OnePass, a FIDO Solution

Strong Authentication – Implementation of FIDO Authentication

Version 1.0

FIDO Introduction

What is FIDO?

FIDO (Fast ID Online) is a revolutionary technology that allows you to securely sign in to websites without using a password.

FIDO is a new technology that lets you sign in to any website that supports it -- securely and without relying on a password. FIDO is what's called a "standard." Like WiFi, or Bluetooth. It works on any web browser and on devices we use every day, including your smartphone, desktop or laptop computer, pad, or smartwatch.

FIDO Introduction

RAON SECURE

FIDO Authentication is the answer to the global password problem

Passwords, and other forms of legacy authentication such as SMS OTPs, are knowledge based, a hassle to remember, and are easy to phish, harvest and replay.

80%	90%	$70	51%
Passwords are the root cause of over 80% of data breaches.	Users have more than 90 online accounts.	Average help desk labor cost for a single password reset is $70	Up to 51% of passwords are reused.

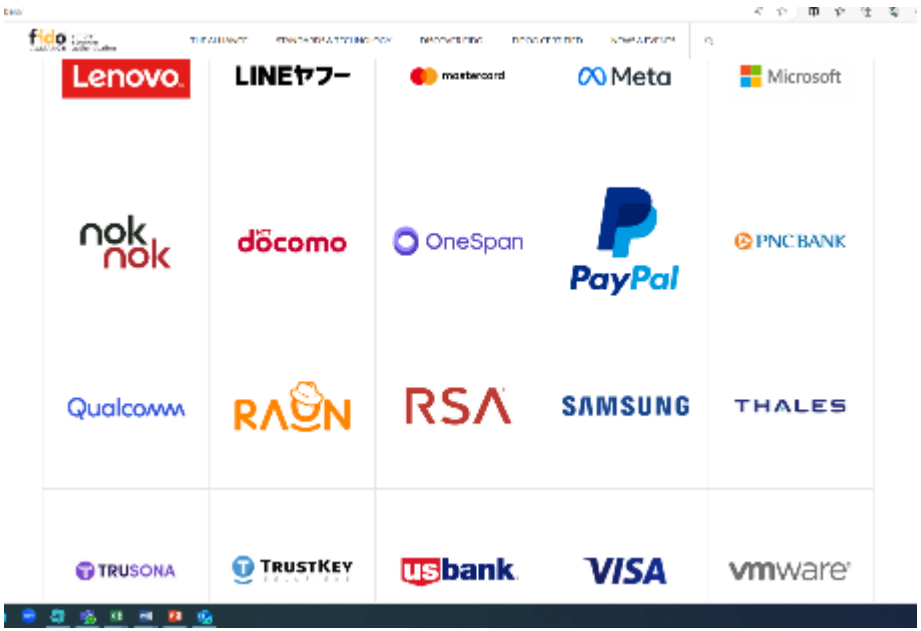
Why FIDO was developed? What problems is FIDO trying to solve?

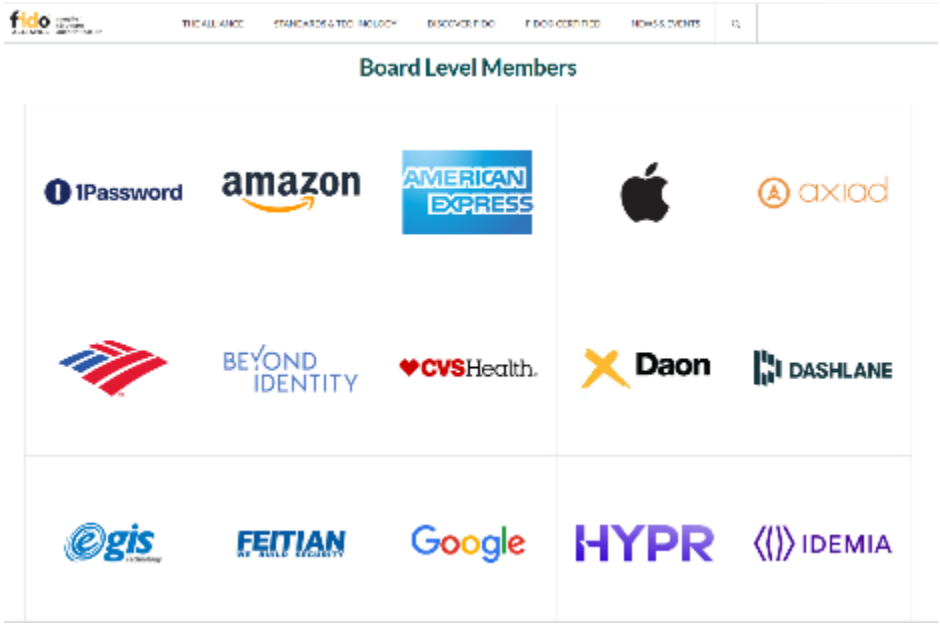
- **Weakness of Password:** Traditional password-based authentication systems are prone to various security risks such as phishing attacks, credential theft, password reuse, and brute-force attacks. Passwords can be easily forgotten, stolen, or compromised.
- **User Convenience and Experience:** Remembering and managing multiple passwords for different accounts can be challenging for users.
- **Need for Stronger Authentication:** With the increasing number of cyber threats and data breaches, there was a growing need for stronger and more secure authentication.
- **Interoperability:** There was a need for an open standard that could be widely adopted across various devices, platforms, and services, ensuring interoperability and ease of implementation.

FIDO Introduction

What is FIDO Alliance?

The FIDO Alliance is an open industry organization that was founded in 2013 with the goal of developing authentication standards that “help minimize the world’s over-reliance on passwords. An organization setting the passwordless login industry standard based on public-key cryptography.





FIDO Introduction

What are the types of specifications from **FIDO** (FIDO 1.0)?

- **FIDO UAF:** Universal Authentication Framework - Aimed to provide passwordless authentication using biometrics, PINs, and other local authenticators to authenticate users to online services without the need for passwords. Users must have a personal device, such as a computer or smartphone, and must register with an internet service to use UAF. This is device bound authentication and require re-register upon change of device such as phone.

