

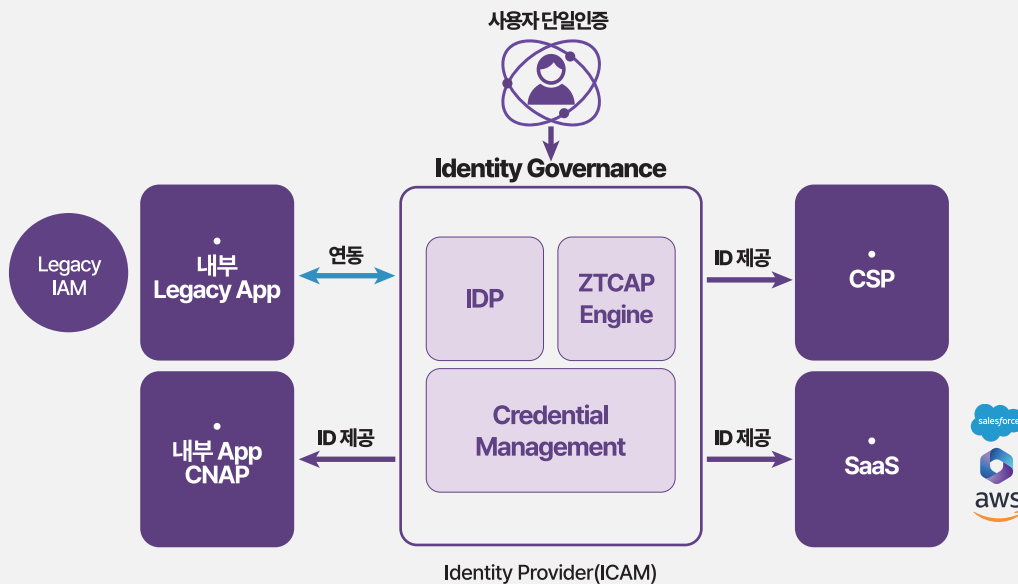
제로 트러스트 기반 클라우드 환경의 통합 계정관리 서비스

물리적 경계가 없는 클라우드 IT 환경에서는 언제 어디서나 인증만 통과되면 계정 사용이 가능해짐에 따라, 사용자 인증이 중요한 이슈로 대두됩니다.

SHIELD ID는 제로 트러스트 기반의 사용자 신원 및 접근 권한 관리를 하고 보안을 유지하는 기능을 제공하며, 웹 어플리케이션에 대한 SSO(Single Sign-On) 및 MFA(Multi-factor Authentication) 등의 인증 서비스를 제공합니다.

조건과 상황에 따라 사용자의 신원확인을 지속 검증하고 결과에 따라 사용과 접근 권한을 달리해 인증, 신원 확인 중심의 제로 트러스트 생태계를 구성합니다.

국내 최초 ICAM, IDP를 동시 제공하는 제로 트러스트 기반 클라우드 환경의 통합 계정관리 서비스입니다.



*IDP=Identity Provider

*ZTCAP(Zero Trust Conditional Adaptive Policy)=모든 접근 행위에 대한 인증과 권한을 제로 트러스트 원칙에 따라 지속적으로 검증하는 정책

제로 트러스트 기반 자격 증명 관리 및 금융규제 샌드박스 등 컴플라이언스 준수

금융규제 샌드박스 부가조건에 의해
'인증관리는 SaaS 이용 불가'인 고객환경에 맞춘
설치형 서비스 지원 및 제로 트러스트 가이드 라인 등
컴플라이언스 준수

아이디 페더레이션(Identity Federation) 지원

사용자가 Windows PC 로그인을 수행하면, 클라우드 서비스까지
접근할 수 있도록 *IDP를 통한 아이디 페더레이션으로 표준 규약
기반의 Microsoft 365 등 다양한 서비스 연동 및 보안성 향상



국제 표준 프로토콜 지원(OAuth2, SAML 등)

인터넷 사용자가 한 서비스의 자격 증명을 사용하여
다른 서비스에 로그인할 수 있게 해주는 'OAuth2' 및
서로 다른 도메인간의 인증, 권한 부여를 할 수 있게 해주는 'SAML'
지원으로 국제 표준 프로토콜 지원

다양한 고객 환경에 맞춘 사용자 프로비저닝

프로비저닝을 통해 사용자의 계정을 연결된 시스템과 연동하고,
새로운 사용자가 등록되면 각 연동된 시스템에 계정을 자동으로
생성, 단순히 사용자 계정뿐만 아니라, 시스템 접속에 필요한 접근 권한
까지도 계정 생성과 동시에 자동으로 배포 지원

SHIELD ID 주요 특징

01 국내 최초 ICAM & IDP 동시 제공

기존 *IAM에서 사용자 인증(Credential)관리를 개선한 *ICAM 및 클라우드 환경의 인증 통합 관리 *IDP 를 동시에 제공하는 국내 최초의 서비스

*IAM = Identity and Access Management

*ICAM = Identity Credential Access Management으로 사용자 인증(Credential)관리를 개선

*IDP = Identity Provider



02 *SSO & 제로 트러스트

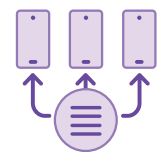
여러 클라우드 서비스를 한 번에 로그인으로 접근할 수 있는 *SSO 제공
표준 규약 기반의 페더레이션(Federation) 인증을 통한 다양한 서비스 연동 및 보안성 향상
및 기업 내부 설치형(On-Premise) 및 클라우드 서비스

*SSO(Single Sign-On) = 1회 사용자 인증으로 다수의 애플리케이션 및 웹사이트에 대한 사용자 로그인을 허용하는 인증 솔루션



03 사용자 프로비저닝

내부의 LDAP, AD, 인사DB 등과 클라우드의 Azure AD 등의 인사정보 소스를 통합 및 클라우드 서비스 가입 사용 시의 사용자 프로비저닝을 통한 계정 및 라이선스 관리 가능



04 컴플라이언스 대응

국내 금융규제 샌드박스의 클라우드 사용자 인증 서비스의 설치형만 사용 가능한 규제 조건을 준수 가능(설치형 제공) 및 과학기술정보통신부 제로 트러스트 가이드라인 준수

