QUICK GUIDE

Getting Started With Passkeys

Crawl, Walk, Run

HYPR

What Are Passkeys?

/ˈpasˌkēs/
noun

Based on FIDO standards, passkeys are a replacement for passwords that provide faster, easier, and more secure sign-ins to websites and apps across a user's devices. Unlike passwords, passkeys are always strong and phishing-resistant.

Passkeys simplify account registration for apps and websites, are easy to use, work across most of a user's devices, and even work on other devices within physical proximity.

> "[We've] known that at some point "traditional MFA" would become "legacy MFA" and need to be reassessed or even replaced... I urge every CEO to ensure that FIDO authentication is on their organization's MFA implementation roadmap."
>
> **Jen Easterly**
>
> Director, CISA

Flavors of Passkeys

SYNCED PASSKEY

- A FIDO2 credential that's synced to a user's devices. Can be shared with others using Airdrop or a QR code.
- Passkey syncing between devices is via your iCloud, Google, or Microsoft accounts.
- Passkeys are not copied between different platforms (e.g. iCloud ⇒ Google).

DEVICE-BOUND PASSKEY

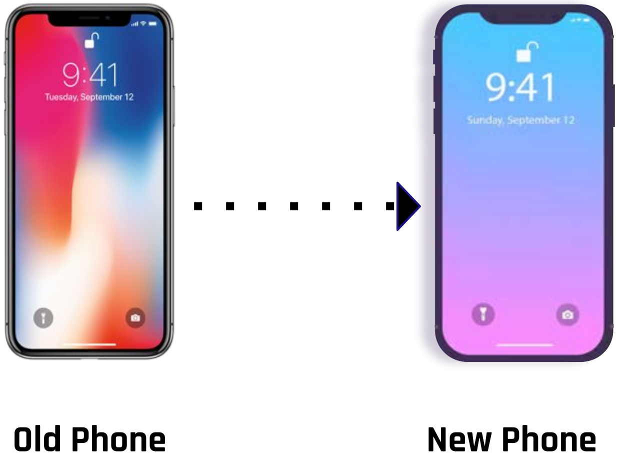
- A FIDO2 credential that stays on a user's device on which it was created. Largely supported by Apple (iOS), Microsoft, and Google (Android).
- Can be used on the device's mobile apps and browsers that support the WebAuthn/CTAP APIs.
- Not automatically synced to your other devices.

APP-LEVEL PASSKEY (fka FIDO UAF)

- Like a device-bound passkey but dedicated to a specific mobile app and not provided by the platform (Google, Microsoft, Apple). Mobile browser capability is unavailable with this type of credential.
- Passkey is not managed by Google, Microsoft, Apple.
- Useful for high value transactions but limits UX.

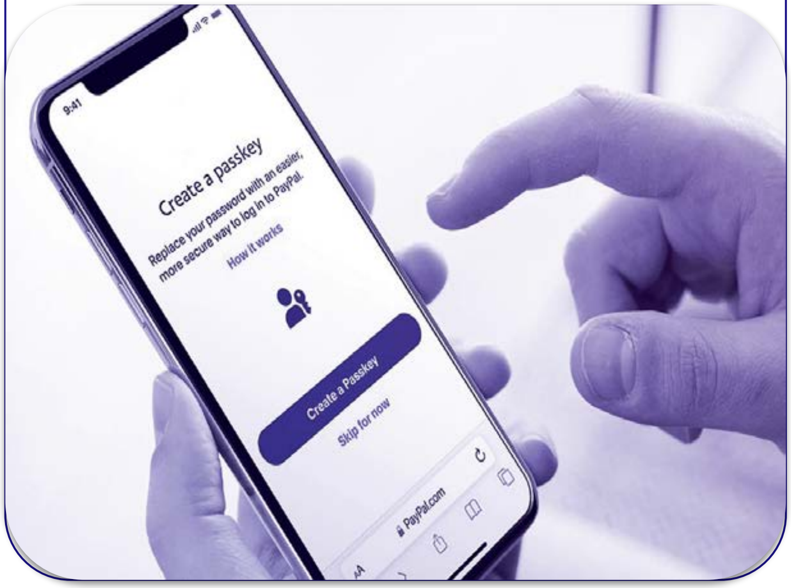
Top Two Benefits of Passkeys

1. **Password management headaches virtually go away**



Users no longer need to enter a password when they get a new phone. This solves a major UX problem.