- **FIDO U2F:** Universal Second Factor - Rather of replacing traditional password-based security, the FIDO U2F protocol complements it. Something they are familiar with, such as their account and password. They have something, such as a registered fob (a small security hardware device with built-in authentication used to control and secure access) or USB device through external hardware security keys, providing a stronger form of authentication.

FIDO Introduction

What are the types of specifications from **FIDO 2**?

- FIDO 2**:** FIDO 2 is an extension of FIDO U2F**.** FIDO2 combines the W3C's Web Authentication (WebAuthn) and FIDO Alliance's Client to Authenticator Protocol (CTAP) specifications.

- FIDO2 incorporates WebAuthn, enabling passwordless authentication using various authentication methods, such as biometrics, security keys, or other authenticators, across different web browsers and platforms. CTAP in FIDO2 facilitates communication between external authenticators (like hardware security keys) and user devices, allowing strong cryptographic authentication without transmitting sensitive information.

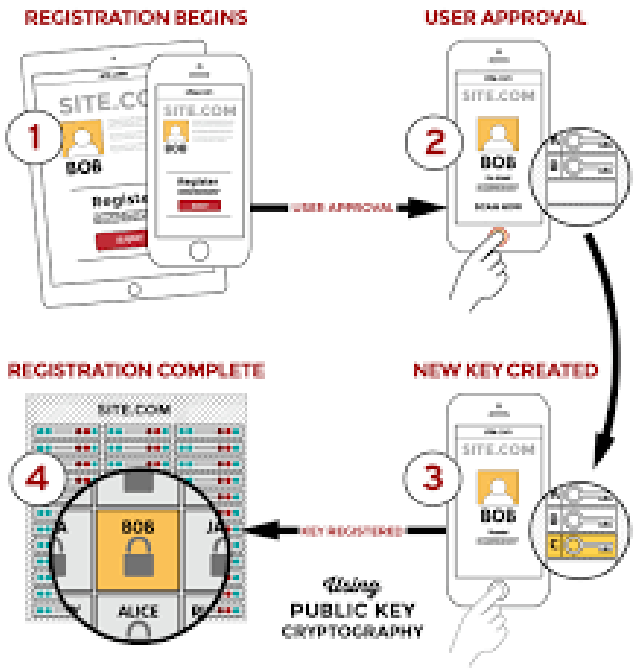
- FIDO2 is a more comprehensive and standardized protocol that is supported by all leading browsers and operating systems, including Android, IOS, MacOS and Windows.

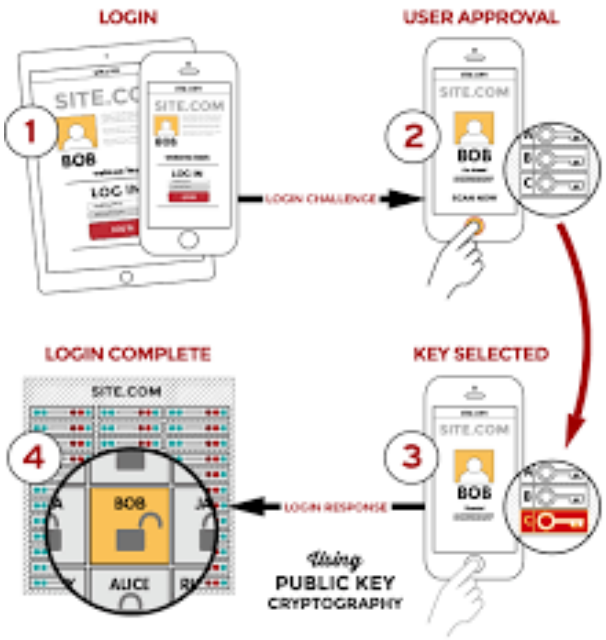
- FIDO2 offers expanded authentication options including strong single factor (passwordless), strong two factor, and multi-factor authentication.

FIDO Introduction

HOW is FIDO Work?

