nurit

비밀번호 없는 세상을 위한

# BaroKEY 솔루션 소개서

2020. 6.

# Content







nurit

# Ⅰ. 솔루션 개요

## 1. 본인인증 방식

개인정보가 포함된 본인인증 방식은 크게 IP 접속제한, 공인인증서, 일회용 인증키, 생체인식 방식 등 4가지로 구분할 수 있습니다.

| IP 접속 제한 | 공인 인증서 | 일회용 인증키 | 생체인식 |
|---|---|---|---|
| IP 접속 제한 방식은 정보 자산(Windows, MacOS, Linux, Unix,Database, 네트워크 장비, 보안장비, 저장장치 등)에 고정된 IP가 필요하기 때문에 IP가 변하는 유동 IP를 사용한다면 접속 제한에 의미가 없음. | 공인 인증서 방식은 솔루션 비용이 비싸며, 공인 인증서 인증 모듈의 불편함 때문에 사용하기가 힘들고, 공인 인증서 의무화가 폐지되어 대체할 대안이 필요함. | 일회용 인증키 방식은 누구나 사용하기 쉽고, 시간과 장소의 제약을 받지 않으며, 본인이 소유하고 있는 스마트 폰에서 인증키를 생성하기 때문에 간편한 인증 방법인 동시에 한번 사용된 인증키는 재사용할 수 없으며, 인증키 유추가 어려워 다양한 해킹 공격에도 강력한 보안성을 제공함. | 요즘 각광 받고 있는 생체 인식 방식은 개인의 신체 특성을 활용하여 개인별로 유일하기 때문에 강력한 보안성을 제공하지만 솔루션 비용이 비싸며, 비밀번호는 해킹을 당할 경우 변경하면 그만이지만, 생체 정보를 해킹 당할 경우에는 변경이 거의 불가능하다. 따라서 최악의 경우 영구적인 피해로 이어질 수도 있음. |

## 2. 일회용 인증키 구분 및 특징

일회용 인증키는 인증서버가 필요한 Hard 방식의 1st 인증키 (1세대 인증키) 와 별도의 인증서버가 존재하지 않아 관리가 필요 없고, 손쉽게 적용할 수 있는 소프트웨어 방식(모듈 호출)의 2nd 인증키 (2세대 인증키) 로 구분합니다.

| 1st 인증키(Hard 인증키) | 2nd 인증키(Soft 인증키) |
|---|---|
| ❖ 서버 인증 방식(SHA-I) | ❖ 소프트웨어 인증 방식(SHA-Ⅱ, SHA-Ⅲ) |
| ❖ 토큰, 카드 위주(인증키 생성기) | ❖ 스마트폰 위주(인증키 생성기) |
| ❖ 개인별 HMac Key 발급 및 관리 | ❖ 개인별 HMac Key 발급 및 관리하지 않음 |
| ❖ 정적 HMac Key 방식 | ❖ 동적 HMac Key 방식 |
| ❖ 일괄 인증키 생성주기(30, 60초) 적용 | ❖ 개별 인증키 생성주기(3~60초) 적용 |
| ❖ 비영구적 사용 / 추가 비용 발생 | ❖ 영구적 사용 / 비용 절감 |
| ❖ 2차 인증(추가 인증) | ❖ 2차 인증(추가 인증) |
| ❖ 고가, 제한적 적용 | ❖ 저가, 다양하고 광범위한 적용 |
| ❖ 사용자 정보 동기화 필요 | ❖ 사용자 정보 동기화 필요하지 않음 |
| ❖ 인증 폭주 시 인증속도 저하 | ❖ 인증 폭주 시 부하분산으로 응답속도 보장 |
| ❖ 인증서버 장애 시 서비스 중단 발생 | ❖ 인증서버 장애 시 유연한 대처 ( 서비스 보장 ) |

### 3. 도입의 필요성

기업 및 개인의 정보 유출에 대한 해킹 피해보도는 잊혀질 만 하면 계속 발생되고 있으며, 이에 대한 피해는 심각한 수준입니다. 보다 근본적으로 해킹에 안전한 2차 인증키(일회용 인증키)를 사용하여 대응하여야 한다는 인식이 사회적으로 확산되고 있습니다.

