KICA 한국정보인증

국가망보안체계 환경에서의 등급별 사용자 인증 방법

2025. 02. 28.

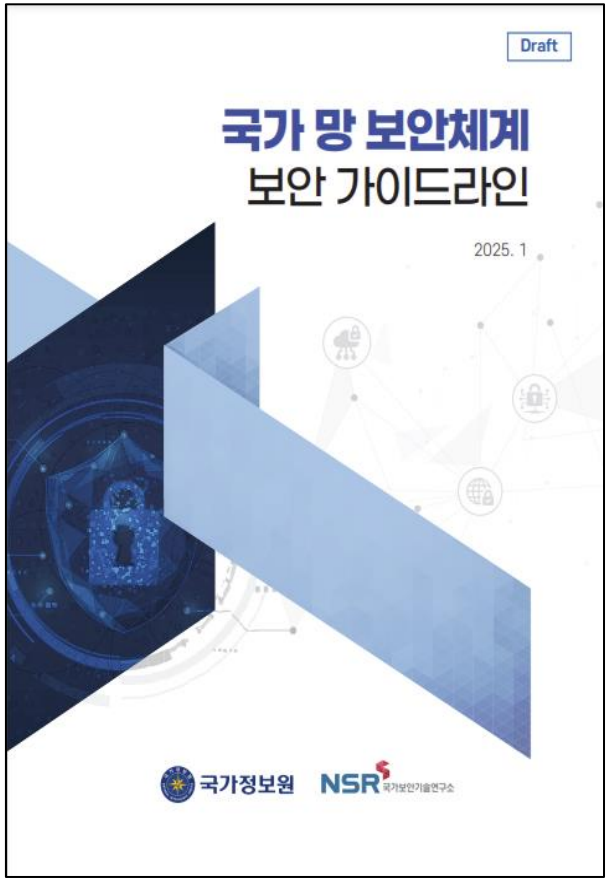
김재중 상무 (jjkim@signgate.com)

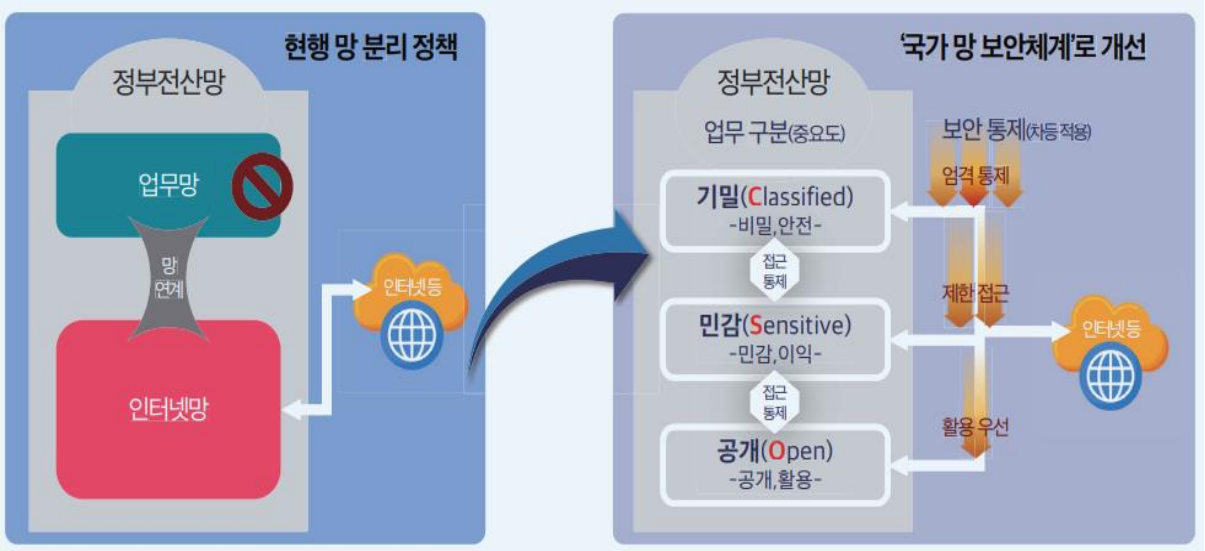
© 2024 KICA inc. All rights reserved.

Contents

기존 망 분리 정책과 국가 망 보안체계 비교

“정보시스템과 데이터 중요도에 따라 기밀(C), 민감(S), 공개(O)로 나눠 보안 체계를 차등 적용”





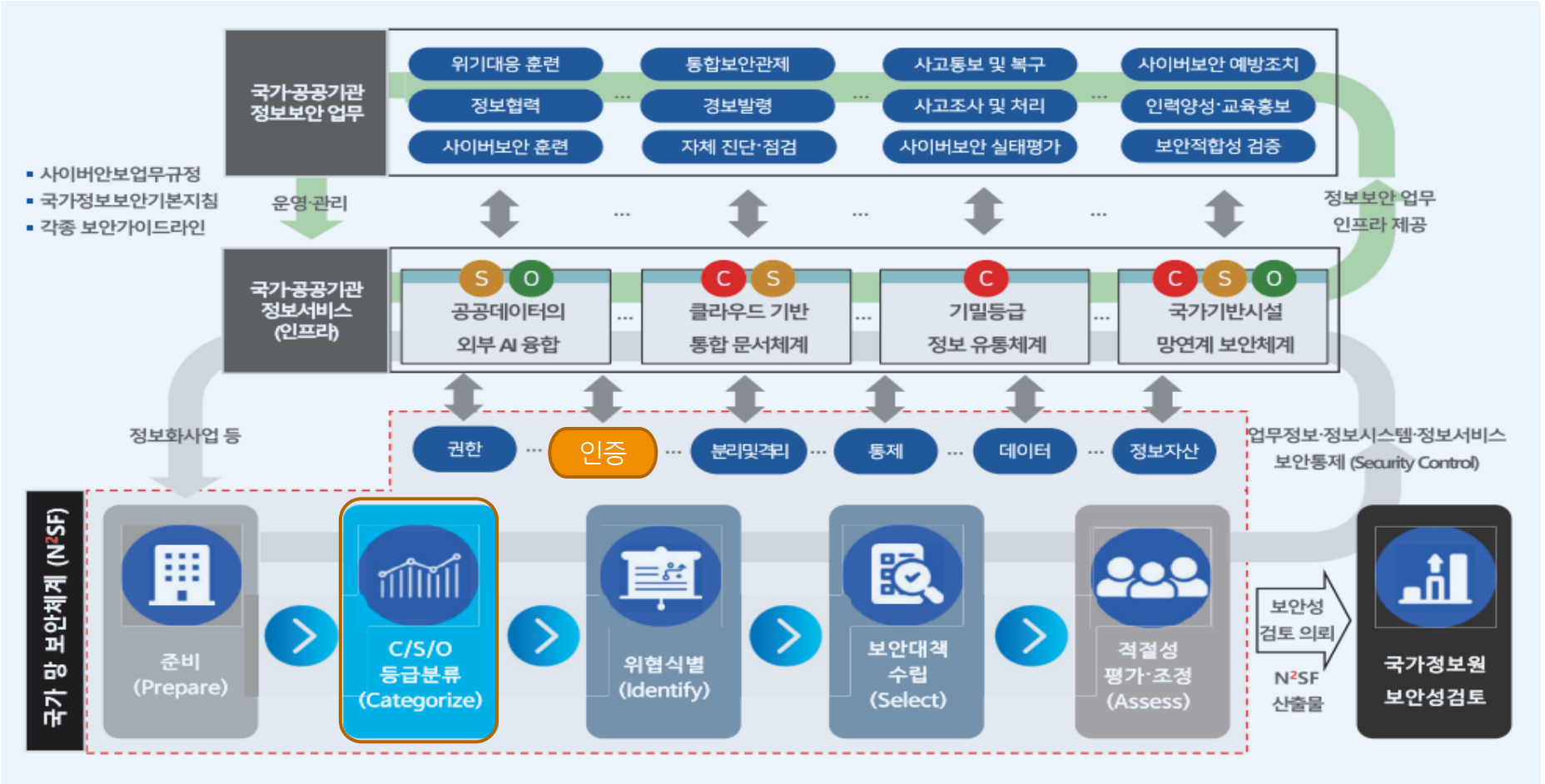
등급		정의
비공개 정보	기밀 (Classified)	• 비밀, 안보·국방·외교·수사 등 기밀정보 및 국민 생활·생명·안전과 직결된 정보
	민감 (Sensitive)	• 비공개 정보로 개인·국가 이익 침해가 가능한 정보
공개 정보	공개 (Open)	• 기밀·민감 정보 이외 모든 정보 및 별도의 조치를 적용한 비공개 정보

(출처: 국가 망 보안체계 보안 가이드라인)

© 2025 KICA inc. All rights reserved.

국가 망 보안체계와 국가·공공기관 정보보안 업무의 관계

"국가·공공기관이 자산을 분석해 위협을 식별하고 적절한 보안대책을 수립"



(출처: 국가 망 보안체계 보안 가이드라인)

© 2025 KICA inc. All rights reserved.

인증 분야 보안 통제 항목 (1/2)

중항목	소항목	보안통제 설명	C	S	O
다중요소 인증 Multi-Factor Authentication (MA)	관리자 계정 다중요소인증	• 사용자에 대한 1) 지식기반 요소, 2) 소유기반 요소, 3) 생체기반 요소 중 2개 이상의 요소를 조합하여 인증한다.	●	●	●
	사용자 계정 다중요소인증	• 지정되지 않은 접속 경로 또는 승인되지 않은 단말을 통한 로그인 시 다중요소인증 적용한다.	●	●	
	다중요소인증 장치 분리	• 다중요소 인증 시에는 인증을 요청한 장치(PC 등)과 분리된 별도의 장치(휴대폰, H/W OTP 등)을 활용한 인증 수행한다.	●	●	
	다중요소인증 경로 분리	• 다중요소 인증 시에는 다중요소인증 시 인증을 요청한 장치의 통신 경로와 분리된 별도의 통신경로를 통해 인증 수행한다.	●		
인증보호 Authentication Protection (AU)	**공개키 기반구조(PKI) 인증서**	• 신뢰할 수 있는 공개 키 인프라(PKI)를 통해 발급된 인증서 사용을 인증서 유효기간 동안 관리하고 보호한다.	●	●	●
인증정책 Authentication Policy (AP)	기관 발급 증명수단 인증 활용	• 기관에서 발급한 **자격 증명수단(모바일 공무원증 등)**을 활용하여 사용자를 인증한다.	●	●	
	특정상황에서의 다중요소 인증	• 특정사항 또는 조건에서는 다중요소 인증을 적용하여 사용자 인증한다.	●	●	
	재인증	• 주기적 또는 특정사항 조건에서는 사용자에게 재인증을 요구한다. – 사용자 자격 증명 변경 시, 시스템 보안설정 변경 시, 특별권한 기능 실행 시, 기타 기관이 지정한 상황	●	●	
	동시 중복 인증 차단	• 정보서비스 특성을 반영하여 동시 중복 인증을 차단한다.	●	●	

(출처: 국가 망 보안체계 보안 가이드라인 부록)

© 2025 KICA inc. All rights reserved.