- FIDO Registration, Login, and how Key Pairs play a role in FIDO protocol

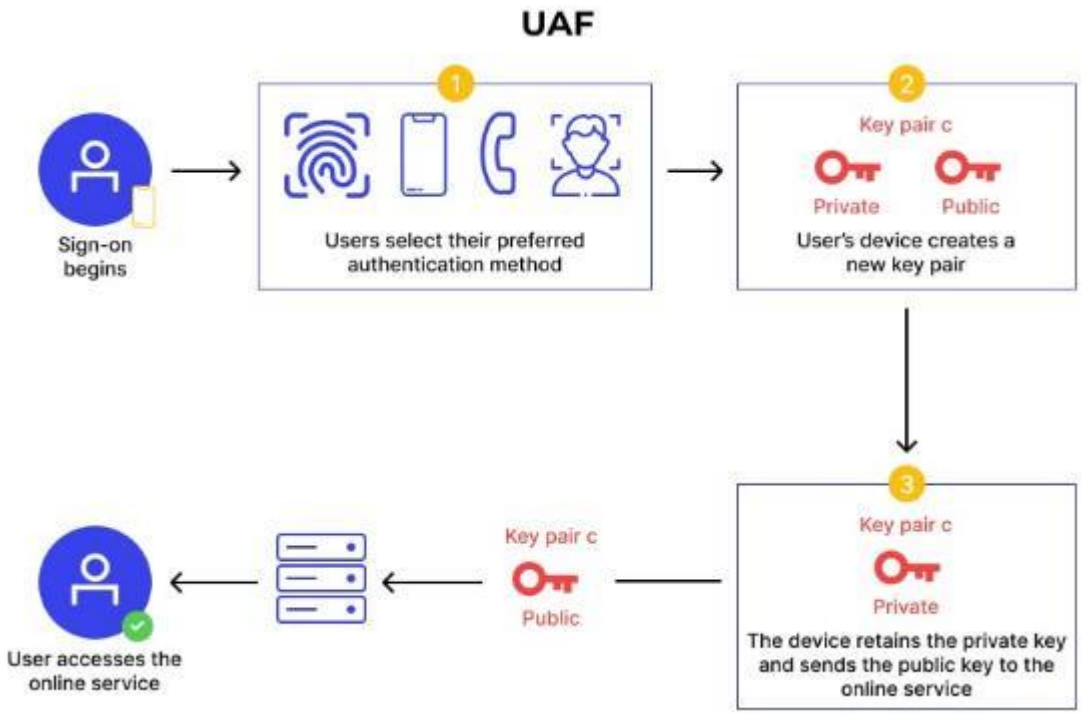




FIDO Introduction

HOW is UAF Registration work

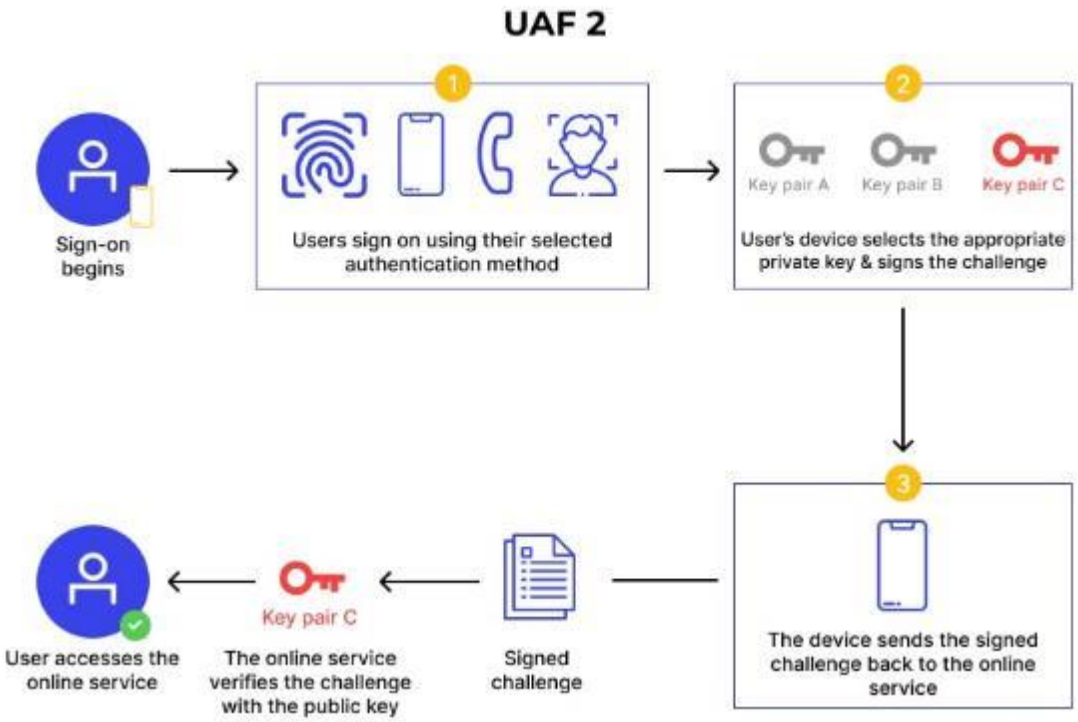
- FIDO Registration, Login, and how Key Pairs play a role in FIDO protocol



FIDO Introduction

HOW is FIDO UAF2 Login Work?

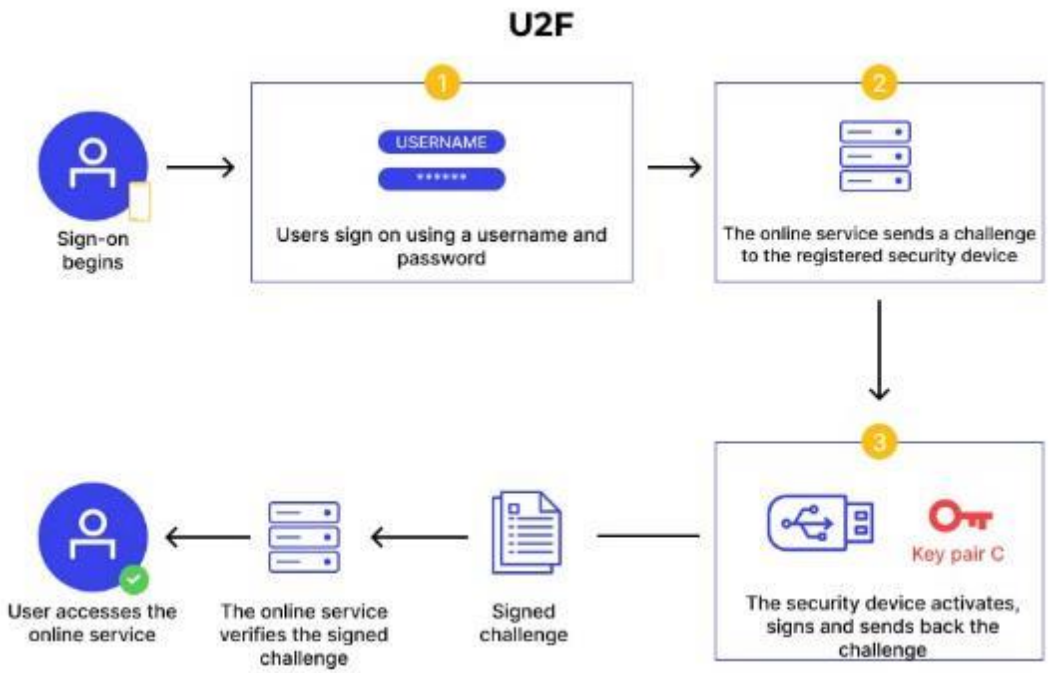
- FIDO Registration, Login, and how Key Pairs play a role in FIDO protocol



FIDO Introduction

HOW is FIDO U2F Login Work?

