Beyond Passwords:
Exploring the Future with Passwordless Authentication
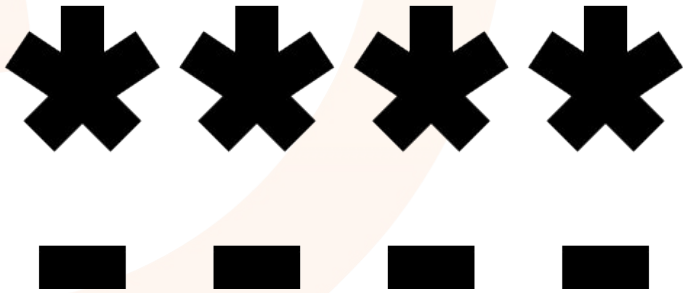
Ankit Ahuja
Senior Security Engineer

IdentityShield

miniOrange

About Me

- Working on IAM Product at miniOrange since 7 years

- Product Lead for Multi-Factor Authentication implementation in our product

- Part of the FIDO2/Passkey integration team

- Hate passwords and managing them
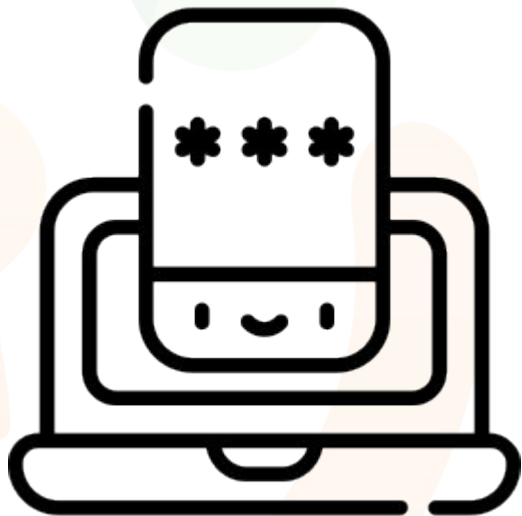
The Password Problem