인증 분야 보안 통제 항목 (2/2)

중항목	소항목	보안통제 설명	C	S	O
인증수단 Authentication Method (AM)	암호모듈 인증	• 관리 법규, 정책 및 규정 등을 **준수한 암호모듈 인증 체계를 적용**한다.	●	●	●
	비밀번호 기반 인증	• **숫자, 문자, 특수문자 등을 혼합하고 주기적으로 변경하는 비밀번호 인증체계를 적용한다.**	●	●	
	공개키 기반 인증	• **신뢰할 수 있는 인증 기관(CA)을 통해 발급된 인증서의 유효성을 검증하고, 인증서의 발급, 갱신, 폐지 등을 관리한다.**	●	●	●
	공개키 기반 저장소 관리	• **네트워크, 운영체제, 브라우저, 응용프로그램을 포함하여 모든 정보시스템에 설치된 PKI 저장소에 대해 관리방안을 수립한다.**	●	●	
	초기 인증수단 변경	• 정보시스템 구성요소 배포/설치 전 기본(초기) 인증수단을 변경한다.	●	●	●
	인증수단 보호	• **정보시스템의 보안 수준에 준하여 인증수단을 보호한다.**	●	●	
	암호화 되지 않은 인증수단 내장 금지	• 암호화되지 않은 인증수단이 응용프로그램 또는 스크립트 등에 내장되거나 기능키 등에 삽입되지 않아야 한다.	●	●	●
	캐시된 인증수단 재사용 차단	• 캐시된 인증수단이 세션 유효 시간이 만료된 이후에 재사용되는 것을 차단한다.	●	●	

(출처: 국가 망 보안체계 보안 가이드라인 부록)

© 2025 KICA inc. All rights reserved.

다중 인증 관련 통제 항목

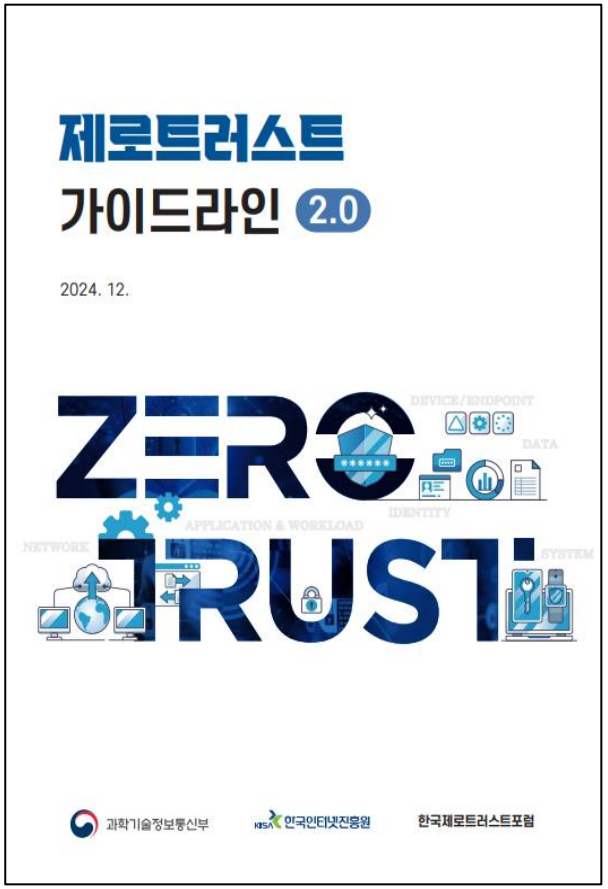
대항목	중항목	소항목	보안통제 설명	C	S	O
인증	인증정책	그룹 계정 사용자 인증	• 그룹 계정 인증 시 해당 그룹에 포함된 **사용자를 식별할 수 있는 인증수단을 적용**하여 사용자 인증을 추가로 수행한다.			
	로그인	로그인 실패에 따른 인증요소 추가	• 정의한 횟수 이상 연속적으로 로그인을 실패한 경우 **추가 인증수단(생체인증, OTP, ARS 등)**을 적용한다	●	●	
통제	원격접속	원격 명령 신뢰성 검증	• 명령을 수행하기 전에 적절한 **인증 체계(암호화된 인증서, 보안 토큰, 또는 사용자 인증)를 적용**하여 명령의 무결성과 출처를 검증한다.	●		
	무선망접속	업무용 무선망 인증 및 암호화	• **사용자 인증, 기기(단말 등) 인증** 및 무선 통신 구간 암호화를 적용한다.	●	●	
데이터	암호 키 관리	암호 키 설정	• 데이터 저장을 위해 암호 키를 생성하는 경우, 유형별 암호 키(대칭 키, 공개 키 등) 및 인증서를 **키 관리시스템(KMS)**을 활용할 수 있다. • 암호 키를 설정 시 C/S/O 보안등급별 암호화 강도, 암호 알고리즘(국산 암호, 국제 표준암호 등), 암호 키 유효기간 및 갱신, 암호 키와 서명용 키 분리, CRL(인증서 폐기 목록) 생성 주기 및 배포 경로 등을 설정 한다.	●	●	●
		전자서명 검증	• 데이터의 전송 및 저장 시 데이터 무결성 확인 및 암호화를 통한 데이터 보호를 위해 전자서명 생성 및 검증 키 관리, 표준화된 서명 검증 알고리즘과 서명용 인증서 관리, **전자서명 검증 기술을 적용**한다.	●	●	●

(출처: 국가 망 보안체계 보안 가이드라인 부록)

© 2025 KICA inc. All rights reserved.

제로트러스트(Zero Trust) 가이드라인 2.0 (2024.12)

"인증 후 접속 및 보호 자원에 접속할 때마다 인증 처리 (동적인증)"



Zero Trust 가이드라인 2.0 기존 원리

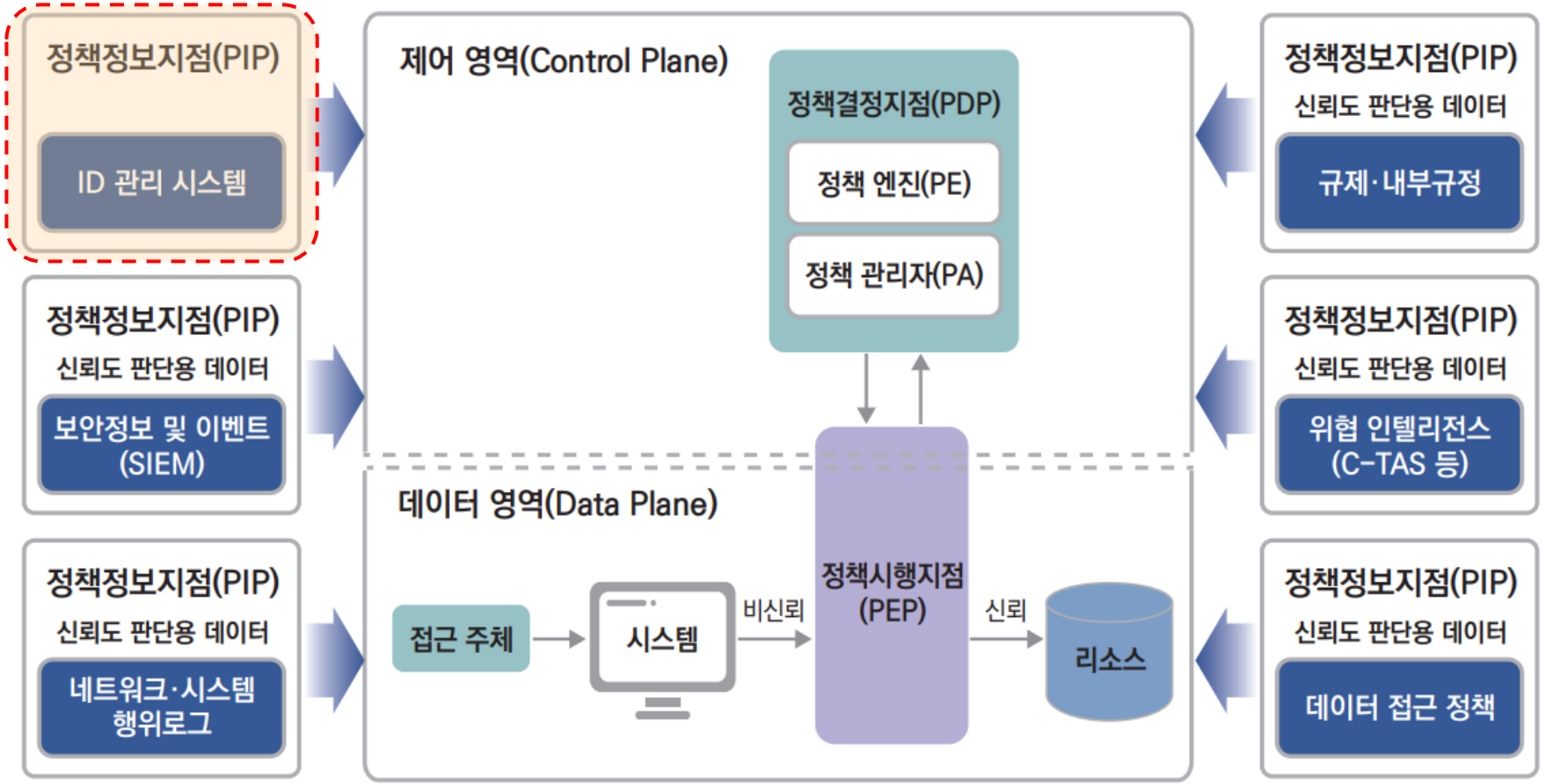
기본 원칙: 모든 종류의 접근에 대해 신뢰하지 않을 것 (명시적인 신뢰 확인 후 리소스 접근 허용)
일관되고 중앙집중적인 정책 관리 및 접근제어 결정, 실행 필요
사용자, 기기에 대한 관리 및 강력한 인증
리소스 분류 및 관리를 통한 세밀한 접근제어 (최소 권한 부여)
논리 경계 생성 및 세션 단위 접근 허용, 통신 보호 기술 적용
모든 상태에 대한 모니터링, 로그 및 이를 통한 신뢰성 지속적 검증, 제어

(출처: 제로트러스트_가이드라인_2.0)

© 2025 KICA inc. All rights reserved.

