불법적인 정보자산에 접근하는 상황을 제한하여 정보자산의 보안을 강화 위한 인증정책 및 보안전략

nurit

2020. 6.

Content

Ⅰ. 개요

Ⅱ. 인증정책

Ⅲ. 보안전략

Ⅳ. 활용 및 응용

Ⅴ. 적용 모습

Ⅵ. 기타

nurit

1.본인인증의 현주소

nurit

2. 본인인증 방식

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

IP 접속 제한

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

공인 인증서 방식은 솔루션 비용이 비싸며, 공인 인증서 인증 모듈의 불편함 때문에 사용하기가 힘들고, 공인 인증서 의무화가 폐지되어 대체할 대안이 필요함.

일회용 인증키

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.

생체인식

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.

3. 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)

4. 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

5. 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

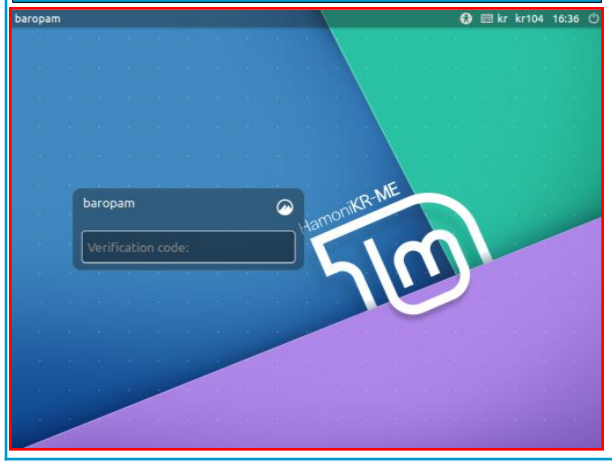
아이라페토브는 "이중인증 옵션 역시 대단히 중요하지만 많이 간과되고 있는 기능" 이라고 짚는다. "중소기업은 웹사이트 관리자 업무를 하는 데 있어서 만큼은 반드시 이중인증을 도입해야 합니다. 다크웹에는 이미 도난 당한 크리덴셜이 활발히 거래되고 있고, 그러므로 비밀번호만으로 뭔가를 보호할 수 있는 시대가 아닙니다. 이중인증이라고 해서 100% 완벽한 건 아니지만, 비밀번호만으로 관리자 페이지를 보호하는 것보다는 훨씬 안전합니다."

6. 적용 방안

정보자산 로그인 시 비밀번호 만으로는 결코 안전하지 않으며 매번 사용할 때마다 비밀번호를 대체 또는 추가 인증(2차 인증)할 수 있는 새로운 적용 방안(추가 인증, 비밀번호 대체, 일회용 비밀번호)이 필요합니다.

1안(추가 인증)

로그인-ID, 비밀번호
이외의 추가 인증(2차 인증)으로
일회용 인증키 적용

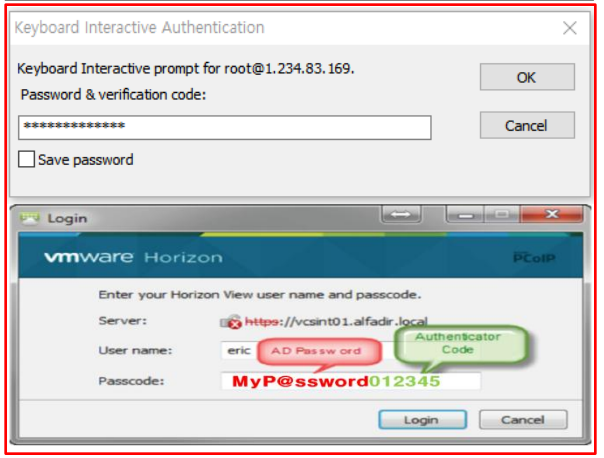


2안(비밀번호 대체)

비밀번호를 제거하고
일회용 인증키로 대체

3안(새로운 비밀번호)

비밀번호와 일회용 인증키 결합하여
비밀번호를 일회용 인증키 생성주기별로
일회용 비밀번호를 적용



nurit

7. 보안 강화

악의적인 목적으로 만들어진 프로그램인 **악성코드를 탐지 및 제거하는 백신** 솔루션과 정보자산 접근제어 **2차 인증**을 통한 **불법적인 원격접속을 차단**하는 솔루션이 결합하여 **정보자산의 보안을 강화**하는 시너지 효과를 낼 수 있습니다.

정보자산 보안 = **악성코드 탐지/제거 (백신)** + **원격접속 차단 (BaroPAM)**

- Windows NT Server
- Mac OS
- Linux / Unix Server
- Application
- Database
- Network 장비
- 저장장치

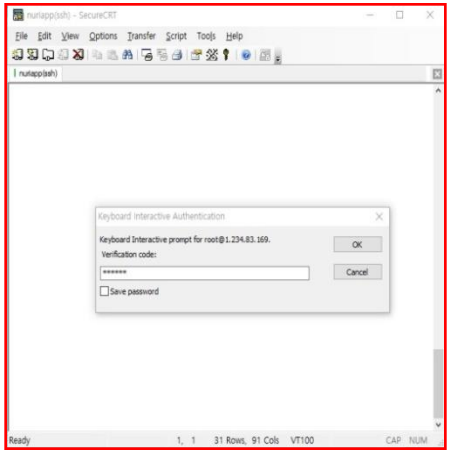
V3

Desktop to Application
Desktop to Desktop
Desktop to Server
Server to Server

nurit

1. 인증 정책

모든 정보자산에 대한 **인증 정책**은 선택이 아닌 반드시 필수로 적용되어야 할 보안 대비책으로 이로 인하여 **보다 안전하게 정보자산을 보호**할 수 있습니다.

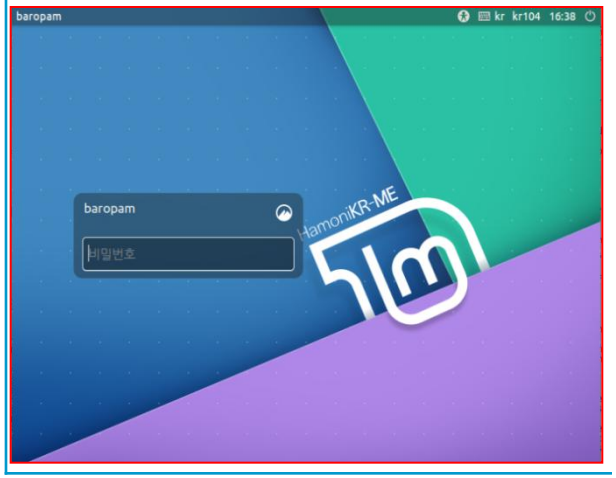
Desktop/PC	Application	Server / Network 장비	Database
지문인식 인증카드나 스마트폰 앱을 이용하여 2세대 인증키를 부여 받아 입력 (일회용 인증키)	지문인식 인증카드나 스마트폰 앱을 이용하여 2세대 인증키를 부여 받아 입력 (일회용 인증키)	지문인식 인증카드나 스마트폰 앱을 이용하여 2세대 인증키를 부여 받아 입력 (일회용 인증키)	지문인식 인증카드나 스마트폰 앱을 이용하여 2세대 인증키를 부여 받아 입력 (일회용 인증키)
			$ sqlplus baropam/baropam Verification code: 276957 SQL*Plus: Release 11.2.0.1.0 Production on 금 11월 30 10:04:09 2018 Copyright (c) 1982, 2009, Oracle. All rights reserved. 다음에 계속됨: Oracle Database 11g Release 11.2.0.1.0 - 64bit Production.

