exceed security standards required in regulation with industries such as finance, healthcare, and government. Passkeys have a robust security framework that makes them well-suited for protecting sensitive information.

Secure Account Recovery

Traditional account recovery often requires password resets or additional authentication steps. Passkeys can be securely synchronized across trusted devices, allowing users to regain account access from another registered device if one is lost or replaced.

Passkeys in APCI eBanking

Users can register for Passkeys within the User Settings menu on desktop or the Settings menu on mobile devices. To begin setup:

1. Log into APCI eBanking
2. Navigate to Security
3. Select the Authentication tab
4. Click the “Register for MFA via Passkey” button

Once enabled, rather than providing a one-time passcode response for an MFA request, users will be able to utilize their passkey to approve the MFA. For example, if using TouchID on an Apple device the user would need to provide a fingerprint to approve the MFA.

Users must first register a Passkey before they can begin to enable Passkeys for MFA. Options to enable Passkeys for MFA will be grayed out until a passkey is registered. A tooltip will display if the user hovers over it or selects indicating “At least one Passkey device is required.”

For more information, users can access our **APCI eBanking Guide to Enrollment and Features** to learn more about Passkeys and how to implement them.