For all services that require user authentication

Ydentity2.0

Next Authentication Platform
Whykeykey

CONTENTS

01

Solution Overview

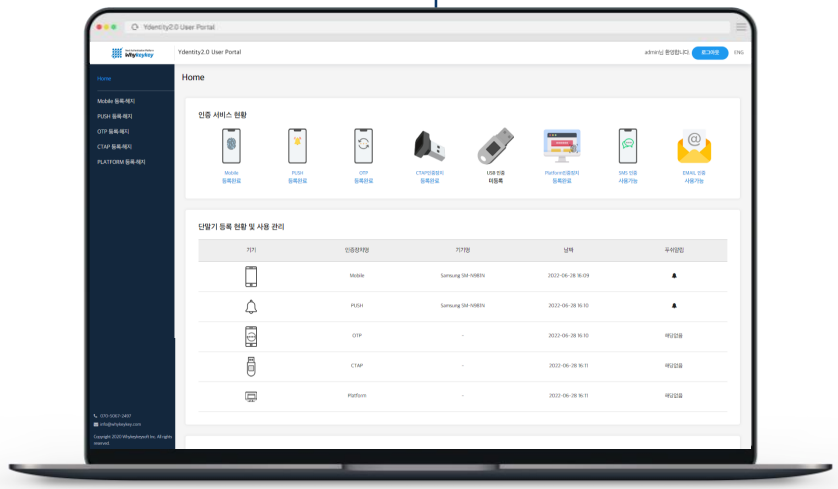
01

Ydentity2.0 – Simple and Fast Authentication Solution

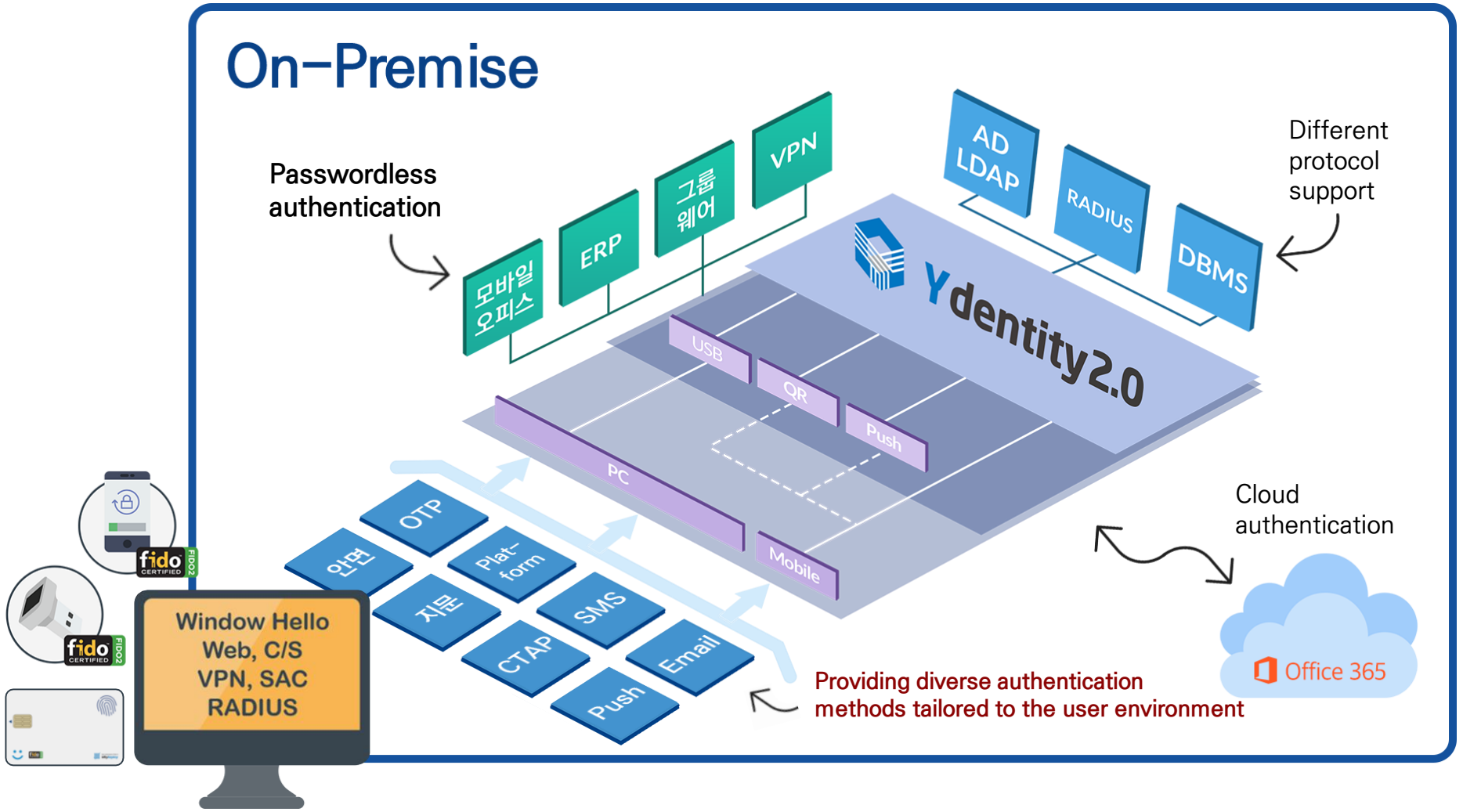
01 Enter only your ID

02 Authenticate fast and easy

03 Login Complete!

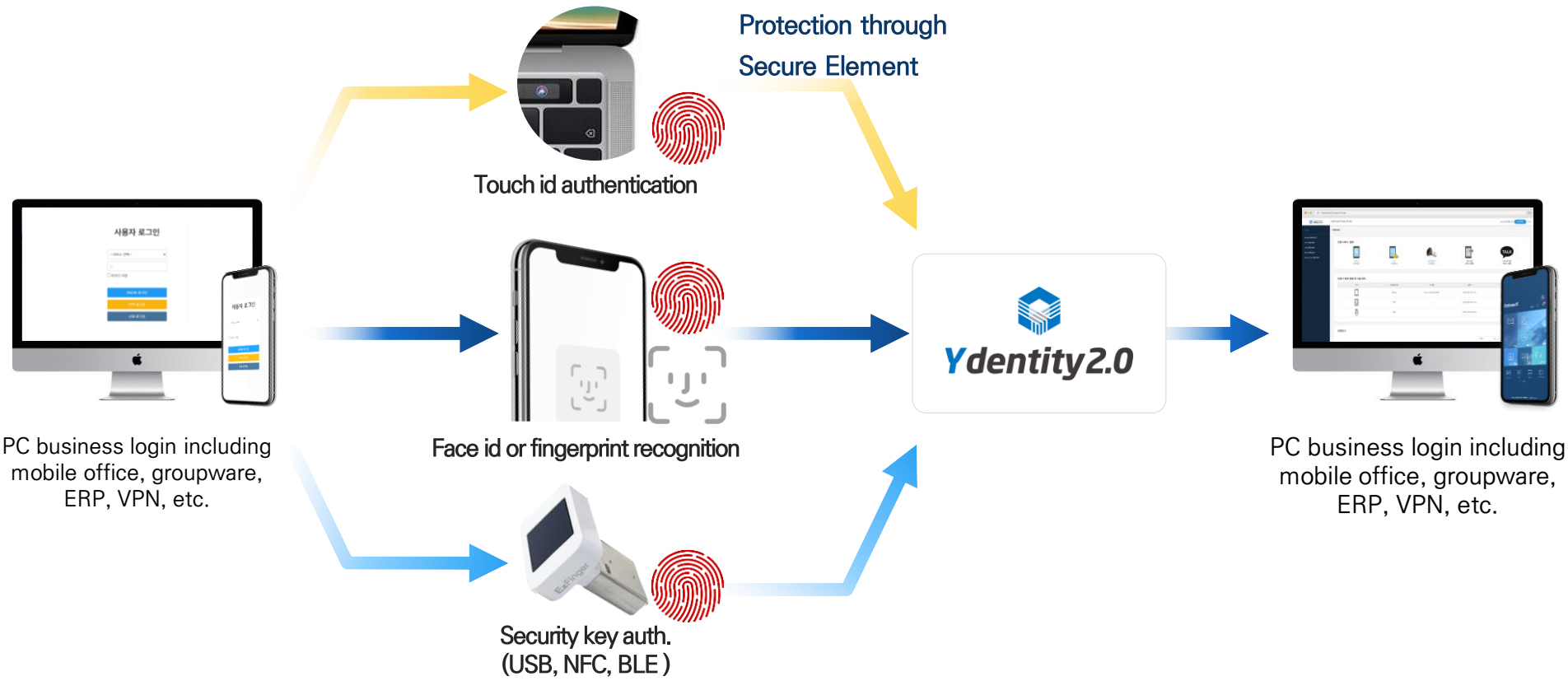


Ydentity2.0 - Integrated Authentication Solution Model



Authentication using Smartphone / Security Key

FIDO2 biometric authentication method enables simple and secure Passwordless authentication for mobile offices and business apps, such as ERP, Groupware, and VPN.



Alternative Authentication Methods

For devices without biometric support, alternative authentication methods such as OTP, Push, SMS, and Email are offered apart from FIDO authentication.

OTP

Push

SMS

PIN

Email

Enhanced versatility

By providing various additional authentication methods such as Push, OTP, SMS, and Email, Ydentity provides a convenient and secure authen tication environment even on devices that do not support biometric authentication.

Expanding legacy auth.

To ensure compatibility with 2G phone users and accommodate the existing SMS and OTP auth. methods, Ydentity can be applied to the legacy en vironment with minimal changes.

Integrated management

Through the integrated policy management function fo r various authentication methods using Ydentity2.0, it enhances management efficiency and effectiveness.

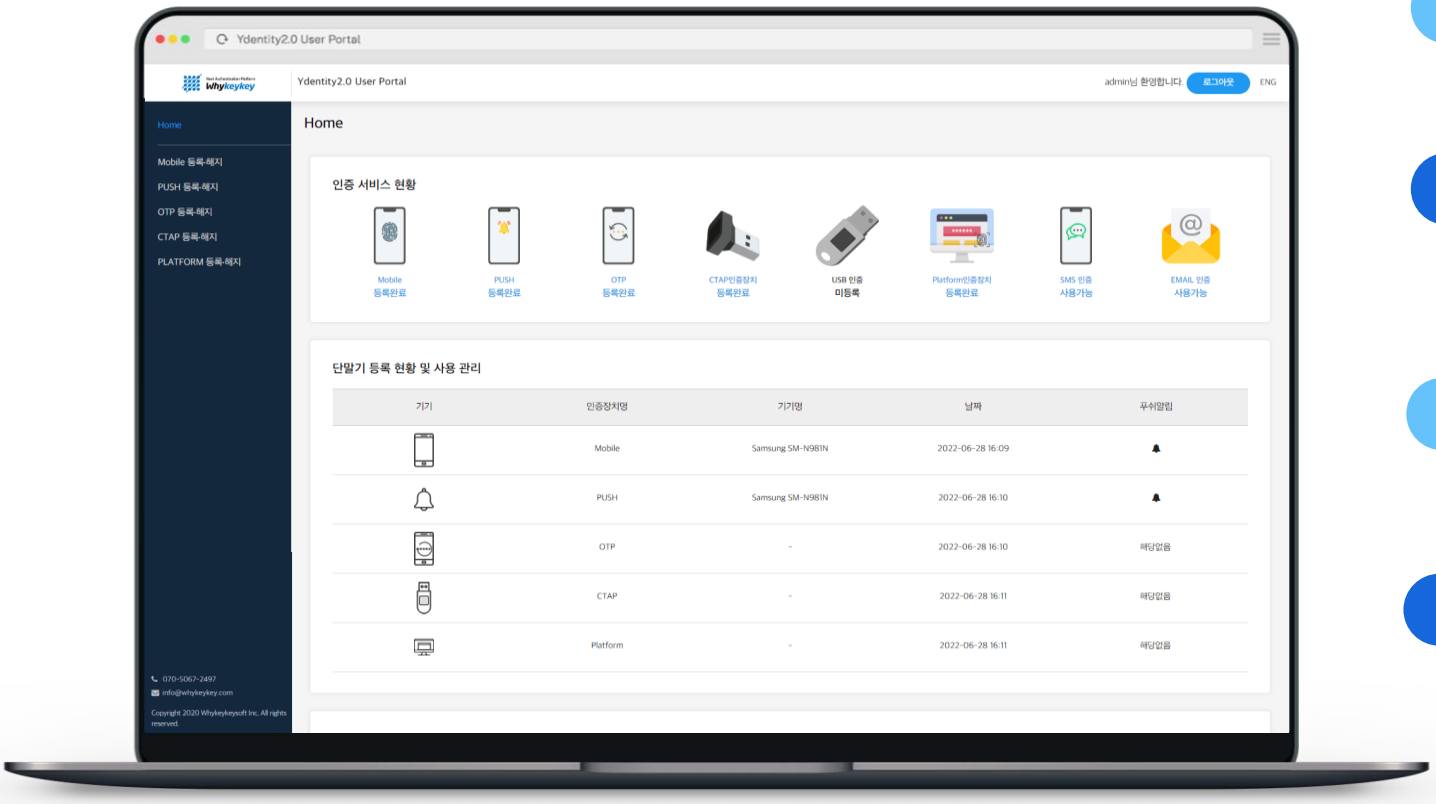
Ydentity2.0 Admin Portal

Admin Portal provides an intuitive dashboard to manage all authentication methods provided by Ydentity2 solution.

1. Updated status information window to facilitate service-specific analysis
2. Management of registered/unregistered users by service
3. Integrated management and view of registered authentication methods such as smartphone and PC biometrics, security keys, and OTP
4. Easy LDAP/DB/AD/Excel integration to quickly upload HR information
5. Support for easy REST API integration for service connectivity

Ydentity2.0 User Portal

Through the User portal, users are allowed to manage the registration and deletion of their authentication methods within the boundaries set by the administrator, which minimizes the admin team's work.



1. Support for Home to identify registered authentication methods

2. Multi-authentication method registration per service (Mobile/Push/OTP/CTAP/Platform/SMS /Email)

3. Self-service support for users to directly register, view, and cancel authentication methods as needed

4. One-time security link request for authentication when the device is not available

02

Solution Features

Reliability – Obtaining Certification Credentials

Ydentity2 solution has been verified for international compatibility by obtaining FIDO certification from the FIDO Alliance. In addition, it has achieved the highest grade of GS certification in South Korea and has been designated as an excellent information protection product, ensuring both reliability and security.

