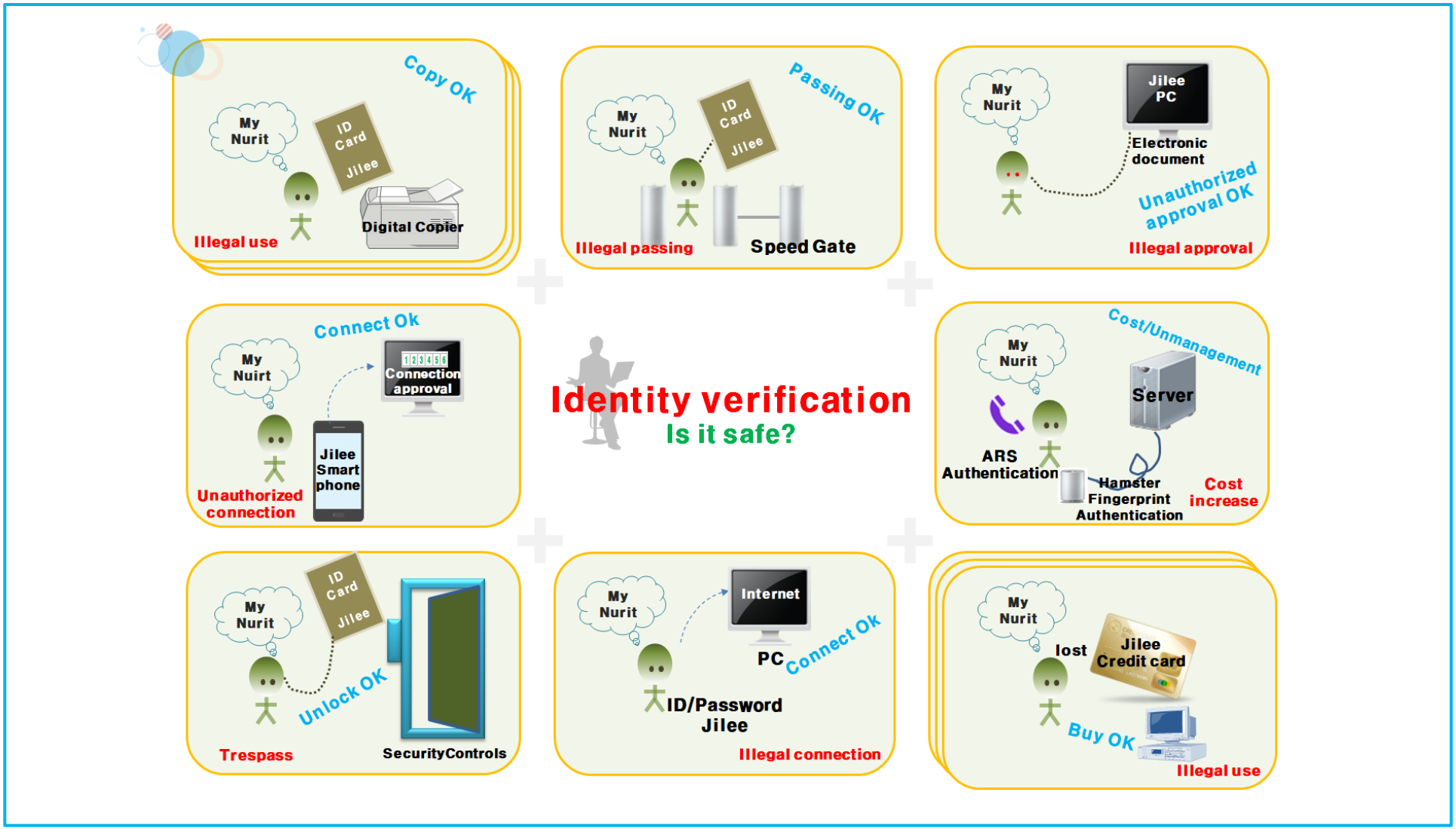
What is identity authentication for user identification and authentication to enhance the security of information assets?

Mar, 2024

Note. Identity authentication

1. Current address of identity verification



Note. Identity authentication

2. Identity verification factor

Identity verification is largely divided into knowledge-based authentication (What I know), possession-based authentication (What I have), attribute-based authentication (What I am), behavior-based authentication (What I do), and location-based authentication (Where you are). It can be divided into several elements.