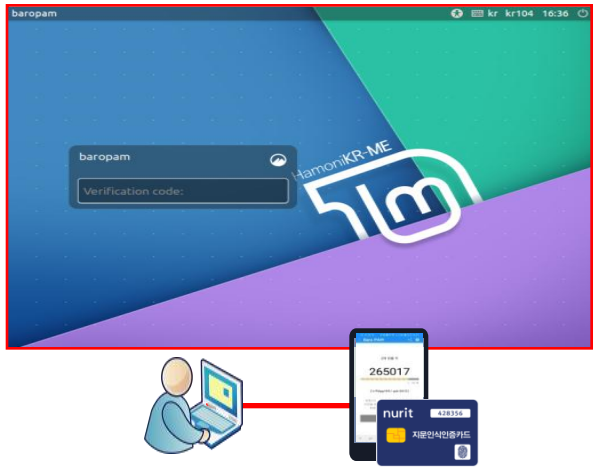
nurit

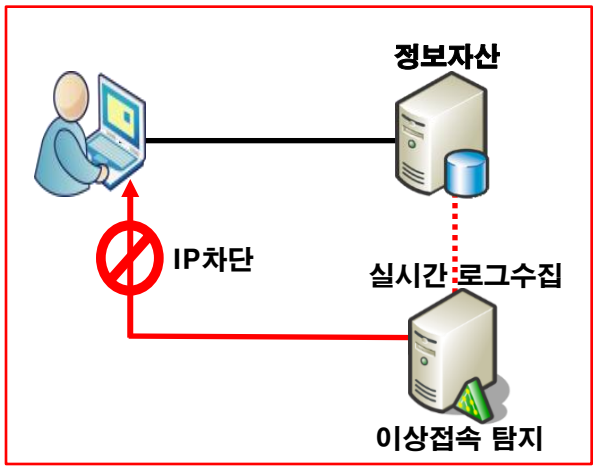
1. 개방형 OS 환경 (하모니카OS / 구름OS / TmaxOS)

개방형OS의 보안 전략은 3단계로 구성되며, 1단계는 전형적인 기본 보안(ID/Password), 2단계는 일회용 인증키를 적용한 보안, 3단계는 이상접속 탐지 및 차단을 통한 불법적인 정보자산의 접속 제어로 구성되어야 합니다.

1단계	2단계	3단계
기존의 전형적인 기본보안 (ID / Password)	지문인식 인증카드나 스마트폰 앱을 이용하여 2세대 인증키를 부여 받아 입력 (일회용 인증키)	각 정보자산의 실시간 로그수집 및 Rule을 적용하여 비정상적인 접속을 탐지 및 IP 차단 (이상접속 탐지 / 차단)



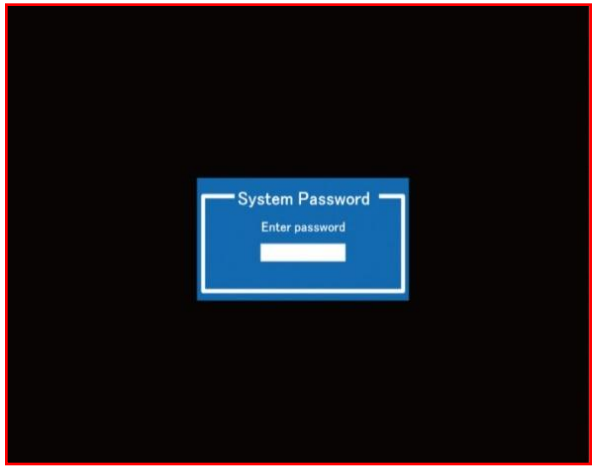
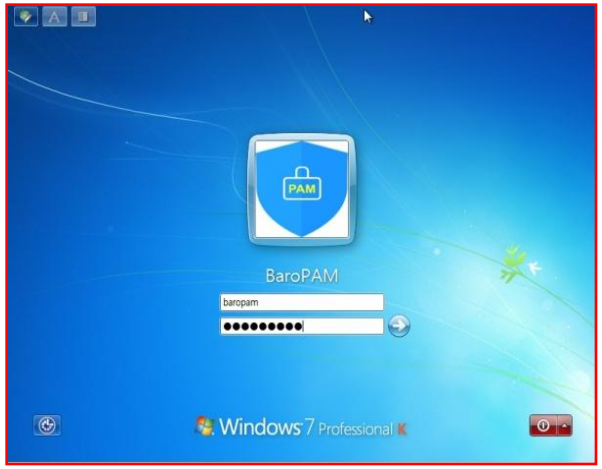




nurit

2. Windows 환경

Windows 환경의 보안 전략은 3단계로 구성되며, 1단계는 Windows 부팅 시 CMOS 보안(Password), 2단계는 전형적인 기본 보안(ID/Password), 3단계는 일회용 인증키를 적용한 보안 전략으로 구성되어야 합니다.

1단계	2단계	3단계
부팅시 CMOS 보안 (Password)	기존의 전형적인 기본보안 (ID / Password)	지문인식 인증카드나 스마트폰 앱을 이용하여 2세대 인증키를 부여 받아 입력 (일회용 인증키)
		

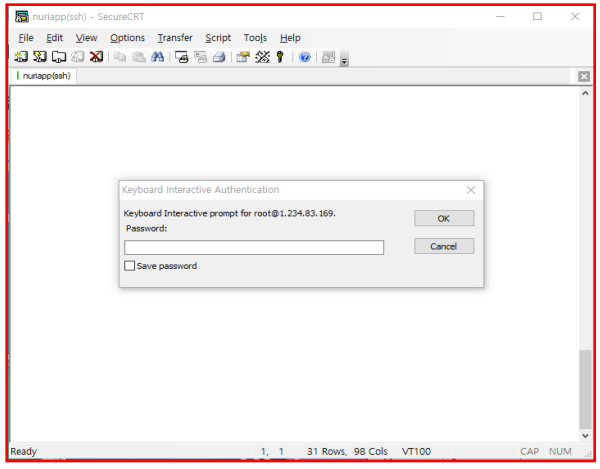
nurit

3. Mac / Linux / Unix 환경

Mac/Linux/Unix의 보안 전략은 3단계로 구성되며, 1단계는 전형적인 기본 보안(ID/Password), 2단계는 일회용 인증키를 적용한 보안, 3단계는 이상접속 탐지 및 차단을 통한 불법적인 정보자산의 접속 제어로 구성되어야 합니다.

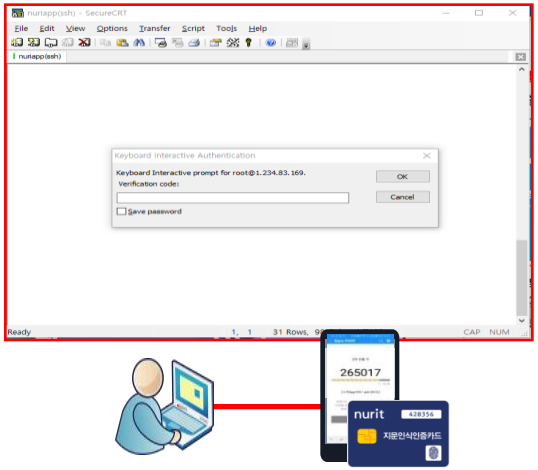
1단계

기존의 전형적인 기본보안
(ID / Password)



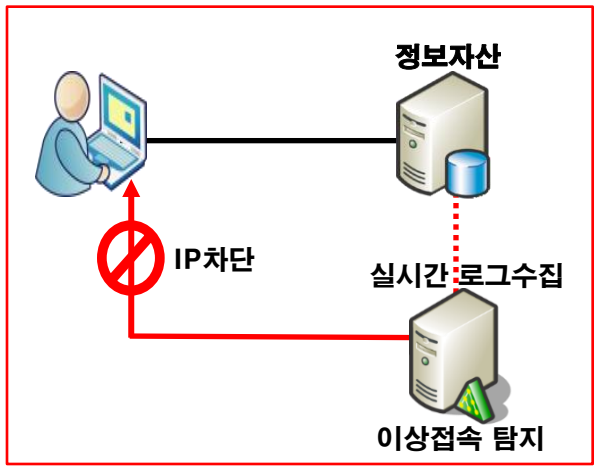
2단계

지문인식 인증카드나
스마트폰 앱을 이용하여
2세대 인증키를 부여 받아 입력
(일회용 인증키)