- 추측 가능한 비밀번호 사용 ( 기념일, 전화번호 등 )
- 기억하기 쉬운 ID/ PW 한 두 개 일원화
- 유출 시 사용자가 유출여부 파악하기 어려움
- 내 컴퓨터는 항상 Virus / 해킹에 노출
- 너무 많은 비밀번호 때문에 사용하기 불편 ( 비밀번호 / 리셋 증후군 )

- 온라인 뱅킹 사고
- 정보자산 해킹
- 정보 노출 / 유출
- 명의 도용
- 불법 이용 / 침입 / 통과
- 불법 접속 / 사용 / 승인
- 무단 접속

❖ 비밀번호 만으로는 결코 안전하지 않으며 매번 사용할 때마다
비밀번호를 대체 또는 추가 인증(2차 인증)할 수 있는 일회용 인증키가 필요

## 4. 규정 및 언론 보도

2013년 12월에 공지된 금융감독원의 전자금융감독규정을 보면, 제14조 9항 신설

"9. 정보처리시스템의 운영체제(Operating System) 계정으로 로그인(Log in)할 경우 계정 및 비밀번호 이외에 별도의 추가인증 절차를 의무적으로 시행할 것."

군사저널 2018. 4, vol 145 정보자산 접속 시 2차 인증의 필요성

정보보안을 위하여 각종 정보자산에 대한 2차 인증은 반드시 필수로 적용되어야 할 보안 대비책이며, 이를 통하여 각종 정보자산에 대한 해킹 위협으로 부터 안전해질 것이다.

ZDNet Korea 2019.12.4 펜타시큐리티, 웹방화벽에 2차 인증 도입

남경문 펜타시큐리티 기획실장은 "관리자 인증 강화는 세계적인 추세이고, 특히 보안 제품의 경우 고성능뿐만 아니라 강력한 관리 보안성을 필수로 인식하고 있다"며 "이번 조치는 고도의 보안성뿐 아니라 웹 환경 MOTP를 적용해 사용자 편의성까지 동시에 추구했다"고 말했다.

국민일보 2020.01.10 갤럭시폰 해킹 우려되면 "2차 인증" 반드시

삼성전자는 "다른 계정의 아이디와 비밀번호를 삼성계정에서 동일하게 사용하지 말고 타인에게 노출되지 않게 하기 바란다" 면서 "비밀번호를 주기적으로 바꾸고 2단계 인증을 반드시 해야 한다" 고 설명했다.

동아일보 2020.01.14 연예인 클라우드 계정 유출 사고 파장…2단계 인증으로 보안강도 높여야

이번 유출사고의 대상이 된 삼성 클라우드도 공식입장을 통해 "갤럭시폰 또는 클라우드 서버가 해킹을 당한 것이 아니며, 개인 사용자의 계정이 유출 및 도용된 사례"라며 "이중보안설정 등 보안강화조치를 취해 주시길 당부한다" 고 설명했다.

매일경제 2020.02.06 네이버 클라우드 도용 막으려면…"2중 잠금 이용해야 "

네이버는 6일 이와 관련해 2단계 인증 주소록 · 클라우드에 대한 별도 암호 기능 등을 적극 활용하라고 주문했다.
단순히 아이디와 비밀번호만 맞는다고 로그인 되게 하지 않고, 추가 인증 단계를 설정하면 도용 피해를 최소화할 수 있다.

보안뉴스 2020.02.08 중소기업의 웹사이트 보안을 위한 가이드 7

아이라페토브는 "이중인증 옵션 역시 대단히 중요하지만 많이 간과되고 있는 기능" 이라고 짚는다. "중소기업은 웹사이트 관리자 업무를 하는 데 있어서 만큼은 반드시 이중인증을 도입해야 합니다. 다크웹에는 이미 도난 당한 크리덴셜이 활발히 거래되고 있고, 그러므로 비밀번호만으로 뭔가를 보호할 수 있는 시대가 아닙니다. 이중인증이라고 해서 100% 완벽한 건 아니지만, 비밀번호만으로 관리자 페이지를 보호하는 것보다는 훨씬 안전합니다."