Knowledge-based (What I know)	Possession-based (What I have)	Attribute-based (What I am)	Behavior-based (What I do)	Location-based (Where you are)
Commonly used IDs and passwords can be cited, and setting questions such as 'what is the name of the dog I raised as a child' when modifying account information also falls under knowledge-based authentication.	OTP, smartphone, security card, security token, etc. that the user has. Smartphones and dedicated applications are commonly used today.	It is a method of authentication through a person's unique characteristics such as fingerprint, face, vein, and iris, and is used in combination with other authentication.	It is authentication through the repeated actions of a certain person or the way a device is used, and various methods such as handwritten signatures are being researched and verified.	The method by which your device is authenticated when connected to a specific network. For example, when a smartphone is connected to a router used at home, it can be set to be used immediately without unlocking the screen, and it is also possible to configure the system to be accessed only from a specific place by using GPS or mobile communication.

Note. Identity authentication

3. Identity verification method

Identity authentication can be largely classified into four methods: IP access restriction, public certificate, one-time authentication key (OTA key or OTP), and biometrics.

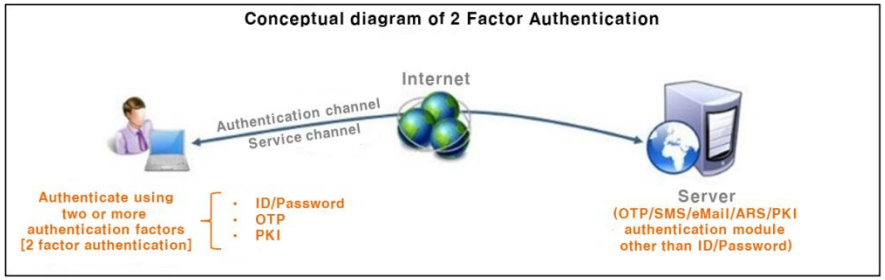
IP access restriction	Public certificate	OTA key [OTP]	Biometrics
Since the IP access restriction method requires a fixed IP for information assets (Windows, MacOS, Linux, Unix, Database, network equipment, security equipment, storage devices, etc.), it is meaningless to restrict access if a dynamic IP whose IP changes is used.	The public certificate method is expensive in solution, difficult to use because of the inconvenience of the public certificate authentication module, and an alternative to the public certificate is required because the mandatory public certificate has been abolished.	The OTA key method is easy for anyone to use, is not limited by time and place, and is a simple authentication method because the authentication key is generated on the smartphone owned by the person, and at the same time, the authentication key once used cannot be reused. It provides strong security against various hacking attacks because it is difficult to infer the key.	Biometrics, which are currently in the spotlight, provide strong security because they are unique to each individual by utilizing individual body characteristics, but the solution is expensive, and the password can be changed if it is hacked, but if the biometric information is hacked, it can be changed this is almost impossible In the worst case, it can lead to permanent damage.

Note. Identity authentication

4. What is 2nd Authentication?

2nd authentication means a separate additional authentication (ownership-based/attribute-based/behavior-based/location-based authentication) procedure in addition to the login-ID and password (knowledge-based authentication) to strengthen the security of information assets. 2nd authentication is divided into 2 factor authentication and 2 channel authentication.

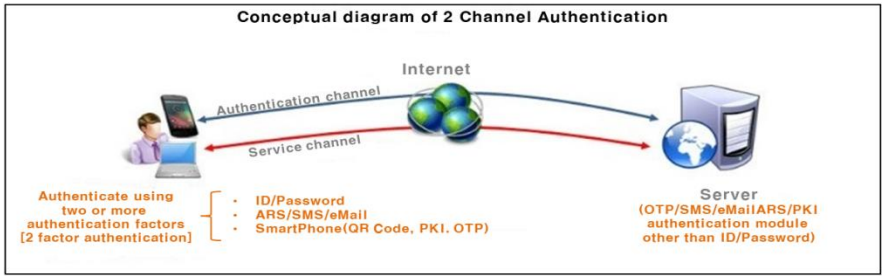
2 Factor authentication



It is an authentication technique in which other elements, such as possession-based authentication and biometric authentication, are added to login-ID/password authentication, which is "knowledge-based authentication", and a form in which a service channel and an authentication channel are combined into one.