3단계

각 정보자산의 실시간 로그수집
및 Rule을 적용하여 비정상적인 접속을
탐지 및 IP 차단
(이상접속 탐지 / 차단)



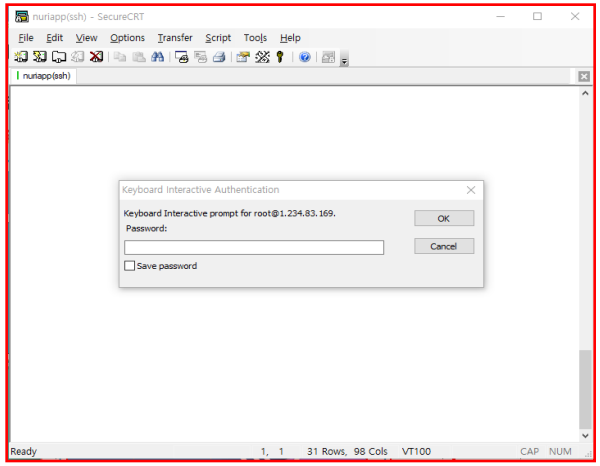
nurit

4. 데이타베이스 환경

데이터베이스 환경의 보안 전략은 3단계로 구성되며, 1단계는 전형적인 기본 보안(ID/Password), 2단계는 일회용 인증키를 적용한 보안, 3단계는 데이터베이스 접속 시 일회용 인증키를 적용한 보안으로 구성되어야 합니다.

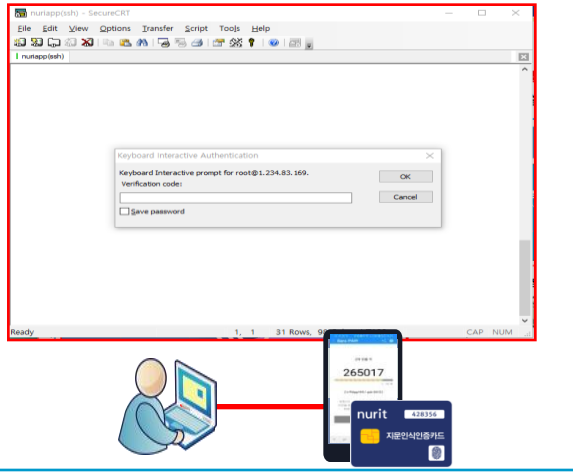
1단계

기존의 전형적인 기본보안
(ID / Password)



2단계

지문인식 인증카드나
스마트폰 앱을 이용하여
2세대 인증키를 부여 받아 입력
(일회용 인증키)



3단계

지문인식 인증카드나
스마트폰 앱을 이용하여
2세대 인증키를 부여 받아 입력
(불법접속차단)

```
$ sqlplus baropam/baropam

Verification code: 276957

SQL*Plus: Release 11.2.0.1.0 Production on
금 11월 30 10:04:09 2018

Copyright (c) 1982, 2009, Oracle. All rights
reserved.


다음에 계속됨:
Oracle Database 11g Release 11.2.0.1.0 -
64bit Production.
```

nurit

1. 본인인증 활용가능 영역

2. 응용분야 - 2차 인증

3. 응용분야 - IC카드

신용카드의 부정사용의 증가로 카드 이용자들의 불만이 사회적인 갈등으로 이어지고 이를 해결하기 위한 관리비용 또한 증가 하고 있으며, 선도 기업으로서의 사회적인 책임을 다하고 디지털 기업의 리딩 자리를 확고히 하기 위해서는 신개념의 결제 채널 확보가 필요 합니다.

nurit

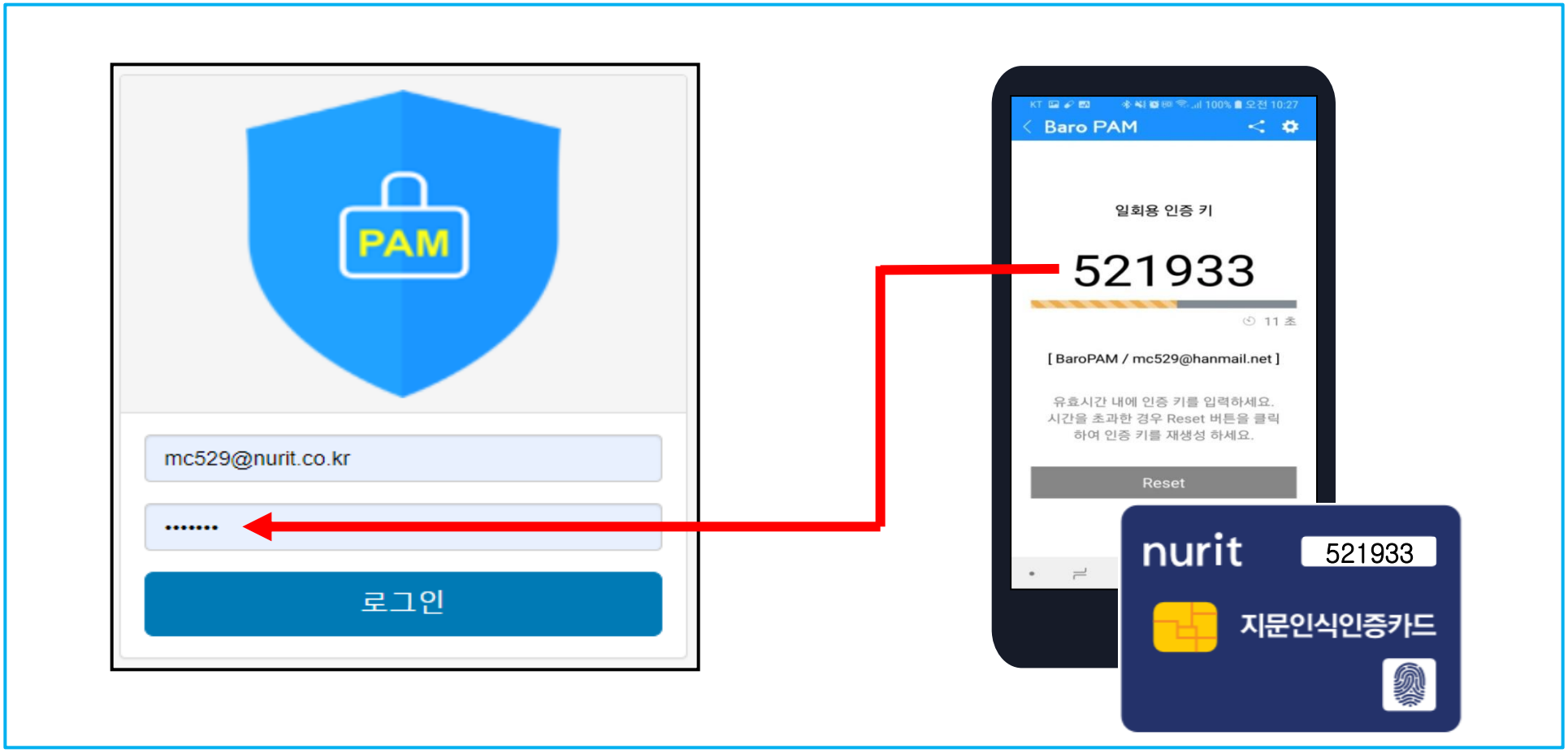
4. 응용분야 - 본인 인증

정보통신기기는 개인정보의 저장과 열람을 위한 장치로 외부 해킹이나 불법 열람에 대한 차단과 통제가 철저 해야 함에도 불구하고 ID 및 비밀번호 관리 소홀로 정보유출 시 심각한 사회 문제를 야기할 수 있으므로 장치의 접근 통제 강화가 필요 합니다.

