# ISign+ White Paper

## All-in-One Appliance-Type Authentication Platform

ISign+ Product Inquiries
infra@pentasecurity.com

Penta SECURITY

# Contents

# Introduction

## Overview

Hacking is a growing threat. People log in daily to countless number of web application services, from web portals and social media platforms to shopping sites and groupware programs. According to a survey conducted by McAfee, an average person possesses 23 online accounts. Web application services provides convenience to the users, but also result in an ever-growing pool of user data. Consequently, the more personal data there are in a database, the higher the risk of hacking.

Based on Verizon's 2020 Data Breach Investigations Report, credential-based attacks (i.e. account hacking) has been the most common cause of data breaches, accounting for 37% of all accumulated cases reported. It also made the second-most common cause of data breaches in 2020 so far (see Fig 1). The reason credential-based attacks are so common is because people tend to reuse passwords for different accounts. At least 65% of people reuse password across different accounts (Google), while 73% of people use the same passwords for their personal and business accounts (Microsoft).

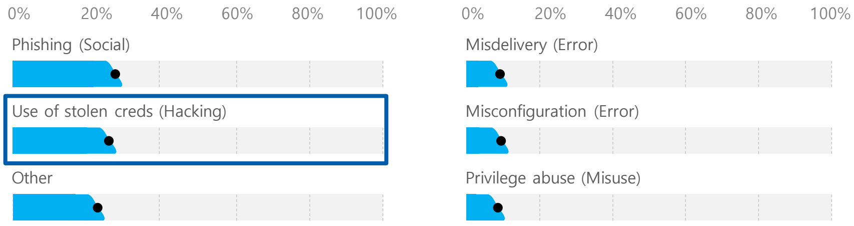


**Fig 1**. 2020 Top threat Action varieties in breaches (n = 2,907)

The theft of account credentials can lead to very severe consequences. IBM's Cost of a Data Breach Report published in 2019 estimated the average financial loss of a data breach to be $3.92 million.

A majority of public and private organizations already use a variety of cybersecurity products and solutions to manage their data security risks. Yet, data breaches still happen frequently because of two loopholes: 1) accounts with excessive authority, and 2) lack of multi-factor authentication (Oracle). Moreover, when installing new solutions, many try to configure them in a way that would not change their existing solutions. The downside of doing so is that when problems arise during use, it can be difficult to identify the exact cause.

To overcome such shortcomings and to prevent data breaches, an appliance-type authentication and authorization solution is essential.

# Introduction

## Case Study: Authentication Security Threat

Data breach incidents are usually caused by a combination of different vulnerabilities. Below is a list of three data breach incidents caused by insufficient authentication and authorization measures.

- **Case 1**: H Supermarket Customer Data Leakage Incident

  H Supermarket, a Korean online grocery platform, leaked the personal data of over **49,000** customers. This had led to unauthorized logins and losses of loyalty points. It was confirmed that an unknown individual gained access to the accounts with a credential stuffing attack utilizing ID/PW combinations stolen from another website.

  After gaining access to the accounts, the hacker went into the purchase history of other users to transfer loyalty points equivalent to more than $4,000. The intrusion took place between October 17, 2017 and October 1, 2018, only to be discovered when users started to report that their loyalty points were not accumulating.

- **Case 2**: M Hotel Data Breach of Guest Information

  On April 1, 2020, international hotel chain M Hotel suffered a data breach that compromised the personal details of **5.2 million** guests, including full names, email addresses, phone numbers, and dates of birth. Third-party real estate agents who were given access to M Hotel's customer database abused their access rights and leaked the personal data of the guests. Following the incident, M Hotel immediately deauthorized their accounts.

- **Case 3**: Profit Management Solution Provider Data Breach

  B Firm, an American-based provider of profit management solutions for healthcare institutions, suffered a data breach that leaked the names, dates of birth, diagnosis codes, and the social security numbers of **274,837** patients.

  Between April 20 and April 30, 2020, hackers stole the login credentials of an employee and spread malware to the internal systems of the company. This was only discovered when malicious codes were found in some servers. The malicious software was later removed by taking the system offline.

# Key Concept

## Authentication & Authorization

Imagine being a visitor to a company, you would first need to prove your identity by telling the receptionist who you are, why you came, who invited you, along with other necessary documents, before being given a visitor pass.

**Authentication** (commonly referred to as **Identity Management**) is the process of verifying whether someone is who they claim to be. In the enterprise context, every organization store data that include valuable information and resources, making it necessary to secure them by verifying the identity of those who request access to such data. Only those who have their identities verified should be granted access to the systems, networks, databases, and website backends.