1등급 GOOD Software

GS Certification Grade 1

〈TTA – 2019〉

fido ALLIANCE

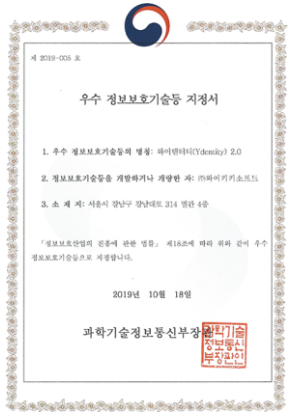
FIDO 1.0 and FIDO2 Certification

〈FIDO Alliance – 2018〉

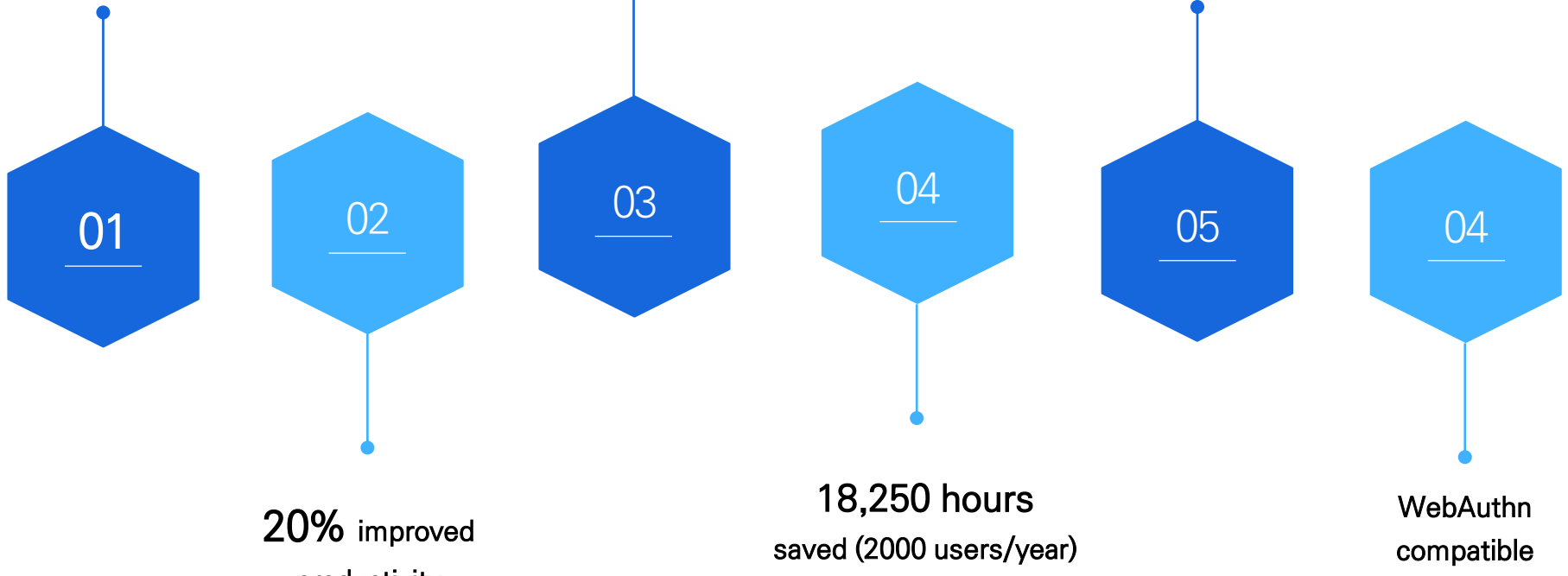
EPISC 우수정보보호제품 Excellent Information Security Product

Designated as an excellent information protection product

Ministry of Science and ICT – 2019



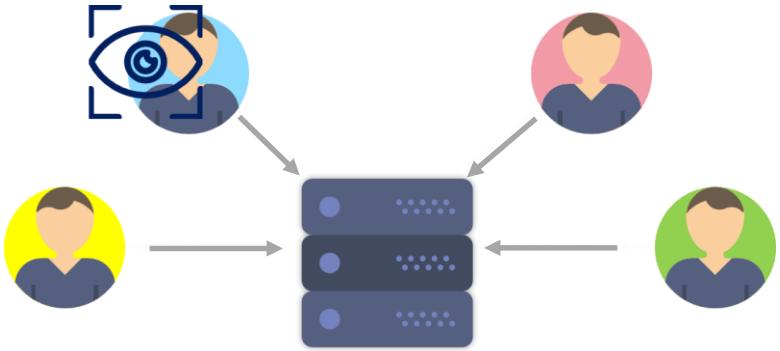
Why to choose Ydentity2.0 integrated authentication solution?



Distribution of Authentication Information based on PKI

Users' authentication information is not stored on vulnerable servers, making it safe from server hacking threats, and it allows for convenient use of various authentication methods without having to remember passwords.

Service provider-focused authentication information



Store/manage auth. data on server

Major hacking target,
2-3 consecutive damages occur when hacked

Distributed authentication information of users

Distributed management by authentication methods

Users keeps and controls the key authentication factors themselves.

A change in the authentication paradigm by innovating Credential storage and usage technology

Expandability – Securing a Wide Market with Flexible Compatibility

Ydentity2.0 can be deployed not only as a password replacement solution but also applied to all services that require user authentication in various areas.

B2C Service

- Service authentication
- User info management
- Online payment
- Digital signature

Enterprise Market

- Smart office and passwordless PC Login
- ERP and enterprise apps
- Online report
- VPN, SAC authentication
- Cloud access (SAC authentication)

03

Use Cases

Key Use Cases

Based on technologies verified by FIDO and GS standards both domestically and abroad, and with being chosen as Excellent Information Protection Technology, we carried out a number of FIDO certification projects.

SK Shieldus Blue Master Project

Applied quantum fingerprint security keys with FIDO standard to Blue Master, an unmanned security control system

AhnLab FIDO2 Project

Deployed Ydentity FIDO2 system to internal system; Binding VPN authentication using Radius protocol; HR information update through LDAP

Daejon Water Systems Project

Integrated FIDO quantum security keys and fingerprint security cards to consumer information systems

Prudential Smart Office FIDO2 Project

Deploying Ydentity2 service to SSO and smart office systems for internal users;
HR account update over LDAP;

Douzone Groupware FIDO2 Project

Deployed Ydentity2 to Groupware and ERP systems with Ydentity lib, SDK
Applied FIDO2 to browsers, messengers, and mobile apps

Nuri Telecom FIDO2 Biometrics Project

Deploying FIDO biometric authentication with CTAP devices

ETRI FIDO Project

Developed FIDO2 BLE technology in partnership with ETRI

KICA Digital Signature Project

Developed no-install HTML5 digital signature and PDF signature service; Multi-OS development of Public Certificate Solution

MegazoneCloud Project

Developed standard different biometrics-based user authentication framework

Bio-data Distributed Management System (FIDO)

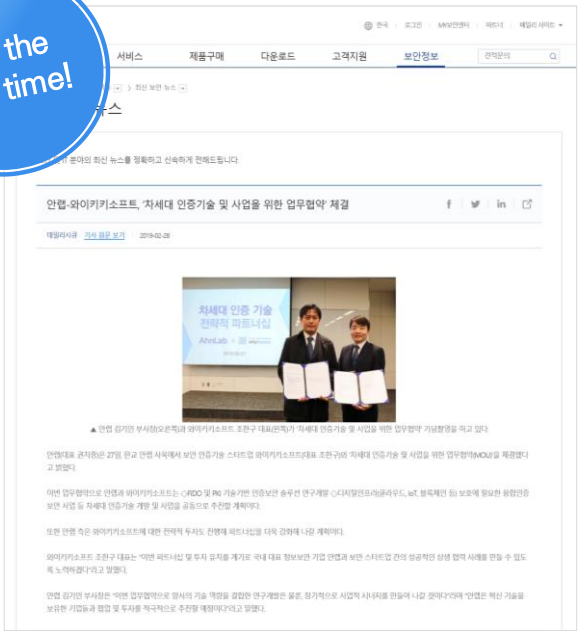
Deploying distributed management system of bio information using FIDO technology

Establishing Alliance and Deploying Authentication Service for AhnLab, Domestic Leader of Security

Strategic Investment

- AhnLab invests in WhyKeyKeySoft, authentication technology startup
- WhyKeyKeySoft deploys AhnLab products with biometric authentication solution
- Establishment of a win-win cooperation model for SMEs;

For the first time!