- Diverse and wide range of applications, simple management and reduced operating costs.
- Since it does not use a communication network, it is not affected by security areas or communication failures, so the service is guaranteed.
- The module authentication method does not require synchronization of user information and guarantees service by not using communication and authentication servers.
- Guaranteed authentication speed by load balancing in case of congestion.

2 Channel authentication



It is common to see it as including 2 factor authentication, and it is a form in which the communication network that performs authentication and service is physically separated into a service channel and an authentication channel.

- Complex implementation, limited application, complex management and increased operating costs.
- Because the communication network is used, the service is interrupted due to the security area or communication failure.
- Synchronization of user information is required in the authentication server method, service interruption in case of authentication server failure, and reduction in authentication speed in case of congestion of authentication.
- Abuse in cybercrime with bypass technology and fatigue attack (Samsung Electronics, Microsoft, Uber, Reddit, etc.)

※ **Multi-factor authentication (MFA) uses at least two authentication factors to verify identity, and 2nd authentication is a type of MFA.**

nurit

Note. Identity authentication

5. Classification and Characteristics of 2nd authentication

2nd authentication is a hard-type 1st authentication (1st generation authentication) that requires a separate authentication server and a software method (jar, so, dll, etc.). It is divided into 2nd authentication (2nd generation authentication) of module call.

1st Authentication Key(Hard Authentication Key)

- Authentication server method (SHA-I), integrated authentication, and the weakest authentication method
- Token, card-oriented (authentication key generator)
- Issuing and managing individual HMac Keys
- Static HMac Key Method
- Batch authentication key generation cycle (30, 60 Sec) applied
- Non-permanent use / additional cost
- 2nd authentication(additional authentication)
- Expensive, limited application, complex management and increased operating costs
- Require user information synchronization
- Decreased authentication speed in case of congestion
- Service interruption in case of communication network and authentication server failure (vulnerable to failure)

2nd Authentication Key(Soft Authentication Key)

- Module authentication method (SHA-II), distributed authentication
- Smartphone-oriented (authentication key generator)
- Individual HMac Key is not issued and managed
- Dynamic HMac Key Method
- Application of individual authentication key generation cycle (3~60 Sec)
- Permanent use / cost savings
- 2nd auth(additional auth), Biometric application
- Low cost, diverse and wide application, simple management and reduced operating cost
- User info synchronization not required
- Guaranteed authentication speed by load balancing in case of congestion
- Communication network and authentication server not used, failure does not occur (service guarantee)

nurit

Note. Identity authentication

6. Text-based and module authentication method 2nd authentication

Text-based 2nd authentication such as SMS and e-mail is divided into integrated authentication with a separate authentication server and distributed authentication with a modular authentication method that does not require management and can be easily applied without a separate authentication server.

Text-based 2nd authentication such as SMS and email

- Authentication server method (SHA-I), Gateway (+Proxy) method, integrated authentication
- No Zero trust security model
- 1st certification (1st generation certification), 1st rank in cyber crime
- Issuance and management of individual HMac Keys
- Static HMac Key method
- Batch authentication key generation cycle (30, 60 sec) applied
- Limited application, complex management and increased operating costs
- Requires synchronization of user information
- Decreased authentication speed in case of authentication congestion
- Service interruption in case of communication network and authentication server failure (vulnerable to failure)
- Cannot be used in secure areas
- Vulnerable to cyber security such as bypass access, remote access, man-in-the-middle attack, bypass technology, and fatigue attack
- Starting from a simple (loose) configuration and not evolving to a more complex (robust) security system

2nd authentication of module authentication method

- Module authentication method (SHA-II), PAM method, distributed (individual) authentication
- Apply a zero trust security model
- 2nd authentication (2nd generation authentication), biometrics applied
- Individual HMac Key is not issued and managed
- Dynamic HMac Key method
- Apply individual authentication key generation cycle (3~60 sec)
- Diverse and wide range of applications, simple management and reduced operating costs
- Synchronization of user information is not require
- Guaranteed authentication speed by load balancing in case of congestion
- Communication network and authentication server not used, failure does not occur (service guaranteed)
- Also available in secure areas
- Strong against cyber security such as bypass access, remote access, man-in-the-middle attack, bypass technology, and fatigue skeleton
- Start with simple (loose) configurations and evolve to more complex (robust) security systems

nurit

Note. Identity authentication

7. 2nd authentication of FIDO authentication and module authentication method

FIDO (Fast Identity Online) uses a person's biometric information (fingerprint, face shape, iris, etc.) or an external authentication device (Yubikey, Titan Security key, etc.) It is an authentication protocol standard that provides a more convenient and secure authentication function using the "Public-Key Cryptography" method.