## 4. BaroKEY란?

**BaroKEY** 솔루션은 ERP, 전자결재, 그룹웨어 등의 어플리케이션 로그인 시 **비밀번호를 대체/추가 인증하는 소프트웨어 방식(어플리케이션 레벨)의 인증 솔루션**으로 일명 **소프트 인증키, 2세대 인증키, 일회용 인증키**로 불립니다.

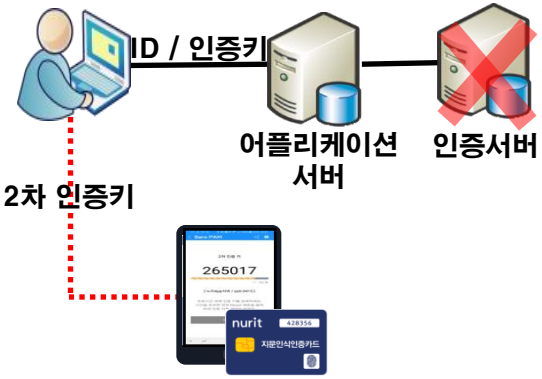
### 강력한 인증 솔루션


- 사용자 인증을 받기 위해서는 매번 새로운 인증키를 사용하여야 하며 휘발성으로 1회에 한해서만 사용 가능하고 로그인ID가 유출 시에도 안전
- 한번 사용된 인증키는 재사용할 수 없으며 인증키 유추가 어려워 다양한 해킹 공격에 강력한 보안성 제공

### 서비스의 용이성


- 별도의 인증키 장치(토큰, 카드)를 휴대하지 않아도 평소 휴대하고 다니는 사용자의 스마트 폰을 이용하여 인증 처리
- 어플리케이션 로그인 시 사용자별 ID, 인증키 만으로 로그인 처리가 가능하므로 Password가 불필요

### 손쉬운 적용




- 각 어플리케이션 서버에 일회용 인증키 검증 모듈을 호출하는 구조로 간단히 적용 가능 (일회용 인증키 검증 모듈은 jar, so, dll 형태로 제공)
- 별도 인증서버가 필요 없는 구조로 관리 및 운영비용 절감



nurit

# Ⅱ. 솔루션 특/장점

**BaroKEY** 솔루션은 **2nd 인증키**로써, **일회용 인증키**의 생성기기 대신에 스마트폰(안드로이드, 아이폰)에 있는 **일회용 인증키**의 생성 모듈(**소프트 인증키**)로 **일회용 인증키**를 생성하여, 인증함으로써, ERP, 전자결재, 그룹웨어 등 기업 내의 어플리케이션 로그인 시 **비밀번호 대체 및 추가인증을 위한 최적의 솔루션**입니다.