The two common vulnerabilities related to authentication is 1) illegal bypass of authentication and 2) loss and theft of login credentials. In fact, "broken authentication and session management" made the second spot on the 2017 OWASP web application vulnerabilities list, showing how crucial it is to have a secure authentication procedure in place.

Authentication can be done with a variety of methods. Based on the authentication procedure used, they can be categorized into knowledge-based, possession-based, biometric-based, and behavior-based methods.

| Authentication Method | Description | Examples |
|---|---|---|
| Knowledge-based | What you know | ID-PW, PIN |
| Possession-based | What you have | Token, Smart Card, OTP, Verification Code |
| Biometric-based | What you are | Biometric Authentication |
| Behavior-based | What you do | Signature, Gait |

Knowledge-based authentication works by comparing a piece of knowledge that is only shared between the user and the authenticator, such as ID-PW and PINs. It is commonly used as the primary authentication method due to its ease of use (i.e. no need to carry any physical items). Yet, due to its vulnerability to credential stuffing attacks, it is usually complemented by another secondary authentication method for enhanced security.

Possession-based authentication requires the use of a third-party medium to generate unique information for one-time authentication purpose. Such media include tokens, smart cards, OTPs (one-time-passwords), and text and email verification codes.

# Key Concept

The major downside is that it is less convenient as the user would have to have their token, card, or smartphone available at the time of authentication. Nevertheless, it is highly secure and is often used as a secondary authentication method.

Biometric-based authentication utilizes the user's biological characteristics (e.g. fingerprints, voice, iris, facial shape, and heart rate) for authentication. This method offers very robust security and convenience. However, if the stored authentication information is leaked, there is no other means of restoring it.

Behavior-based authentication analyzes the user's behavioral characteristics, such as signatures and gait. In particular, gait recognition analyzes the individual's walking speed, stride length, knee bending angle to verify the identity of the user.

In the past, authentication was performed only with passwords. As smartphones become increasingly prevalent, mOTP (mobile OTP), QR, fingerprint, and iris authentication have been introduced in various web and application services. To provide enhanced authentication security, two-factor authentication (2FA) and multi-factor authentication (MFA) that use two or more authentication methods at the same time gained popularity. The FIDO (Fast Identity Online) protocol further enabled the authentication method of smart devices to a web server.

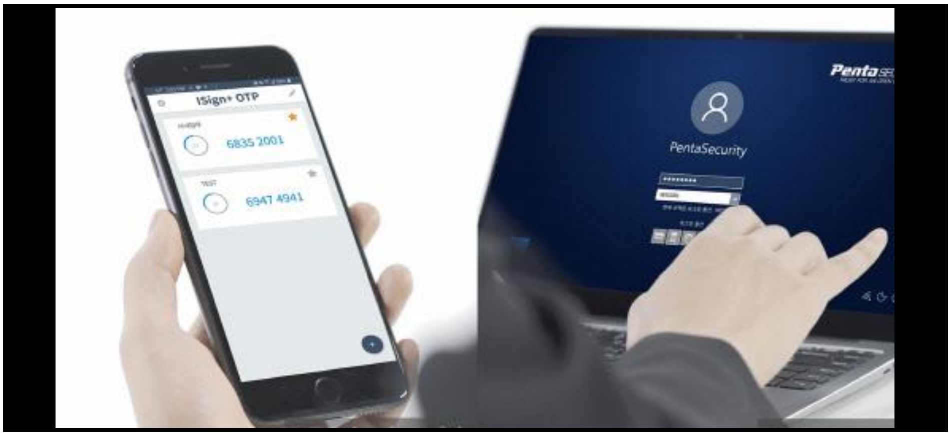


**Fig 2**. Logging in with mOTP

# Key Concept

A typical business contains of a variety of information systems. It would be extremely inefficient to have different types of authentication procedures for each system. **Single Sign-On (SSO)** was introduced to solve this problem.

SSO enables secure authentication for all connected services by allowing the user to manage all passwords through one single login. With SSO, enterprises can achieve business simplification and standardization with centralized user management.

The SSO procedure consists of an authentication server, an integrated agent, and the Lightweight Directory Access Protocol (LDAP). The integrated agent manages authentication information for each divided information system. During the SSO authentication process, strong authentication using PKI, biometrics, and OTP is implemented. Encrypted communication such as SSL is utilized to help the user to securely connect to each service.

SSO can be constructed with two different models – authentication agency model and authentication information delivery model. Authentication agency model is often implemented when it is difficult to alter the existing authentication method of each service. Every time a user logs in to a service, the integrated agent substitutes the original authentication methods. Under the authentication information delivery model, the user requests an integrated token from the authentication system, then uses that token to log in to each service (see Fig. 3).