FIDO authentication

- 2-step authentication and integrated authentication with a gateway method and complex architecture
- Use of Public-Key Cryptography
- A structure that generates and transmits a PKI after biometric authentication in a smartphone
- Fixed static security (vulnerable to security), such as password, fingerprint, iris, face, etc
- It is difficult to apply easily to information assets in various environments
- When introducing, a separate server and DB are required (at least 3 servers are required)
- Expensive, complex to manage and increase operating costs
- Requires synchronization of user information
- Decreased authentication speed in case of authentication congestion (slow authentication speed)
- Service interruption in case of communication network and authentication server failure (vulnerable to failure)
- Cannot be used in security areas, not applicable to embedded systems
- If the user device is changed, all services are re-registered
- Service is unavailable if the device is broken or lost

2nd authentication of module authentication method

- Modular authentication method, 3-step authentication with a simple architecture, distributed authentication
- Use of 512Bit standard hash function recognized worldwide
- A structure that generates an OTP after biometric authentication on a smartphone (Time Sync)
- Dynamic security (strong on security), such as one-time/volatility that changes every time or is used once and discarded
- Easily applicable to information assets in various environments
- When introduced, no separate server or DB is required
- Low cost, simple management and reduced operating costs
- Synchronization of user information is not required
- Guaranteed authentication speed by load balancing in case of authentication rush (fast authentication speed)
- Communication network and authentication server not used, failure does not occur (service guaranteed)
- Can be used in security areas and can be applied to embedded systems
- If the user device is changed, all services are not registered
- Provides an alternative method even if the device is broken or lost (WebOTA, emergency OTA key)

nurit

Note. Identity authentication

8. How security solutions are applied

Security solution application methods can be largely classified into five types: Gateway (+Proxy), Sniffing, Agent, LKM (Loadable Kernel Module), and PAM (Pluggable Authentication Module) methods.

Gateway(+Proxy) method	Sniffing method	Agent method	LKM method	PAM method
After installing a passage for access, the user accesses and logs in to the server, network, or DB only through the passage, or must pass through the gateway to execute the process after logging in, and all logins and thorough control are carried out. Hackers love bypass and remote access solutions, but security experts don't even treat this category of solutions as security solutions.	It is a method of copying the packets exchanged between the user and the server and forwarding them to the server. It is not a good thing that others have installed it, and you must go through an embedded test or a pre-introduction review. Security solutions, once installed, are very difficult to remove and may be left unattended even if they do not function properly.	It is a way to install access control on the server. Depending on the solution, it is designed to be accessed only by the agent, or some solutions control access by sending internal packets to the external server after installing a separate external server.	It is a technique for adding an executable function as a module to a running operating system kernel without recompilation of the kernel. It is currently used in many operating systems including Linux, Solaris, and FreeBSD. If a Trojan horse-infected module is present in LKM, even if the system is rebooted, the infected LKM module is reloaded like other kernel modules during the booting process. As a method used for typical server access control, Secure OS adopts and uses this method.	It is a method that supports a centralized authentication mechanism in Linux/Unix systems. The basic principle of PAM is to allow PAM to directly perform authentication instead of an application program reading the password file. PAM doesn't care what authentication mechanism the system administrator wants. When a program authenticates a certain user with a library, it calls a function in the PAM Library. PAM provides a library of corresponding functions so that applications can request authentication of specific users.

Note. Identity authentication

9. Current address of login

Reports of hacking damages related to information leakage of companies and individuals continue to occur as long as they are forgotten, and the damage is serious. More fundamentally, the awareness that it is necessary to respond by using additional authentication (2nd authentication) that is safe from hacking is spreading socially.