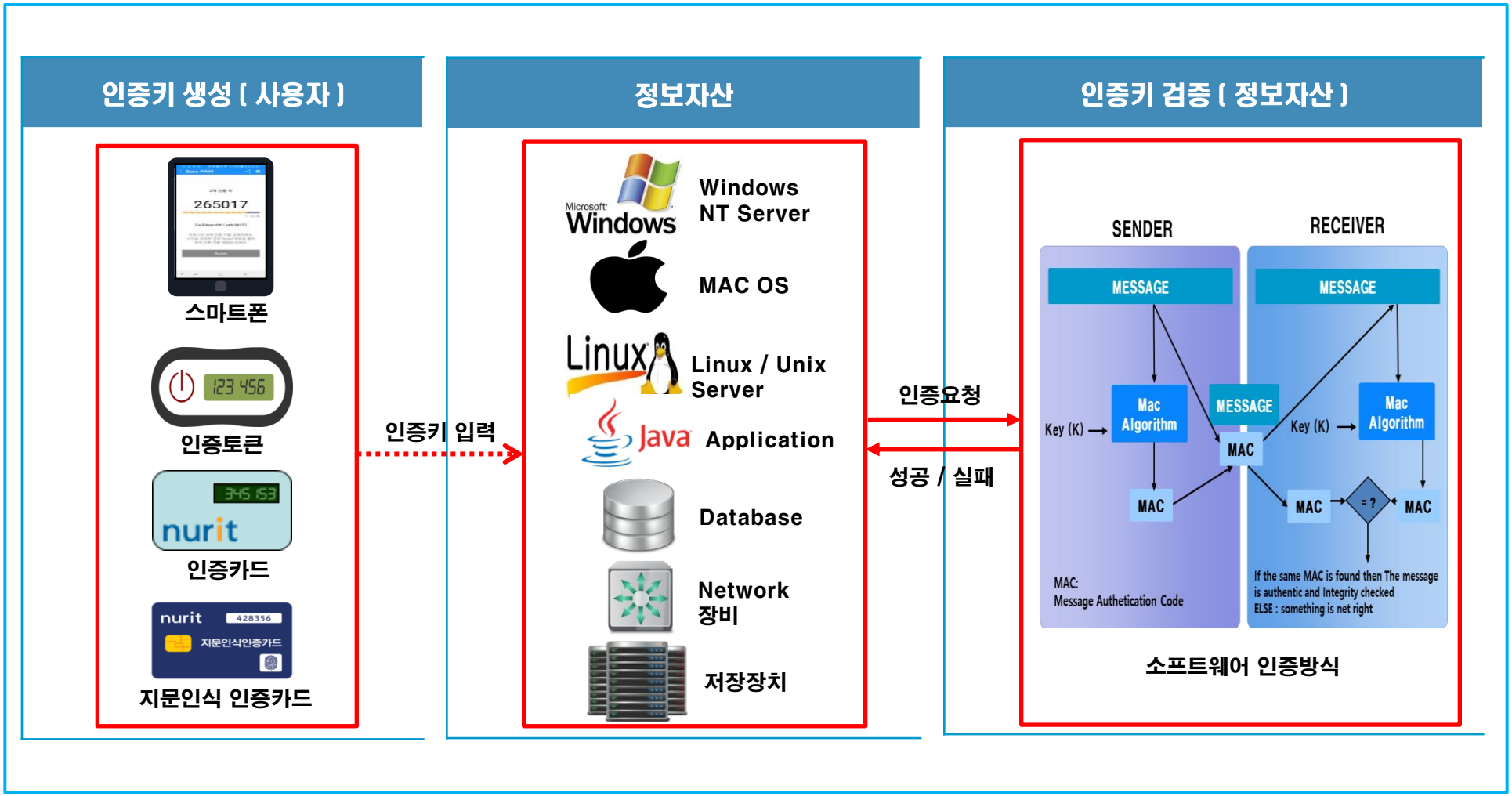
- 인증서버가 별도로 필요하지 않는 소프트웨어 방식
- 로그인ID별 일회용 인증키 및 생성주기(3~60초) 개별부여
- Hard 인증키와는 다른 Soft 인증키 로 영구적 사용이 가능
- 전세계적으로 인정된 512Bit 표준 Hash 함수 사용 ( HMAC-SHA512 / 인터넷 보안표준 IETF RFC 6283 )
- 스마트폰 등을 인증키 생성 매체로 하는 간편한 편의성 제공
- 금감원에서 권장하는 Time-Sync , 동적 HMAC Key 방식
- 스마트폰 분실시 인증정보 노출에 대비한 PIN번호 기능 제공
- 어플리케이션 등 사용자 인증이 필요한 모든 분야에서 사용가능
- 2차(2-Factor/2-Channel) 인증의 비밀번호 대체 지원
- 자유로운 Customizing 및 다양한 응용 프로그램과의 연동 개발 제공 ( Java, C 등의 API 연동 )

※ **HMAC (Hash-based Message Authentication Code) : 해쉬 기반 메시지 인증 코드**

HMAC는 Key를 조합하여 Hash 함수를 구하는 방식으로, 송신자와 수신자만이 공유하고 있는 Key와 메시지를 혼합하여 Hash 값을 만드는 방식이다. 또한 채널을 통해 보낸 메시지가 훼손되었는지 여부를 확인하는데 사용할 수 있으며, MAC 특성상 역산이 불가능하므로, 수신된 메시지 와 Hash 값을 다시 계산하여, 계산된 HMAC과 전송된 HMAC이 일치하는지를 확인하는 방식이다.