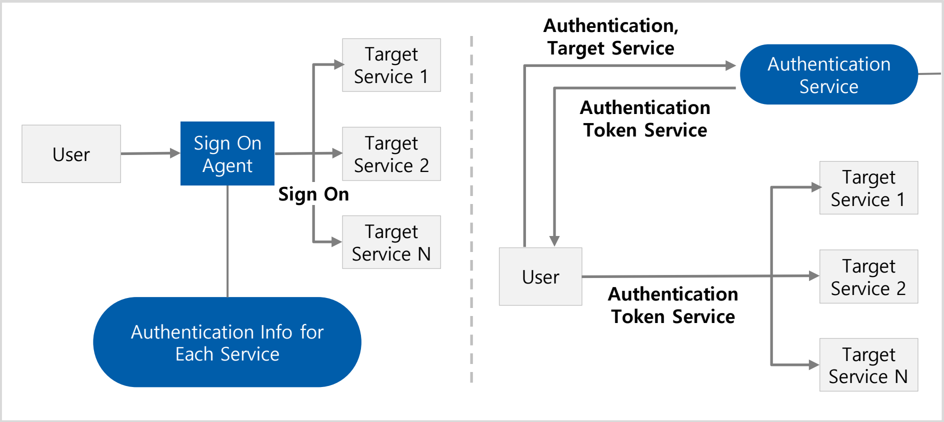


**Fig 3**. SSO Construction Models

Now imagine you have received a guest pass to the company you are visiting, you are now allowed into certain areas of the office. Yet, there would still be restricted areas where you are not allowed into.

# Key Concept

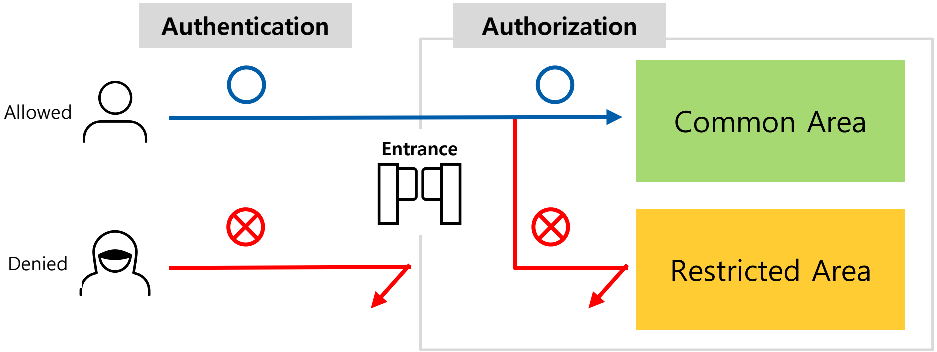


**Fig 4**. Identity and Access Management Based On Authentication and Authorization

**Authorization** (commonly referred to as **Access Management**) happens one step after authentication. After a user logs in to the account, authorization is the process of granting the user access to certain resources while restricting them from the rest. In other words, authorization manages behaviors that take place inside the system. Authorization can be done by utilizing different criteria such as role, group, location, time of the subject, etc.

Role-based access control (RBAC), for example, is where the authorizer grants the user with rights according to their roles within the organization. The United States' Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and the Payment Card Industry Data Security Standard (PCI DSS) both require the use of RBAC for user authorization.

Lastly, Extranet Access Management (EAM) is a security solution that can differentially control access to resources based on authorization. Simply put, EAM is a combination of an SSO and an integrated access management solution. Access to user information can be controlled centrally through EAM.

Access management mainly uses the role-based authority control (RBAC) method, after which EAM can be used to monitor real-time user status.

# Key Concept

## Multi-Factor Authentication & FIDO

Important items are always stored with multiple layers of protection. The same goes for information and digital resources. To provide enhanced protection for sensitive information and resources, multiple authentication methods are combined. A combination of two authentication methods is called **two-factor authentication (2FA)**, whereas combining multiple authentication methods is referred to as **multi-factor authentication (MFA)**.

With MFA in place, even if the password for an account is exposed, it would be still very difficult for a hacker to pass through due to a second layer of protection. According to research by Google, with device-based two-factor authentication applied, 100% of bots and 96% of phishing attacks can be mitigated.

With the advent of FIDO, discussions on replacing existing passwords with biometric authentication began. Companies such as Google, Microsoft, PayPal, and Samsung Electronics have established the FIDO Alliance to create a simple and secure authentication system using biometrics. The FIDO Alliance created protocols like the UAF[1] and U2F[2]. These FIDO protocols are recognized as the international standard by the World Wide Web, the International Telecommunication Union (ITU), and the International Organization for Standardization (ISO).