1. **Fastest & easiest way to reduce ATO Fraud by way of phish-resistant authentication.**


9:41

Create a passkey

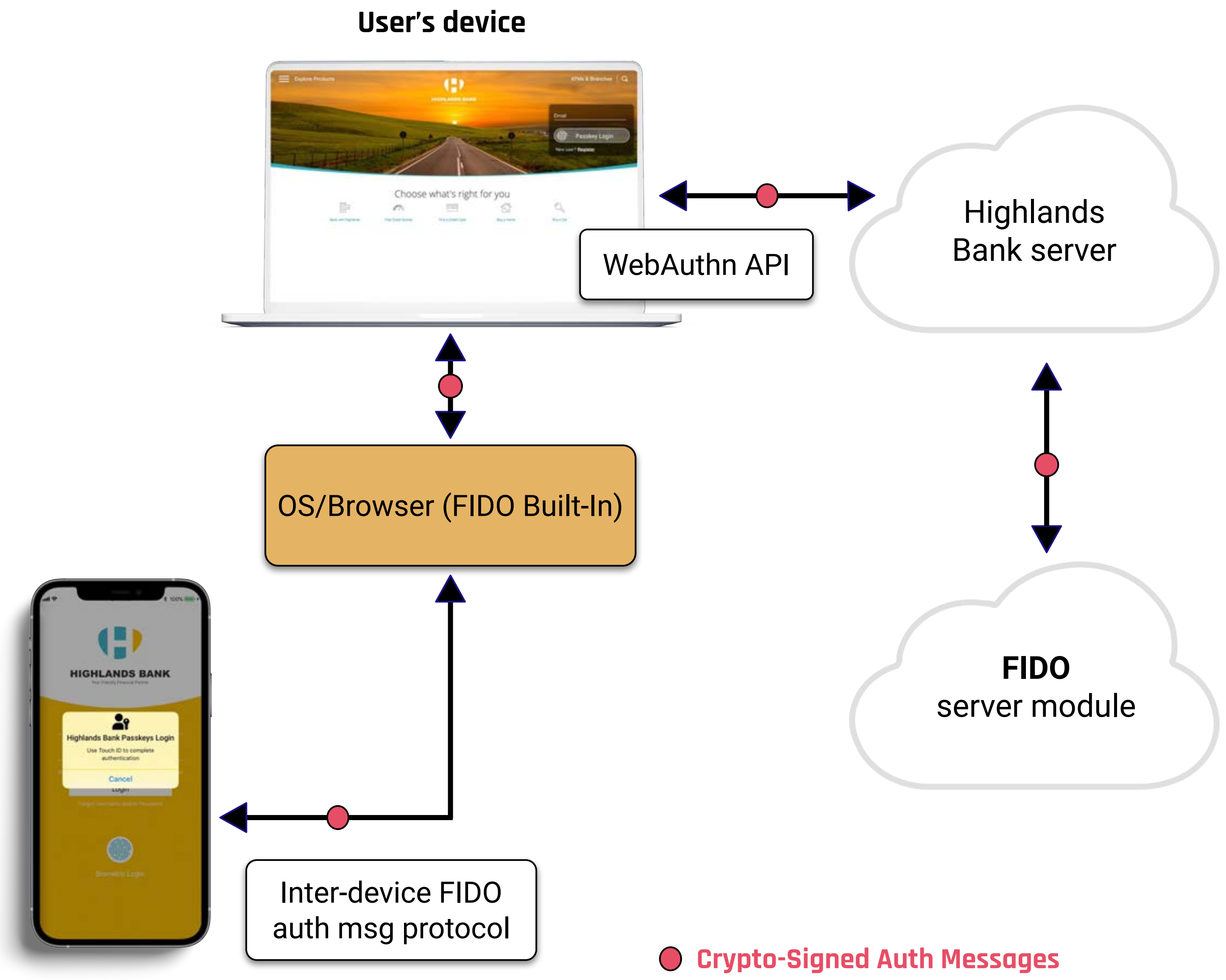
Replace your password with an easier, more secure way to log in to PayPal.

How it works

Passkeys & Phishing Resistance

FIDO Ensures:

- ✓ Right user present
- ✓ No phisher in the middle


User's device
Choose what's right for you
Passkey Login
WebAuthn API
Highlands Bank server
OS/Browser (FIDO Built-In)
FIDO server module
HIGHLANDS BANK
Highlands Bank Passkeys Login
Use Touch ID to complete authentication
Cancel
Inter-device FIDO auth msg protocol
● Crypto-Signed Auth Messages

Are Passkeys Considered MFA?

The answer is that it depends. Here's why...