nurit

1. 어플리케이션 로그인

ERP, 전자결재, 그룹웨어 등의 어플리케이션 로그인 시 로그인-ID를 입력한 후 스마트폰 앱에서 일회용 인증키를 생성합니다. 생성한 일회용 인증키를 입력한 후 로그인 버튼을 클릭하여 어플리케이션에 로그인 합니다.



nurit

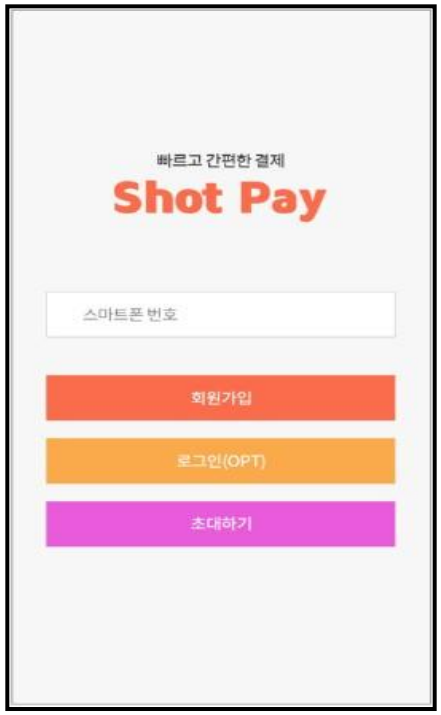
2. 전자문서 인증

전자문서 중 많이 사용하고 있는 전자 세금계산서를 확인하기 위해서 "(세금)계산서 보기" 버튼을 클릭하여 일회용 인증키를 입력할 수 있는 "Verification code" 항목을 추가하여 보안을 강화한 모습입니다.

nurit

3. 간편결제 / 계좌이체 인증 (핀테크)

간편결제 및 계좌이체 시 앱에서 **OTP번호생성** 버튼을 클릭합니다. 생성한 **OTP번호**는 앱에 표시되며 결제버튼을 클릭하여 결제합니다.



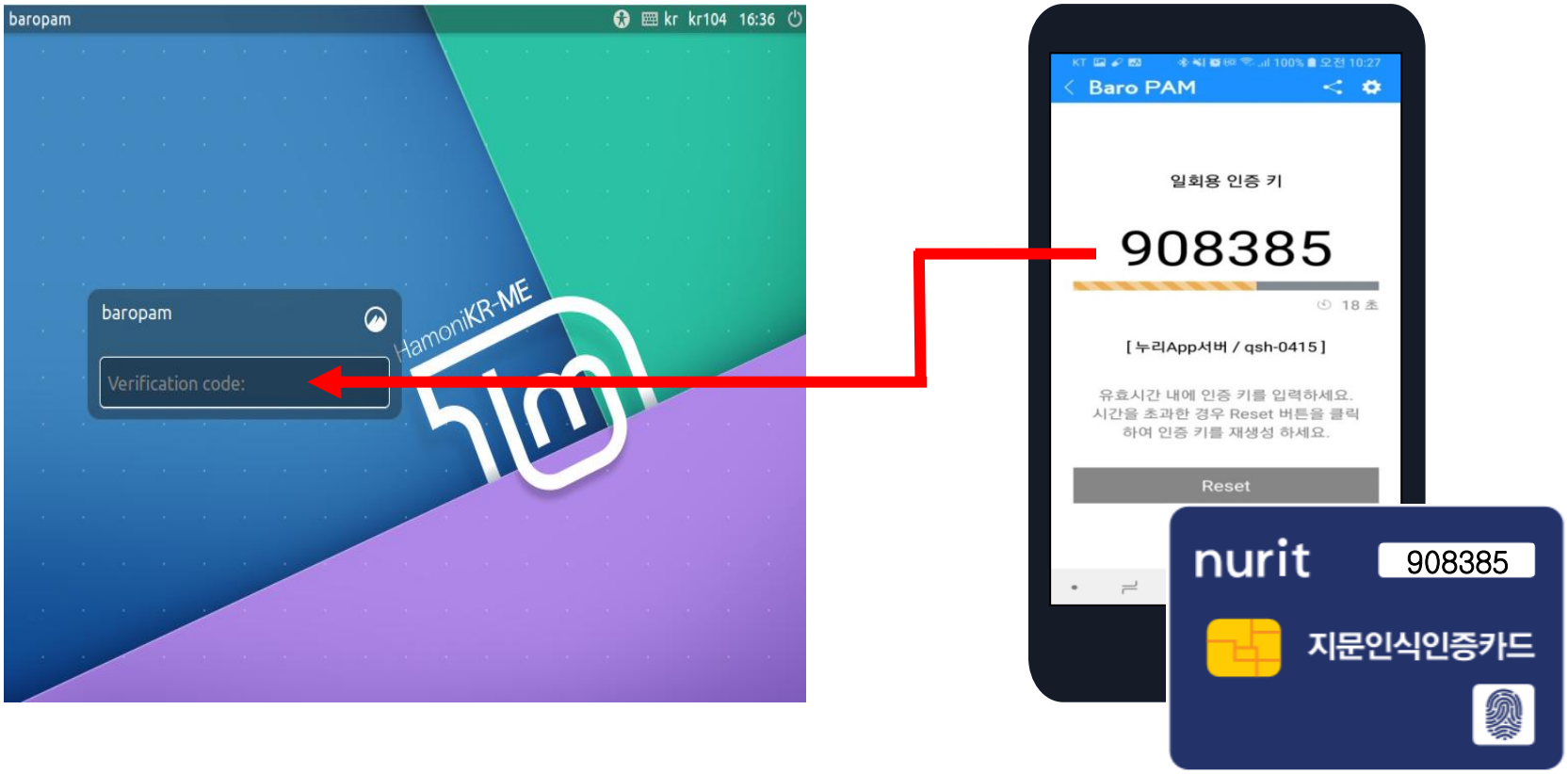
카드결제 시 OTP 생성 규칙 = 카드번호 + 결제금액 + 고유번호
계좌이체 시 OTP 생성 규칙 = 계좌번호 + 이체금액 + 고유번호

→ 서버에서 OTP 검증을 통해서 결제/이체 정보의 위변조 여부를 확인.

nurit

4. 개방형OS 로그인(하모니카OS/구름OS/TmaxOS)