제로트러스트 아키텍처 보안 모델 및 논리 구성 요소

"ID 관리시스템은 기업 사용자의 계정 및 식별 기록 생성, 저장, 관리"



(출처: 제로트러스트_가이드라인_2.0)

© 2025 KICA inc. All rights reserved.

제로트러스트 성숙도 모델 정의

구분	1. 기존(Traditional)	2. 초기(Initial)	3. 향상(Advanced)	4. 최적화(Optimal)
	정적, 경계 기반, 수동	일부 자동화	자동화, 중앙집중적, 통합	자동화, 중앙집중적, 통합
정의	• 주요 구성 요소들이 수동으로 설정되며, 정적인 보안 정책으로 인해 유연하지 못하게 정책 시행 • 경계 기반 보안 위주의 보안 아키텍처 구성 • 수동으로 사고에 대응하며, 시스템에 대한 가시성이 제한적	• 일부 프로세스가 자동화되며, 핵심 요소별 연계가 일부 이루어짐 • 속성 할당과 생명주기 관리가 부분적으로 자동화되며, 내부 시스템에 대한 기본적인 모니터링 제공 • 프로비저닝 이후 최소 권한 변경에 대응 가능	• 자동화의 범위가 확장되고, 중앙 집중 제어가 강화되는 단계 • 중앙 집중식으로 통합된 가시성 제공 • 중앙 집중식 ID 관리를 통해 핵심 요소 간 상호작용에 기반한 정책 시행	• 자산 및 리소스에 대한 속성이 완전히 자동으로 할당되며, 동적인 정책이 적용되는 단계 • 자동화된 트리거에 기반한 동적 정책 생성 • 자산에 대해 동적 최소 권한 기반 접근 허용 • 구성요소 간 상호운용성을 위한 개방형 표준 준수 이행 및 강화

식별자·신원 성숙도 모델

구분	1. 기존(Traditional)	2. 초기(Initial)	3. 향상(Advanced)	4. 최적화(Optimal)
식별자 · 신원	• 온프레미스ID 사용 • 패스워드 혹은 다중인증 방식 • 수동접근 및 자격증명 관리	• 클라우드와 온프레미스 기반 ID 연계 • 다중인증 및 FIDO 기반인증 • 수동 및 정적 규칙 기반 위험 판단	• 컨텍스트 기반 ID 인증 • 일부 자동화된 및 동적 • 규칙을 이용한 위험도 평가 • 세션 기반 접근 지원	• 클라우드와 온프레미스 시스템 전반에 걸친 글로벌ID • AI 기반 위험도 결정 및 지속적 보호 • 자동화된 적시·최소 권한 접근 적용

© 2025 KICA inc. All rights reserved.

식별자·신원 핵심 요소에 대한 제로트러스트 성숙도 모델

기능	1. 기존(Traditional)	2. 초기(Initial)	3. 향상(Advanced)	4. 최적화(Optimal)
식별자 관리	• 온프레미스 ID 사용	• 클라우드와 온프레미스 시스템을 기반으로 ID 연계 • SSO 지원	• ID 통합 관리 시스템 구축	• 클라우드 및 온프레미스 환경 전반에 걸쳐 글로벌 ID 활용
인증	• 패스워드 혹은 다중인증 방식	• 다중인증 방식 기반 인증 • FIDO 기반 인증	• 컨텍스트 기반 ID 인증	• 접근권한 승인 때 뿐만 아니라, 지속적인 신원 검증
위험도 평가	• 위험에 대한 제한된 결정	• 수동 분석과 정적 규칙을 기반으로 식별자 위험도 판단	• 일부 자동화된 분석과 동적 규칙을 사용한 위험도 평가	• AI 기반 실시간 사용자 행동 분석을 통해 위험도 결정 및 지속적 보호
접근관리	• ID 기반, 수동으로 관리되는 그룹 및 역할을 사용하여 접근 관리 • 시스템 별 각기 다른 관리 기능	• 관리 기능 통합 • 최소 권한 원칙에 따라 접근 정책 검토	• 사용자 및 리소스에 맞는 조정된 권한을 사용하여 세션 기반 접근 지원	• 자동화를 통해 개별 요구사항에 맞는 적시·최소권한 접근 적용
가시성 및 분석	• 기본적이며 정적인 속성을 기반으로 사용자 활동에 대한 가시성 분류	• 기본 속성으로 사용자 활동에 대한 가시성 집계 후 분석 및 보고를 통한 수동적 개선	• 일부 사용자 및 엔티티에 대한 자동화된 분석 수행·가시성을 위한 수집 정보 확대	• 높은 정확도의 속성, 사용자 및 개체 행동 분석(UEBA) 솔루션을 통해 사용자 가시성 확보 및 중앙 집중화
자동화 및 통합	• ID와 자격 증명을 수동으로 관리·통합	• ID 연계 및 ID 저장소를 통한 관리 허용을 위한 기본 자동화 통합	• ID 연계 및 ID 저장소를 통한 관리 허용을 위한 기본 자동화 통합	• ID 생명 주기를 완벽히 통합하고, 동적 사용자 프로파일링, 동적 ID 및 그룹 멤버십, 적시·최소권한 접근제어 구현

(출처: 제로트러스트_가이드라인_2.0)

© 2025 KICA inc. All rights reserved.

다중인증 (MFA) 성숙도 정의

성숙도 수준	성숙도 수준에 따르는 정의
기준	• 기본적인 패스워드 방식과 함께 MFA 도입 및 설정 (예: SMS 코드, 이메일 확인) • MFA 지원 시스템 구축
초기	• 다양한 MFA 방법 구현으로 보안 수준 강화 (예: 인증 앱, 하드웨어 토큰) • MFA 정책 표준화 및 적용 • FIDO 기반 인증 기법 적용
향상	• 상황에 맞춘 맞춤형 MFA 기능 제공 및 새로운 인증 방법 지속 도입 • MFA 절차 자동화 및 사용자 경험 최적화 • 컨텍스트 기반 ID 인증 방식 채택
최적화	• 비정상적인 로그인 시도 실시간 탐지 및 대응 • MFA 기반 고급 보안 정책 설정 • 이상 행위 발생 시 자동 재인증 요구 등 지속적 신원 검증 수행

지속인증 성숙도 정의

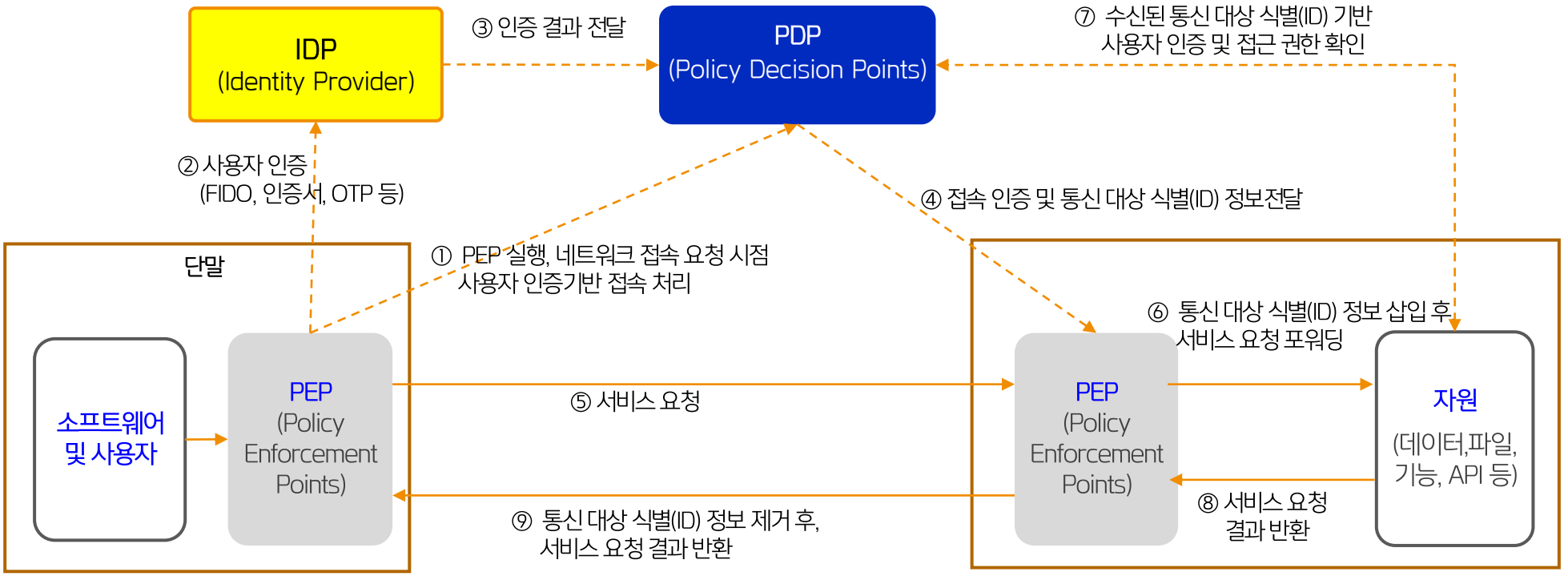
성숙도 수준	성숙도 수준에 따르는 정의
기준	• 세션 기반 인증 • 사용자 행동 및 접속 상태 모니터링
초기	• 모니터링을 통한 이상행위 탐지 및 추가 인증 요구 • 사용자 세션 중 추가 인증 요구 시스템 도입
향상	• 동적 인증 기술 적용으로 실시간 인증 상태 조정 • 지속 인증을 위한 고급 분석 및 경고 기능 통합
최적화	• 이상 행위 탐지 시 세션 종료 또는 재인증 요구 등 동적 자동 인증 상태 조정

(출처: 제로트러스트_가이드라인_2.0)

© 2025 KICA inc. All rights reserved.