Authentication service for employees

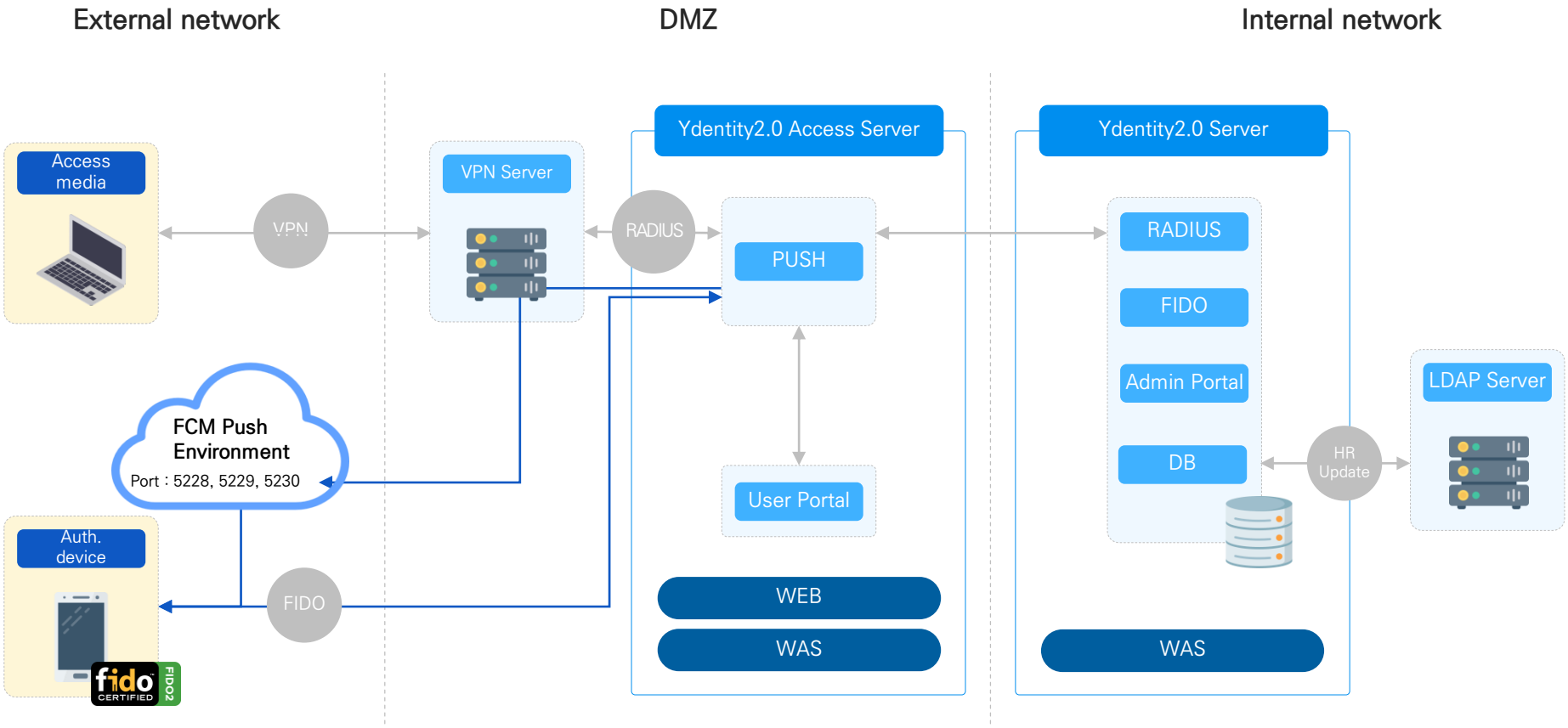
- Deploying fingerprint-based authentication for executives and employees;
- No impact for the existing legacy environment;
- Use of RADIUS protocol;

Enhancing VPN authentication

- Fast and simple authentication and secondary additional authentication for VPN customers;
- Cost and time-saving effects with built-in authentication;

AhnLab Use Case

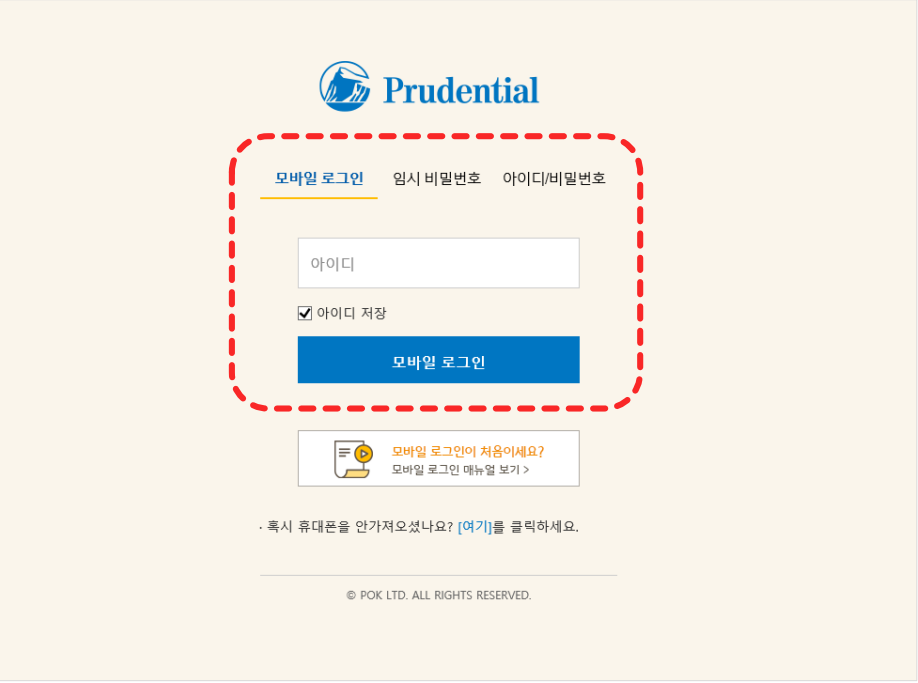
Established partnership with AhnLab and deployed passwordless authentication solution, with VPN authentication by Ydentity's own RADIUS protocol, and HR data update option through LDAP



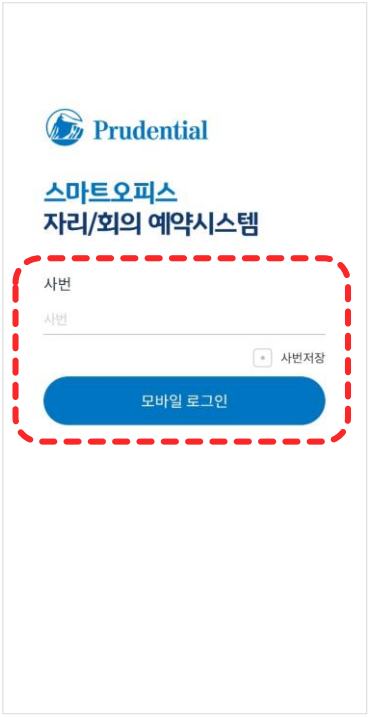
Prudential Life Insurance Use Case

Prudential introduced Ydentity2.0 solution as a smart office authentication system, and as an authentication login method for SSO and seat reservation service for customers.