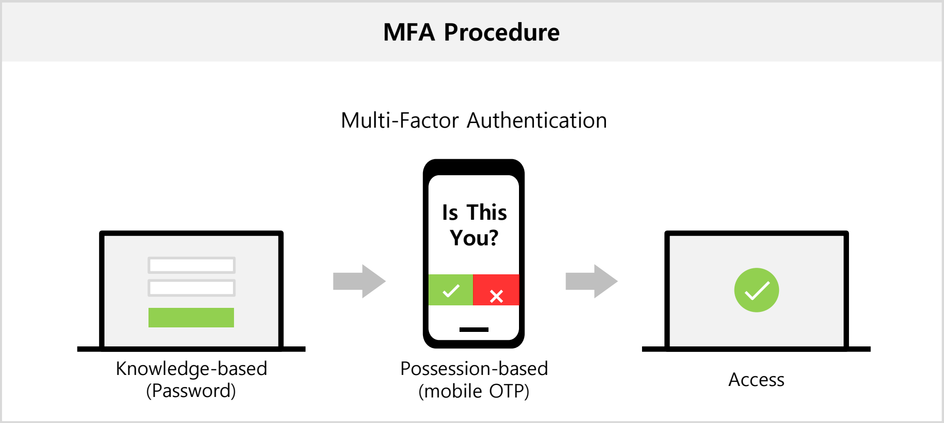


**Fig 5**. Multi-factor authentication significantly decreases risk of hacking

FIDO reduces the risk of hacking by storing biometric information in the device rather than the server, then authenticating by verifying the public key. Developed from FIDO 1.0, which started in mobile environment in 2014, FIDO2 that is applied in all

[1] UAF : Universal Authentication Framework

[2] U2F : Universal 2nd Factor

# Key Concept

environments including PC and web appeared in 2018. Web applications with FIDO2 are much easier and safer to authenticate than conventional passwords.

## Appliance

Appliance refers to an information device that can be deployed and used immediately by connecting to a power supply, without the need to install any operating system or application software.

The main advantages of appliance-type products are that they are quick to execute and easy to maintain. Server, storage, network hardware, operating system, and applications are integrated and optimized prior to purchase, significantly reducing system configuration time. Most businesses today prefer appliance-type products as they save plenty of time and resources. Hence, for authentication security products, where easy of maintenance and stability are the top priority, an appliance-type product like ISign+ makes the perfect solution.

# ISign+ for Security

## Robust Authentication Security and Access Management

Secure SSO/EAM ISign+

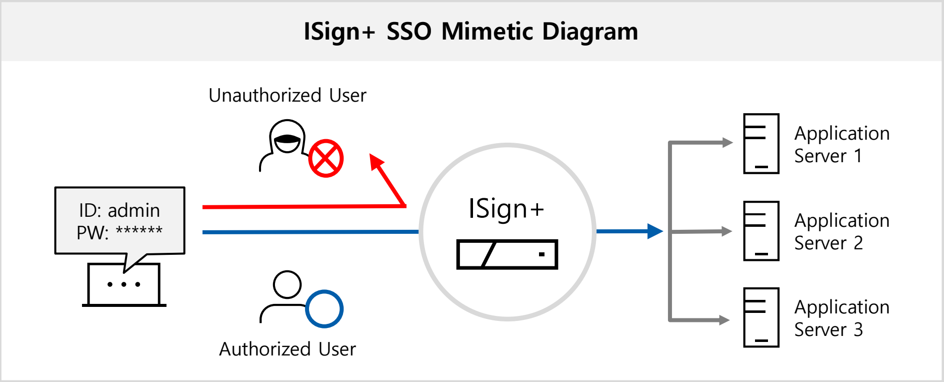
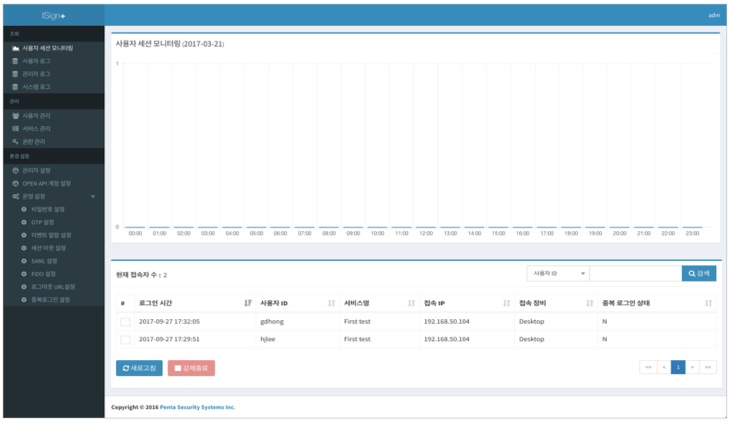


**Fig 6**. ISign+ Secure SSO Feature Allowing Only Authorized Users to Access the System

ISign+'s Secure SSO allows authorized users to have secure, repeatable access to authorized systems without authentication. It also includes an integrated account management function that collects, processes, and transmits various accounts existing in each business system to the required applications.

