nurit

Comparison of BaroPAM and other authentication solutions for 3-step authentication to strengthen the security of information assets

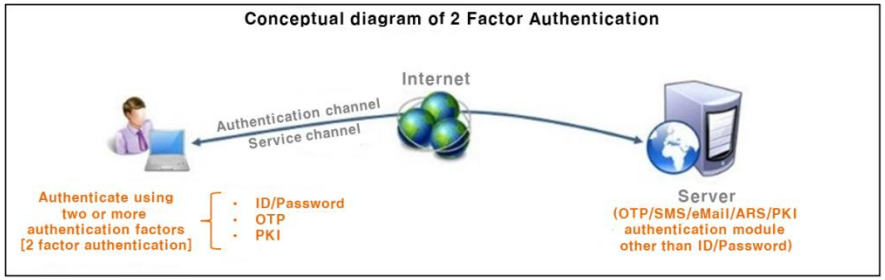
Mar, 2024

Authentication Solutions Comparison

1. 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.

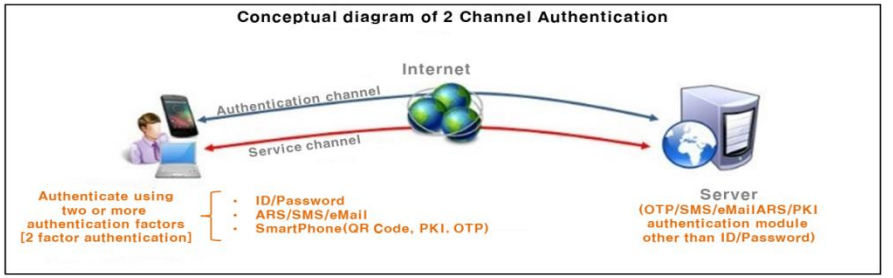
2 Factor authentication



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

Authentication Solutions Comparison

2. 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(Third party)

- Authentication server method (SHA-I, SHA-II:SHA-256), integrated authentication, and the weakest authentication method
- 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(BaroPAM)

- Module authentication method (SHA-II:SHA-512), distributed authentication
- 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

Authentication Solutions Comparison

3. 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(Third party)

- Authentication server method (SHA-I, SHA-II:SHA-256), 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 (BaroPAM)

- Module authentication method (SHA-II:SHA512), 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

Authentication Solutions Comparison

4. 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 (Third party)

- 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 (BaroPAM)

- 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

Authentication Solutions Comparison

5. 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".

Authentication Solutions Comparison

6. 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

nurit

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

Thank You!

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