Prudential SSO(PC)

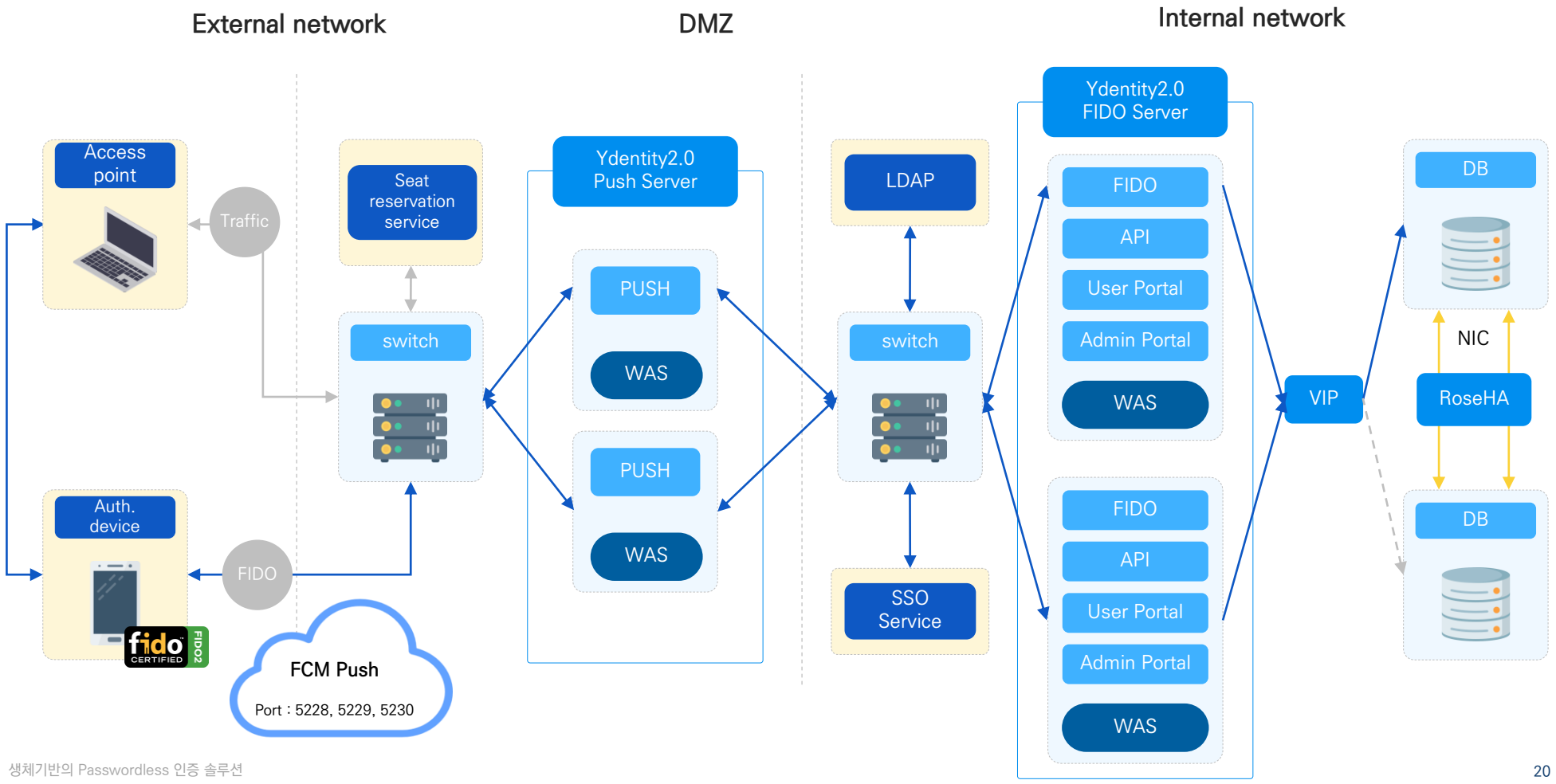


Prudential Seat reservation Service (Mobile)



Prudential Life Insurance Use Case

Below is a model of the authentication solution, Ydentity2, deployed into Prudential company's internal system, which enables easy and fast SSO authentication, user account linking through LDAP, and easy authentication for seat reservation service.



SK Shieldus(ADT) - Unmanned Security Control System

SK Shieldus(ADT) implemented Ydentity2 solution as a pilot infrastructure and operation project for 2021 quantum encryption, and applied it as a secondary authentication jointly with Blue Master, an unmanned security control system.

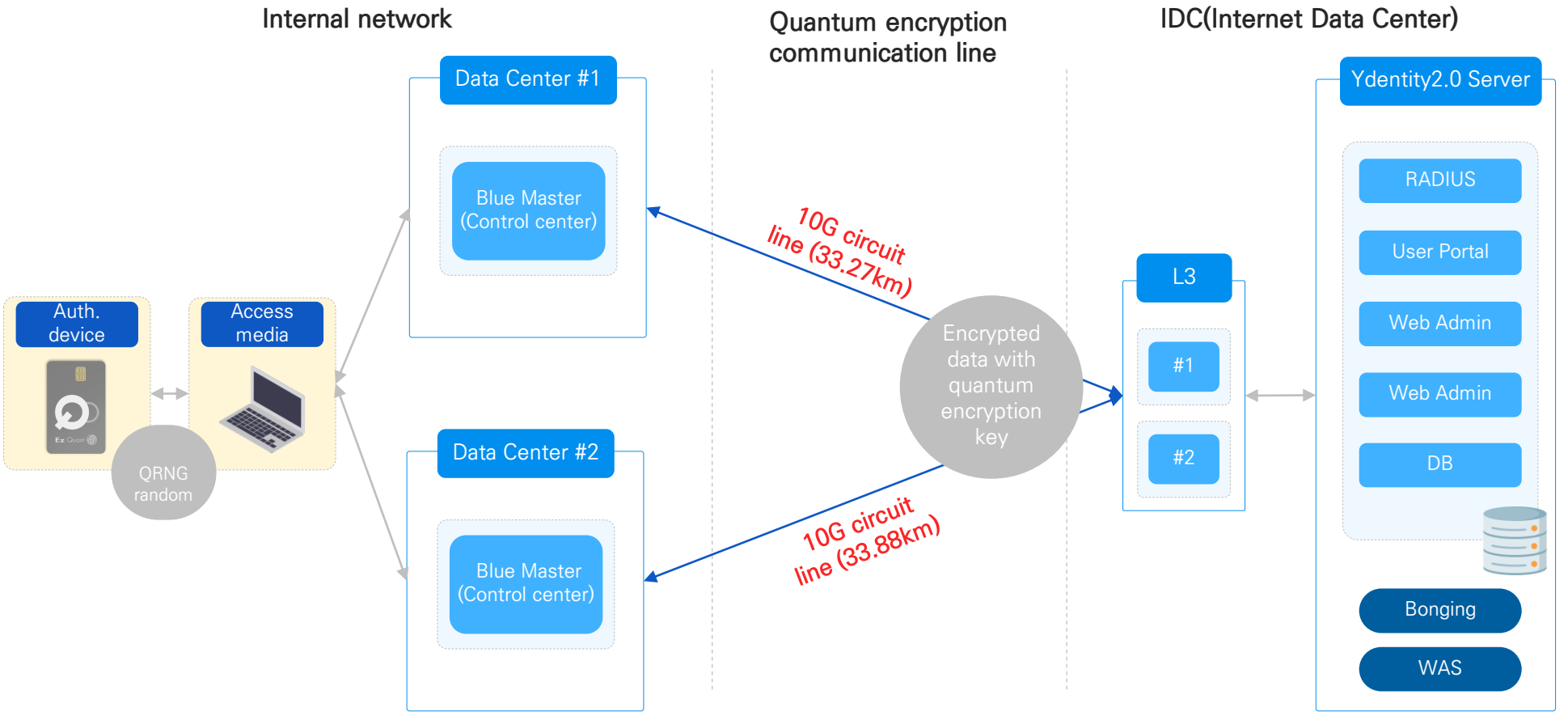
Powerful and simple
quantum encryption

EzQuant Security Card

- FIDO fingerprint security key using quantum technology;
- Generates unpredictable, un-hackable encryption keys;
- Portable and convenient;
- Physical and online authentication at once;
- Fingerprint recognition technology that accurately identifies users;
- Comes with USB type card reader;

SK Shieldus(ADT) Use Case

SK Shieldus implemented Ydentity 2.0 authentication solution, two Blue Masters in data centers were integrated to authenticate with a security key card, EzQuant, a communication line dedicated to quantum encryption was established.



Daejon City Water Supply Unit - Consumer Information System

Daejeon City Water Supply Unit integrated Ydentity2 solution as a pilot infrastructure for quantum cryptography encryption and applied it as an authentication method for access to consumer information system.