By using ISign+, managers can conveniently monitor user/service status in real time. Through ISign+'s web management tool, managers can check and manage logs such as login/logout and status including time, account, access equipment and redundant login status of real-time users. In particular, dual login protection prevents user account theft/session extortion.



사용자 세션 모니터링 (2017-03-21)

현재 접속자 수 : 2

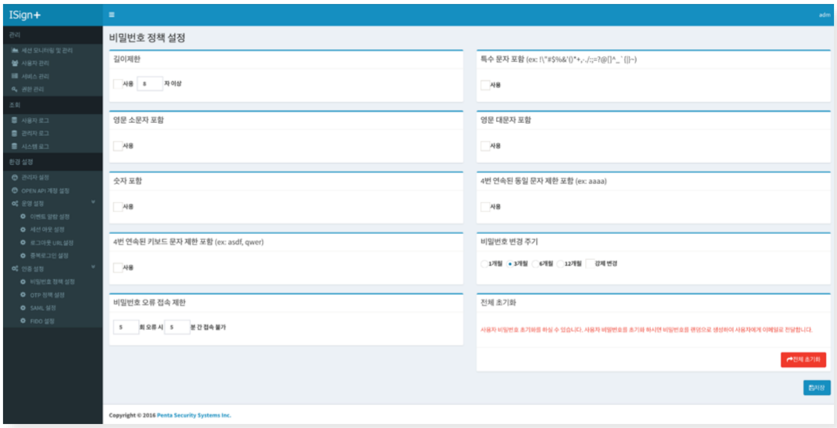
| # | 로그인 시간 | 사용자 ID | 서비스명 | 접속 IP | 접속 장비 | 중복 로그인 상태 |
|---|---|---|---|---|---|---|
| □ | 2017-09-27 17:32:05 | gdhong | First test | 192.168.50.104 | Desktop | N |
| □ | 2017-09-27 17:29:51 | hjlee | First test | 192.168.50.104 | Desktop | N |

Copyright © 2016 Penta Security Systems Inc.

**Fig 7**. ISign+'s Web Management Tool Screen [User/Service Status]

# ISign+ for Security

ISign+'s password management feature allows security to be strengthened through password policy setting, and passwords can be safely managed through encryption when stored. In addition, ISign+ has functions such as limiting the number of logins, warning of illegal login attempts, and re-authentication of major information systems, and satisfies the user authentication-related checklists of the Information Security Management System (ISMS) operated by the Korea Internet & Security Agency.



비밀번호 정책 설정

길이제한: □ 사용 8 자 이상

특수 문자 포함 (ex: !\"#$%&'()*+,-./:;=?@[]^_`{|}~): □ 사용

영문 소문자 포함: □ 사용

영문 대문자 포함: □ 사용

숫자 포함: □ 사용

4번 연속된 동일 문자 제한 포함 (ex: aaaa): □ 사용

4번 연속된 키보드 문자 제한 포함 (ex: asdf, qwer): □ 사용

비밀번호 변경 주기: ○ 1개월 ● 3개월 ○ 6개월 ○ 12개월 □ 강제 변경

비밀번호 오류 접속 제한: 5 회 오류 시 5 분 간 접속 불가

전체 초기화: 사용자 비밀번호 초기화를 하실 수 있습니다. 사용자 비밀번호를 초기화 하시면 비밀번호를 랜덤으로 생성하여 사용자에게 이메일로 전달합니다.

Copyright © 2016 Penta Security Systems Inc.

**Fig 8**. ISign+'s Web Management Tool Screen [Password Management]

ISign+ has a secure session management function to prevent replay attacks. It is verified every time a session is connected using an authentication token with a special value inserted. Upon completion of verification, the verified token will be discarded, and the singular value will be updated. It blocks all access if an attempt is made to access via extorted authentication token.