- FIDO Registration, Login, and how Key Pairs play a role in FIDO protocol



FIDO Introduction

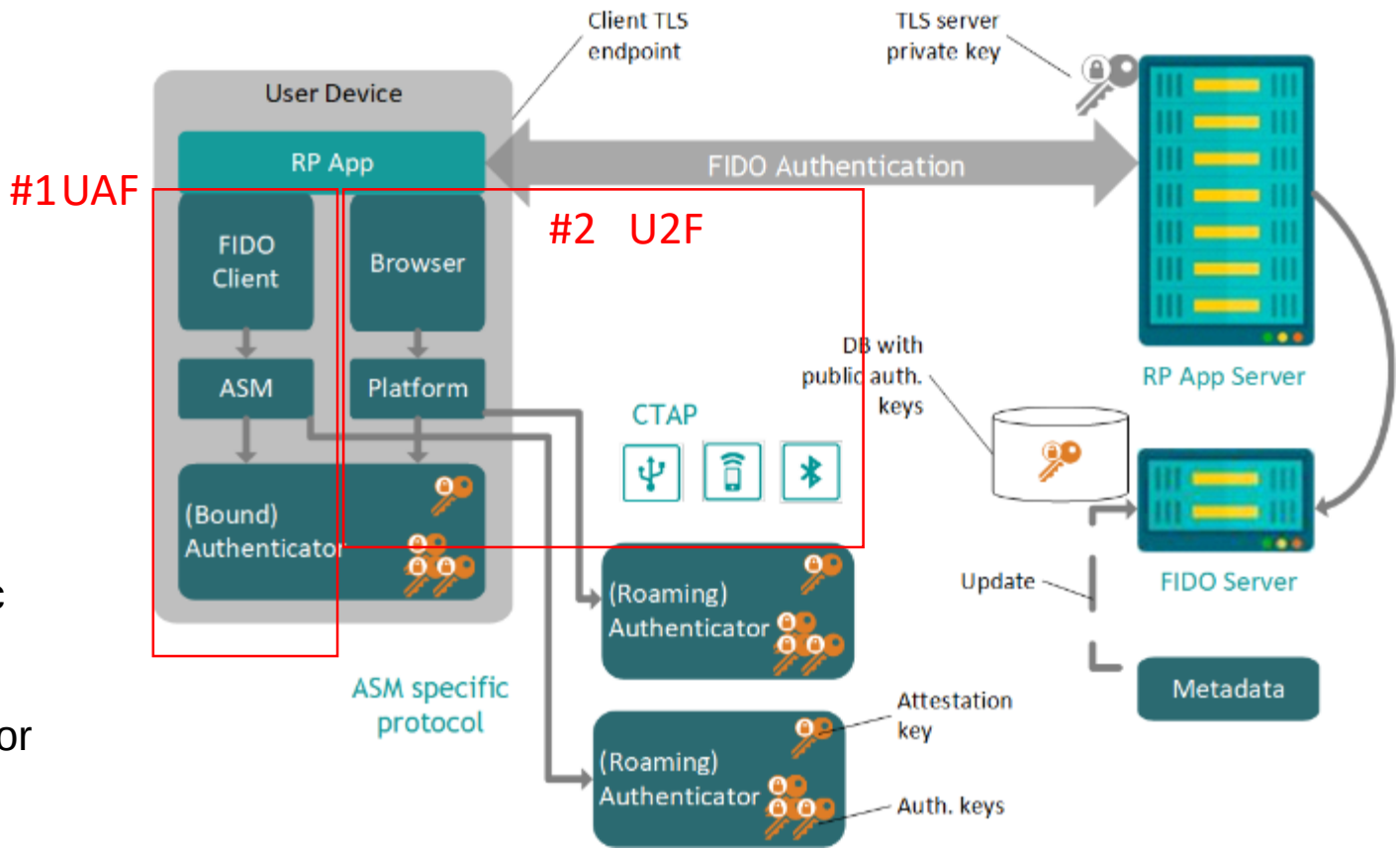
RAON SECURE

FIDO Components and System Architecture

FIDO UAF User Device Components

FIDO U2F User Device Components

- RP:Relying Party
- ASM: Authenticator Specific Module
- CTAP- Client to Authenticator Protocol
- Metadata – Information about registered/secured platform

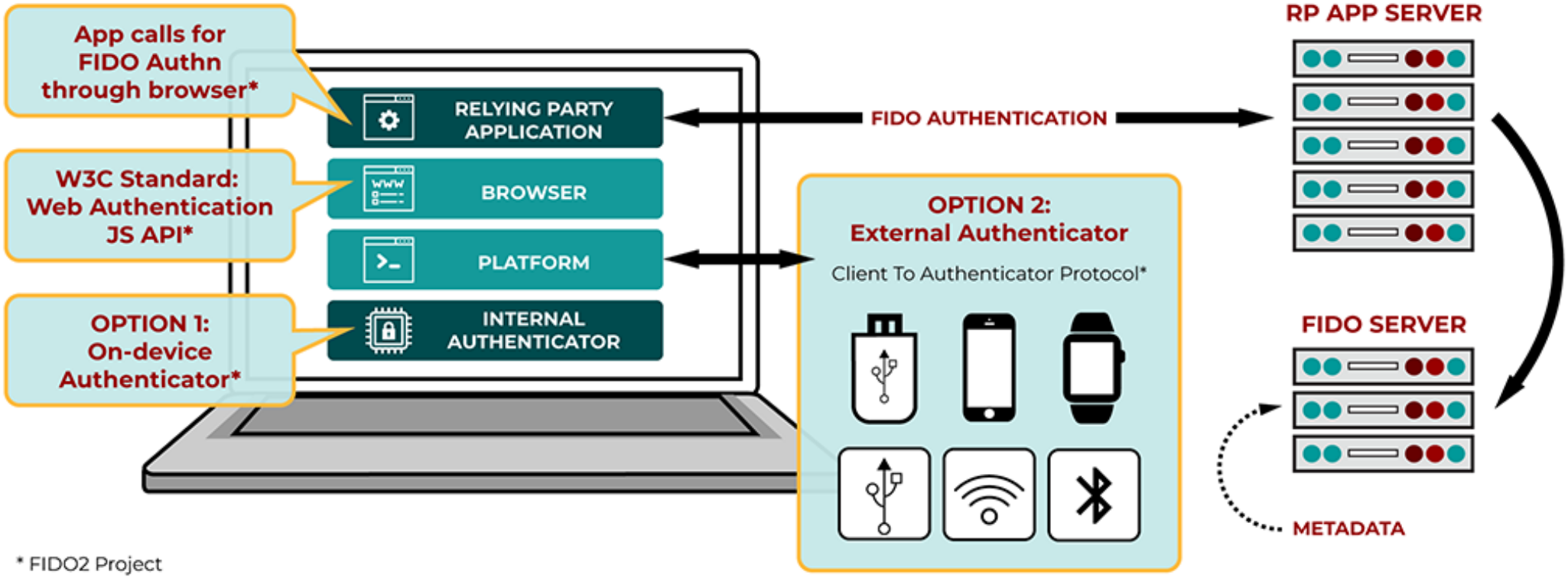


FIDO Introduction

RAON SECURE

FIDO2 Components and System Architecture

- FIDO2 Client Components are OS Platform Specific
- Option 1: Manufacturer Authenticator Device and Option 2 is external Authenticator Device