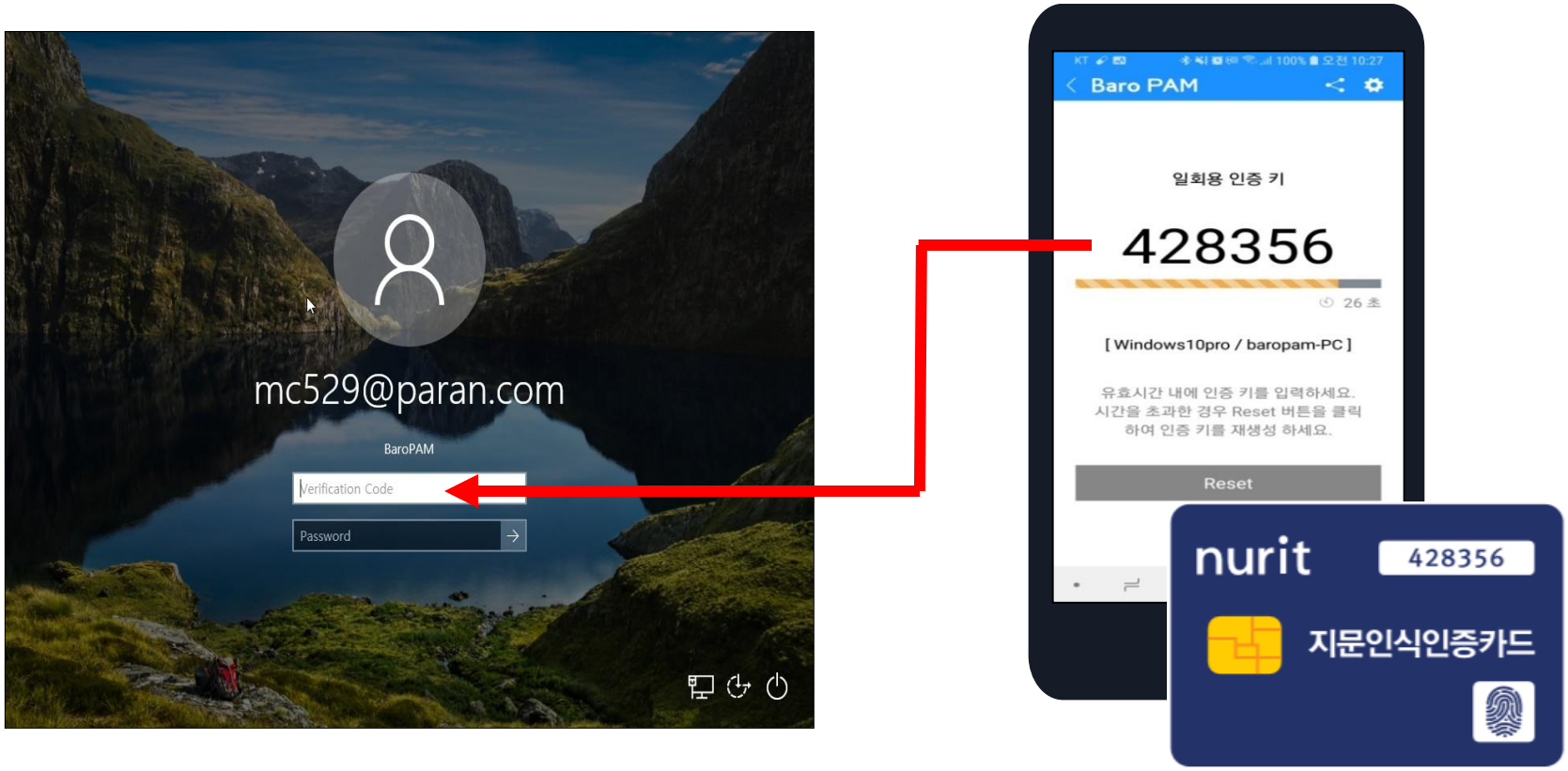
Windows 환경을 대체 및 보안에 강한 국산 OS인 하모니카OS에 로그인 시 로그인-ID를 입력한 후 스마트폰 앱에서 일회용 인증키를 생성합니다. 생성한 일회용 인증키를 입력한 후 로그인 버튼을 클릭하여 로그인 합니다.



nurit

5. Windows 로그온

Windows 로그온 시 스마트폰 앱에서 일회용 인증키를 생성합니다. 생성한 일회용 인증키와 비밀번호를 입력한 후 로그온 버튼을 클릭하여 Windows에 로그온 합니다.

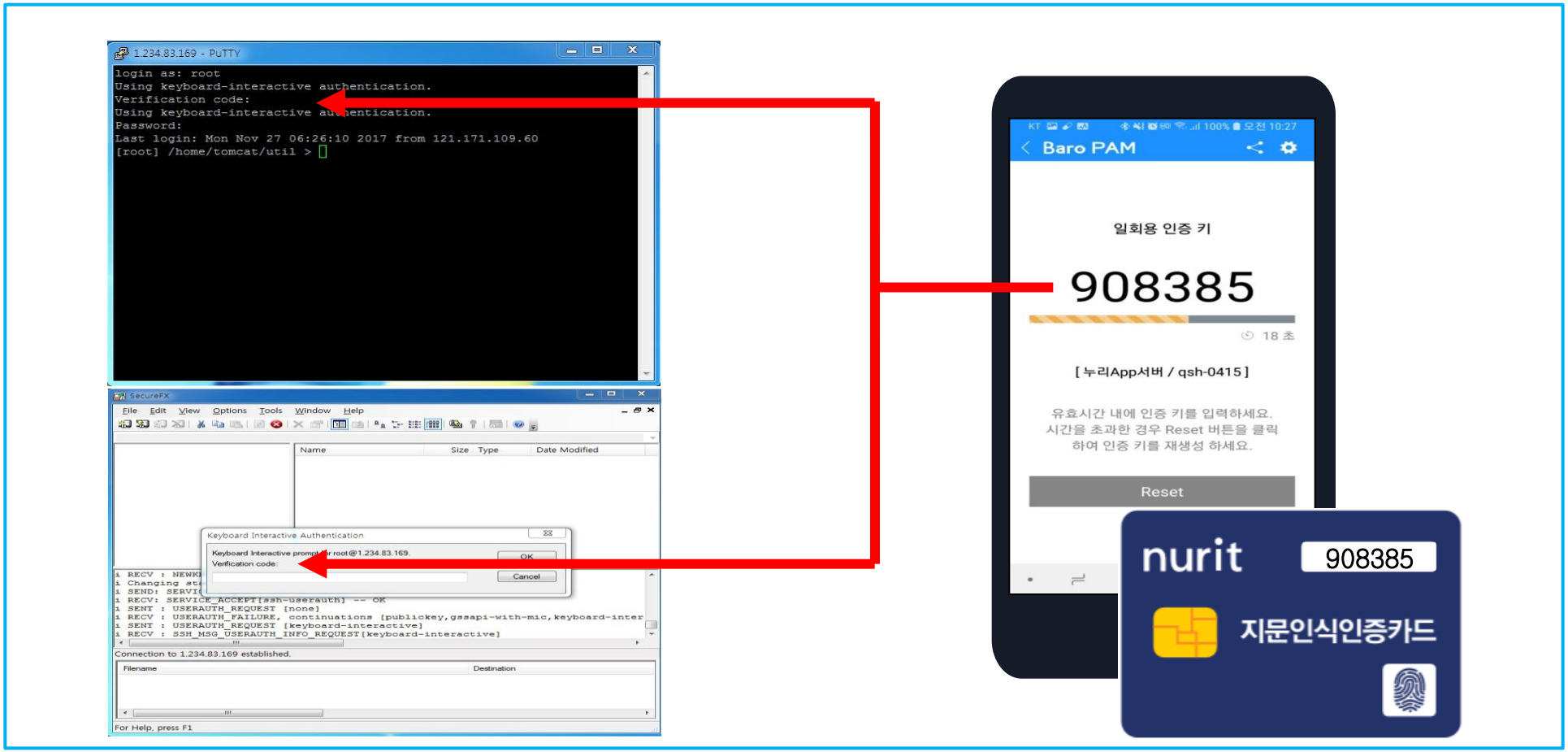


nurit

6. Mac / Linux / Unix 로그인

Mac / Linux / Unix 환경에 로그인 시 로그인-ID를 입력한 후 스마트폰 앱에서 일회용 인증키를 생성합니다.

