level1 GOOD Software

FIDO CERTIFIED FIDO2

nipa 정보통신산업진흥원

Ministry of Science and ICT

OMS One More Security

OneMorePASS (OMPASS)

On-Premise/Cloud

Comply with FIDO Alliance international standard based on public key

FIDO (Fast IDentity Online) Solution

Biometric and passwordless authentication

Phishing resistant MFA(Multi-Factor Authentication) Service

OneMorePASS (OMPASS)

On-Premise/Cloud

FIDO (Fast IDentity Online) Solution

biometric and passwordless authentication
Phishing resistant MFA(Multi-Factor Authentication) Service

▶ Certifications

level1 GOOD Software

Software Quality
certified as level 1
Good Software by TTA
(ISO/IEC 25023, 25041, 25051)

fido CERTIFIED FIDO2

Secured Login
with FIDO Authentication
certified by FIDO Alliance

nipa

Cloud Computing Quality
certified under
the accredited test by NIPA

MSIT Minister's Awards
Information Security Merit

MSIT Minister's Awards
Excellent Company

☐ Necessity of Introducing

· Increasing demand for user authentication technology that guarantees strong security and user convenience

· Perfectly solves the risk factors of password authentication according to FIDO standard authentication method based on public key

Several Risks of Password Authentication

·Most users use less than 5 passwords

·More than 50% of users have never changed their passwords in 5 years

·Passwords are the leading cause of 80% of data loss

·Most users reuse the same password across multiple sites

☐ Next-Generation Integrated Authentication Solution

Resolves the inconvenience and anxiety of password methods Guarantees user convenience and security at the same time

High Security
Based on PKI

User Convenience
with No Passwords

Multi-Scalability
to Applicate Various AuthN Methods

☐ Advantages

·**User Convenience**
Apply various authentication methods and manage integrated authentication lifecycle with this one OMPASS (mobile authentication device).

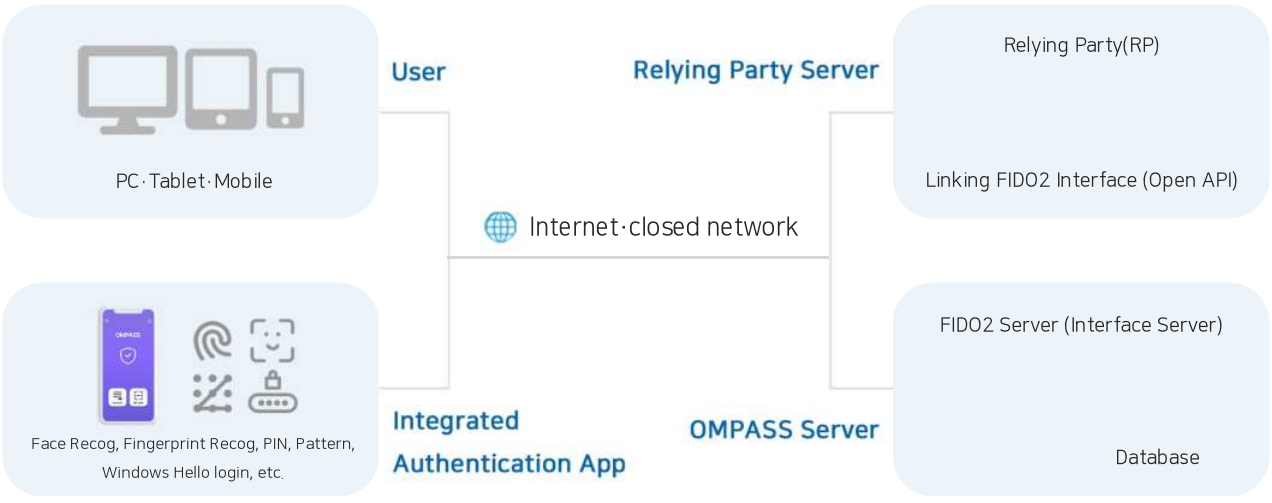
·**Completely Eliminate Security Vulnerabilities**
Through the "passwordless login", complete removal of security vulnerabilities due to password use and management and also satisfy one's security compliance.

·**Compliance with International Standards**
Comply with FIDO Alliance international standard based on public key.

·**Establishing a zero trust environment**
Complete a zero trust environment by establishing a strong and reliable FIDO authentication system.

☐ Specification Diagram

System Specifications
·Server: Windows, Linux (Intel Xeon 2GHz or higher, RAM 64GB, HDD 1TB or higher recommended)
·Client: Android, iOS



☐ Key Points

Various AuthN Methods

·**Various authentication methods can be expanded**

Application of the latest various user authentication technologies based on public Key

·**User-selectable authentication**

Supports various authentications such as Face Recog, Fingerprint Recog, PIN, Pattern, Windows Hello login, and more

Customer-Centric Flexibility

·**Customer-Centric Service**
Provides an optimized service for the environment of customer needs through user integrated authentication app or SDK

·**Minimize Developing Time**
Provides linking module (interface server) to minimize applying time and developing work

·**Integratable authentication services**
Possible to link web-based service, Windows client, Windows login, mobile app, Linux PAM, MaxOS, Radius, Redmine, Gooroom login, etc. client

·**Optimized the Customer Environment**
Supports UAF (Universal Authentication Framework) and U2F (Universal Second Factor)

·**Optimized the Network Environment**
Full support for Internet and closed network environments

Enhanced System Security

·**Secured Security**
Conducted penetration testing through a professional white hacker team and completed security measures

·**Enhanced Administrator Authentication**
Requires OMPASS authentication separately when accessing the admin page