Zero Trust 아키텍처 및 역할

"KICA 가 보유하고 있는 인증서, OTP, FIDO 등을 통한 IDP 서비스 제공 가능"

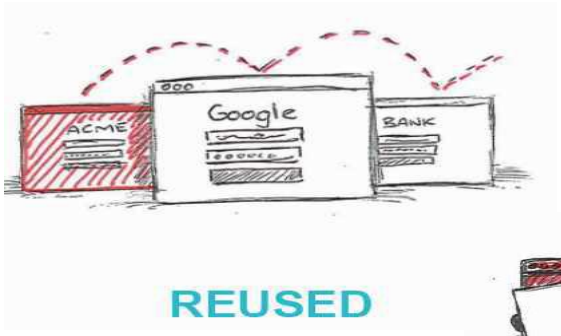


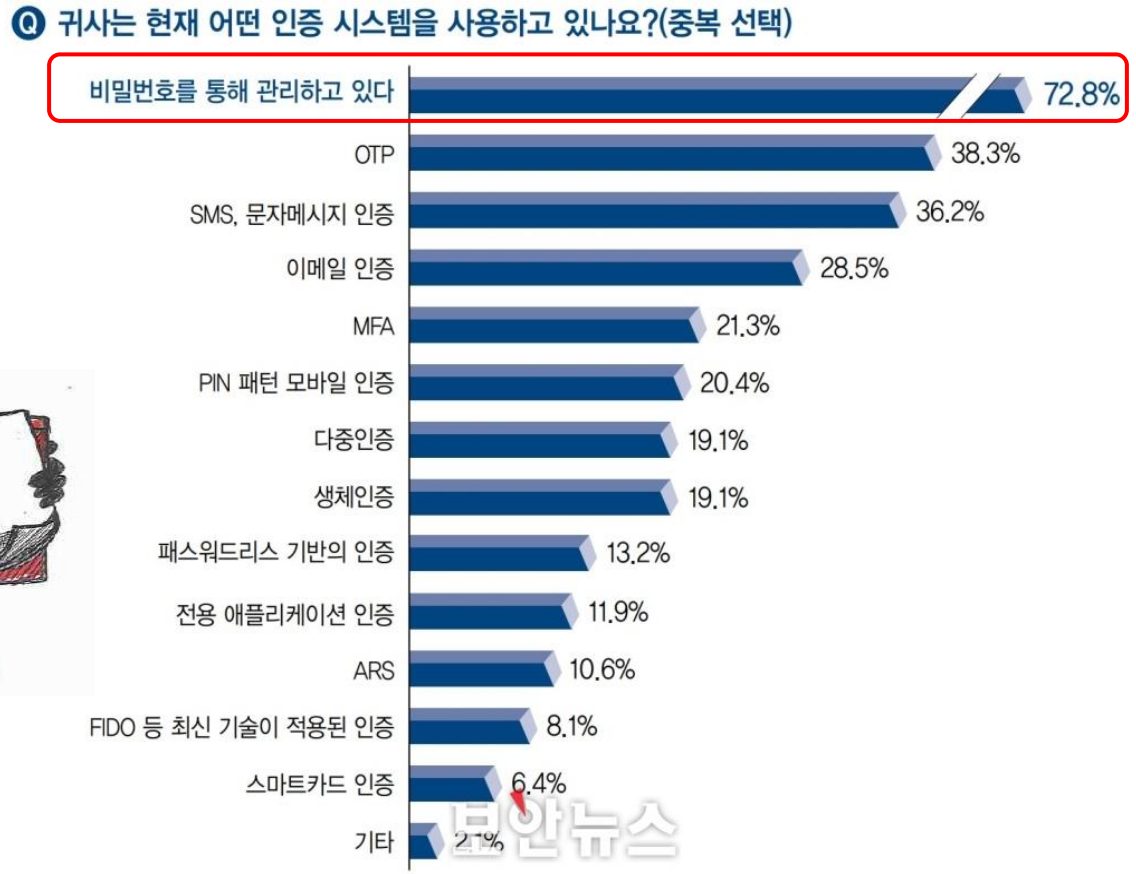
(출처: 제로트러스트_가이드라인_2.0)

© 2025 KICA inc. All rights reserved.

비밀번호(Password)의 문제점

"비밀번호는 해킹, 유출, 망각의 위험이 있고 가장 많은 72.8%가 사용 중임 "





(출처:보안뉴스)

© 2025 KICA inc. All rights reserved.

다중인증 방식(MFA) 종류

"다중인증 방식은 두가지 이상의 인증 방법을 조합하여 사용자 인증하는 방식 "

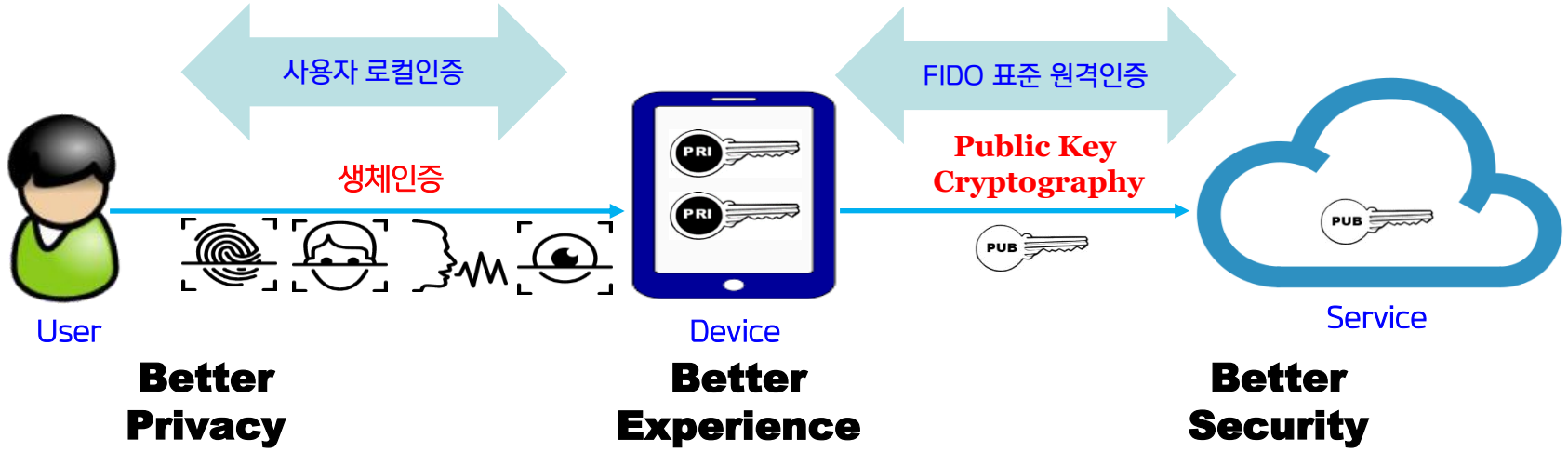
종류	특징	예시
지식 기반	인증자와 검증자만 아는 지식을 비교해 인증	아이디/패스워드, PIN, 보안패턴 등
소지 기반	사용자만 알고 있는 정보를 기반으로 한 인증	인증서, OTP, 휴대전화, 인증서, 신분증 등
생체 기반	인증자의 신체적인 특성을 이용해 인증	지문, 음성, 얼굴, 정맥, 홍채 인식 등

* MFA: Multi-Factor Authentication

© 2025 KICA inc. All rights reserved.

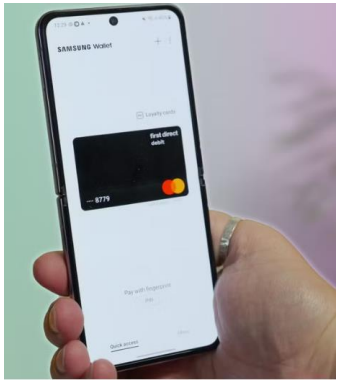
FIDO(Fast IDentity Online) 인증

"FIDO 인증은 비밀번호 대신 생체인증 기술을 활용하여 더 안전하고 편리한 인증 제공"



(출처:FIDO Alliance)

삼성페이 적용 사례



SAMSUNG pay

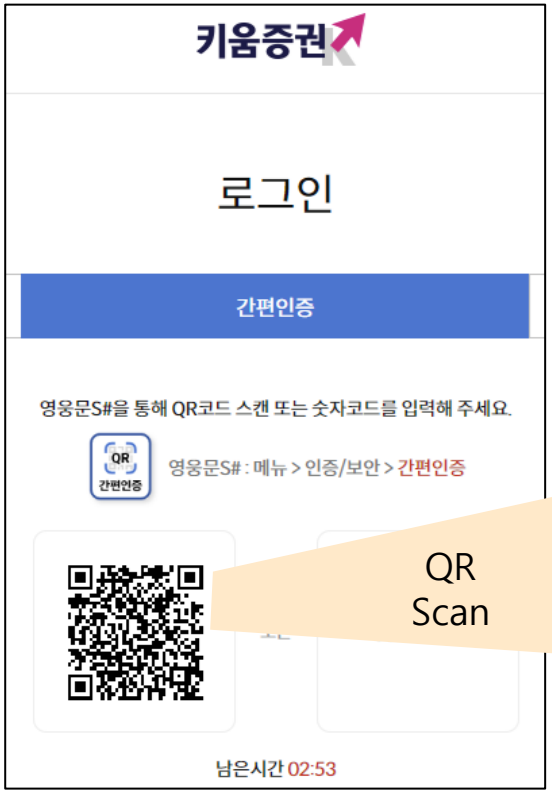
(출처:삼성전자)

© 2025 KICA inc. All rights reserved.

키움증권 QR 간편인증 사례

"PC에서 모바일 QR 간편인증으로 쉽고 편리하게 다양한 인증 수단으로 로그인 가능"

① [PC] 홈페이지 방문



[PC]

QR Scan

③ [스마트폰] QR 스캔하기

② [스마트폰] 영웅문앱 → 간편인증

④ [스마트폰] 생체인증 등 인증방법 선택

⑤ [스마트폰] 인증 완료

[SmartPhone]

(출처: 키움증권)

© 2025 KICA inc. All rights reserved.

A 공공기관 통합인증 구축 사례

"FIDO, QR 인증, OTP 등 다양한 인증방식을 서비스에 따라 선택적으로 적용 가능"

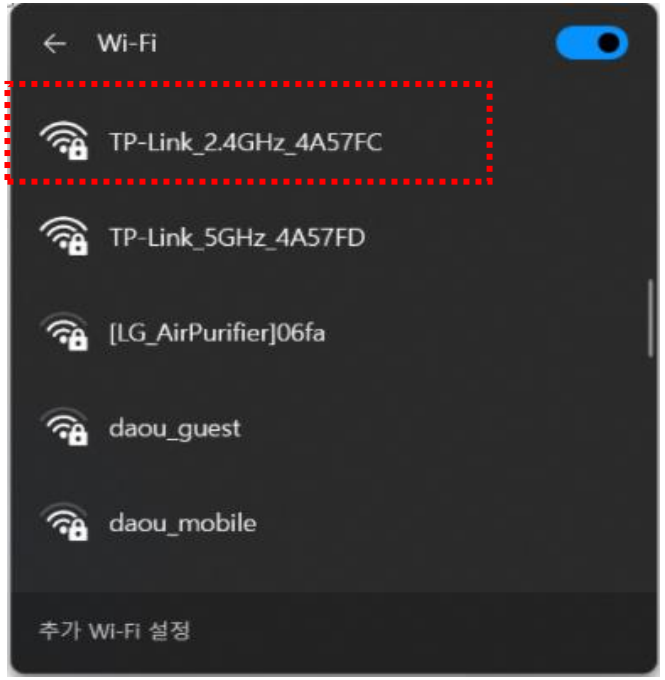
SSO | 웹메일 | SSL VPN | 업무용 메신저 | 화상 회의 | 홈페이지

© 2025 KICA inc. All rights reserved.