SYNCED PASSKEY

- Automatically synced across Apple/Google/MS accounts
- Can be exported and shared by tools such as AirDrop
- Recoverable via Google, iCloud, etc.
- Utilizes OS and browser-based UI

DEVICE-BOUND PASSKEY

- Cannot be exported
- Not recoverable if lost or when users get new devices
- Utilizes OS and browser-based UI

APP-LEVEL PASSKEY

- Support for transaction signing
- Key generation independent of device type
- Support for custom authenticators
- Customizable user experience

Common Passkey Attributes

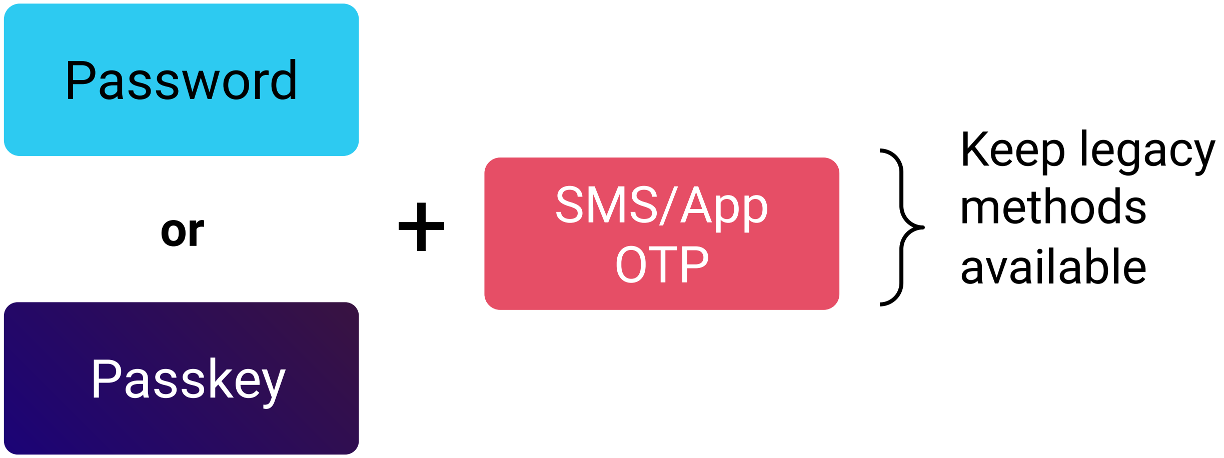
- Bound to Origin
- Cryptographic Key Pair
- Phishing Resistant
- Attestable
- Recoverable via Relying Party

Is It MFA?	SYNCED PASSKEY	DEVICE-BOUND PASSKEY	APP-LEVEL PASSKEY
	No, at least not by itself.	**Yes**	**Yes**

Deploying Passkeys: Crawl

RECOMMENDATION:

Deploy passkeys as an alternative, more user friendly second factor of authentication.