생성한 일회용 인증키를 입력한 후 로그인 버튼을 클릭하여 로그인 합니다.



nurit

7. Database 접속(Oracle/Tibero/CUBRID/Altibase/Mercury)

CUBRID 오픈소스 DBMS에 CSQL 인터프리터, 백업 및 복구, 데이터베이스 재구성 등에 일회용 인증키를 적용한 모습입니다.(CUBRID GUI 도구인 CUBRID Manager에 "CM 사용자", "CM 비밀번호" 이외에 일회용 인증키를 입력할 수 있는 "Verification code" 항목을 추가하여 보안 강화)

1. CSQL 접속 방법

```
$ csql -C -u db_user -p 'qwe123' -k '108992' demodb@localhost

$ csql -C -u db_user -p 'qwe123' -k '108992' demodb@192.168.0.100

$ csql -S -u db_user -p 'qwe123' -k '108992' demodb
```

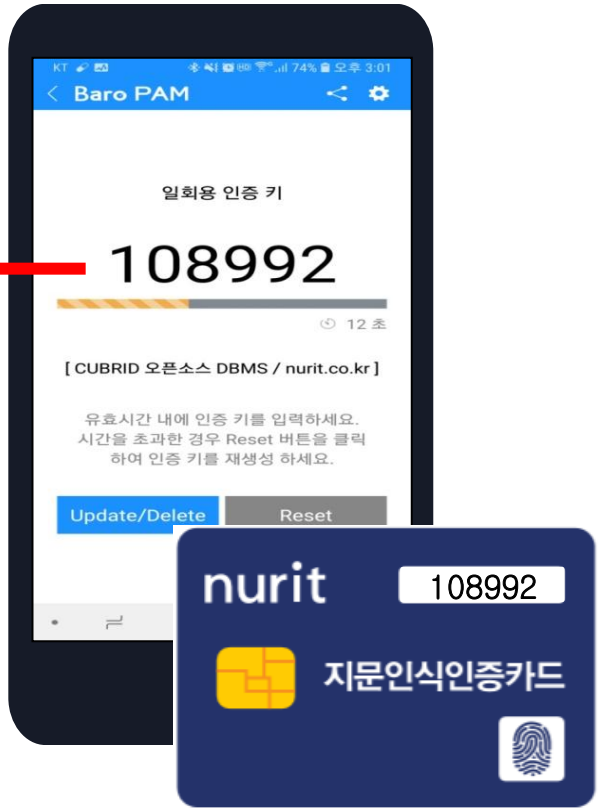
2. 백업과 복구

```
$ cubrid backupdb -C -z -r -k '108992' -D /CUBRID/databases/demodb -l 0
demodb

$ cubrid restoredb -k '108992' -d 19-02-2015:17:39:00 demodb
```

3. 데이터베이스 재구성

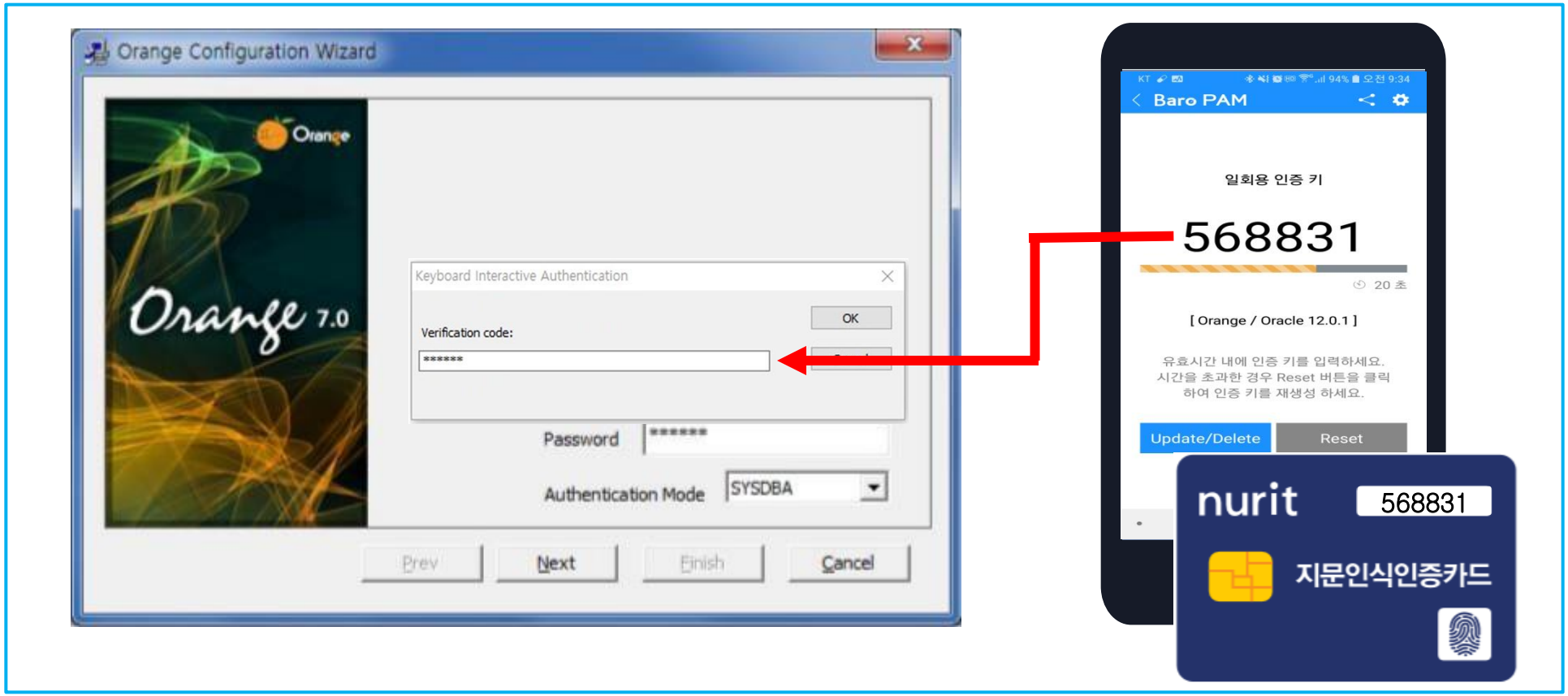
```
$ cubrid unloaddb -u dba -p 'password' -k '108992' -S -O /data/unload --
output-prefix=demodb demodb.bak
```