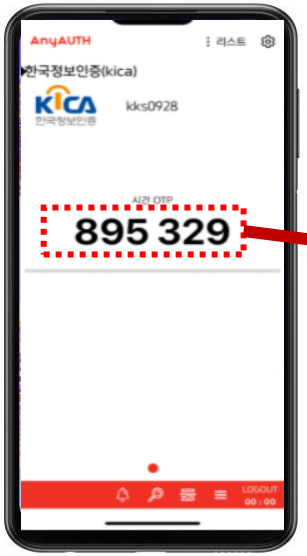
A 공공기관 무선 AP 장비 2차 인증 적용 사례

"업무용 무선 망 및 사내 업무시스템에 2차 인증솔루션(GrippinTower)을 적용하여 보안성 강화"

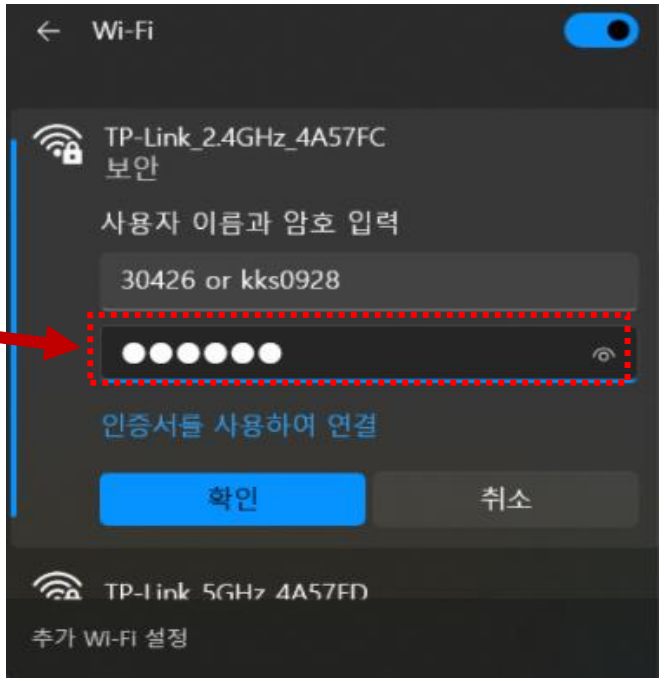
① [PC] 업무용 무선망 선택



② [스마트폰] OTP 번호 생성



③ [PC] OTP 번호 입력 및 무선망 접속



© 2025 KICA inc. All rights reserved.

B 기관 VDI(가상 데스크탑 인프라) 2차 인증 적용 사례

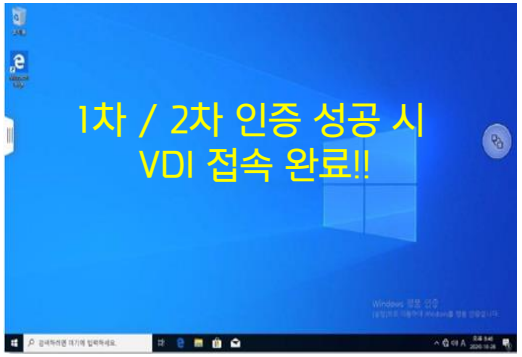
“ 원격으로 사내 업무망 접속시 2차 인증솔루션(GrippinTower)을 적용하여 보안성 강화”

① [PC] ID/PW 로그인 수행(1차 인증)

② [PC] 회사 PC 원격 접속 요청

④ [PC] OTP 번호 입력(2차 인증)

⑤ [PC] 회사 PC VDI 접속 완료



③ [스마트폰] OTP 번호 생성

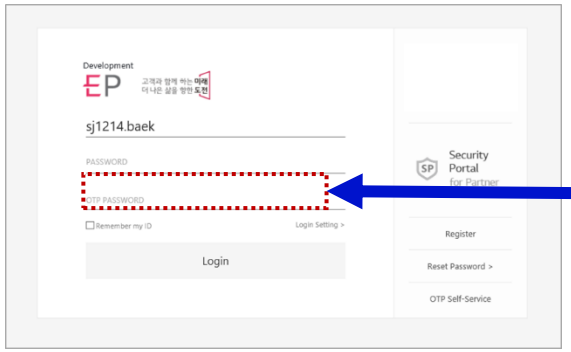
* VDI: Virtual Desktop Infrastructure

© 2025 KICA inc. All rights reserved.

C 기관 – SSO, 그룹웨어 2차 인증 적용 사례

"SSO나 그룹웨어로 사내 업무 시스템 접속시 2차 인증솔루션(OTP/FIDO)을 적용하여 보안성 강화"

① [PC] ID/PW 로그인 수행(1차 인증)



② [스마트폰] OTP 번호 생성 (2차 인증)

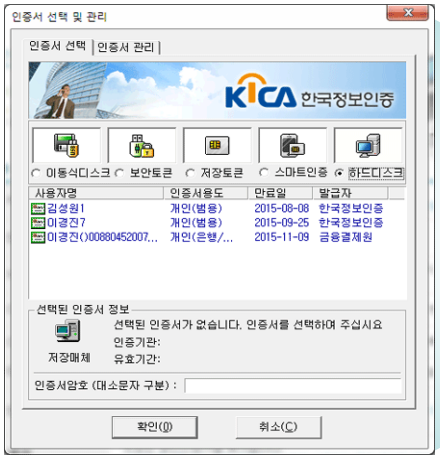
FIDO 인증

* SSO: Single Sign On

© 2025 KICA inc. All rights reserved.

본인확인서비스 제공 현황

"공인인증기관은 공동 인증서 기반 본인확인 서비스(UCPID)를 제공"



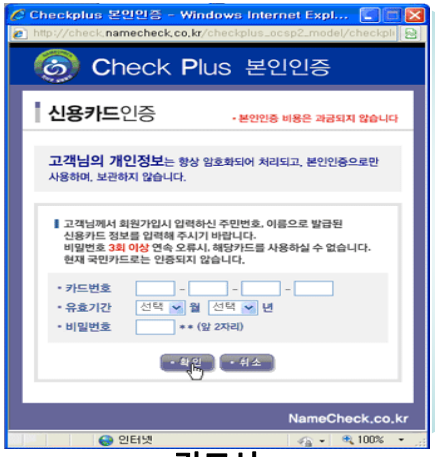
공인인증기관

인증서
암호

- 이름
- 전화번호
- 생년월일
- 성별
- 통신사
- 내국인/외국인

이동통신사업자

본인확인서비스



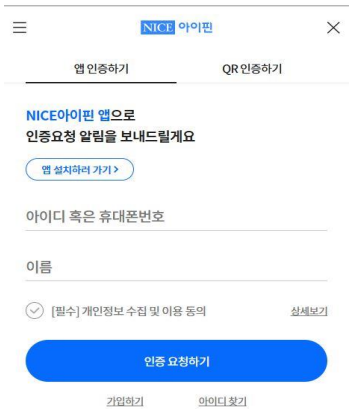
카드사

- 신용카드 번호
- 유효기간
- 비밀번호(2자리)

신용카드

아이핀

- 아이디
- 휴대폰번호
- 비밀번호



아이핀

* UCPID: Use of accredited Certificate for Personal IDentification)

© 2025 KICA inc. All rights reserved.

비대면 공동인증서 (개인사업자) 발급

“개인사업자 공동인증서를 비대면으로 쉽고 편리하게 발급 가능”

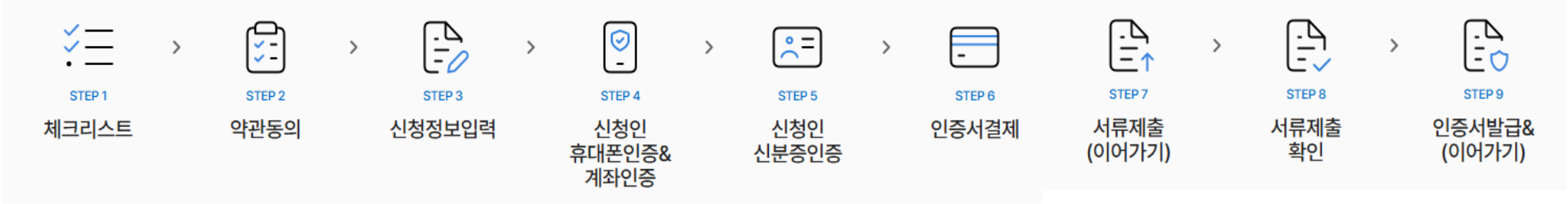
대면 개인 공동인증서 발급 절차

공동인증서 신청서 작성 및 인쇄 → 은행 등 창구 방문 → 공동인증서 신청서 제출 → 신분증 제출 (본인확인) → 인증서 발급 인가

실물 신분증 촬영 절차 대체

비대면 개인사업자 공동인증서 발급 절차 (www.signgate.com)