- Use guessable passwords (anniversaries, phone numbers, etc.)
- One or two easy-to-remember ID/PW unification
- In case of leakage, it is difficult for the user to determine whether or not it has been leaked
- My computer is always exposed to viruses / hacking
- Inconvenient to use because of too many passwords (password/reset syndrome)

- Online banking accident
- Information Asset Hacking
- Information exposure / leakage
- Impersonation
- Illegal use / Intrusion / Passage
- Illegal access / Use / Approval
- Unauthorized access

❖ **Password alone is never safe, and a one-time authentication key(OTA key) that can replace or additionally authenticate the password (2nd authentication) is required each time it is used.**

nurit

Note. Identity authentication

10. Regulations and media coverage

Looking at the Electronic Financial Supervisory Regulations of the Financial Supervisory Service announced in December 2013, Article 14, Paragraph 9 was newly established.

"9. When logging in with an operating system account of the information processing system, a separate additional authentication procedure besides the account and password must be implemented."

Looking at the detailed enforcement regulations of the Electronic Financial Supervisory Regulations of the Financial Supervisory Service related to telecommuting announced in November 2020, the amendment to Article 2-2 Paragraphs 1 and 2 (<Appendix 7> Network Separation Alternative Information Protection Control)

Authentication for remote access applies 2-factor authentication (e.g. ID/PW + OTP), blocking access when authentication fails over a certain number of times (e.g. 5 times)
Although the authentication method is not specified, two authentication methods belonging to different methods among knowledge-based, possession-based, and specific-based authentication methods are combined

According to the password guidelines recently published by the National Institute of Standards and Technology (NIST), changing passwords periodically does not prevent online hacking breaches. Not only is periodic password change more likely to generate weak passwords, users end up writing dozens of passwords down because they can't remember them. Through the revision of the password guidelines, NIST removed the mandatory requirement to combine passwords with multiple characters, including special characters, and to change them at regular intervals.

What Microsoft recommends to corporate security administrators (security standards) is that the PC operating system Windows 10 and Windows Server security standards strengthen passwords in a situation where the assertion that periodic password changes do not substantially help security is gaining strength. Deleted the provision that it must be periodically changed.

Google announced on its blog that it reduced account hacking by 50% through 2-factor authentication, which Google automatically activated for its services last year (2021).

2024.2 Financial authorities announce changes to the revised 'Electronic Financial Supervision Regulations' regulations
The regulations that specifically specified user password setting methods were deleted, and financial companies were allowed to introduce password and authentication method management methods that they deemed safe.

Zero Trust grants different access rights to different systems, even for highly trusted employee accounts. It is a security model that verifies the opponent whenever an actual access is made, and is considered the best security measure to respond to increasingly intelligent cyber attacks.

Note. Identity authentication

11. Necessity of introduction

"Is there an alternative if the login-ID/password of the information asset is leaked?"

1. To strengthen security, apply a two-step authentication system using OTP for user identification and authentication

Application of secondary authentication (e.g. ID/PW + OTP), blocking access when authentication fails more than a certain number of times (e.g. 5 times) and authentication means are not specified. Two authentication means belonging to the method must be used in combination.

2. Blocks illegal bypass/remote access by malicious code, a program created for malicious purposes

After illegally acquiring information asset access information (Desktop to Application, Desktop to Desktop, Desktop to Server, Desktop to Database, Server to Server, etc.) Remote access should be blocked.

3. Applied to reset user password due to loss, theft, or hacking

Log in by yourself-Enter ID, specific item, and one-time authentication key to register and use a new password if correct.

"If you do nothing, the middle goes" is an old saying, and it doesn't work in the cloud era. In the new era, a new protective device suits. Guarding the gate with a single password is an older method. Systems and infrastructure are constantly changing to new ones, and it's time for each to examine for themselves why they are holding onto the old ones.

"For strengthening the security of information assets, password replacement or 2nd authentication (additional authentication) is not an option, but a solution that must be applied!"