Relies on **What You Know**

High Risk of Identity Theft and Phishing

Easily Hacked Through Brute Force Or Dictionary Attacks

Can be leaked in data breaches

2FA to the Rescue but…

Relies on **What You Have**

Became Imperative Due to Password Thefts

Poor User Experience

Doesn't Contain Identity

Users can lose physical keys

IdentityShield

miniOrange

Introducing Passkeys

Relies on **Who you Are**

Login without username, password and 2FA

Never leaves the user's device

Uses Biometric Authentication

Built in all major OS and browsers

What Exactly is a Passkey

Discoverable

WebAuthn

Credentials

1. Contains information about the user

2. Does not require entering a username

1. JS Browser API to create and use Credentials

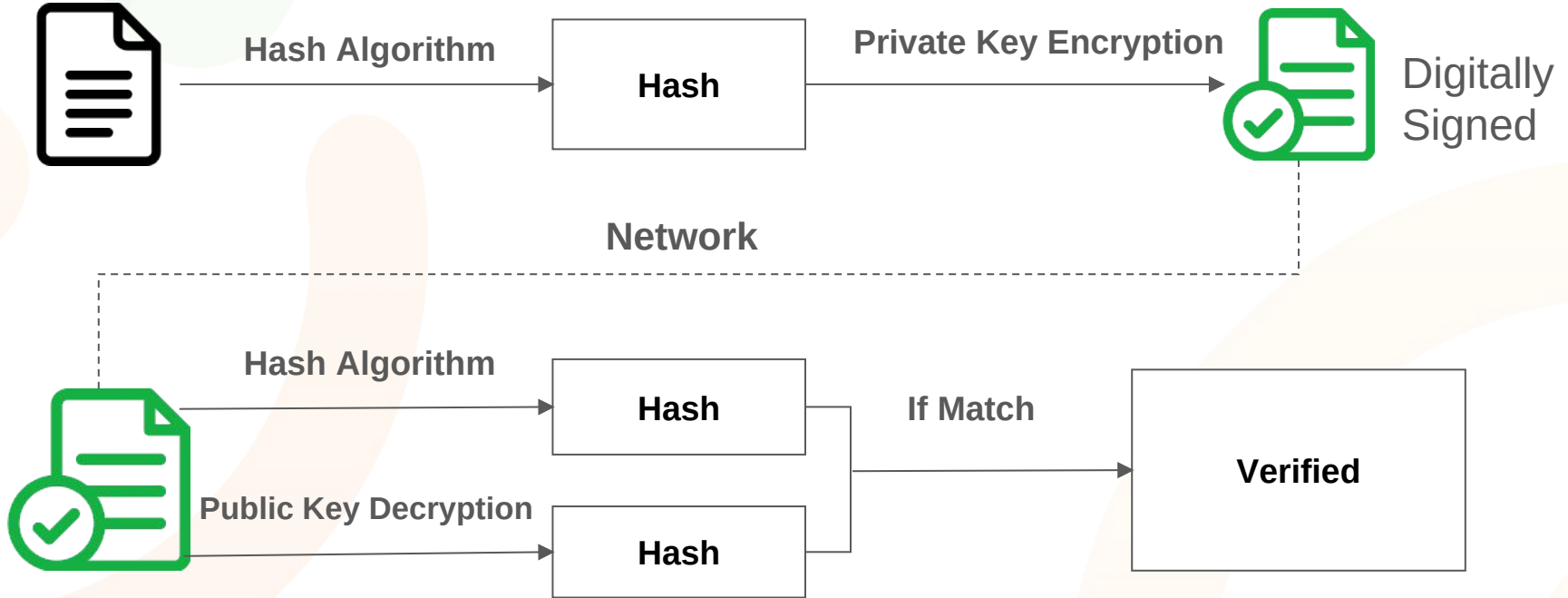2. Gives websites access to built-in client authenticator technology

1. Private keys that live on the device
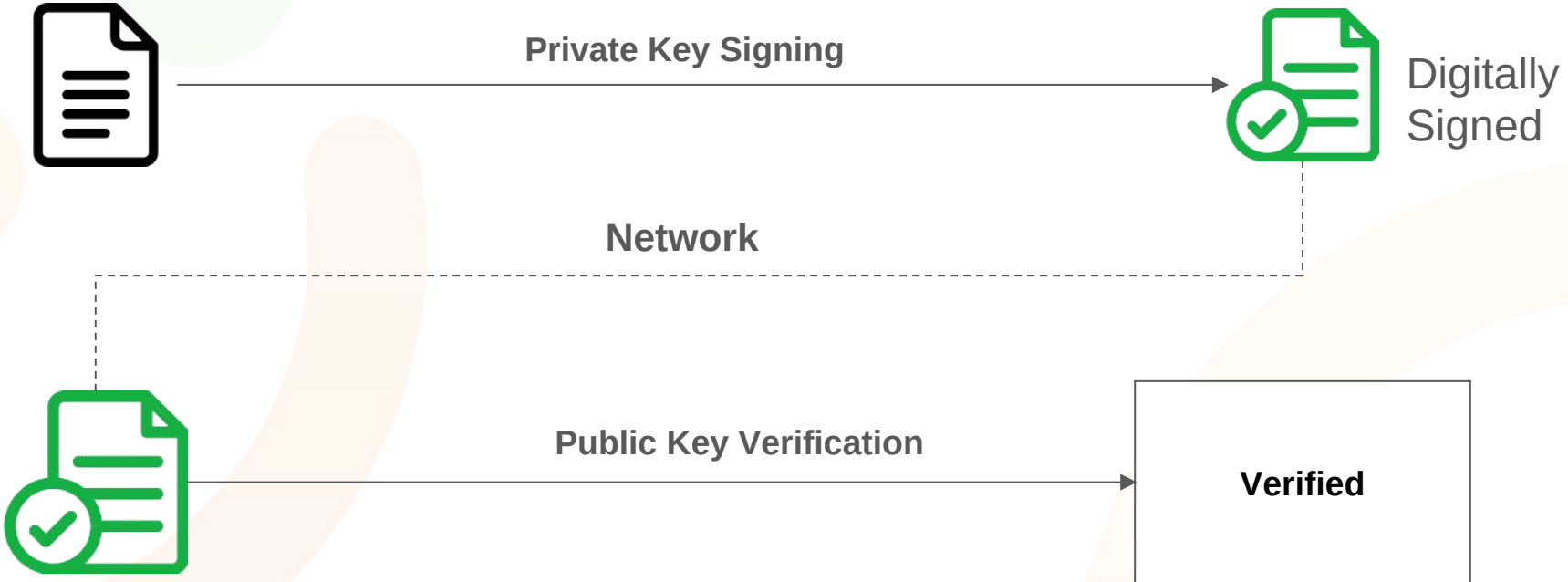
2. Unique keys bound to website and username

miniOrange

How Passkeys Work?