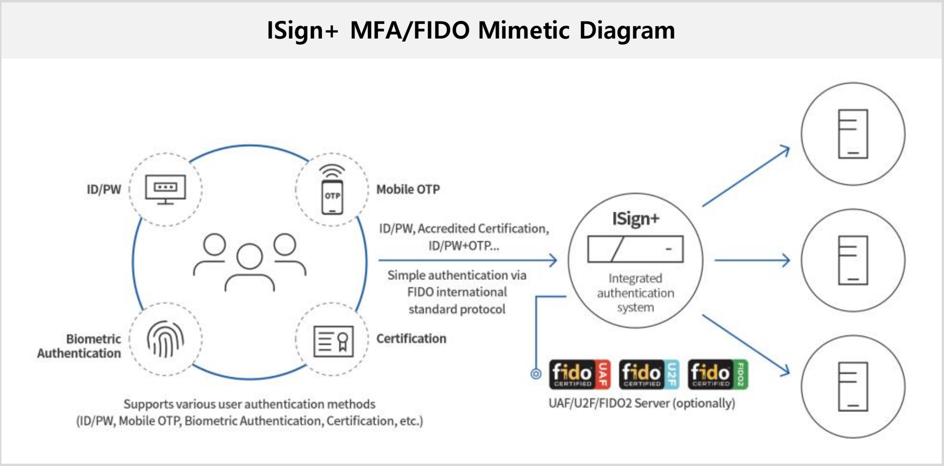
ISign+ has a user authority management feature. This feature provides system access control environment according to user role (permission) as well as IP control through allow list and deny list for each user and service. System and resources can be effectively managed with role-based access control.

ISign+ is a Secure SSO/EAM solution that executes secure authentication security and authorization management through features such as session management, password management, and user management.

# ISign+ for Security

## Multi-Factor Authentication (MFA) & FIDO

ISign+ can protect corporate assets from internal threats with powerful Multi-Factor authentication and authorization management feature.


ISign+ MFA/FIDO Mimetic Diagram

ID/PW
Mobile OTP
OTP
ID/PW, Accredited Certification, ID/PW+OTP...
Simple authentication via FIDO international standard protocol
ISign+
Integrated authentication system
Biometric Authentication
Certification
fido CERTIFIED UAF
fido CERTIFIED U2F
fido CERTIFIED FIDO2
UAF/U2F/FIDO2 Server (optionally)
Supports various user authentication methods (ID/PW, Mobile OTP, Biometric Authentication, Certification, etc.)

**Fig 9**. Authentication Methods Supported by ISign+

ISign+ is one to multi-factor authentication that can accommodate clients' complex authentication conditions. ISign+ supports accredited authentication environment based on Non-ActiveX/HTML5 and supports accredited authentication (NPKI, GPKI, EPKI, etc.) environment without installing additional programs such as ActiveX or plug-in.

| Type | Supported Methods |
|---|---|
| One-Factor Authentication | ID/PW, Public Key Infrastructure (PKI) |
| Multi-Factor Authentication | One-Factor Authentication Method **+** Self-certified solutions such as mOTP, QR Code, Pattern, etc. Or $3^{rd}$ party authentication solutions such as Bio and NFC. |

ISign+ provides convenient and safe authentication solutions via biometric authentication by acquiring FIDO UAF Server, Client/Authenticator, U2F Server, and FIDO2 Server authentication. Biometric authentication can be performed using FIDO Client installed on Samsung/LG/Apple smartphones, and it also provides interworking with 3rd party biometric authentication products.

Through the ISign+ mOTP App, you can enhance security and convenience of the Web Agent system by introducing complex authentication using ID/PW and OTP together, single authentication using only ID and OTP, and additional authentication functions used for approval of critical matters.

# ISign+ for Security

By introducing ISign+ mOTP solution for corporate information system access and data access, both data security and convenience are expected to significantly improve.

| ISign+ Products | Details |
|---|---|
| ISign+ UAF/U2F | Provides authentication service complied with FIDO UAF and FIDO U2F standard protocol. |
| ISign+ mOTP | Provides one-time authentication number generated by your smartphone for double security to log in. |
| ISign+ WA | Provides web environment accredited authentication service and section encryption feature. |
| ISign+ MA | Provides mobile environment accredited authentication service and certificate transmission feature. |
| ISign+ EE | Provides terminal login multi-authentication solution. |

**ISign+** provides several models depending on the authentication method and function. Clients can select and deploy the desired ISign+ product in accordance with function/convenience. By deploying ISign+, companies can strengthen authentication security through multi-factor authentication and simple authentication using FIDO.

## All-in-One Appliance ISign+

ISign+ is South Korea's first All-in-One Appliance type authentication security platform, via various authentication methods while providing a safer user login environment. Compared to S/W products, it reduces deployment time and cost by more than 50%, and is equipped with authentication system, repository, and management tools, which are essential components of the authentication security platform.