# Ⅲ. 솔루션 구성

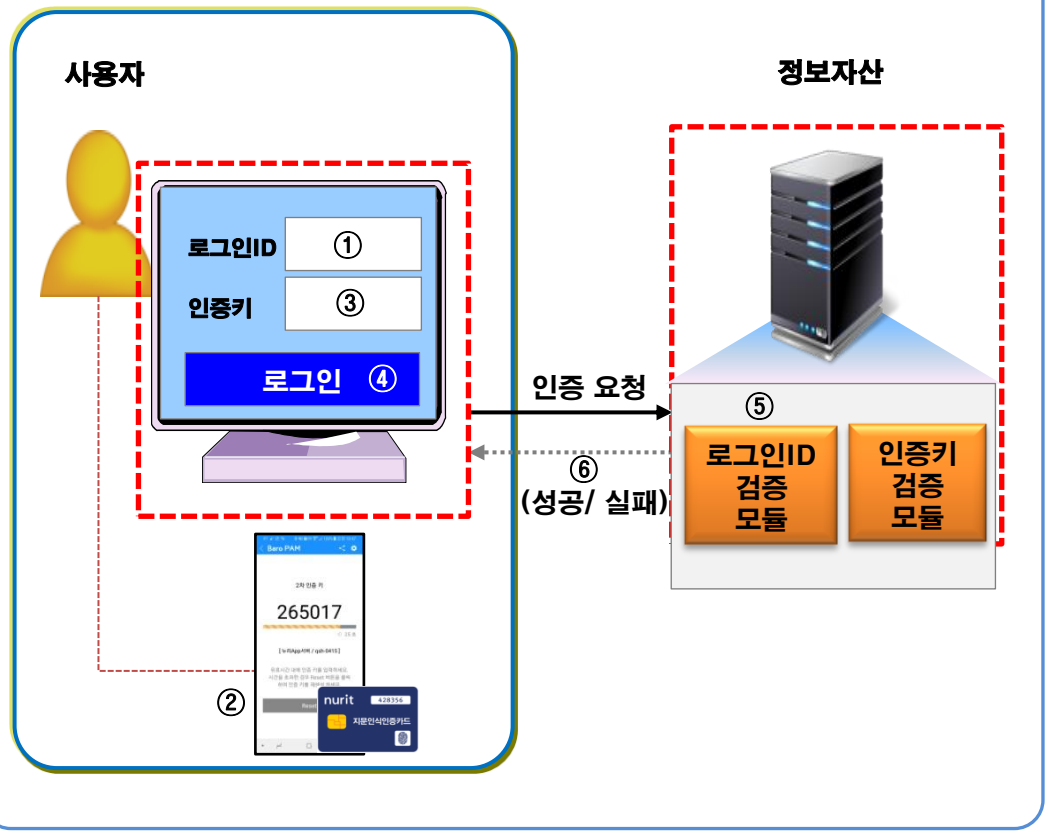
**BaroKEY 솔루션은 사용자가 일회용 인증키를 생성하는 장치, 일회용 인증키를 적용하는 정보자산, 정보자산의 일회용 인증키를 검증하는 부분으로 구성되어 있습니다.**



# Ⅳ. 솔루션 처리 FLOW

## 1. 2-Factor 인증 적용시 인증 Flow

**2-Factor 인증**은 기존의 "**지식기반 인증**"인 **ID/Password** 인증에 **일회용 인증키**와 같은 2개 이상의 인증 요소를 사용해 인증하는 기법입니다.




### 인증 처리 Flow

① 로그인 화면에 접속하여, 로그인ID를 입력한다.
② 스마트폰 앱을 통하여 **일회용 인증키**를 생성한다.
③ 로그인 화면에 생성한 **일회용 인증키**를 입력한다.
④ 로그인 버튼을 클릭한다.
⑤ 정보자산 내부 모듈에서 로그인ID 및 **일회용 인증키**를 검증한다.
⑥ 인증이 성공되면 다음 화면을 띄우고, 실패하면 재 로그인 처리를 수행한다.