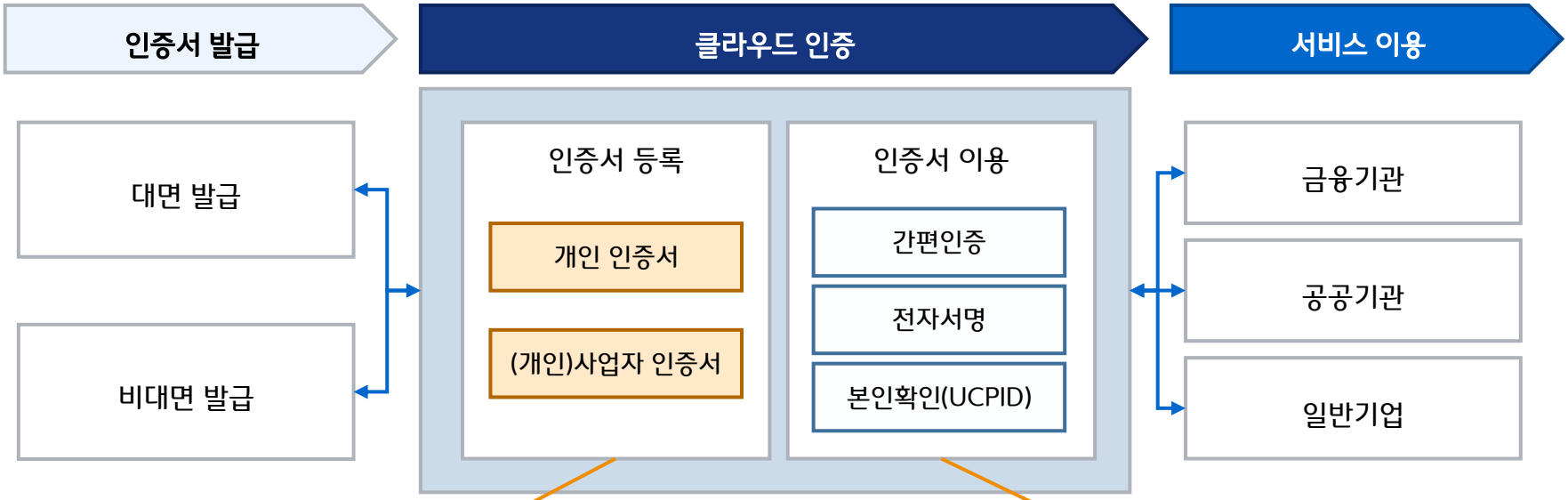
공동인증서 신청서 작성 → 대표자 휴대폰 본인확인 → 계좌 점유 인증 → 신분증 촬영 및 진위 확인 → 사업자등록증명원 전자지갑 제출 → 인증서 발급

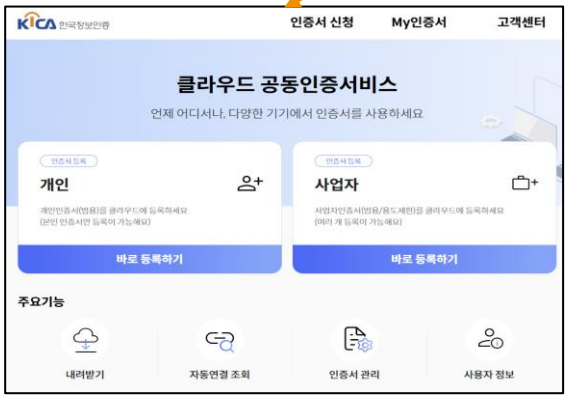


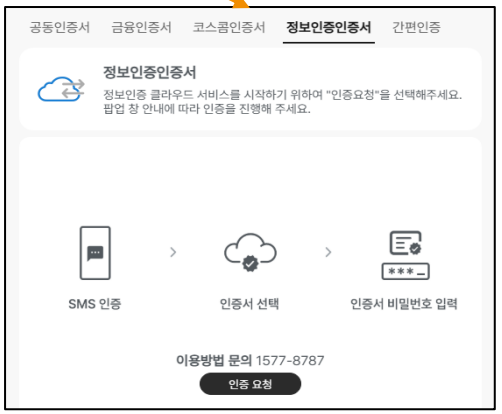
© 2025 KICA inc. All rights reserved.

클라우드 공동인증서비스 구성

“클라우드 공동인증서비스 등록을 통해 다양한 서비스에서 이용 가능”







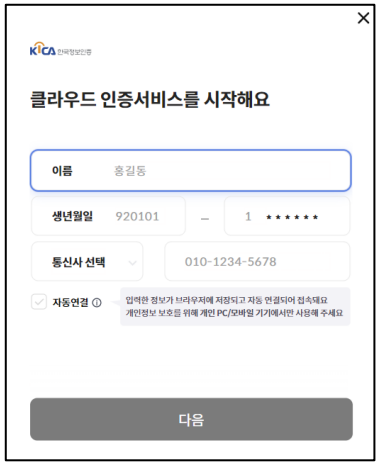
© 2025 KICA inc. All rights reserved.

클라우드 공동인증서비스 발급 절차

① 인증서 선택

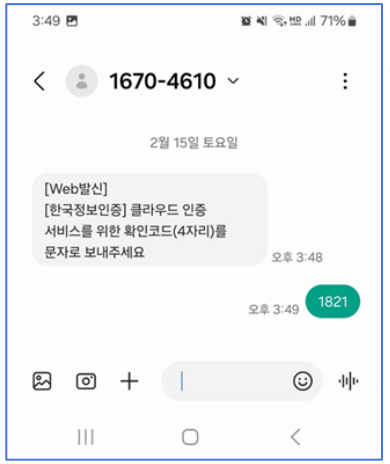
② 이용약관 동의

③ 사용자 정보 입력

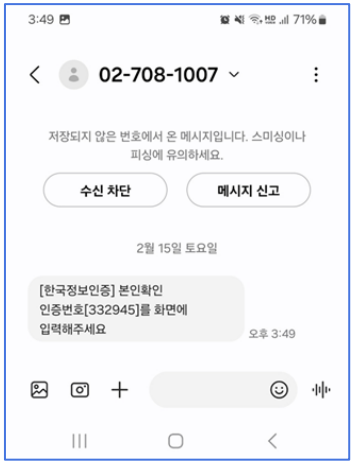


④ MO 인증

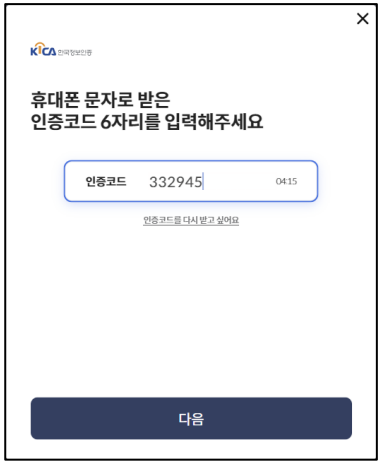
⑤ MO 인증: 입력



⑥ 휴대폰 본인확인 문자



⑦ 휴대폰 본인확인 입력



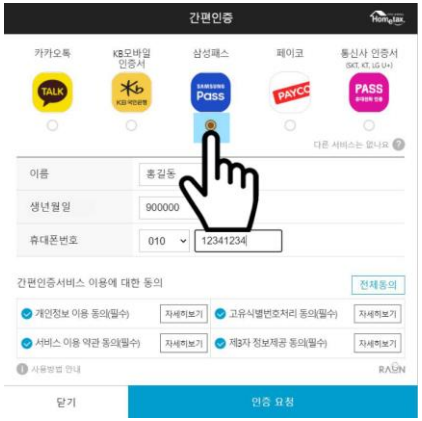
⑧ 인증서 등록 완료

© 2025 KICA inc. All rights reserved.

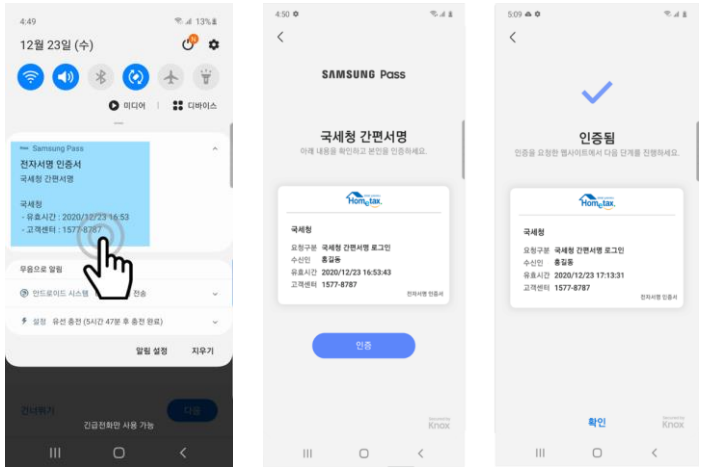
삼성 PASS : 공공기관 간편인증 로그인 사례

“삼성 PASS 인증서로 국세청, 경찰청, 보건복지부 등 공공기관에 로그인 가능”

① [PC] 간편인증 선택 및 정보 입력



② [스마트폰] 삼성패스 인증



③ [PC] 간편인증 인증 완료

(출처: 삼성전자)

© 2025 KICA inc. All rights reserved.

모바일 신분증 개요

“행안부 주도, 조폐공사가 관할하는 온 • 오프라인 통합형 신분증”

2021년

모바일 공무원증

2022년~2024년

모바일 신분증

모바일 운전면허증

모바일 국가보훈등록증

2025년 ~

모바일 신분증

모바일 주민등록증 (‘25년)
모바일 장애인 등록증 (‘26년)
모바일 청소년증 (‘27년)

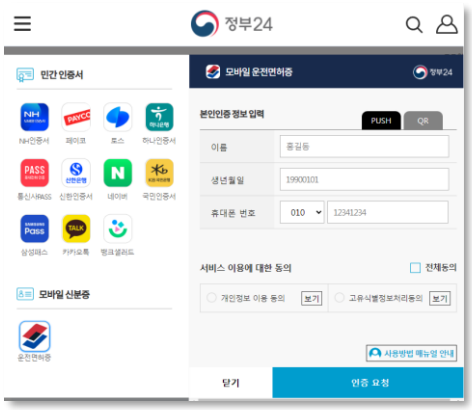
* 블록체인 기반의 DID(Decentralized Identity)기술 적용

© 2025 KICA inc. All rights reserved.

모바일 신분증 활용 분야

"간편인증, 신원확인, 자격확인 등에서 활용 가능"

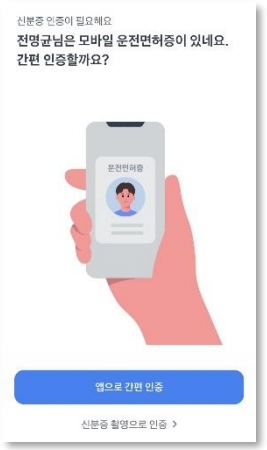
간편인증



신원확인,로그인,회원관리에 이용

(사례) 정부24 간편인증 로그인에 이용

신원확인



온/오프라인에서 신원에 대한 확인

(사례) 은행 비대면 계좌 개설 시 이용

자격 및 성인 확인

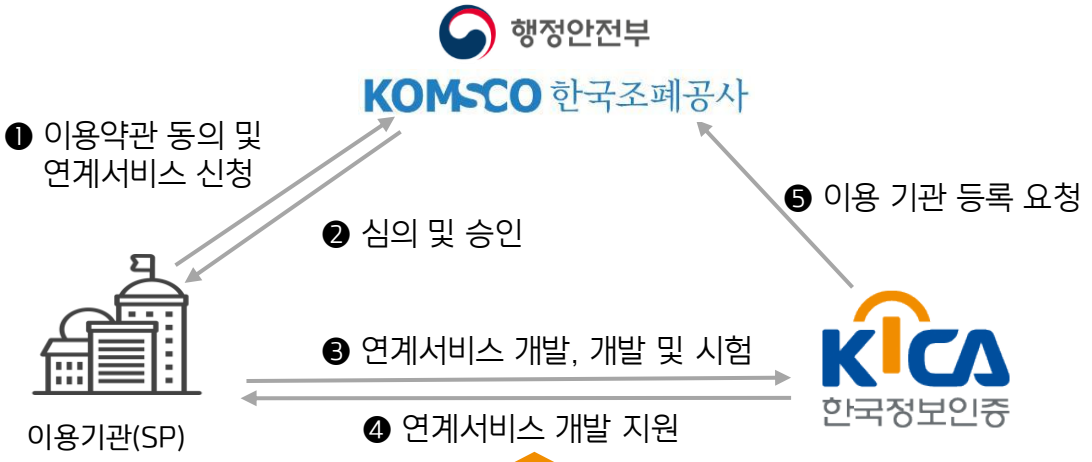
운전면허 자격 또는 성인여부 확인

(사례) 렌터카 운전면허 자격 확인 시 이용

© 2025 KICA inc. All rights reserved.