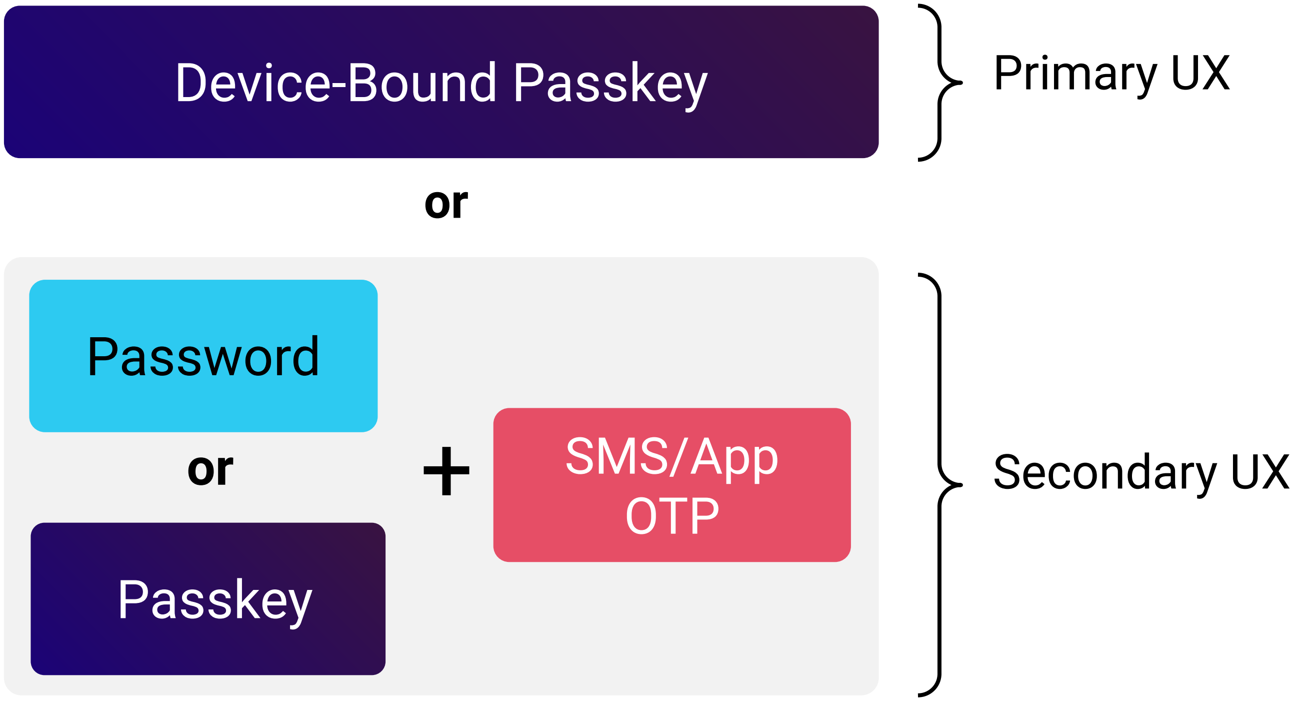


- ✓ Monitor and measure usage of passkeys for 30-90 days carefully.
- ✓ Passkeys will provide a phishing resistant option to users.

Deploying Passkeys: Walk

RECOMMENDATION:

Deploy single device passkeys as alternative, user friendly primary method of authentication.

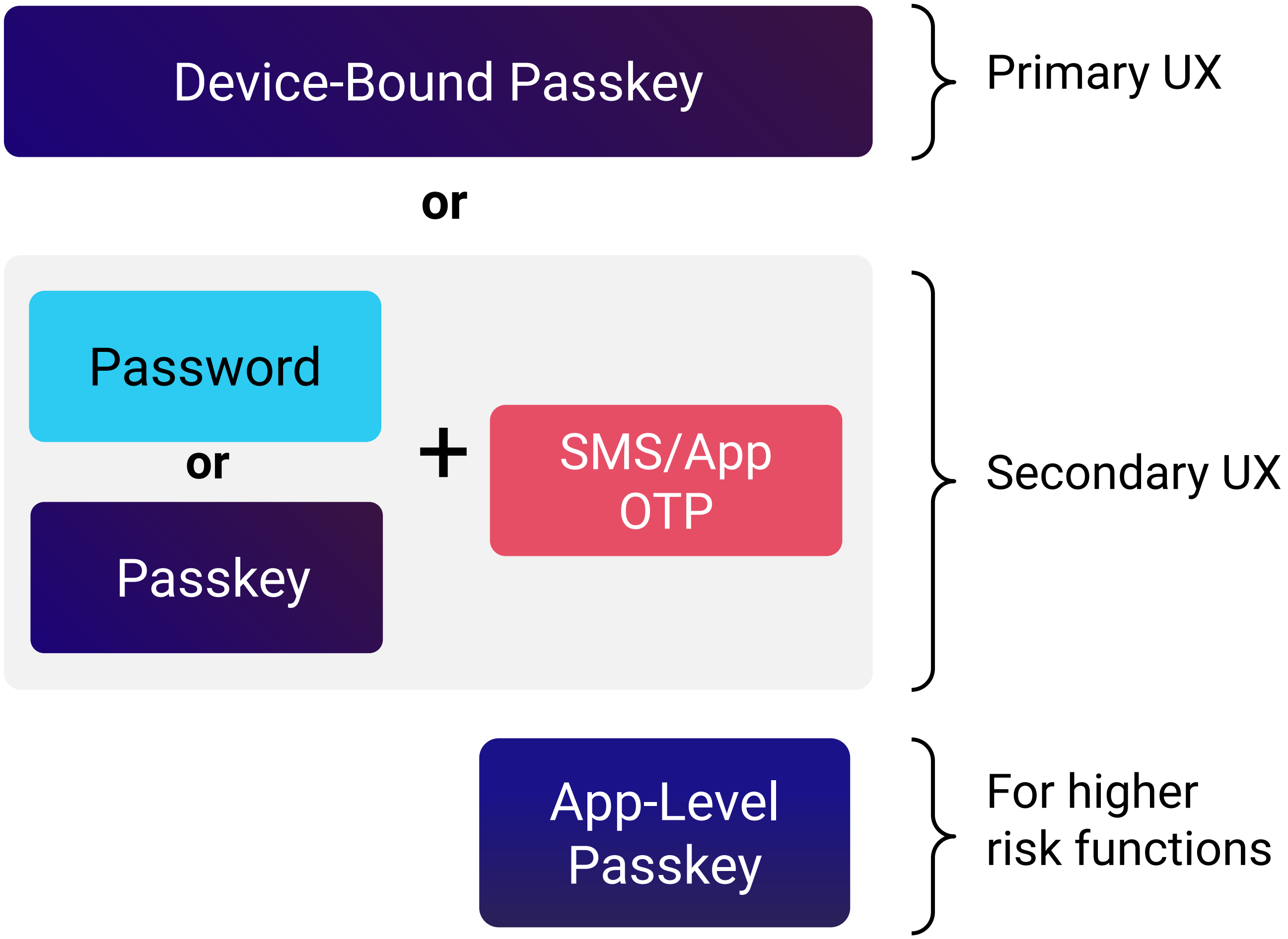


- ✓ Will result in fewer password reset requests to service desk, especially when users get new devices.
- ✓ Users have multiple phishing resistant methods of authentication.