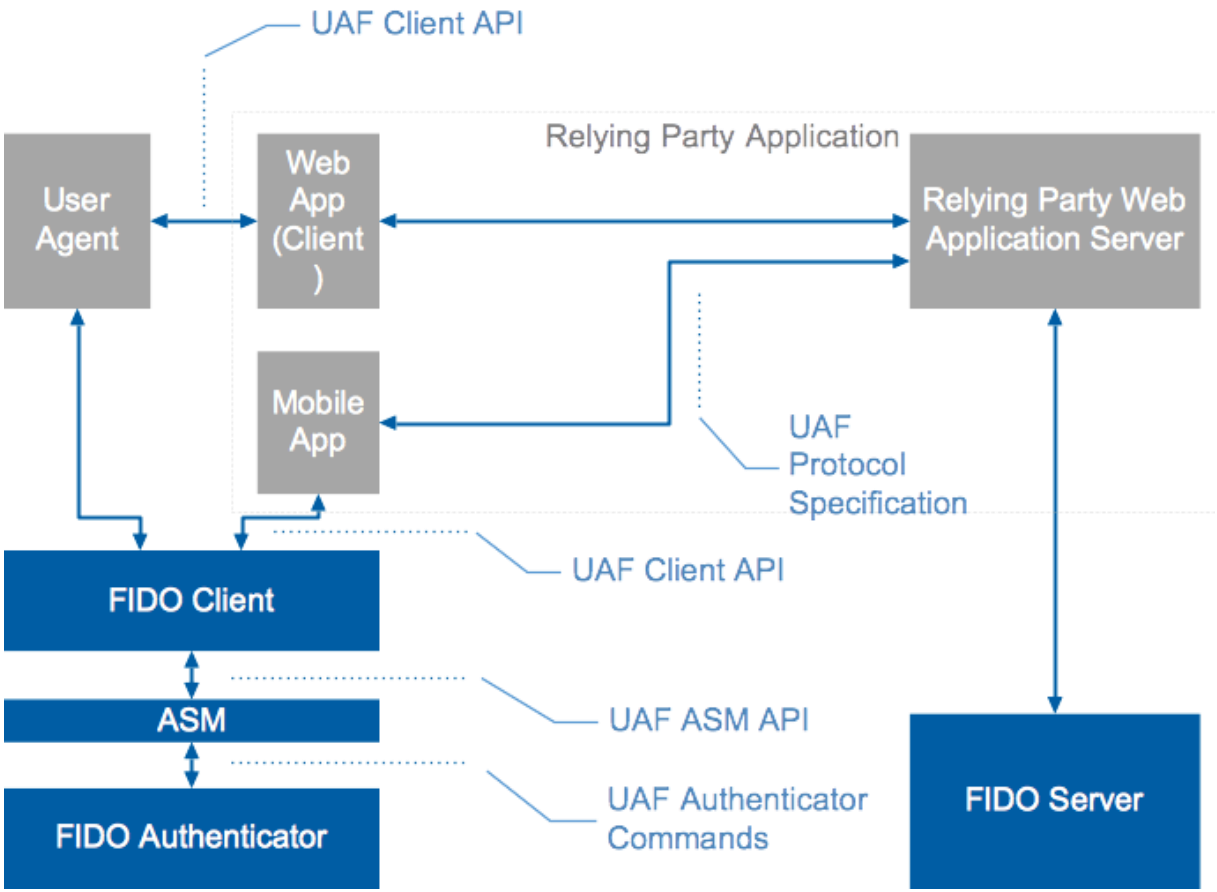


* FIDO2 Project

FIDO Introduction

FIDO 1.0 UAF Components and System Architecture with API Calls

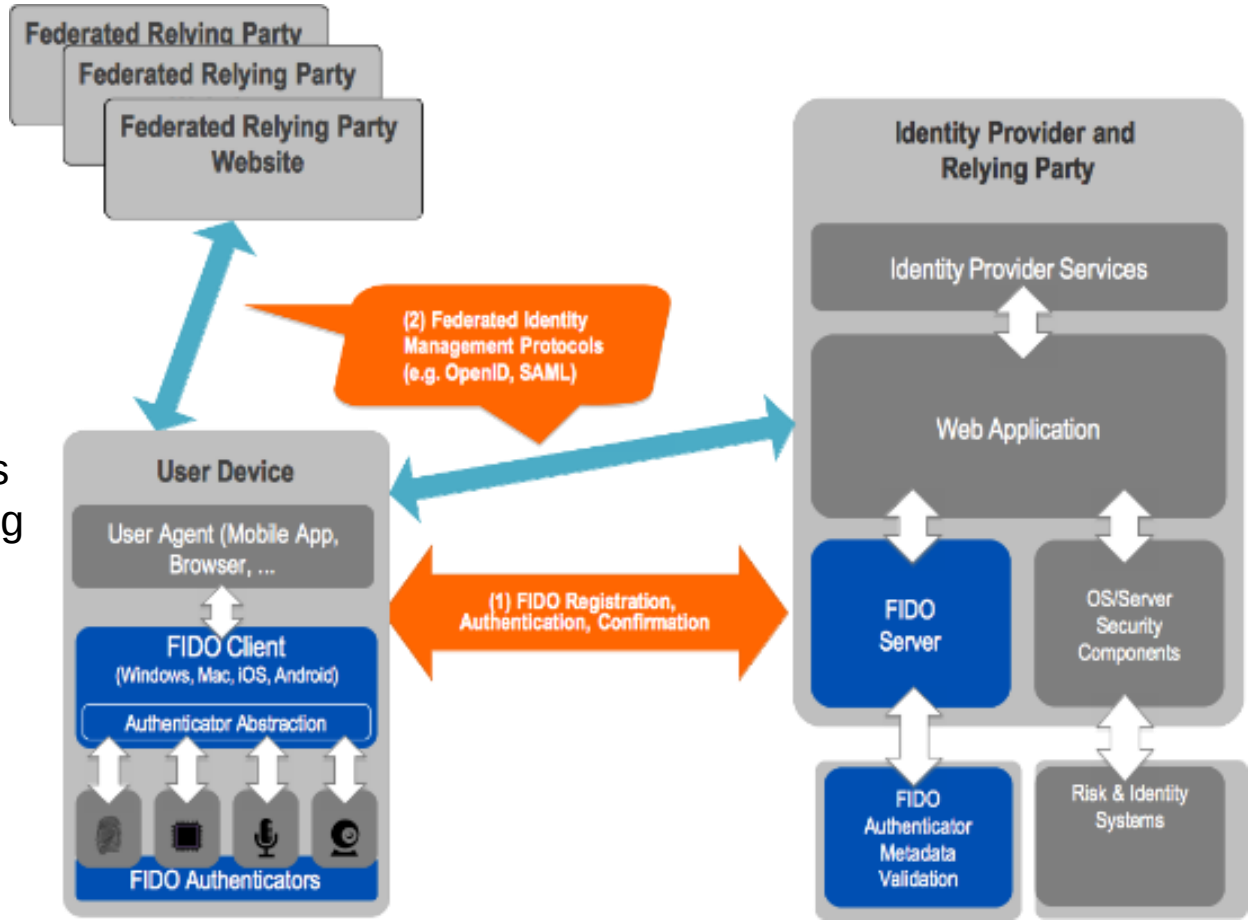
- User Agent examples – Chrome, IE, Safari or ther Web Browser
- Web App (Client Application Visa Web)
- Mobile App – Example Banking Mobile App



FIDO Introduction

Using FIDO to Set Up Federated Environment such as SSO

- Identity Provider System Component to integrate FIDO Server and develop Federated functionality such as SSO
- Using SAML and OpenID protocols to achieve SSO token for accessing multiple relying party web sites without additional authentication



FIDO Introduction

RAON SECURE

FIDO OnePass Service Components

Category			Descriptions
OnePass v2.0.1	Server	Server	• ONEPASS_SERVER_2.0.version.revision.zip
		Admin	• ONEPASS_ADMIN_2.0.version.revision.zip
	Client	Android	• TouchEn OnePass 2.0 SDK for Android v2.0.version.revision.zip
		iOS	• TouchEn OnePass 2.0 SDK for iOS v2.0.version.revision.zip
	DB	FETCH DB	• FIDO2 • MDS • Default
		NEW DB	
Documentation			• Installation Manual • Features and Functions • Administrator Manual • API Documentation

FIDO Introduction

RAON SECURE

FIDO OnePass Server Components and Requirements for Installation

The below OnePass Server configuration is recommended to process up to 1,000,000 active users.
For OnePass Server configuration above 1M active users, please consult Raonsecure OnePass Product Manager for recommended server configuration.

Category		Description
Hardware	CPU/ Memory/ Hard Disk	• CPU: 2CPU, 4Core or Higher • Memory: 32GB or Higher • Disk: 1TB or Higher
	NIC	• 10/100/1000 Ethernet Port x 1EA
Software	OS	• CentOS 7.0 64bit or Higher
	DBMS	• Oracle 11g (Minimum 9i 1.0.10.0 or above)
	Others	• Apache Tomcat 8.0 or above (Minimum 6.0 or above)
		• Java 1.8 or above (Minimum 1.6 or Above)

FIDO Introduction

RAON SECURE

FIDO OnePass Admin Server Components and Requirements for Installation

This is required specification of OnePass Admin module installation. For more information on details of Admin module will be supplied via Installation documentation.

.

Category		Description
Hardware	CPU/ Memory/ Hard Disk	• CPU: 1CPU, 4Core or Higher • Memory: 16GB or Higher • Disk: 1TB x 1EA or Higher