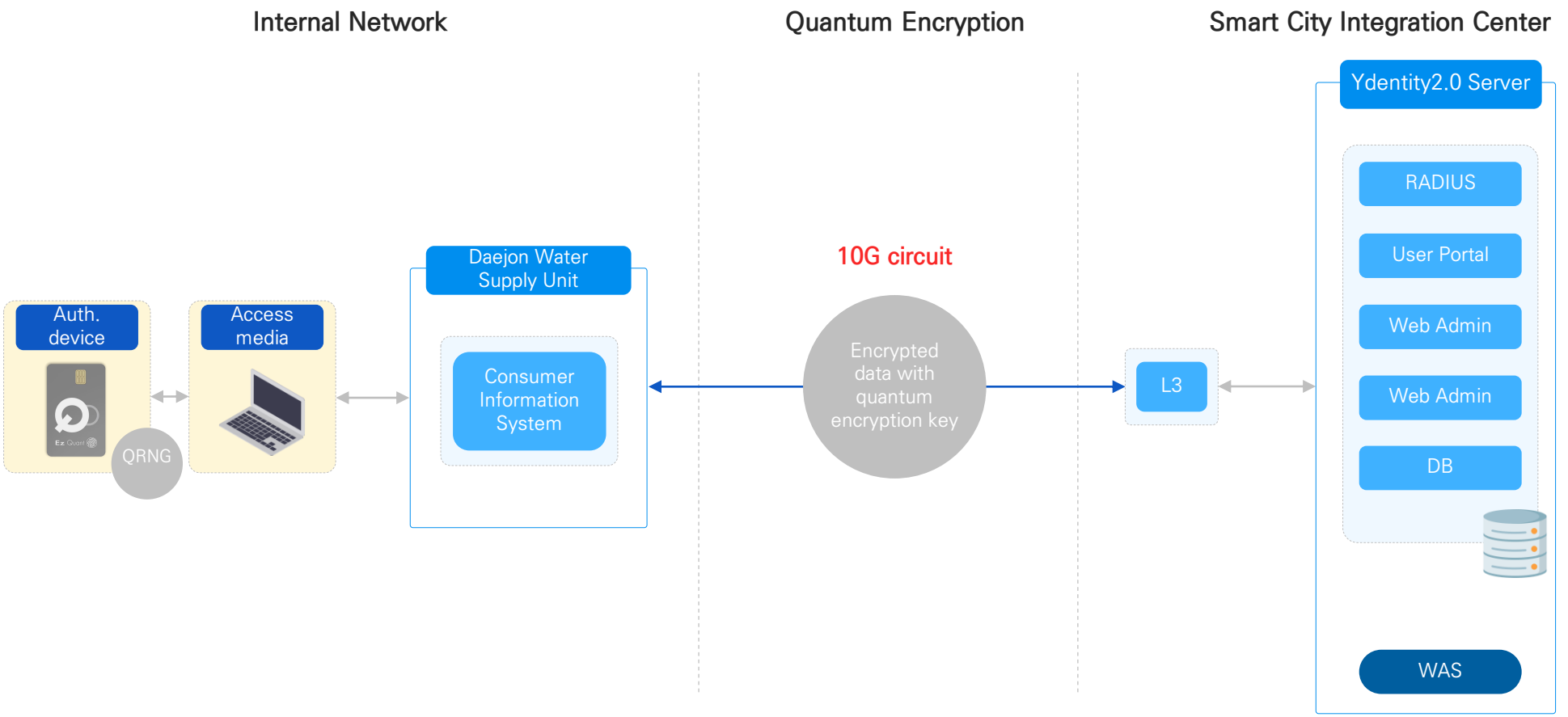
Powerful and simple
quantum encryption

EzQuant Security Card

- FIDO fingerprint security key using quantum technology;
- Generates unpredictable, un-hackable encryption keys;
- Portable and convenient;
- Physical and online authentication at once;
- Fingerprint recognition technology that accurately identifies users;
- Comes with USB type card reader;

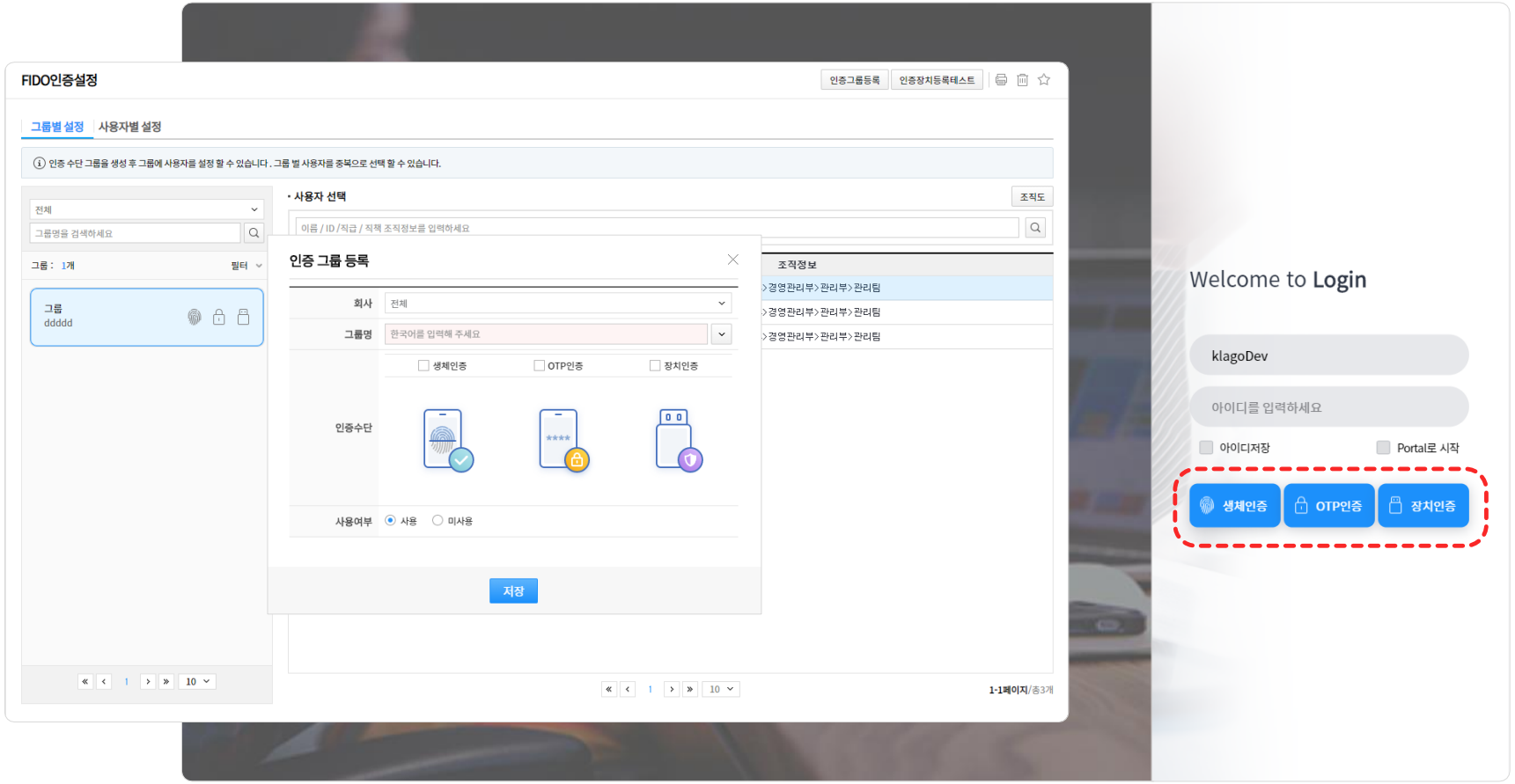
Daejon City Water Supply Unit - Consumer Information System

This is a configuration model of Ydentity2, deployed into the consumer information system of Daejeon City Water Supply Unit, in which user data is protected through quantum encryption through a security key card authentication.