Deploying Passkeys: Run

RECOMMENDATION:

Require phishing-resistant authentication methods and layer in higher assurance credential for high risk transactions.



Device-Bound Passkey

Primary UX

or

Password

or

Passkey

+

SMS/App OTP

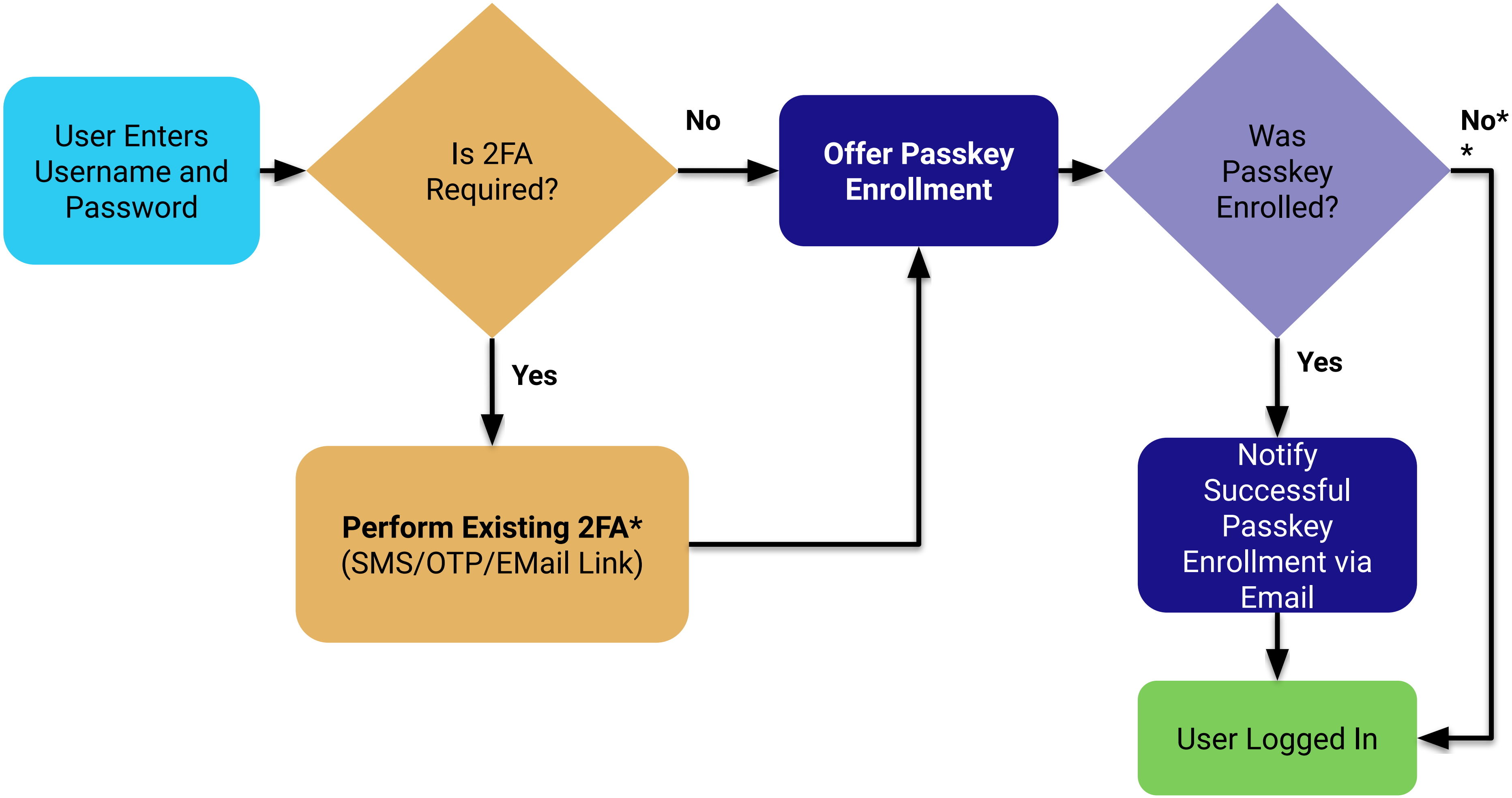
Secondary UX

App-Level Passkey

For higher risk functions

User Flows for Synced Passkeys

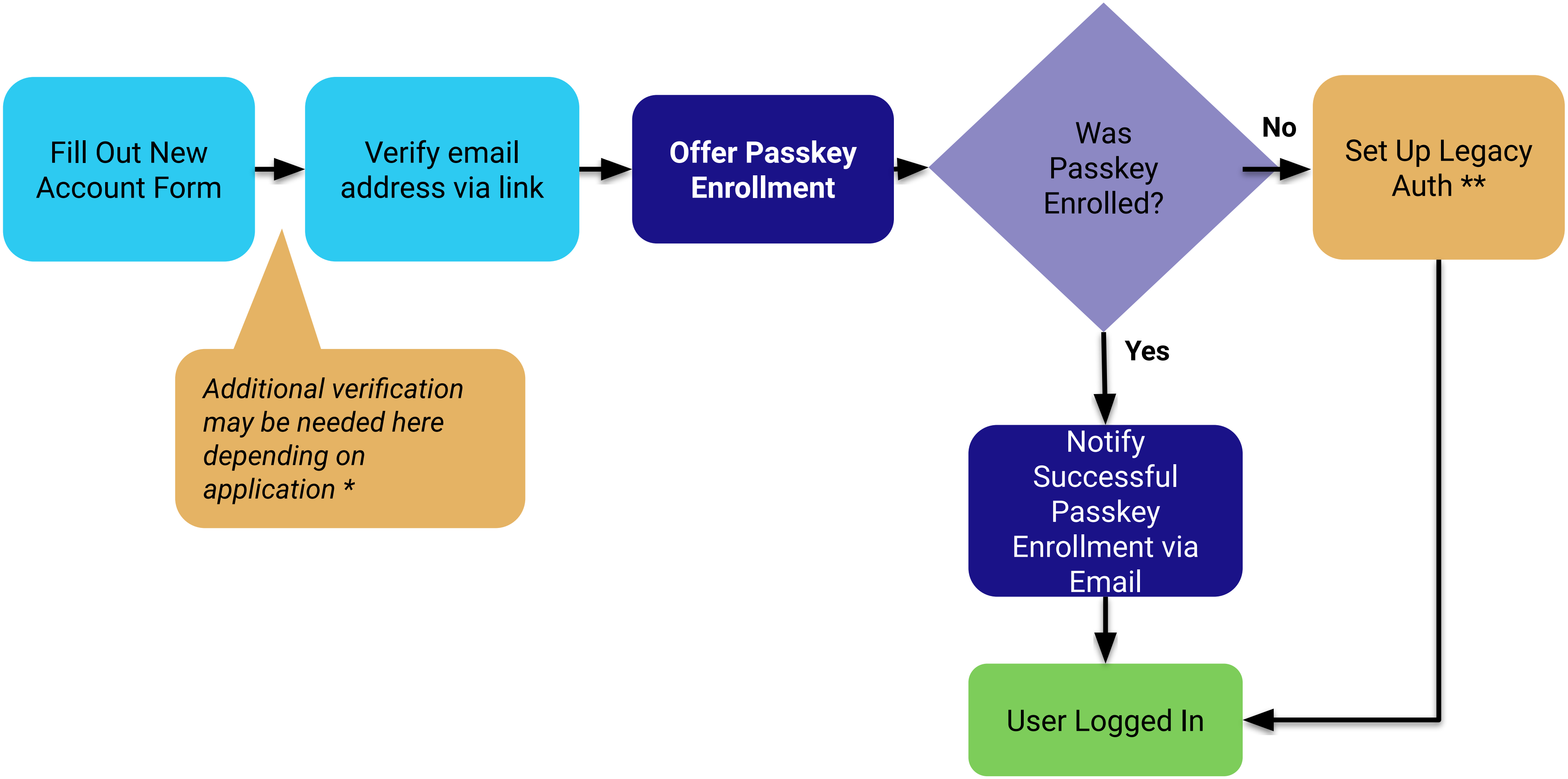
User Flows: Enrolling Synced Passkey for Existing User Account


User Enters Username and Password
Is 2FA Required?
No
Yes
Perform Existing 2FA* (SMS/OTP/EMail Link)
Offer Passkey Enrollment
Was Passkey Enrolled?
No**
Yes
Notify Successful Passkey Enrollment via Email
User Logged In

* Your 2nd factor may differ depending on application type. The most common 2nd factors today are SMS/OTP/email Link. Note that all of these are easy to phish which is why we're adding passkeys!