ISign+'s Overall Mimetic Diagram

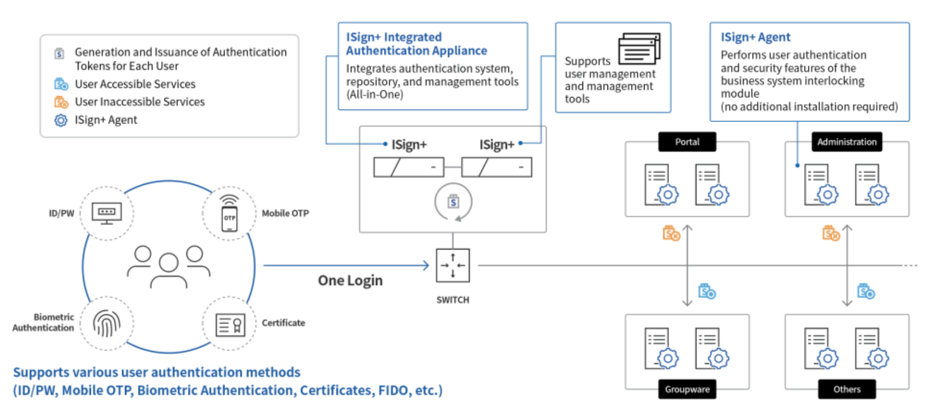

Generation and Issuance of Authentication Tokens for Each User
User Accessible Services
User Inaccessible Services
ISign+ Agent
ISign+ Integrated Authentication Appliance
Integrates authentication system, repository, and management tools (All-in-One)
Supports user management and management tools
ISign+ Agent
Performs user authentication and security features of the business system interlocking module (no additional installation required)
ISign+
ISign+
Portal
Administration
ID/PW
Mobile OTP
Biometric Authentication
Certificate
One Login
SWITCH
Groupware
Others
Supports various user authentication methods
(ID/PW, Mobile OTP, Biometric Authentication, Certificates, FIDO, etc.)

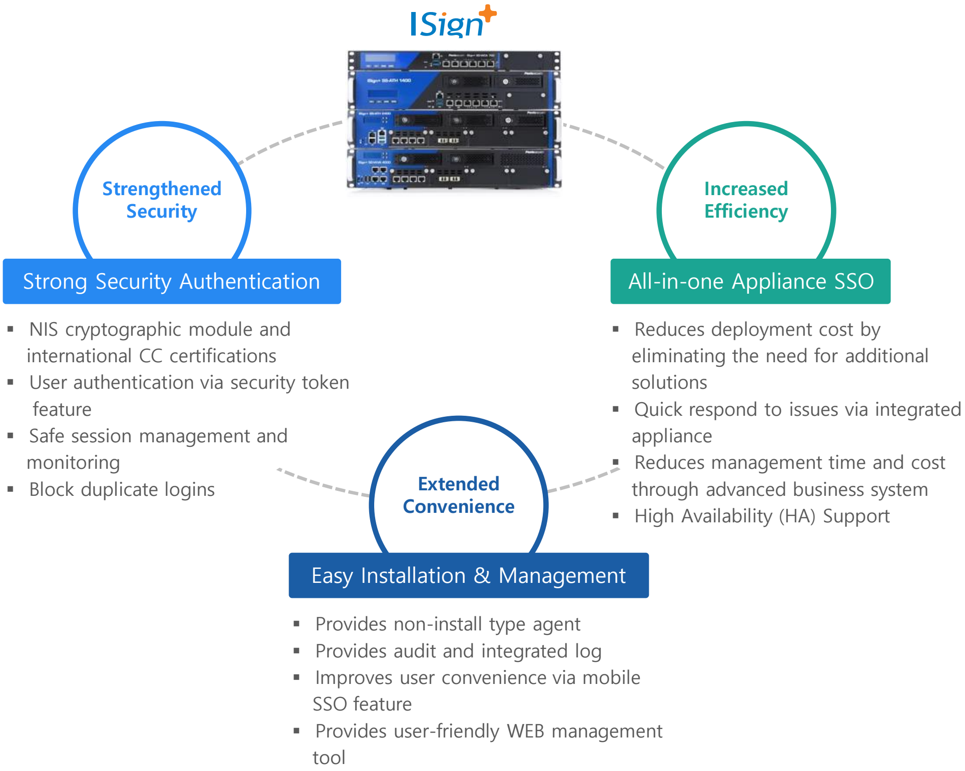
**Fig 10**. The Overall Mimetic Diagram of ISign+, an all-in-one appliance type authentication security platform

# ISign+ for Security

ISign+ appliances are easy to maintain. It is easier to find the cause of the problem than the S/W type product in which each component is made of a different company products, and it is easier to solve technical problems and update. ISign+ has quick recovery automatic failure recovery function. In the event of a failure, the system is automatically restored within 1 minute, reducing the cost of managing failure response and improving administrator convenience.