Technical Deep Dive

Public Key Cryptography

Hash Algorithm → **Hash** → Private Key Encryption → Digitally Signed

Network

Hash Algorithm → **Hash**

Public Key Decryption → **Hash**

If Match → **Verified**

IdentityShield

miniOrange

Public Key Cryptography

Creating a Passkey

Welcome, ankit!

Your name:

ankit ✏️

Your registered passkeys:

No credentials found.

🔒 CREATE A PASSKEY

SIGN OUT

Creating a Passkey

Welcome, ankit!
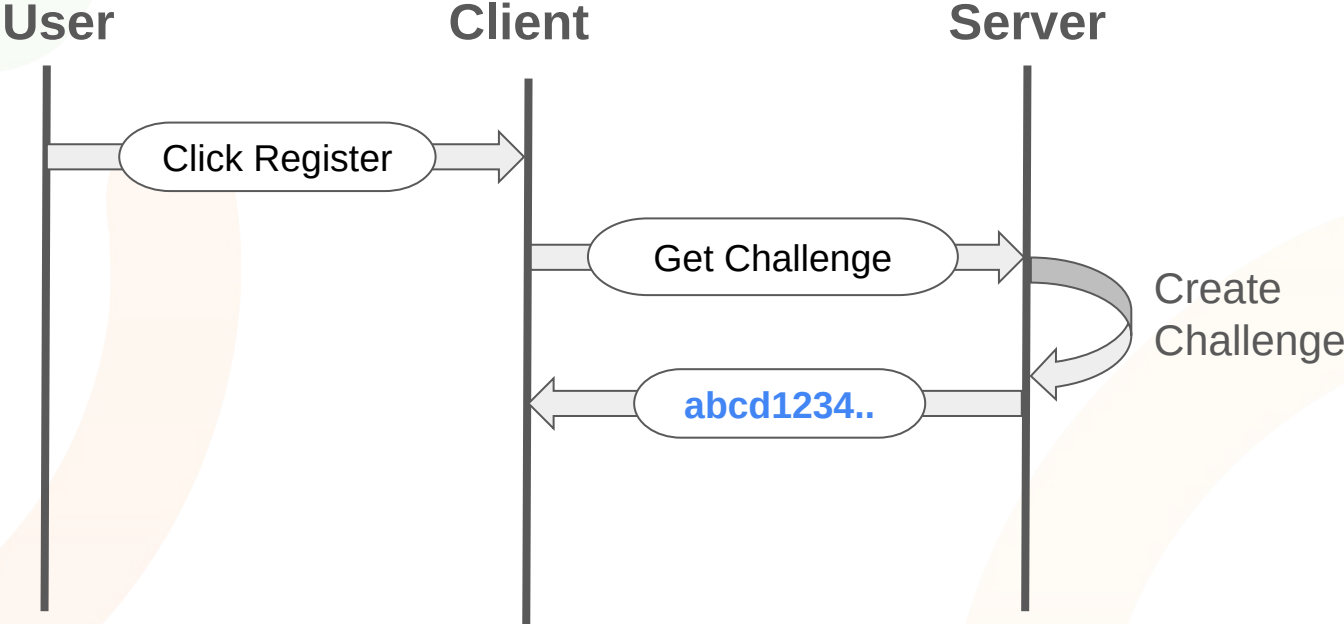
Your name:

ankit

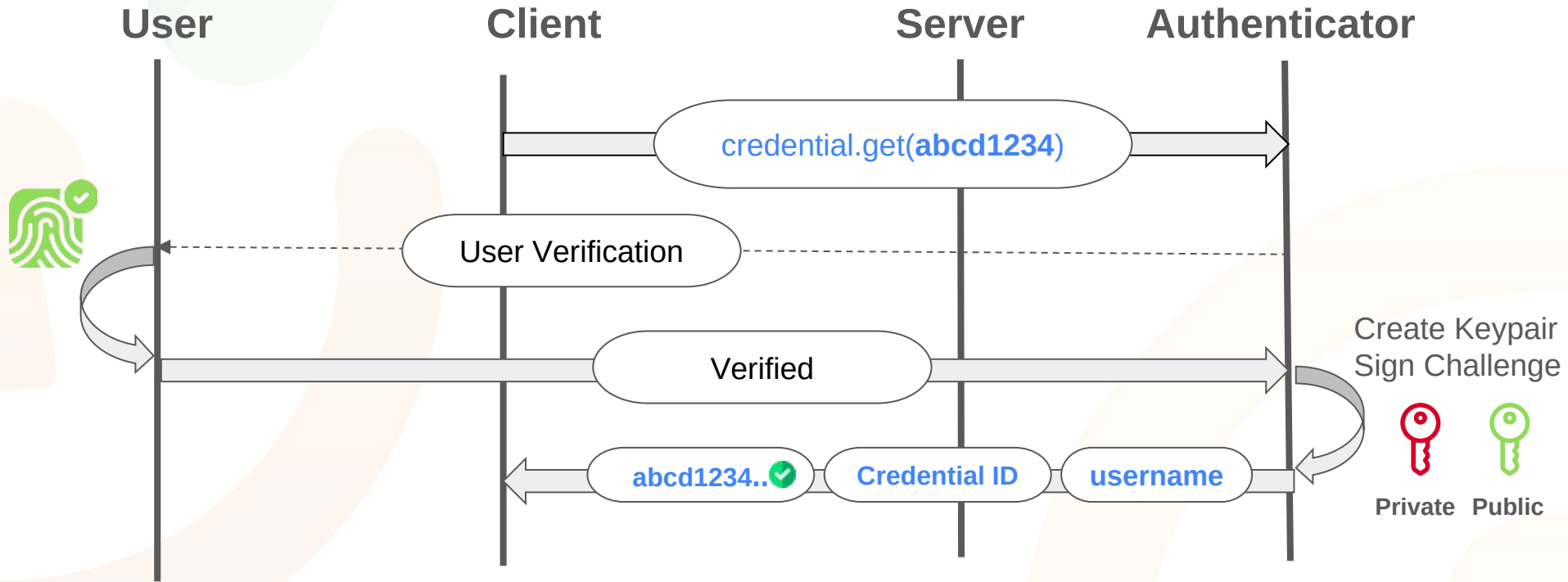Your registered passkeys:

No credentials found.
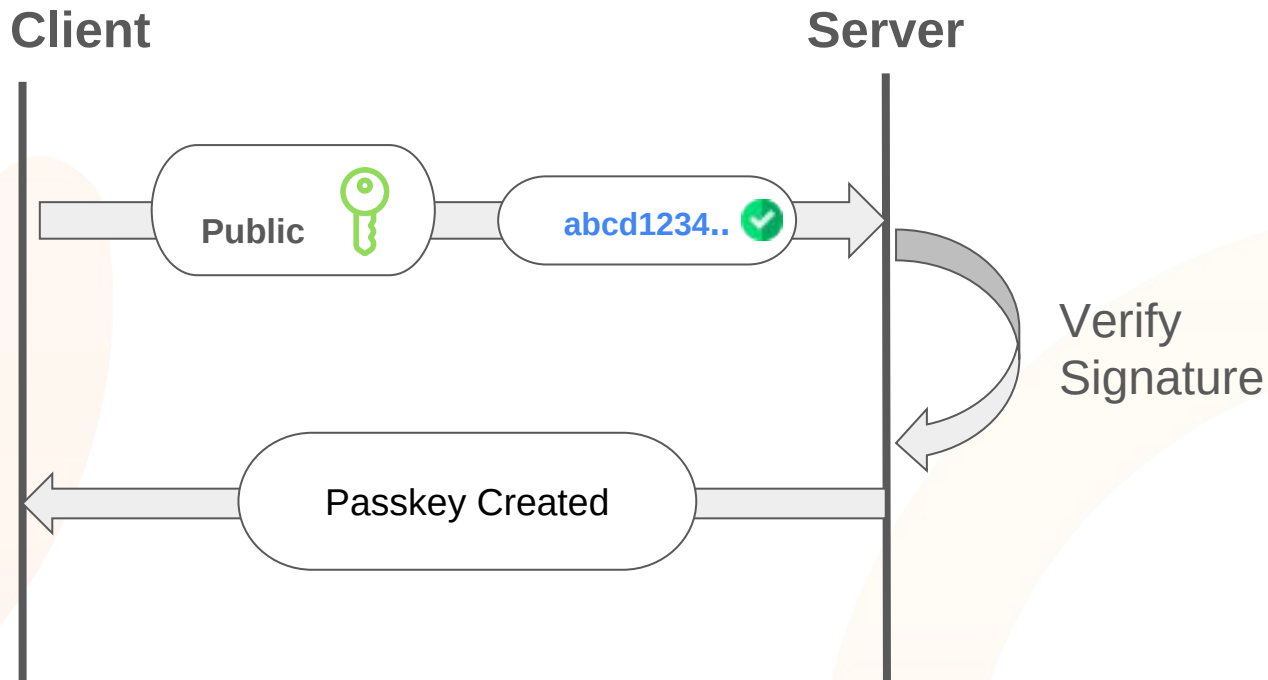
🔒 CREATE A PASSKEY