** If a user does not enroll a passkey, it is helpful to show them a message explaining the value of passkeys.

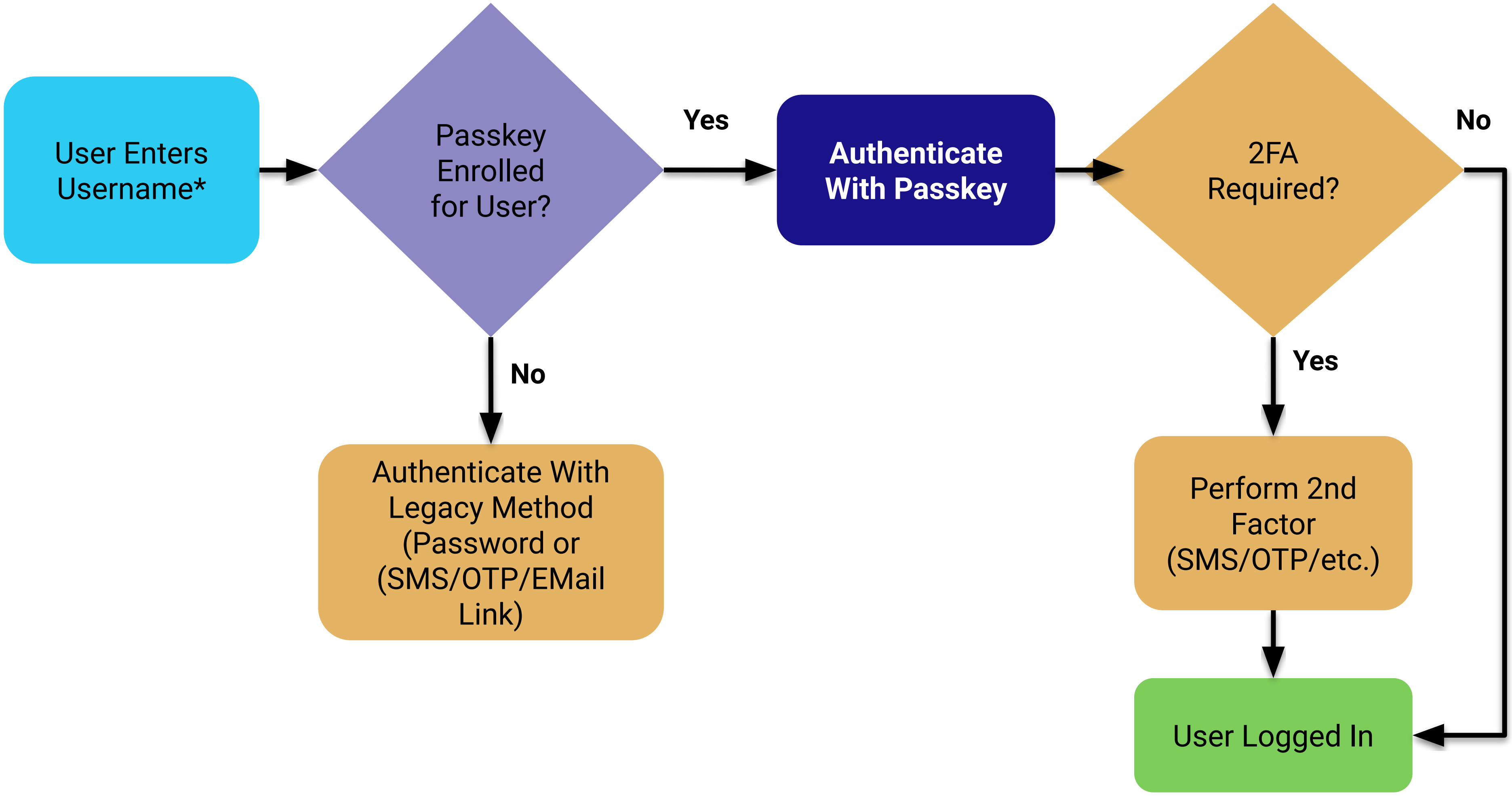
User Flows: Enrolling Synced Passkey for New User Account


Fill Out New Account Form
Verify email address via link
Offer Passkey Enrollment
Was Passkey Enrolled?
No
Set Up Legacy Auth **
Yes
Notify Successful Passkey Enrollment via Email
User Logged In
*Additional verification may be needed here depending on application **

* Many financial services new account flows include additional user verification such as ID scan or even in-person document verification. Other apps such as Uber require users to verify their phone number via SMS. E-Commerce apps usually only require email address verification.