모바일 신분증 구축 방안

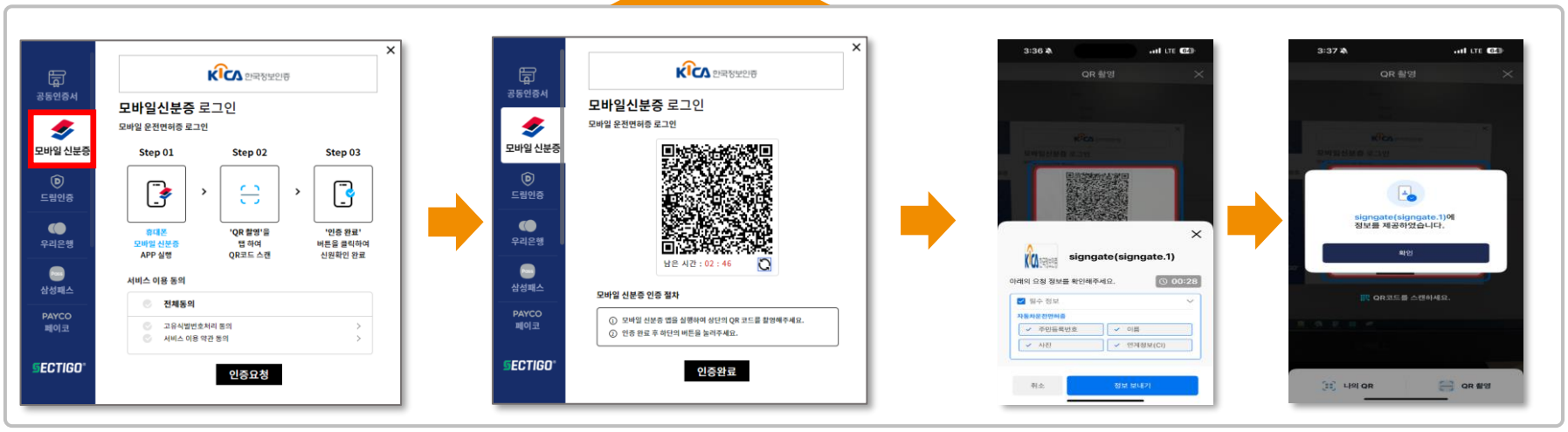
"KICA는 리드노드 공식 수탁기관으로 모바일 신분증 연계 서비스 개발 지원 가능"



리드노드 공식 수탁기관

R

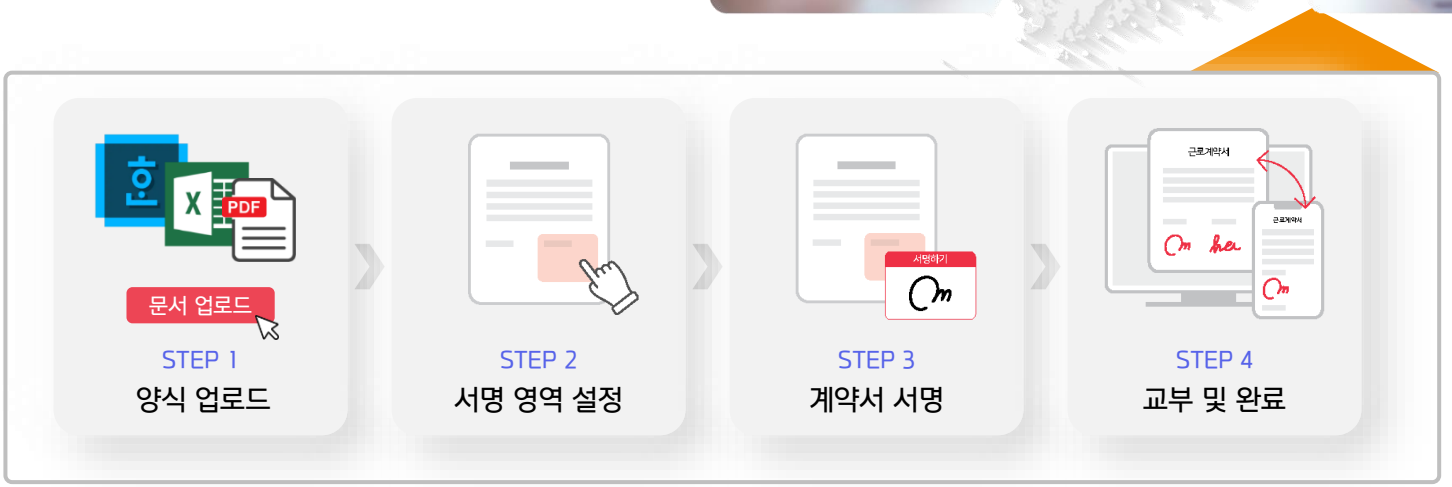
Node



© 2025 KICA inc. All rights reserved.

싸인오케이 서비스

"싸인오케이 서비스는 계약의 모든 과정을 하나의 서비스로 처리할 수 있는 전자서식 서비스"



© 2025 KICA inc. All rights reserved.

싸인오케이로 업무 효율을 높인 공공기관 사례

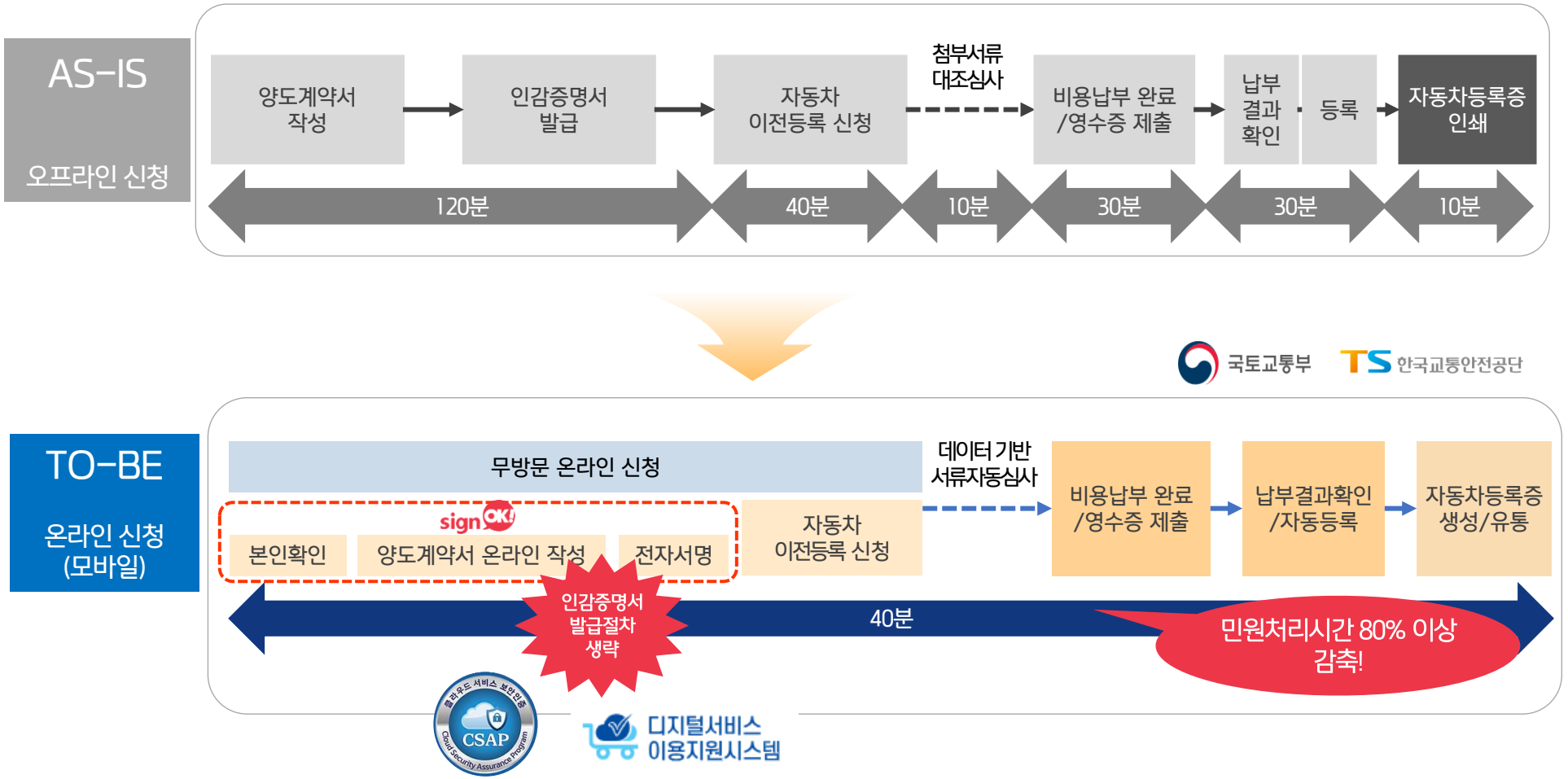
"근로계약, 신청서, 민원서류, 동의서 등 서면으로 받았던 서명을 전자화하여 paperless 실현"

기관 명	싸인오케이 활용 문서
한국교통안전공단	자동차 등록 신청서
도로교통공단	고용보험계약, 개인정보 수집 이용 동의
국민건강보험공단	협력업체 계약(제약 등)
대한법률구조공단	법률구조신청서, 소송위임장, 개인정보수집이용동의 등
서울신용보증재단	분할상환 약정서, 변제 합의서 등
서울시복지재단	청년통장 약정서
한국농수산식품유통공사	해외진출컨설팅, 약정서 등
한국인삼공사	중도금 신청서
대한무역투자진흥공사	근로계약 (정규, 계약)
경기평택항만공사	서류제출 확인서, 신청서 등
세종시시설관리공단	근로계약서
중소기업은행	상품등록신청서

© 2025 KICA inc. All rights reserved.