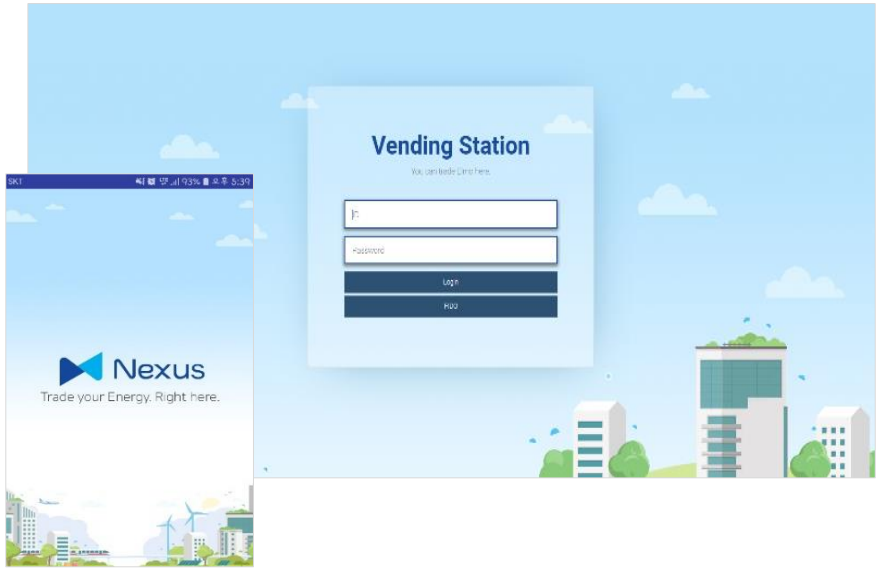
D Group Use Case

Company D integrated Ydentity2 SDK solution to their groupware (ERP) solution, which has the largest number of users in South Korea.



Expanding the solution to a variety of services that require user authentication

Africa Ghana
Cryptocurrency exchange for electric power transactions



- Provided biometrics-based, PIN-based Ydentity2 authentication service for cryptocurrency exchanges
- Verified flexibility through AWS (European)-based cloud environments

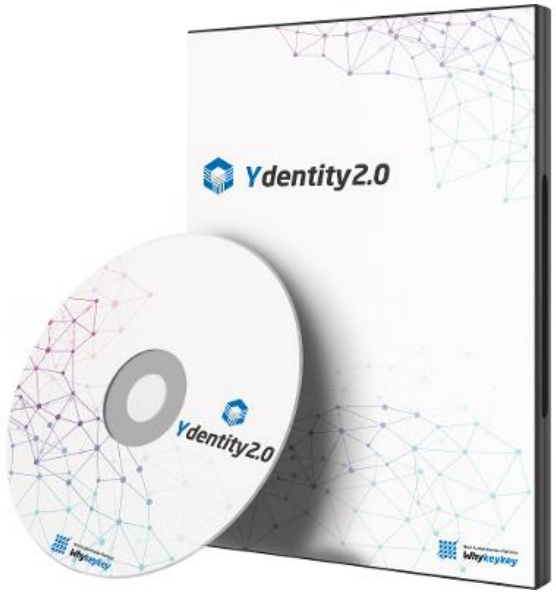
Incorporation of next-generation authentication solution for future smart vehicles

(Research project of the Ministry of Science and ICT)

04

Deployment and Maintenance

Procurement Registration Info



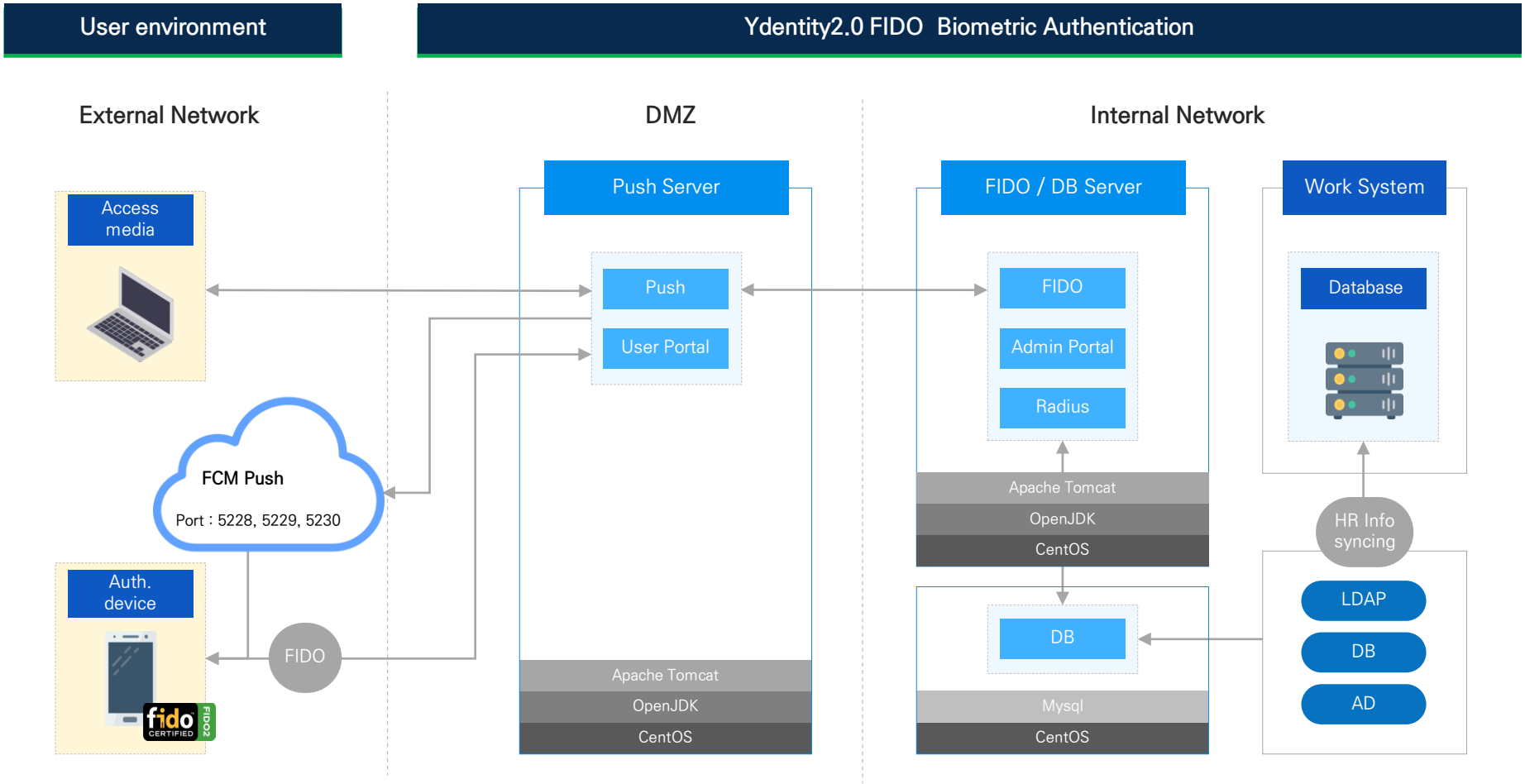
A simple and fast authentication management software with both reliability and security

- Completed interoperability testing and obtained certification for FIDO1.0 and FIDO2 from FIDO Alliance;
- Fast and easy authentication solution with biometrics-based, CTAP, OTP and other options instead of traditional login methods ID/PW and public certificate;
- All authentication factors and integration systems can be managed in one platform;
- Applicable for various online services including ERP, online banking, mobile payment, games, portals, e-signatures, groupware, and authentication services.