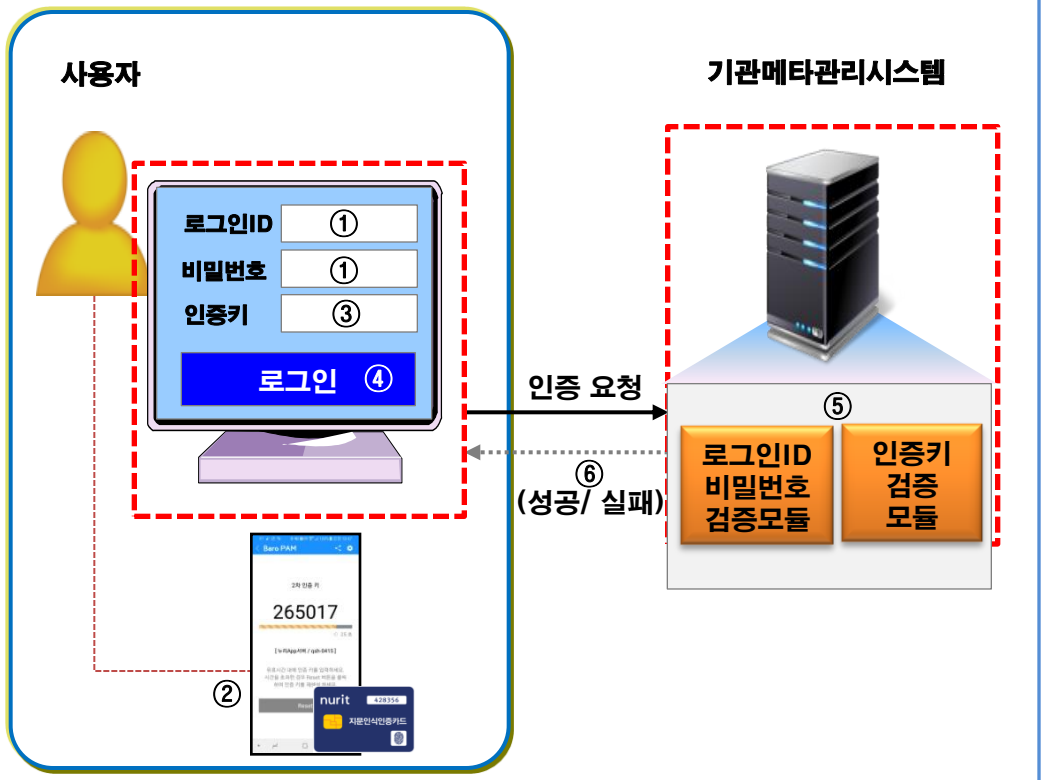



nurit

# Ⅳ. 솔루션 처리 FLOW

## 1. 2-Factor 인증 적용시 인증 Flow

**2-Factor 인증**은 기존의 "**지식기반 인증**"인 **ID/Password** 인증에 **일회용 인증키**와 같은 2개 이상의 인증 요소를 사용해 인증하는 기법입니다.




### 인증 처리 Flow

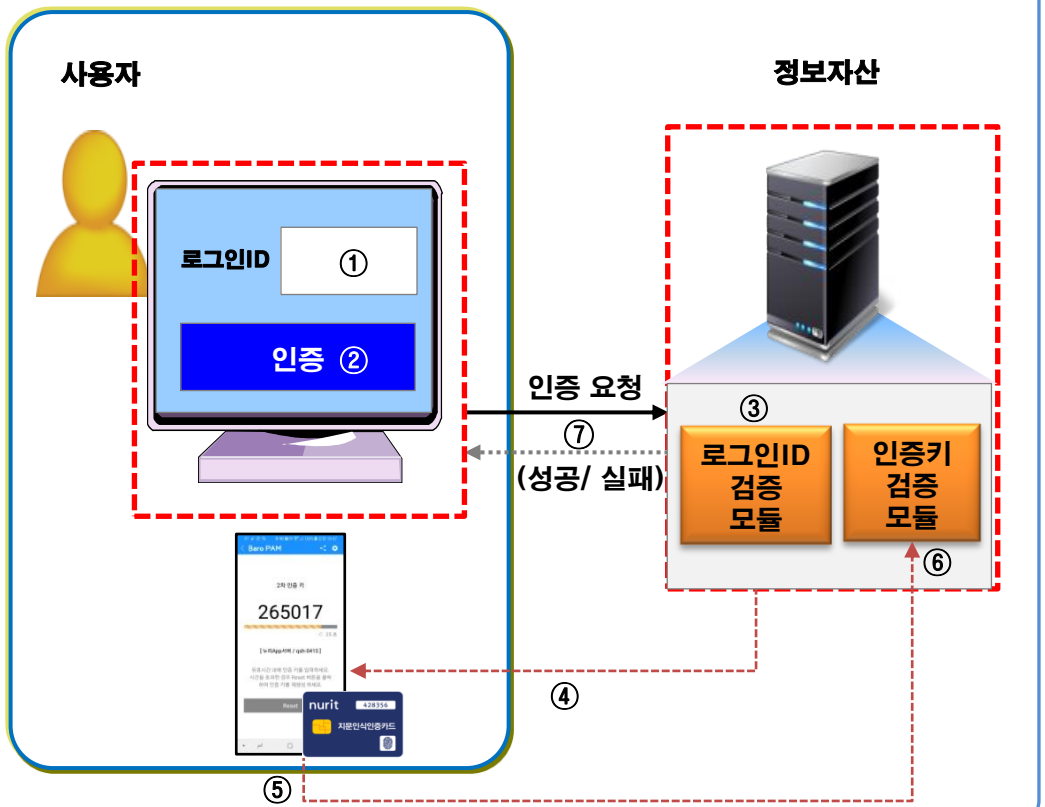
① 로그인 화면에 접속하여, 로그인ID/비밀번호를 입력한다.
② 스마트폰 앱이나 지문인식 인증카드를 통하여 **일회용 인증키**를 생성한다.
③ 로그인 화면에 생성한 **일회용 인증키**를 입력한다.
④ 로그인 버튼을 클릭한다.
⑤ 기관메타관리시스템 내부 모듈에서 로그인ID/비밀번호 및 **일회용 인증키**를 검증한다.
⑥ 인증이 성공되면 다음 화면을 띄우고, 실패하면 재 로그인 처리를 수행한다.




nurit