	NIC	• 10/100/1000 Ethernet Port x 1EA
Software	OS	• Windows 7d Professional or Above • CentOS 7.0 or Above
	WAS	• Tomcat • Weblogic

FIDO Introduction

RAON SECURE

FIDO OnePass Client Components and Requirements for Installation

This is required specification of OnePass Client module installation. For more information on details of Client module will be supplied via Installation documentation.

Category			Descriptions
	Android (Manufacturer or S/W Authentication Device)	Finger	• Embedded Finger Sensor, Android 6.0 or Above ※ Android 6.0 Above – A few devices exceptions Please check a fully supported device from the most Release Note
		Face	• Android device has BIOMETRIC_STRONG (Class 3) face authentication ※ ex) Google Pixel 4
		Pattern	• Android 6.0 Above
		PIN	• Android 4.4 Above
		Silent	• Android 4.4 Above
	iOS (framework)	Finger	• Built-in Touch ID, iOS 9.0 Above
		Face	• Built-in Face ID, iOS 11.0 Above
		Pattern	• iOS 8.0 Above
		PIN	• iOS 8.0 Above
		Silent	• iOS 8.0 Above
FIDO2		Windows	• Windows Hello (Version 1903 Above) - Browser: Chrome 75.0.3770.100, FireFox 68, Opera 62.0.3331.43, Edge 44.18362.1.0
		macOS	• macOS 10.13.6 Above - Browser: Chrome, Opera
		Android	• Android 7.0 Above - Browser: Chrome

FIDO Introduction

What are **benefits** to implement FIDO in many industries?

- Stronger Security: FIDO protocols utilize stronger authentication methods like biometrics, hardware tokens, or cryptographic keys, reducing reliance on easily compromised passwords.
- Reduced Password Vulnerabilities: FIDO reduces the risks associated with password-based authentication, such as phishing, brute force attacks, and password reuse.
- User Convenience: FIDO enables easier and more convenient authentication methods, such as fingerprint or face recognition, improving user experience by eliminating the need to remember complex passwords.
- Interoperability: FIDO specifications are designed to be interoperable across various devices and platforms, providing a standardized method for authentication.
- Privacy Enhancement: FIDO protocols often employ cryptographic techniques that don't require the sharing of personal identifiable information during authentication, enhancing user privacy.