Note. Identity authentication

12. Matters to consider when introducing

1. Is the concept of Zero Trust applied?
2. Is it a separate authentication server method or a module authentication method?
3. Integrated Authentication or Distributed Authentication?
4. Is the key used when generating and verifying the authentication key static or dynamic?
5. Can you limit the number of times within a limited time?
6. Is it easy to apply and manage across various operating systems and applications?
7. Can you start with a simple (loose) configuration and evolve to a more complex (robust) security system?
8. How much does the authentication speed decrease in case of congestion?
9. Are you using the network?
10. Can bypass the security system and block remote access?
11. Are they affected by security areas or communication barriers?
12. Are there any problems with circumventing the authentication process by forging or altering data during the authentication process?
13. Can it defend against man-in-the-middle attacks, such as theft of login accounts or personal information, espionage, sabotage of communications, data alteration, etc.?
14. Is it possible to defend against SIM-swapping attacks that occur when authentication codes are sent through mobile text messages?
15. Is it a structure that can bypass authentication by applying a technology such as a reverse proxy?
16. Can it defend against "MFA fatigue attacks", attacks that exhaust the adversary by constantly sending push notifications, causing them to accidentally hit the login authorization button?

The bottom line is that "what kind of 2nd authentication was introduced", such as technology and security, is the key, not "introduced 2nd authentication".

Note. Identity authentication

13. Risks of applying Google Authenticator

1. Not a commercialized authentication solution
Many hacking cases have already occurred with open source and many users have suffered damage, and Google does not take any responsibility.

2. OTP registration key value (Secure key) exposed
Leaked Google MFA authentication code in Android malware, etc.
It is easy to expose the registration key value, and duplicate registration is possible.
In the case of a QR code, when read with a reader, the key value is exposed in plain text, so others can easily know my OTP registration key value.
When the app is deleted, if the key value is not stored somewhere, the registered OTP registration key value must be newly received and the key value must be changed.

3. Very vulnerable to hacking
Since it is an open source-based free service, there are no basic security devices such as algorithm leakage and app forgery prevention by source disclosure.

4. No countermeasures against hacking of members' Google accounts.
If your account is hacked, you cannot use Google OTP-applied business services for a certain period of time.

5. Use a low hash function
SHA-1 is used. (The National Intelligence Service recommends using at least SHA-256 or higher, and the US NSA recommends using SHA-384 or higher for VPN)
NIST recommends migrating to SHA-2 or SHA-3 as the US NIST is phasing out SHA-1 completely by December 31, 2030.

6. Secure key(Seed key) problem
Secure key is not encrypted or obfuscated, but converted only to Hex.
Confusion during upgrade due to different seed keys for each SHA function. (SHA-1,224,256: 20 Byte, SHA-384: 32 Byte, SHA-512: 64 Byte)

7. Technical support issues
Because it is open source, you must solve the problem yourself.
China loses access to Android updates due to US-China trade war. Google Play store is not available.

8. Expect Google's free service to become a paid service at some point.

Google Authenticator may be suitable for small Linux or applications, but not for large Linux or applications.

Note. Identity authentication

14. Concluding remarks

It is absurd to say that security will be strengthened due to network separation (internal network/external network), and we are in an era where a major change in perception of information security is needed.

The reality is that this method, which is vulnerable to security, is still being used
- ▶Hackers' favorite application method among 2nd authentication: Gateway (+Proxy) method
- ▶The weakest authentication method among 2nd authentication: Text-based auth such as SMS and e-mail
- ▶Among the 2nd authentication, hackers use bypass technology and authentication method vulnerable to fatigue attacks: 2-channel authentication
- ▶Link method that is prone to phishing attacks: QR code method

The most important fundamentals for strengthening the security of information assets
- ▶How to protect against data forgery and falsification during the authentication process?
- ▶How do we prevent account information theft and abuse?
- ▶How to protect against browser automatic login?
- ▶How to block bypass connections?
- ▶How to block remote connections?
- ▶How to defend against man-in-the-middle attacks?
- ▶How to block multi-factor authentication (MFA) bypass technology?
- ▶How to defend against multi-factor authentication (MFA) fatigue attacks?

Above all, the best way to prevent information security incidents is to generate the authentication key yourself using the authentication key generation medium you own and enter it yourself.

The conclusion is not that "they introduced 2nd authentication", but rather "what kind of 2nd authentication was introduced" such as technology and security

"trust nothing" = "trust no one" = "keep verifying"

nurit

Password you don't need to remember!
BaroPAM will be with you.

Thank You!

www.nurit.co.kr
mc529@nurit.co.kr