SIGN OUT

Get a Challenge

Sign Challenge

User   **Client**   **Server**   **Authenticator**

credential.get(**abcd1234**)

User Verification

Verified

Create Keypair
Sign Challenge

abcd1234..   **Credential ID**   **username**

Private   **Public**

Verify Challenge

Authentication with Passkey

Authentication with Passkey

Enter a username

username

Any username can be accepted.

NEXT

USE ONE BUTTON SIGN-IN INSTEAD

IdentityShield

miniOrange
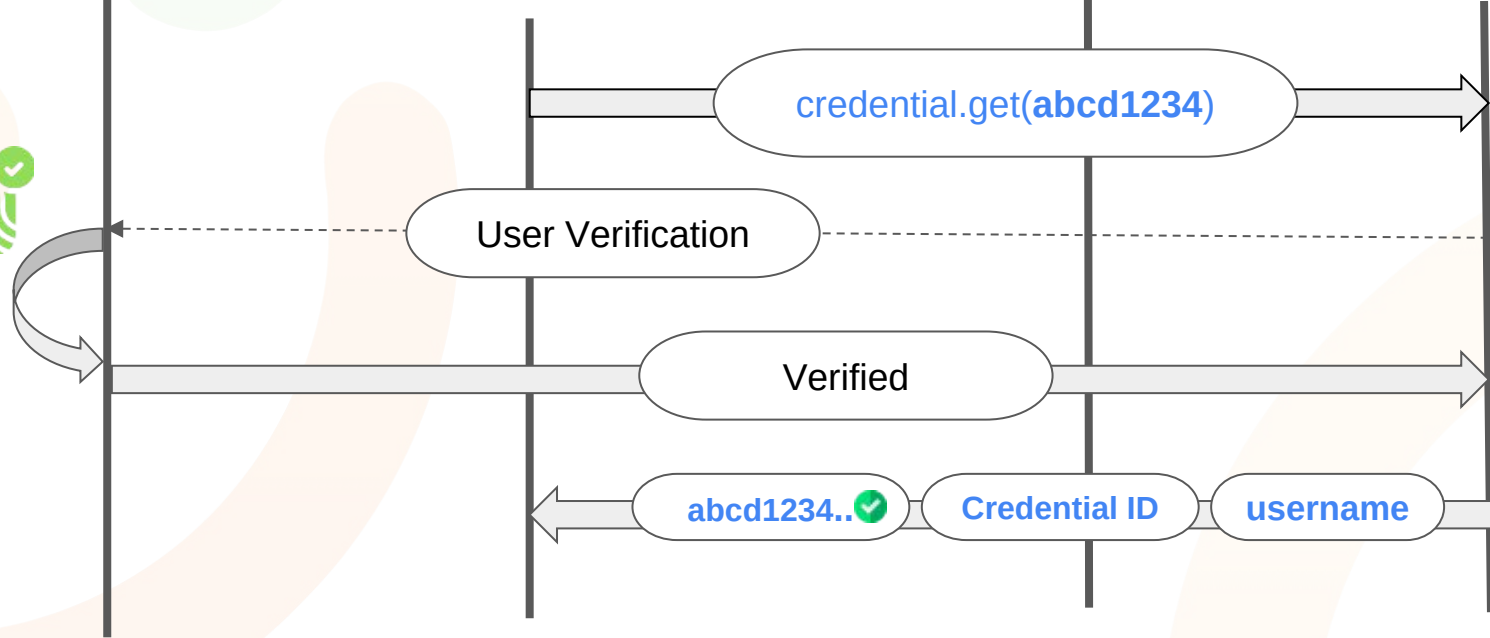
Get a Challenge
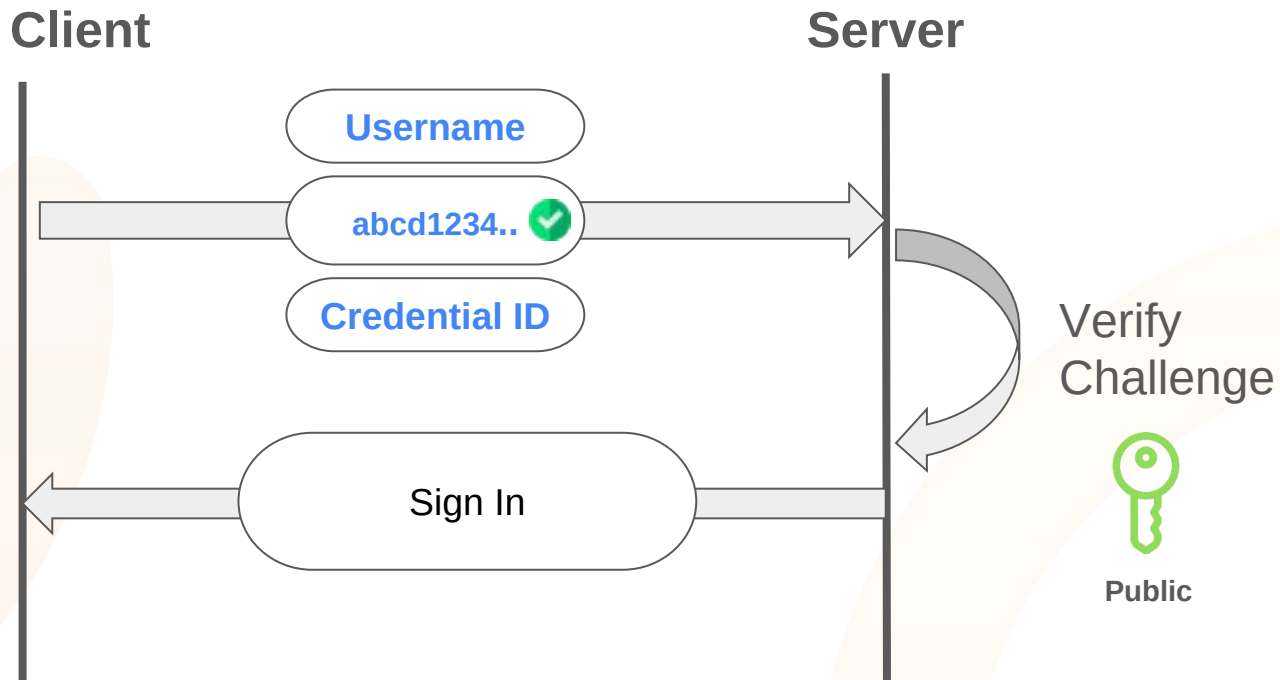
Sign Challenge

Verify Challenge

Challenges with Integrating Passkeys

Legacy Systems

Overcoming integration challenges with legacy authentication systems.

Developer Adoption

Encouraging developers to integrate passkey support into their applications and websites.

Compatibility Testing

Ensuring passkey compatibility with a wide range of devices and platforms

Key Takeaways

Passwords are not reliable for authentication anymore

2FA options are reliable but compromise usability

Passwordless Authentication using passkeys is more secure and easier to use

Available across all major OS and browsers

Single Sign on with FIDO2 supported IAM solution can allow easy integration of passkeys.

References

- Passkeys.io

- What is WebAuthn

- Passkeys.dev

Questions/Feedback?

Thank You!!

ankit@xecurify.com

ankitahuja07