싸인오케이 SaaS 적용 사례: 자동차 온라인 대리등록신청 표준서비스

"전자서식 서비스(SaaS) 적용한 온라인 신청을 통한 민원처리시간 80%이상 단축 가능"



© 2025 KICA inc. All rights reserved.

IoT 기기 인증

"IP Phone, 전기차 충전기, 스마트홈, 자율주행차 등 IoT 기기에 기기 인증 적용을 통한 신뢰성 향상"

C-ITS (V2X certificate)

Smart Home (Matter Certificate)

Smart Home (Device Certificate)

EV Charging (OCPP certificate)

IP Phone of public Sector (Device Certificate)

IP Phone

Charging Station

VPN

VPN Server

VPN Client

Wall Pad

Home Appliances

Connected Car

RSU

CCTV

Center

Motion detector

RWIS

VMS

Labacon

Tripod

- EV: Electric Vehicle
- V2X: Vehicle to Everything
- RSU: Road-Side Unit
- C-ITS: Cooperative-Intelligent Transport Systems
- RWIS: Road Weather Information System
- VMS: Variable Message Sign

© 2025 KICA inc. All rights reserved.

무자각 인증

"무자각 인증은 사용자의 패턴, 혹은 환경 등 행동양식을 분석해 신원 인증의 방법"

- 무자각 인증의 기본 개념: 유저의 행동 패턴(키보드를 치는 방식, 키 입력 간의 시간 간격, 키를 누르고 있는 시간, 모바일 화면을 넘기는 방법, 마우스를 움직이는 방법, 등) 혹은 환경 등을 분석 및 저장해서 정기적으로 명시적인 인증 없이 지속적으로 사용자의 신원을 인증하는 방식

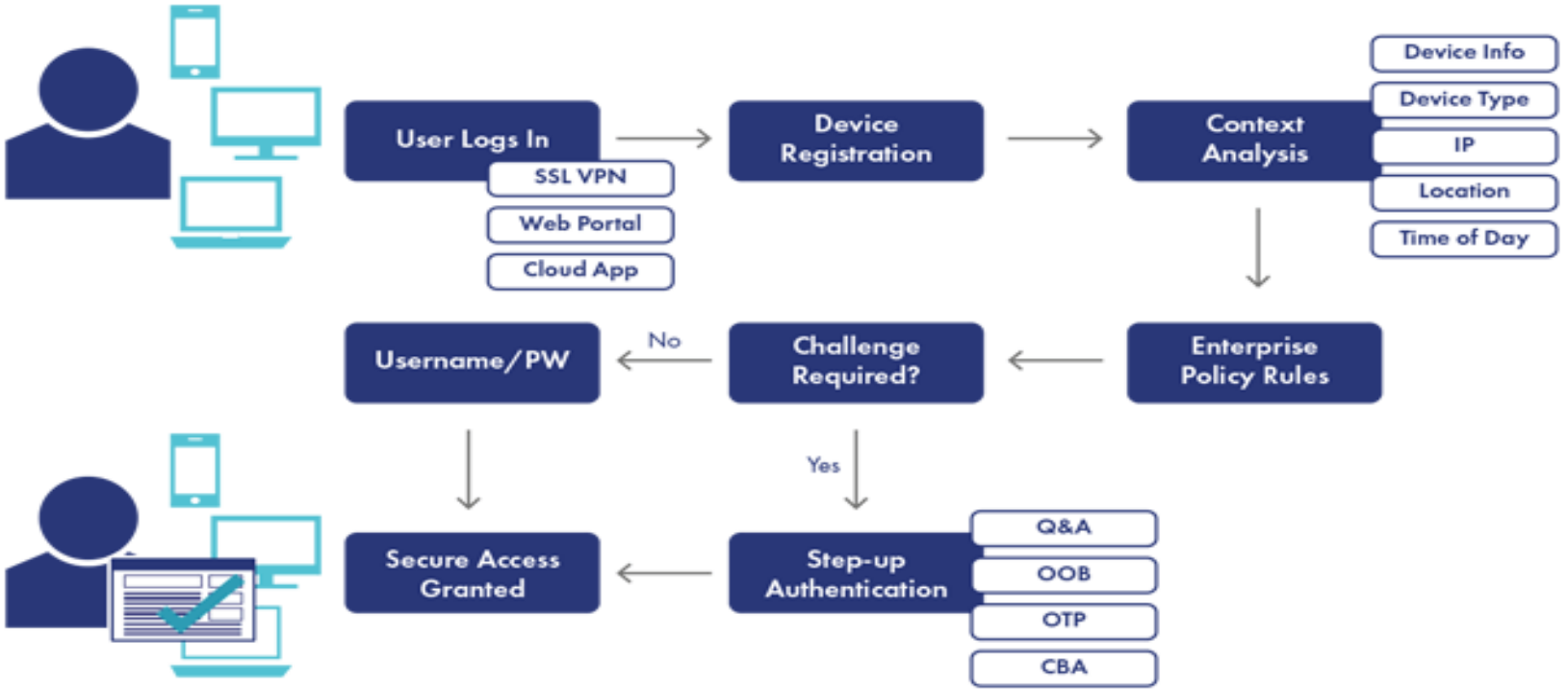
구분	설명
얼굴	• 안면 특징(각 부분의 위치, 크기, 모양, 피부나 머리카락의 질감, 주름, 패턴, 반점) 등을 사용해서 구분
음성	• 음성 기관에 차이와 말하기 방식의 차이로 오는 다른 음성 서명을 이용
걸음걸이	• 골격, 근육, 장애 여부 등의 신체적 특징으로 인해 개개인마다 다른 걸음걸이를 이용
키스트로크 다이나믹스	• 키보드 키를 입력하는 방식, 리듬, 간격 등 타이핑 패턴을 기반으로 식별하는 인증 방식
마우스 다이나믹스	• 마우스를 움직이는 방식(마우스 이동, 클릭 등의 각도, 속도, 이동거리 등의 특성)으로 식별하는 방법
터치 다이나믹스	• 사용자가 터치스크린 사용 시 손가락으로 스와이프 하는 방식들로 식별하는 방식
문체	• 사용자의 단어 사용, 문법 등 언어적인 특성들로 사용자를 식별하는 인증방식
위치	• 사용자가 생활 패턴에서 얻을 수 있는 장소들로 사용자를 식별하는 방식
앱 사용습관	• 사용자의 동작, 컨트롤 유형, 핸드폰 사용 시간 등의 특징적 요소들로 식별하는 방식
모바일 장치 사용	• 모바일 장치(스마트폰, 웨어러블)와 상호 작용하는 방식에 따라 사람을 식별하는 방식

(출처: IDEATEC)

© 2025 KICA inc. All rights reserved.

컨텍스트 기반 ID 인증

- 사용자가 애플리케이션에 로그인할 때 평가하는 여러 추가 정보를 기반으로 하는 인증 방법
- 가장 일반적인 유형의 컨텍스트 정보에는 사용자의 위치, 시간, IP 주소, 장치 유형, URL과 애플리케이션의 평판 정보가 포함

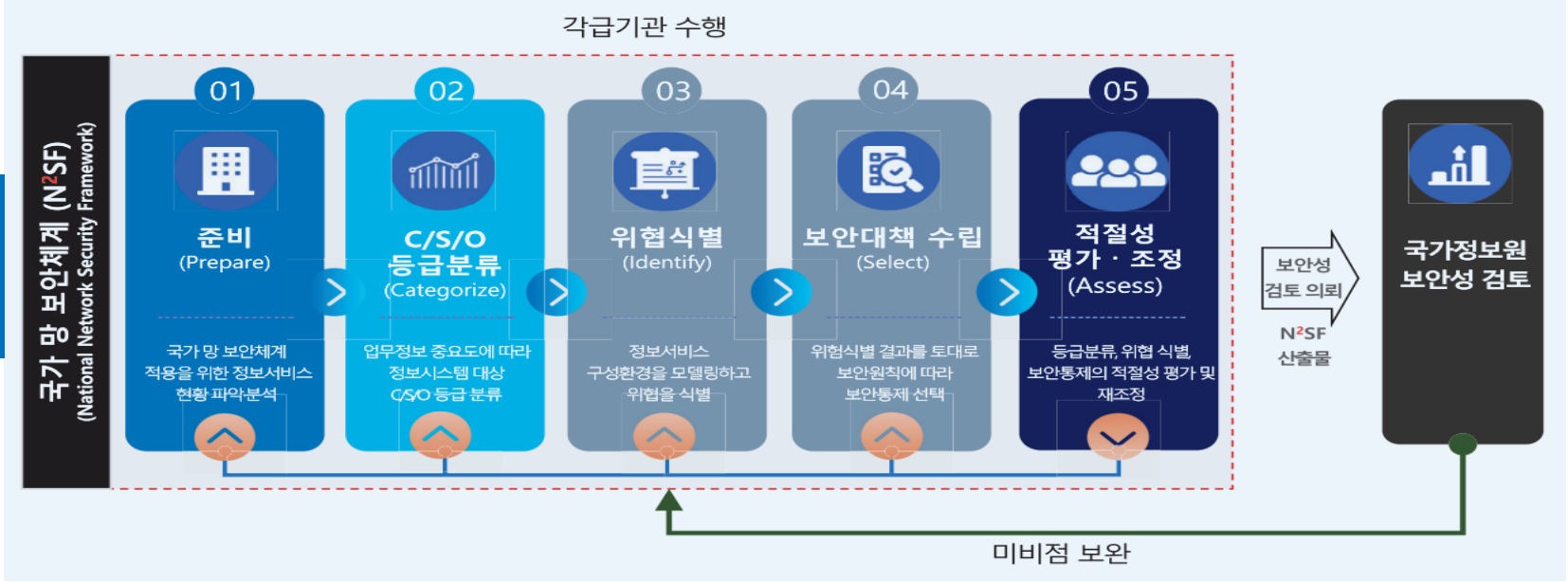


(출처: THALES)

© 2025 KICA inc. All rights reserved.

“보안 대책에 맞는 최적의 인증 방안 적용으로 안전한 국가망 보안 체계 구축”

국가 망 보안체계 적용 절차



(출처: 국가 망 보안체계 보안 가이드라인)

보안 등급에 따라 다양한 사용자 인증 방안 적용

© 2025 KICA inc. All rights reserved.

KICA 한국정보인증

감사합니다.

상담: 3번/4번 전시부스(한국정보인증)

© 2025 KICA inc. All rights reserved.