nurit

8. DBMS 관리 툴 접속

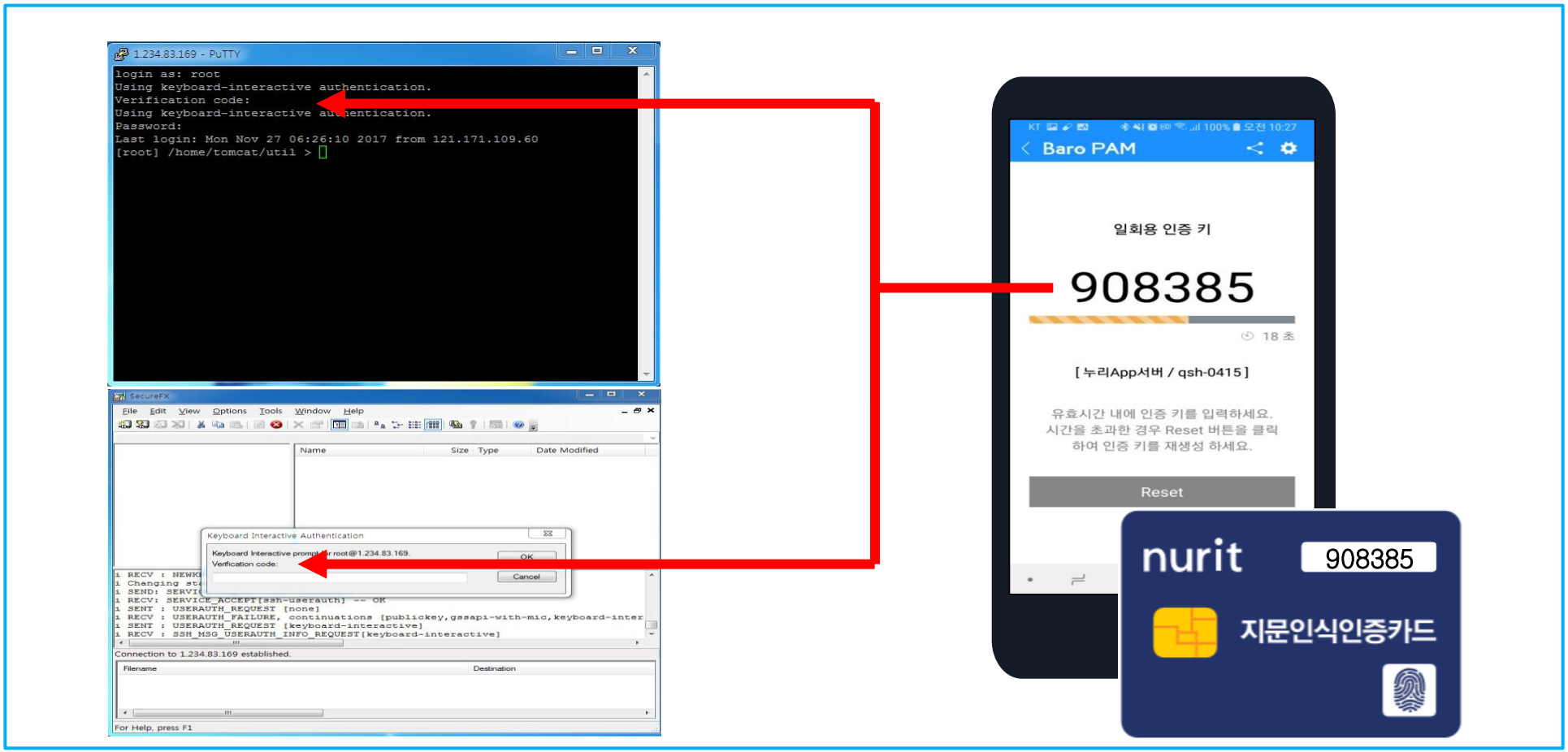
Orange/ SQLGate/Toad 같은 DBMS 관리 툴을 통한 DBMS 접속 시 일회용 인증키를 입력할 수 있는 "Verification code" 항목을 추가하여 보안을 강화한 모습입니다.



nurit

9. 네트웍스 장비 로그인

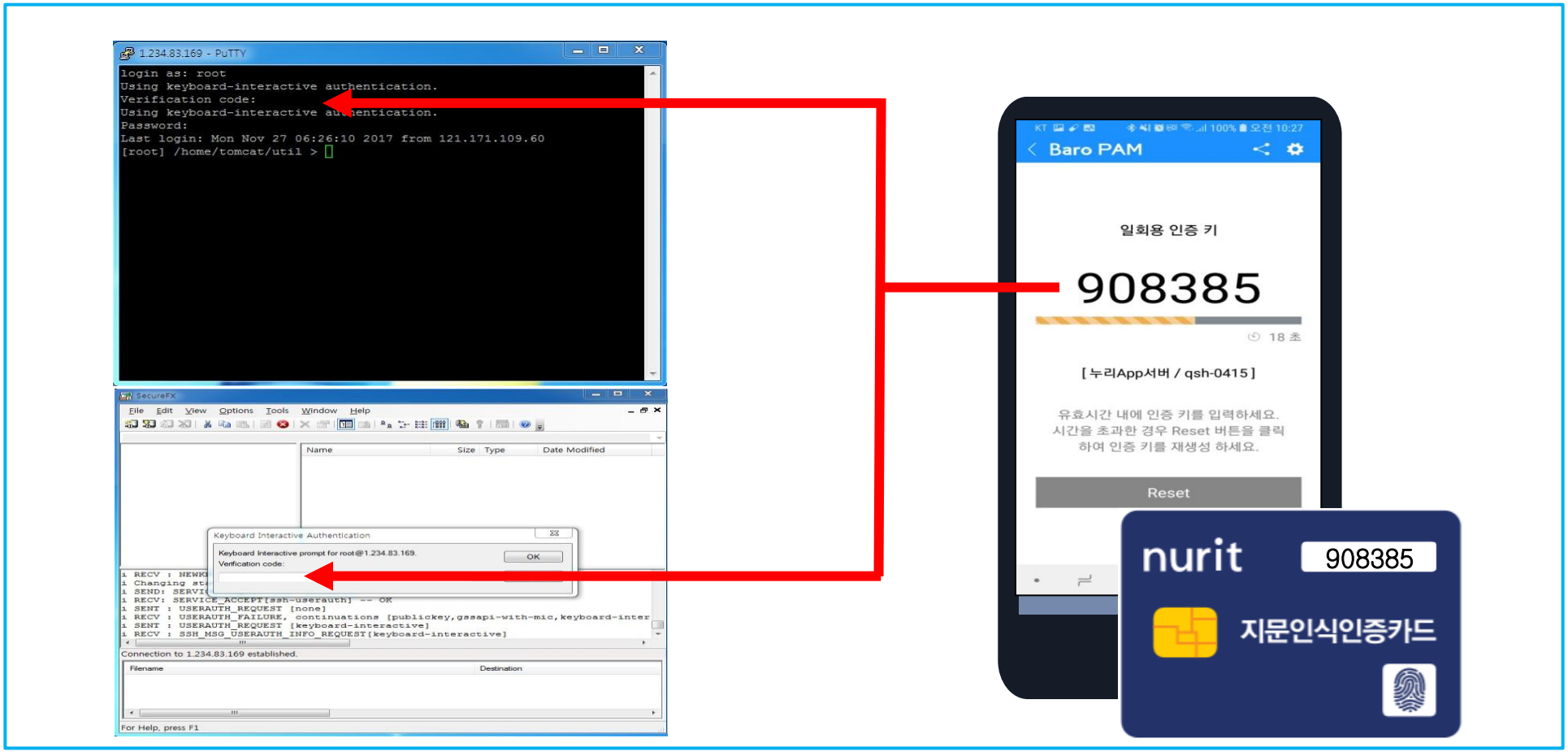
네트웍스 장비 로그인 시 로그인-ID를 입력한 후 스마트폰 앱에서 일회용 인증키를 생성합니다. 생성한 일회용 인증키와 비밀번호를 입력하여 네트웍스 장비에 로그인 합니다.



nurit

10. Dell EMC 저장장치 로그인

Dell EMC 저장장치 로그인 시 로그인-ID를 입력한 후 스마트폰 앱에서 일회용 인증키를 생성합니다. 생성한 일회용 인증키와 비밀번호를 입력하여 Dell EMC 저장장치에 로그인 합니다.