Category	License	Client/iOS	Client/Android	FIDO 2.0 Server
Inventory No.	43231512-24350015	43231512-24350014	43231512-24350013	43231512-24346834
Classification No.	43231512	43231512	43231512	43231512
Identification No.	24350015	24350014	24350013	24346834
Registration date	2021-09-02	2021-09-02	2021-09-02	2021-08-31
Item Name	인증관리시스템, 와이키키소프트, Ydentity v2.0, 연동 라이센스	인증관리시스템, 와이키키소프트, Ydentity v2.0, FIDO 2.0 Client/iOS	인증관리시스템, 와이키키소프트, Ydentity v2.0, FIDO 2.0 Client/Android	인증관리시스템, 와이키키소프트, Ydentity v2.0, FIDO 2.0 Server

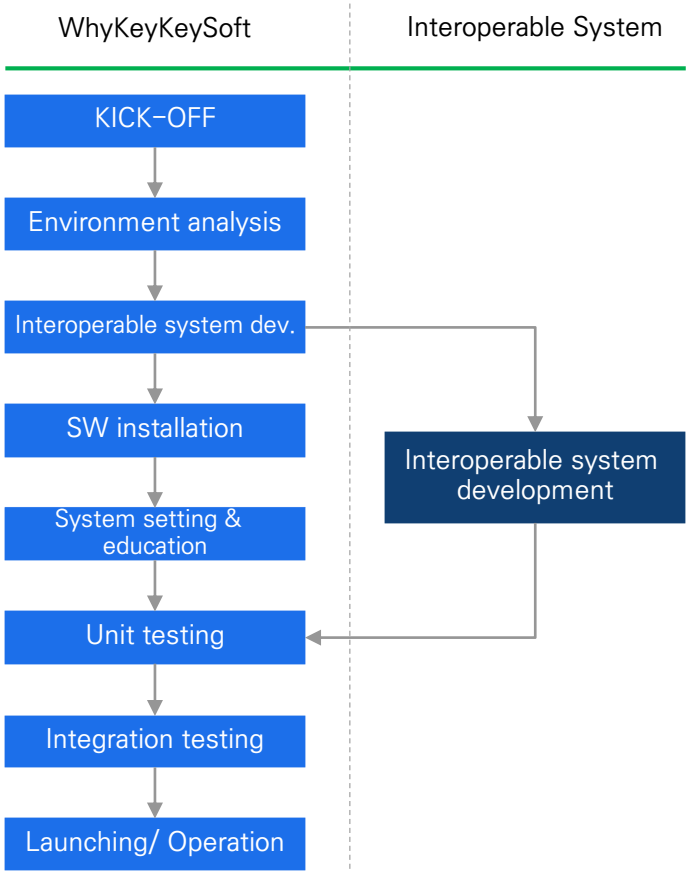
Solution Configuration

Ydentity2.0 consists of Push Server, FIDO Server, and DB Server. It is configured based on customer requirements, using either a single server or three separate servers.



Deployment Roadmap

WhyKeyKeySoft is successfully building FIDO-based authentication systems through a systematic deployment process that accurately checks necessary requirements with pre-environmental analysis.

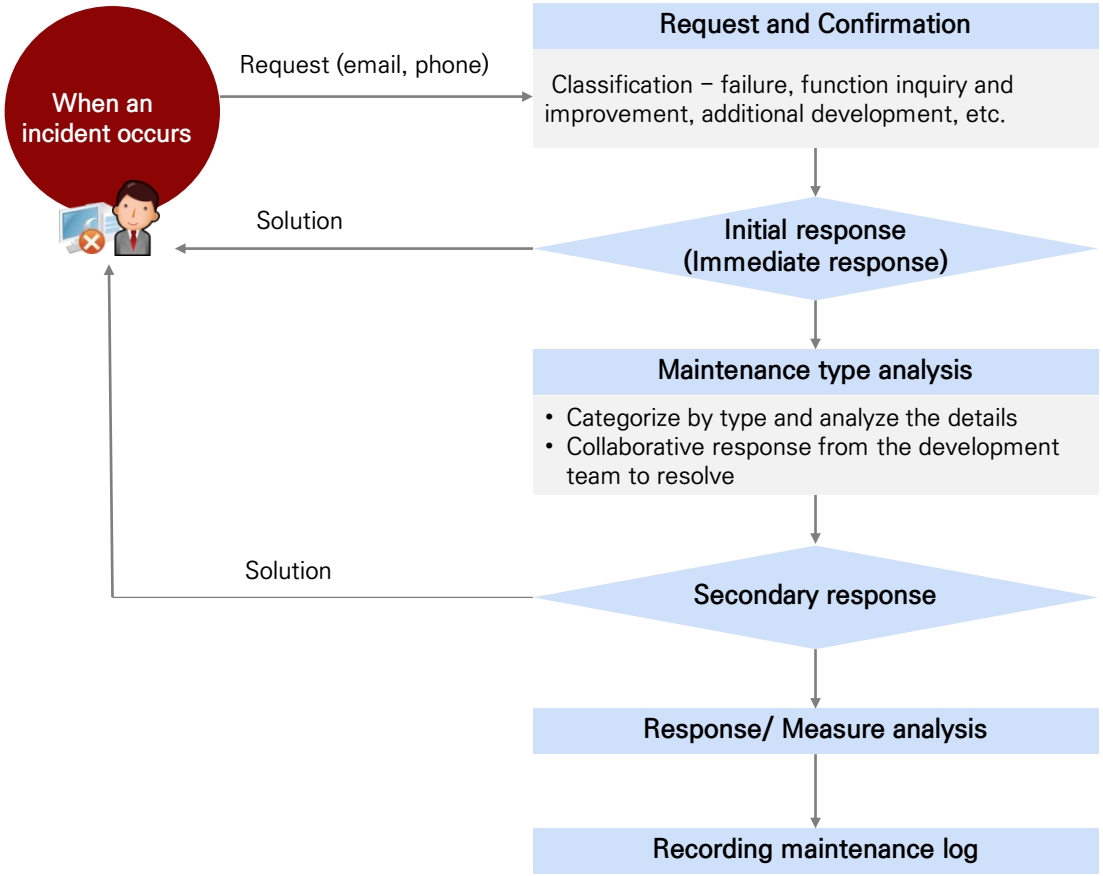


Step	Specifics
KICK-OFF	• Providing guidance on contract terms and contact person; • Discussing deployment schedule and providing guidance on necessary items
Environment analysis	• System environment analysis (OS, DB, redundancy, network, firewall settings, etc.)
Interoperable system dev.	• API provisioning for interoperable system development
SW installation	• Ydentity2.0 installation (server, mobile, etc.)
System setting & education	• Integration of HR data (LDAP, AD, etc.) and education of administrators for SMTP and authentication policy settings
Interoperable system development	• Developing customized page for Ydentity2.0 login (developed by the target system developer)
Unit testing	• Testing of HR data integration, SMTP, and authentication policy application with Ydentity2.0 • Login testing with the integrated system;
Integration testing	• Integration testing • Operation testing
Launching	• Ydentity2.0 launching and operation

Maintenance

We promptly address any issues that occur within the free or paid maintenance period through immediate initial measures via hot-line and secondary measures including on-site visits to resolve the situation.

Maintenance Process



1. Receipt of maintenance request

- Request : Customer → Support team
- If a problem is identified beforehand, the maintenance support team immediately informs the customer representative.

2. 1st Maintenance measure

- Immediate resolution of issues that can be resolved quickly.
- If it is difficult for the support team to solve the problem, they notify the development team for joint response.
- Action management and similar situation response through type analysis.

3. 2nd Maintenance measure

- Depending on the situation, the development team cooperates with the maintenance support team and takes appropriate action.
- In situations requiring an on-site visit, the support team visits the customer's site.

4. Reporting response result

- Reporting results from maintenance measures

5. Maintenance log

- Record maintenance results and manage history.

THANK YOU

Next Authentication Platform
Whykeykey

A. 서울시 강남구 테헤란로 87길 57 감령빌딩 5층(06166)

T. 02-576-4746

F. 02-578-4745

W. www.whykeykey.com