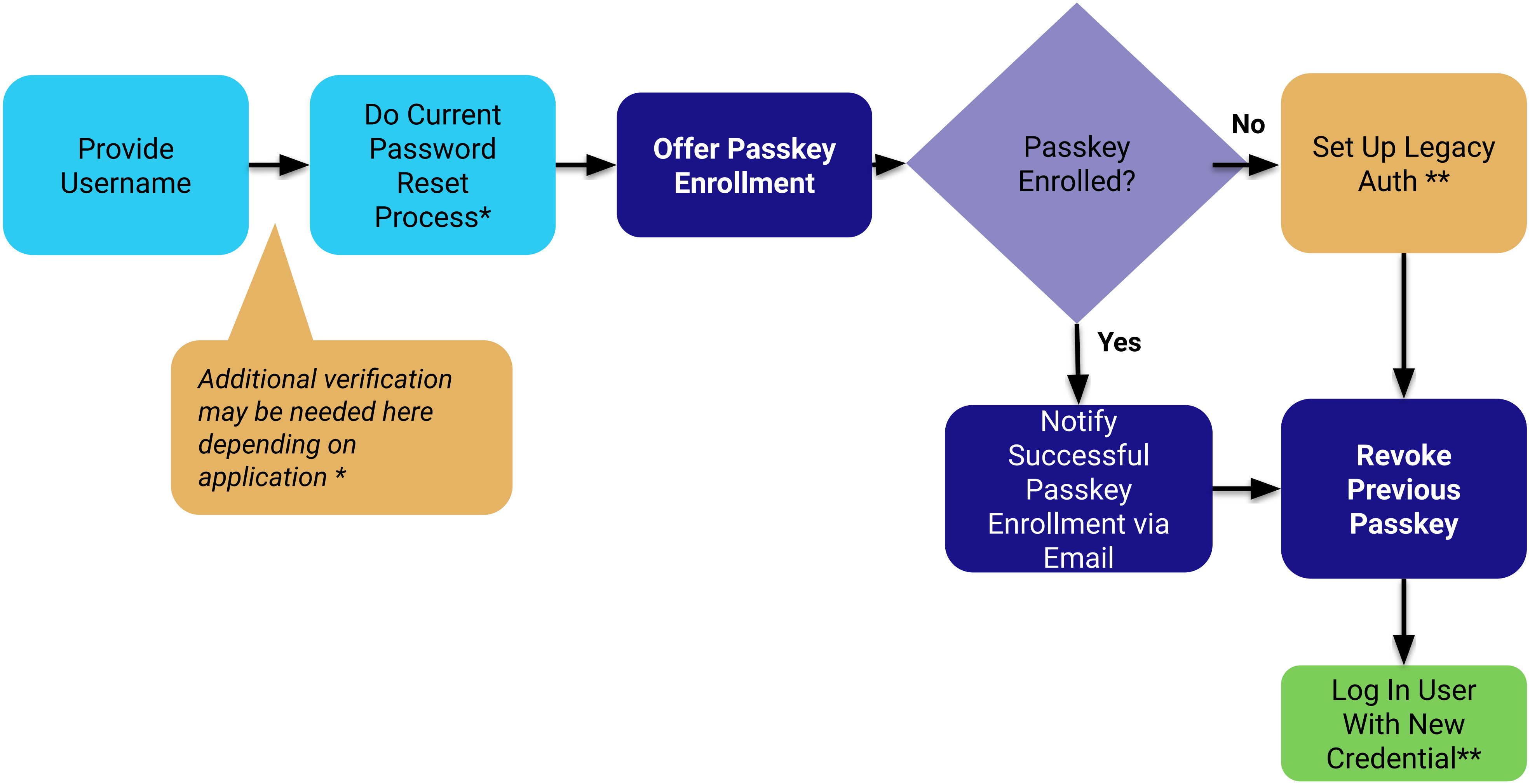
** This would most likely result in the user setting up a password or other legacy and easily phishable authentication factor. It is recommended that once a user enrolls a passkey, that this option goes away.

User Flows: Authenticating With Synced Passkeys


User Enters Username*
Passkey Enrolled for User?
Yes
Authenticate With Passkey
2FA Required?
No
No
Yes
Authenticate With Legacy Method (Password or (SMS/OTP/EMail Link)
Perform 2nd Factor (SMS/OTP/etc.)
User Logged In

* Note that the username is usually remembered by the user's browser so they may not need to enter it if they're coming from a known device. Passkeys can also be invoked without the entry of a username but the experience may vary across platforms.

User Flows: Dealing With Lost Passkeys (Synced)


Provide Username
Do Current Password Reset Process*
Offer Passkey Enrollment
Passkey Enrolled?
No
Set Up Legacy Auth **
Yes
Additional verification may be needed here depending on application *
Notify Successful Passkey Enrollment via Email
Revoke Previous Passkey
Log In User With New Credential**

* Your current password reset process is most likely a email/SMS link. For more critical applications a digital document verification or service desk process may be required.

** The new credential will either be the passkey that was created or the legacy (less secure) method.

HYPR Accelerates Passkeys Deployments

Fortune 10 Healthcare Corporation

1,000,000+

Passkey Users Deployed in 10 Weeks With HYPR

Contact HYPR to learn more.

Companies Using Passkeys

CVS specialty™
BANK OF AMERICA
Google
Robinhood
Uber
PayPal
Microsoft
amazon
Nintendo®
GitHub
BEST BUY
Adobe

HYPR

THE IDENTITY ASSURANCE COMPANY

See HYPR in action:
Visit **hypr.com/demo**