FIDO Introduction

What are **benefits** to implement FIDO in many industries?

- Regulatory Compliance: Implementing FIDO can assist organizations in complying with regulatory standards related to data security and user authentication, such as GDPR or PSD2.
- Reduced Operational Costs: As FIDO reduces the instances of password-related support and security breaches, it can potentially decrease operational costs associated with user account management and security incidents.
- Scalability: FIDO offers scalability, accommodating both individual users and large-scale deployments in enterprise environments without compromising security

FIDO Introduction

RAON SECURE

Case Study by Shinhan Bank and PNC Bank

FIDO Introduction

RAON SECURE

What are **challenges** in implementing FIDO by many industries?

- Integration Complexity: Integrating FIDO into existing systems and applications might require significant changes to the authentication infrastructure, potentially causing disruptions or compatibility issues.
- User Adoption and Education: Users may initially resist or struggle to adapt to new authentication methods. Educating users about the benefits and proper use of FIDO technology is crucial for successful adoption.
- Device and Platform Support: Not all devices or platforms may fully support FIDO protocols, leading to limitations in where and how FIDO-based authentication can be implemented.
- Costs of Implementation: Initial setup costs, including hardware tokens or biometric scanners, might be prohibitive for some organizations. Additionally, training staff and users on the new technology can also add to implementation costs.
- Fallback Mechanisms: In cases where FIDO authentication fails or is unavailable, organizations need to establish robust fallback mechanisms to ensure users can still access their accounts securely.

FIDO Introduction

RAON SECURE

What are **challenges** in implementing FIDO by many industries?

- Regulatory and Compliance Challenges: Adhering to specific regulations and compliance standards while implementing FIDO can pose challenges, especially if there are stringent requirements or conflicting regulations in certain regions or industries.

- Risk of Device Loss or Theft: Since FIDO often relies on specific devices or biometric data, the risk of losing these devices or compromising biometric information raises security concerns that need to be addressed.

- Standardization and Compatibility: Despite being designed for interoperability, different versions or implementations of FIDO protocols might not always be fully compatible, creating interoperability issues across systems.

FIDO Introduction

What are **challenges addressed** by transitioning **from FIDO to FIDO 2**?

- Interoperability: FIDO2 was developed to enhance interoperability across various platforms and devices. It unifies two specifications, CTAP (Client to Authenticator Protocol) and WebAuthn (Web Authentication), enabling a broader range of devices and browsers to support passwordless authentication.

- User Experience: FIDO2 emphasizes user convenience by enabling a seamless and consistent authentication experience across different devices and browsers. It supports various authentication methods, including biometrics and hardware tokens, improving usability.

- Wider Adoption: FIDO2's design aimed to encourage broader adoption by offering simpler integration methods and more flexibility in terms of supported devices and platforms, making it easier for developers and organizations to implement.

- Enhanced Security: While the original FIDO protocols were highly secure, FIDO2 enhances security further by providing stronger cryptographic mechanisms and eliminating the dependency on passwords entirely. This helps mitigate phishing attacks and other forms of identity theft.

FIDO Introduction

RAON SECURE

What are **challenges addressed** by transitioning **from FIDO to FIDO 2**?

- Expansion of Use Cases: FIDO2 extends beyond web-based applications, enabling its use in native applications and operating systems. This expansion broadens the scope of FIDO-based authentication, making it applicable across various domains.

- Reduced Dependence on Plugins: FIDO2, particularly WebAuthn, reduces reliance on browser plugins for authentication, providing a standardized API directly integrated into browsers, thus improving compatibility and usability.

- Privacy Enhancement: FIDO2 continues the trend of preserving user privacy by ensuring that the authentication process doesn’t involve sharing sensitive personal information or credentials with service providers

FIDO Introduction

RAON SECURE

FIDO Credential Management - FIDO (Fast Identity Online) credentials refer to the cryptographic keys and data used during the authentication process. These credentials are generated and stored securely on a user's device or within a dedicated hardware token.

Registration Credentials:

- When a user enrolls in a FIDO-enabled service or platform, registration credentials are created. These credentials consist of a key pair—a public key and a private key.
- The private key is securely stored on the user's device or hardware token, while the public key is sent to the service provider during registration.
- The registration credentials are unique to each device or token and are used to authenticate the user during the login process.

Authentication Credentials:

- During authentication, the user's device or hardware token uses the private key to sign a challenge issued by the service provider.
- The signed challenge is sent back to the service provider along with the corresponding public key, proving the user's identity without transmitting any sensitive information (like passwords).
- The service provider verifies the signature using the stored public key and grants access if the signature is valid.

FIDO Introduction

RAON SECURE

FIDO Credential Management

Credential Generation:

- When a user enrolls in a FIDO-enabled service or platform, the FIDO device or token generates a key pair—a public key and a private key.
- The private key remains securely stored within the device or token, while the public key is sent to the service provider for registration.

Secure Storage:

- The private key is securely stored within a Trusted Execution Environment (TEE), Secure Element (SE), or another isolated and protected area within the device or hardware token.
- This secure storage ensures that the private key cannot be accessed or extracted by unauthorized parties, providing strong protection against theft or compromise.

Isolation and Encryption:

- FIDO credentials are isolated from the device's main operating system or any software running on it to prevent potential attacks or breaches.
- Encryption and hardware-level security mechanisms protect the stored credentials, making it extremely difficult for attackers to access or manipulate them.

FIDO Introduction

RAON SECURE

FIDO Credential Management

Authentication Process:

- During authentication, the service provider sends a challenge to the user's device or token.
- The device or token uses the stored private key to sign the challenge, creating a response that is sent back to the service provider.

Verification:

- The service provider verifies the received response using the associated public key stored during registration.
- If the signature is valid and matches the public key, the user is authenticated, and access is granted.

Revocation and Updates:

- If a device or token is lost, compromised, or no longer used, FIDO credentials can be revoked or updated.
- Revocation mechanisms ensure that even if a device is lost, the stored credentials cannot be misused for unauthorized access.