## 2. 2-Channel 인증 적용시 인증 Flow

**2-Channel 인증은 2-Factor 인증을 포함한다고 보는 것이 일반적이며, 인증과 서비스를 수행하는 통신선로를 서비스 채널과 인증 채널로 물리적으로 분리하여 인증을 수행합니다.**




### 인증 처리 Flow

① 로그인 화면에 접속하여, 로그인ID를 입력한다.
② 로그인 화면에서 인증버튼을 클릭한다.
③ 로그인ID의 유효성을 확인한다.
④ 스마트폰 앱으로 인증을 요청한다.
⑤ 스마트폰 앱을 통하여 일회용 인증키를 생성하고, 스마트폰 앱에서 인증 버튼을 클릭한다.
⑥ 정보자산 내부 모듈에서 일회용 인증키를 검증한다.
⑦ 인증이 성공되면 다음 화면을 띄우고, 실패하면 재 로그인 처리를 수행한다.

### 3. 어플리케이션 로그인

**BaroPAM** 솔루션의 정보자산 접근제어 **2차 인증**에 대한 시스템 Flow는 다음과 같이 처리됩니다.


① Application 로그인 화면에 접속한다.

② 로그인ID 입력 화면에 로그인ID를 입력 한다.

③ 스마트폰 앱을 통하여 **일회용 인증키**를 생성 한다.

④ 생성한 **일회용 인증키**를 Verification code 입력항목에 입력한다.

⑤ 로그인 버튼을 클릭하면 Application 내부 모듈에서 로그인ID와 **일회용 인증키**를 검증 한다.