·**Service Access Control**
By browser, user location, IP address, and time schedule

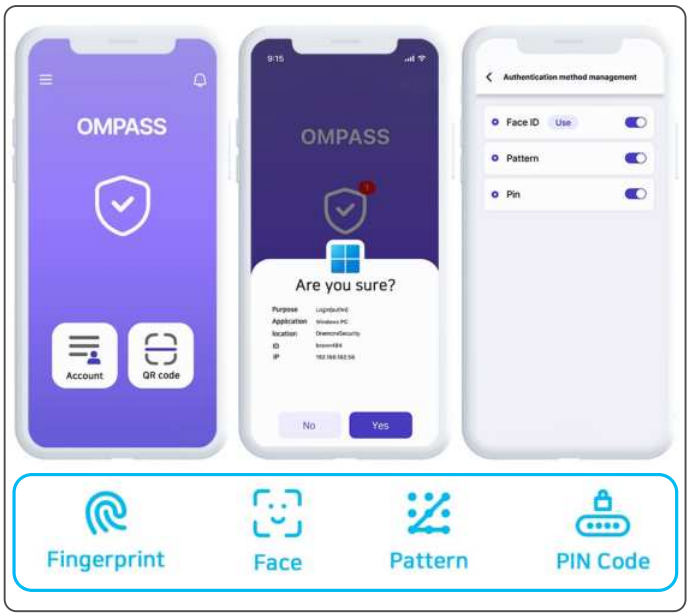
·**Prespond Strongly againt Phishing Attack**
Verifies the user access device (or browser)

·**Reinforcement of Mobile Authentication Device Security**
Verifies the jailbreak, forgery, and latest version of the user device

·**Policy Violation Alarm Service**
Sends a push notification or email to administrator or user in case of violation of authentication policy

☐ Main Screen

Mobile App

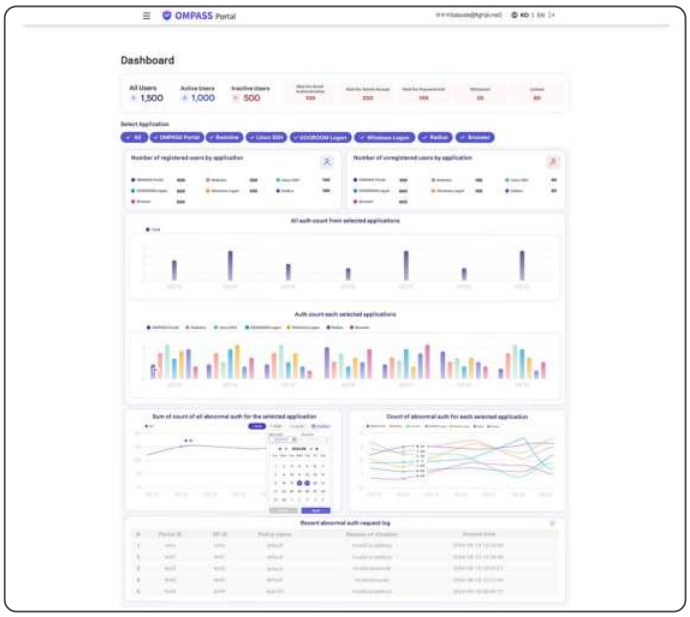


- Allows users to log in with mobile authentication devices
- Provide user selection row authentication methods

Windows Login

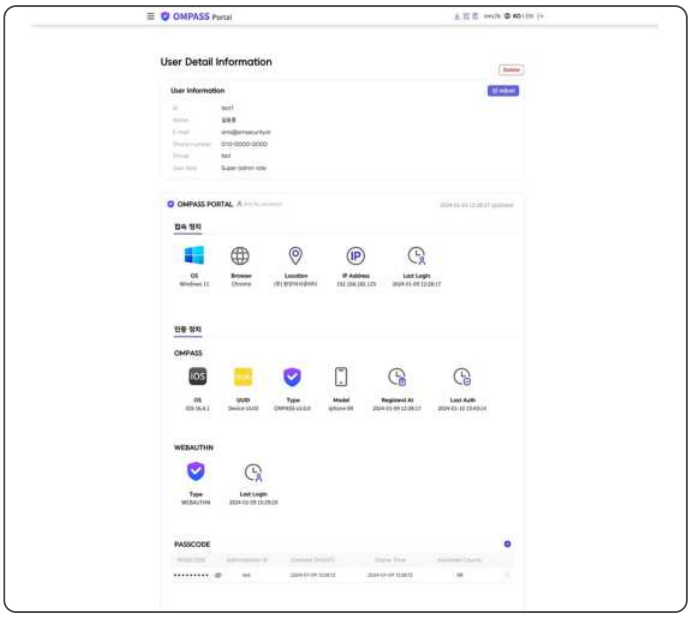
- Provides Windows login service
- Provides OTP authentication methods in an offline environment

Admin Page



- Provides dashboard functionality for administrators
- Provides application management, user management, and log management capabilities

Managing device properties



- Provides user and authentication device details management services
- Providing PASSCODE certification services for non-certified persons

We will keep create

customer-centric innovative technologies

with passion and insight.

For Any Inquiries,

Nury Kang

Manager

partner@omsecurity.kr

+82 10 5913 3882

www.omsecurity.kr

Unit 601 Smart Hub 1, 2150, Hannuri-daero, Sejong-si, Republic of Korea

OneMorePASS (OMPASS)

On-Premise/Cloud

FIDO(Fast IDentity Online) Service

OMS
One More Security