FIDO Introduction

What are **known risk or fraud possibilities with FIDO**?

- **Device Compromise**: If the user's device or hardware token storing FIDO credentials is compromised or stolen, there's a risk of unauthorized access. However, the security measures implemented within these devices, such as secure elements or Trusted Execution Environments, make it extremely challenging for attackers to extract the stored credentials.

- **Biometric Spoofing**: For FIDO implementations that use biometric authentication, there's a theoretical risk of biometric spoofing or replication. However, modern biometric technologies often include measures to detect spoof attempts, and the level of difficulty in successfully spoofing a biometric factor can be very high.

- **Man-in-the-Middle (MITM) Attacks**: While FIDO protocols are designed to prevent MITM attacks through cryptographic measures, there might be vulnerabilities in certain implementations or instances where sophisticated attackers could attempt to intercept communications between the device and the service provider. But, Almost impossible.

- **Phishing and Social Engineering**: While FIDO significantly reduces the risk of traditional phishing attacks that target passwords, there's still a possibility of social engineering attacks convincing users to authenticate on a malicious website or inadvertently approve a fraudulent transaction. But

Multi-Factor Authentication

RAON SECURE

Why OnePass? The best passkey solution today

OnePass provides All-In-One total authentication management solutions for FIDO based biometric, PIN, Pattern, Mobile OTP, FIDO2. Advanced management features and proven track records of performance.

Biometric | PIN/Pattern | USB | BLE | Policy

Global Certification

FIDO Certified , FIPS140-2, KCMVP, NIS, GS Certifications

Easy Implementation to Passwordless

Lost Phone

Frictionless & Passwordless environment using FIDO Authentication

Supports Multi-Channel Management

ONEPass

FIDO1.0 — Mobile Authentication

FIDO2 — Browser Authentications

Optimized for Cloud Environment

License Management

User Self Service

ONEPass

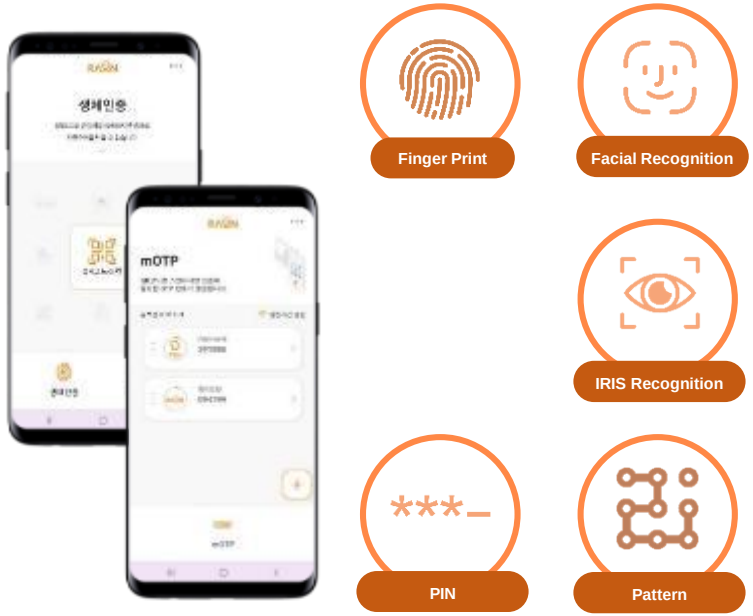
Auto Scaling

Usage Statistics

Architecturally designed and management functions built for the most optimal cloud base environment

OnePass Differentiation Overview

1 Various FIDO1.0 Based Authentication Methods



MFA(Multi-Factor Authentication)

- Supports iOS, Android, and other platforms

Modularized Authentication Features

- Each Authentication method is available as a module
- Choose the most suitable & secure method for frictionless

2 Supports FIDO2 Authentication Device

FIDO2

- FIDO2 uses W3C's WebAuthn API and FIDO CTAP to authenticate
- OnePass supports various stage of FIDO adoptions by client and offers flexible ways to manage authentication schemes

A Single Solution for All FIDO1.0, FIDO2, OTP

- OnePass supports FIDO1.0, FIDO2, OTP Simultaneously
- Supports various mobile devices and biometric schemes

Enhanced Security Level

- User bio is never stored on server or sent across network
  ※ Stored on only user owned device TEE(Trusted Execution Environment)
- No need to install due to default authentication API

Device Flexibility

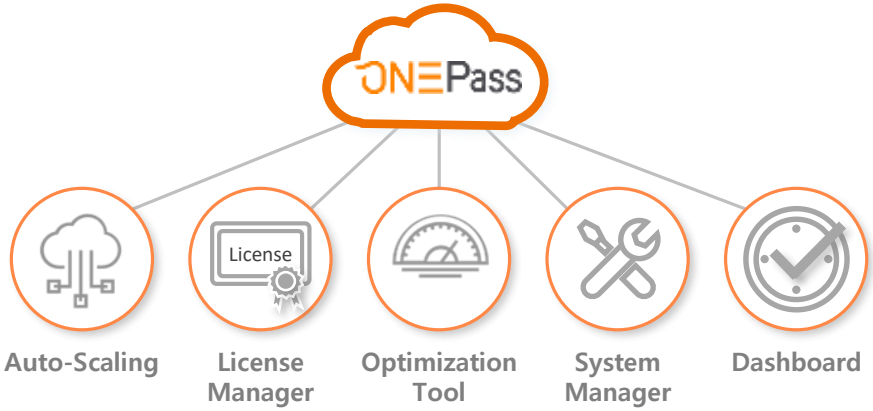
- Supports device without authentication mechanism by supporting USB, Dongle, NFC, or BLE types of external device

3 Optimized Architecture for Cloud Environment

Supported Environments

Supports all types of customer cloud environment with the most optimal cloud architecture

Management Tools Built for Cloud Environment



OnePass is proven for its highest availability, minimal manual intervention, and low maintenance operation.

OnePass Major Clients

Standard Chartered
SC제일은행

신한은행

Hyundai Card

MetLife

Prudential
푸르덴셜, 당신의 삶을 담다

kakao

citibank

AMOREPACIFIC

kakaopay

bithumb

JEJUair