ISign+ supports section encryption by installing CIS-CC, a self-developed NIS-certified encryption module, and applied SSL[1] to major communication sections. This prevents Session Hijacking (a man-in-the-middle attack vulnerability) that steals the session in the communication between the server and the client and disguises itself as a normal session.

ISign+, an all-in-one appliance type authentication security platform, obtained international CC certification from the IT Security Certification Office and obtained GS certification from the Korea Information and Communication Technology Association (TTA).



Strong Security Authentication

- NIS cryptographic module and international CC certifications
- User authentication via security token feature
- Safe session management and monitoring
- Block duplicate logins

All-in-one Appliance SSO

- Reduces deployment cost by eliminating the need for additional solutions
- Quick respond to issues via integrated appliance
- Reduces management time and cost through advanced business system
- High Availability (HA) Support

Easy Installation & Management

- Provides non-install type agent
- Provides audit and integrated log
- Improves user convenience via mobile SSO feature
- Provides user-friendly WEB management tool

[1] SSL : Secure Socket Layer

# Customer Success Stories

So far, we have looked at authentication and authorization (access management), which are essential concepts to prevent data breaches. Companies should have a security system including authentication/authorization to protect important data and users' personal information. **ISign+** is the best way for companies to manage and control access by applying login security and authentication security.

- **Case 1**: K Financial

  ISign+'s terminal login multi-authentication solution 'ISign+ EE-WIN' was supplied to financial companies such as K Financial Group, one of Korea's leading financial groups. The financial sector uses various dedicated business applications, so it can be a financial burden for the company to manage integrated authentication from terminal login to mainframe login. As various authentication methods such as mobile authentication and biometric authentication are becoming more common, the burden of authentication management continues to increase. In addition, the demand for a safe and convenient way to access work servers (even whilst working from home) is also rapidly increasing. 'ISign+ EE-WIN' provides strong security and high convenience throughout the entire business from terminal login to mainframe login in all business environments of financial institutions and can respond perfectly to various security audits.

- **Case 2**: M Medical

  Appliance type authentication security platform ISign+ successfully entered the Singaporean market through a contract with a leading medical technology company. M Medical, which has more than 4,000 clinics, felt the need to strengthen its certification security due to the growing demand for certification. As the demand for cybersecurity rapidly increased, Penta Security's all-in-one appliance-type integrated authentication security solution was introduced and deployed successfully. The solution had integration of essential components such as authentication server, database, and policy server and the company was able to enjoy the benefits of FIDO2-compliant features.

# Conclusion

In order to protect data from internal and external threats and strengthen corporate security, authentication security platform ISign+ is the key solution to your agile management.

1. ISign+ is an appliance type SSO solution that can be easily installed, operated, and supported on existing servers.

2. ISign+ is an SSO/EAM solution that enables secure access to multiple services with a secure SSO (Single Sign On) and manages user rights via role-based access control.

3. ISign+ is an SSO/EAM solution with strong security that achieved CC certification and GS certification in addition to section encryption through CIS-CC, a self-developed NIS authentication encryption module.

4. Multi-Factor authentication is critical to prevent data breaches, and ISign+ supports multi-factor authentication via 3rd party solutions such as Bio and NFC, as well as authentication through PKI certificate and mOTP in addition to ID/PW.

5. ISign+ is a FIDO UAF/U2F, FIDO2 certified product, and enables simple and safe authentication using biometric authentication through the FIDO protocol.

# About Penta Security Systems Inc.

Penta SECURITY
TRUST FOR AN OPEN SOCIETY

Penta Security is a leader in web, IoT and data security solutions and services.

Since its founding in 1997, Penta Security has developed a set of security technologies to allow individuals and corporates to share information safely without any restrictions. To this end, we have been conducting R&D for more than 20 years based on encryption technology, which we believe is the basic and core of cybersecurity.

Penta Security's three core products for corporate cybersecurity, including data, web, and authentication security, have become essential security elements to protect valuable information across the world, and Penta Security is proud to be evaluated as a leader in the global cybersecurity market.

For more information on the All-in-One Appliance type authentication security platform ISign+, refer to the product homepage hhttps://www.pentasecurity.com/product/isign-plus/ or contact globalbiz@pentasecurity.com.

**Key words**

#authenticationsecurity #loginsecurity #accountmanagement #SSO #Single-Sign-On #FIDO #OTP #mOTP #OTPauthentication #MFA #2FA #Authentication #Authorization #accesscontrol #authenticationserfice

Penta SECURITY

TRUST FOR AN OPEN SOCIETY

**Penta Security Systems Inc.**

20F, 25, Gukjegeumyung-ro 2-gil,
Yeongdeungpo-gu, Seoul, Korea
Tel. 82-2-780-7728 Fax. 82-2-786-5281