nurit

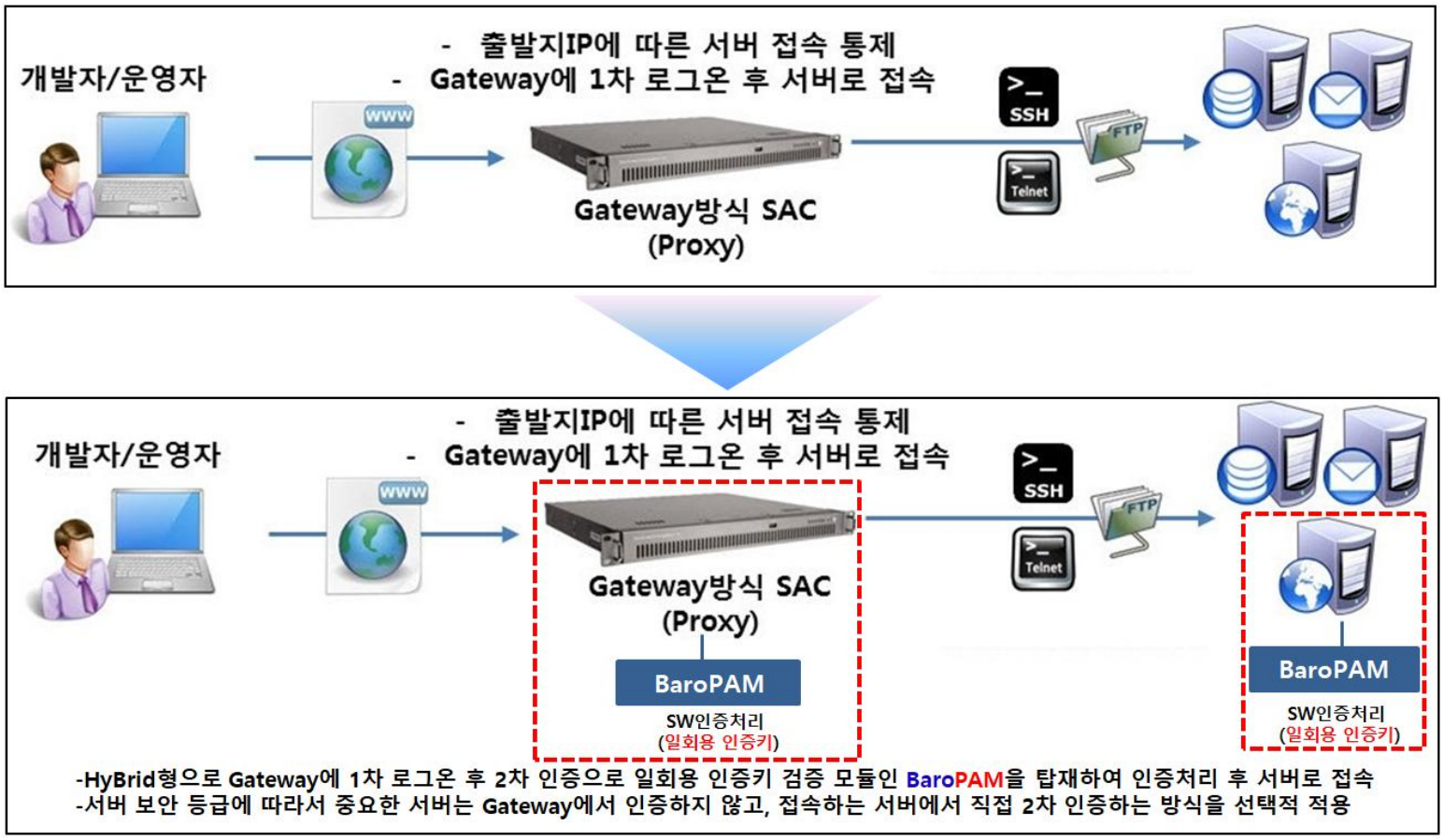
11. SSO(Single Sign On) 솔루션과 융합

SSO(Single Sign On)는 1회 인증으로 여러 시스템을 이용할 수 있는 통합 인증 기능으로 단일화된 ID로 SSO로 그인시 각 업무시스템을 별도의 인증절차 없이 권한에 따라 차등적, 선별적으로 각 시스템에 접근할 수 있는 환경을 제공하는 솔루션입니다.

nurit

12. SAC(System or Server Access Control) 솔루션과 융합

SAC(System or Server Access Control) 솔루션은 계정통합관리 및 접근제어(Access Control)와 감사(Audit) 기능을 제공하는 솔루션입니다.



nurit

13. SSO(Single Sign On)/SAC(System Access Control)의 인증

단일화된 ID로 SSO/SAC 로그인시 로그인-ID를 입력한 후 스마트폰 앱에서 일회용 인증키를 생성합니다. 생성한 일회용 인증키 입력하여 사용자의 한번 인증으로 연결된 모든 정보자산으로 접속 할 수 있는 통합 로그인 합니다.

일회용 인증키 적용 전	일회용 인증키 적용 후
❖ 정보자산별 / 계정별 고정된 비밀번호 사용	❖ 정보자산별 / 계정별 일회용 인증키 사용
❖ 비밀번호 생성 규칙 적용	❖ 해시 알고리즘(SHA512)에서 발생한 값 적용
❖ 비밀번호 정보 DB에 보관	❖ 필요시 스마트폰 앱에서 직접 생성
❖ 암호화 기술 등을 이용한 보안 조치(단방향 암호화) 필요	❖ 암호화 기술 등을 이용한 보안 조치 불필요
❖ 유출 위험 및 피해 발생	❖ 유출 위험 및 피해 발생하지 않음
❖ 의무적으로 비밀번호 변경주기 적용	❖ 개별 인증키 생성주기(3~60초) 적용
❖ 비밀번호 증후군 / 비밀번호 리셋 증후군 호소	❖ 비밀번호 증후군 / 비밀번호 리셋 증후군 발생하지 않음

1. 회사 소개

일반현황

상호:	주식회사 누리아이티
설립일:	2018년 1월 19일
주사업분야:	지문인식 인증/출입카드 및 정보자산 2차 인증 보안S/W
사업장:	서울시 강서구 공항대로 186, 617호(마곡동, 로뎀타워)
주요 품목:	BaroPAM, BaroCARD, BaroKEY, BaroCRYPT, BaroCollector, BaroFDS, BaroIDS

「작지만 강한 회사, 기술력이 강한 회사, 소수 정예 회사」

연혁

2019.11	개방형OS인 하모니카OS와 협업
2019.10	자인컴 OCS, EMR 솔루션에 BaroPAM 임베디드 공급
2019.09	(주) 엘리시스 제품 공급 파트너 계약
2019.07	반디에스앤씨㈜ 솔루션에 BaroPAM 임베디드 공급
2019.04	지문인식 출입카드 출시
2019.04	BaroPAM GS인증 누리아이티 -> 주식회사 누리아이티로 양도양수
2019.03	BaroPAM 저작권 등록
2019.03	주식회사 트루인테크놀로지스 제품 공급 파트너 계약
2019.01	사업장 이전(마곡동 로뎀타워 617호)
2018.11	㈜솔루비스와 제품 공급 파트너 계약
2018.11	주식회사 반디데이타와 제품 공급 파트너 계약
2018.07	BaroPAM 인증카드 및 지문인식 인증카드 출시
2018.07	BaroPAM 인증카드용 Firmware 개발
2018.07	㈜디에이치솔루션과 제품 공급 파트너 계약
2018.07	㈜소프트일레븐과 제품 공급 파트너 계약
2018.07	㈜디지탈리치와 제품 공급 파트너 계약
2018.07	주식회사 이노아이엔씨와 제품 공급 파트너 계약
2018.05	인증서버 기능 추가
2018.04	금융결제용 OTP카드 Firmware 개발
2018.01	주식회사 누리아이티 설립
2017.11	BaroIDS (이상접속 탐지 및 차단) 제품 출시
2017.09	BaroPAM 어플 서비스 개시
2017.07	BaroIDS(이상접속 탐지 및 차단) 출시
2017.07	바로팜 V1.0(BaroPAM V1.0) GS인증 1등급 인증
2017.05	BaroCRYPT(암복호화) 제품 출시
2016.11	BaroPAM(정보자산 2차 인증) 제품 출시
2016.05	BaroKEY(일회용 안증키) 제품 출시
2016.01	BaroFDS(이상금융거래 탐지시스템) 제품 출시
2015.10	BaroCollector(실시간 로그 수집기) 제품 출시
2014.04	특허출원(OTP카드를 이용한 본인인증 결제시스템 및 그 방법)
2011.08	누리 어플만들기 무료서비스 개시
2009.11	누리아이티로 상호 변경
2008.11	피엘 인포텍으로 상호 변경
2007.12	Wily Add-on 모듈 개발
2006.03	케이피엘 인포텍 설립(대방동 경원빌딩)

2. 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

3. 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