⑥ 검증이 완료되면 Application에 로그인 한다.



nurit

## 4. 어플리케이션 로그인 (프로그램)

어플리케이션의 로그인 화면에서 로그인 시 입력한 비밀번호인 **일회용 인증키**를 검증하는 프로그램에 다음과 같은 코드를 삽입하면 된다.


```
...
import com.barokey.barokey;
...
로그인 ID 유효성 확인 하여 성공인 경우만 인증키 검증 모듈을 호출
...
boolean bauth_key = barokey.verifyKEYL(String login_id, String phone_no, String
cycle_time, String corr_time, String key_method, String tkey);

if (bauth_key == true) {
    // 검증 성공
} else {
    // 검증 실패
}
...
login_id: 로그인 화면의 로그인-ID 항목에 입력한 ID를 설정.
phone_no: 사용자의 스마트 폰 번호를 숫자만 설정.
cycle_time: 사용자별로 지정한 일회용 인증키의 생성 주기(3~60초)를 설정.
corr_time: 일회용 인증키의 보증오차시간(초)으로 인증카드인 경우만 설정.
key_method: 일회용 인증키의 생성 방식(app1, app256, app384, app512: 앱, card1,
card256, card384, card512: 인증카드)을 설정.

tkey는 로그인 화면의 비밀번호에 입력한 일회용 인증키를 설정해야 한다.

만약, 사용자/고객/회원 정보의 스마트 폰 번호 및 개인별로 지정한 일회용 인증키의
생성 주기가 일회용 인증키의 생성기와 다른 경우 일회용 인증키가 달라서 검증에
실패할 수 있다. 반드시 정보를 일치 시켜야 한다.
```

# Ⅴ. 적용분야

**BaroKEY 솔루션은 정보자산, 도어락 등 사용자에 대한 2차 인증이 필요한 모든 분야에서 사용 가능합니다.**




nurit

# VI. 기타

## 1. 소프트웨어 품질인증 ( GS 인증서 / 시험성적서 / 특허증 / 저작권 등록증 )


2017년 7월
GS인증 1등급


2014년 6월
특허번호
제 10-1413971호


전자신문 광고


TTA 시험성적서


저작권 등록증



nurit

## 2. BaroSolution 제품군

| 구 분 | 설 명 | 비고 |
|---|---|---|
| BaroPAM | Windows/MAC/Linux/Unix의 운영체제에서 2차 인증으로 일회용 인증키(소프트 인증키)를 접목시켜 중앙 집중적 인증 메커니즘을 지원하는 단순하면서도 강력한 정보자산(Windows, MAC, 서버, DB, 네트워크장비, 보안장비, 저장장치 등)의 접근제어 인증 솔루션. | |
| BaroCRYPT | Feistel 암호를 사용하여 크기가 작고 구현이 쉬운 블록 암호화 알고리즘인 XXTEA (Extended Extended Tiny Encryption Algorithm)를 기반으로 하는 가볍고 가장 빠른 암호화 알고리즘을 적용한 솔루션. | |
| BaroCARD | 생체정보인 지문정보를 적용한 최적의 본인인증 솔루션으로 생체정보인 지문정보를 플라스틱 카드에 등록한 후 등록된 지문정보를 인식하면 일회용 인증키를 생성하는 카드(지문인식 기능과 인증카드를 내장한 신개념 카드) 로 지문인식 인증카드 솔루션. | |
| BaroKEY | 어플리케이션 로그인 시 비밀번호를 대체해 주는 소프트웨어 방식(어플리케이션 레벨)의 인증 솔루션으로, 일명 소프트 인증키, 2세대 인증키, 일회용 인증키 솔루션. | |
| BaroCollector | 다양한 Source에서 발생된 많은 양의 로그 데이터(Big Data)를 중앙의 데이터 저장소로 효율적으로 수집해 주는 분산처리, 신뢰성, 가용성을 갖춘 실시간 로그 수집기. | |
| BaroFDS | 이상금융거래탐지 및 대응업무에 대한 모금융기관의 2년간의 Know-how을 바탕으로 개발된 금융권 유일의 검증된 FDS 솔루션으로서 복잡한 금융권 환경에서 쉽고 빠르게 적용하여, 구축 즉시 효과를 발휘할 수 있음. | |
| BaroIDS | 정보자산(서버, 네트워크장비, 보안장비, 저장장치, 데이터베이스, 어플리케이션, 기타)의 이상접속 탐지 및 차단에 대한 현장의 Know-how을 바탕으로 FDS(Fraud Detection System)를 적용하여 개발된 솔루션. | |

# 감사합니다!

www.nurit.co.kr

서울시 강서구 공항대로 186, 617호(마곡동, 로뎀타워)
주식회사 누리아이티  대표전화 :  010-2771-4076