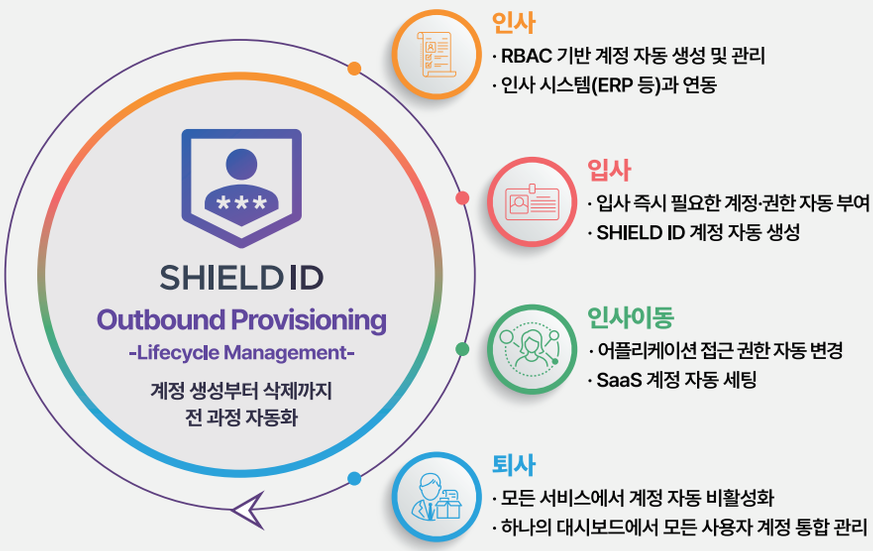
SHIELD ID

제로 트러스트 기반
클라우드 환경의 통합 계정관리 서비스

아무리 튼튼한 금고라도 비밀번호만 알고 있으면 쉽게 열 수 있는 것처럼
강력한 보안을 적용한 시스템도 권한 사용자 계정이 있다면 쉽게 들어갈 수 있습니다.

SHIELD ID는 다양한 SaaS 환경에서 발생할 수 있는 계정정보에 대한 관리나 이슈를
편리하면서도 강력한 인증과 인가 정책으로 안전하게 보호합니다.



*RBAC 기반의 아웃바운드 프로비저닝(Outbound Provisioning)

시스템 내의 역할(Role)을 기준으로 사용자의 권한을 부여하고,
입사-인사이동-퇴사 등 라이프사이클 이벤트에 따라
IT 리소스 접근 권한을 자동으로 관리(Lifecycle Management) 합니다.

*RBAC = Role Based Access Control

제로 트러스트 기반의 자격 증명 관리

제로 트러스트(*ZTCAP) 기반의 자격 증명 체계를 적용하여,
사용자 행위 및 디바이스 상태에 따라 유연한 인증 정책을 지원하고,
금융권과 같이 SaaS 환경이 제한된 고객에게는 설치형 서비스로
컴플라이언스를 준수합니다.

*ZTCAP = Zero Trust Conditional Access Policy

SHIELD ID

ID 패더레이션 (Identity Federation) 지원

Window PC 로그인만으로 Microsoft 365 등 주요 SaaS 서비스에
안전하게 접근할 수 있도록, IdP 기반의 아이디 페더레이션을 지원하며
표준 규약 기반의 통합 인증으로 보안성과 편의성을 향상시킵니다.

국제 표준 프로토콜 지원 (OAuth2, SAML 등)

사용자가 한 서비스에서 인증한 자격 정보를 활용해
다른 서비스에 로그인할 수 있도록 지원하는 OAuth2와
서로 다른 도메인 간에 인증 정보를 안전하게 주고 받을 수 있도록 하는
SAML 등 다양한 국제 표준 프로토콜을 지원합니다.

SHIELD ID 주요 특징

01 *RBAC 기반 아웃바운드 프로비저닝

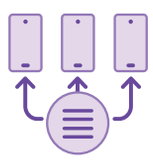
사내의 LDAP, AD, 인사 DB 등과 연계하여 역할(Role)에 따른 접근 제어(RBAC)를 통해 클라우드 서비스 이용 시사용자 계정, 권한, 라이선스를 자동으로 프로비저닝 및 관리합니다. 또한, 사용자 정보 변경 시 외부 SaaS에 자동 반영되어 계정 수명주기를 효율적으로 관리할 수 있습니다.

*RBAC=Role Based Access Control

02 ICAM & IDP 동시 제공

기존 *IAM에서 사용자 인증(Creditional) 관리를 개선한 *ICAM 및 클라우드 환경에서 통합 계정 관리를 실현하는 *IdP를 함께 제공합니다.

*IAM = Identity and Access Management
*ICAM = Identity Credential Access Management로 사용자 인증관리를 개선
*IdP = Identity Provider



03 *SSO & 제로 트러스트

여러 클라우드 서비스를 한 번에 로그인으로 접근할 수 있는 *SSO를 제공하며, 표준 규약 기반의 페더레이션(Federation) 인증을 통한 다양한 서비스 연동 및 보안성이 향상되는 기업 내부 설치형(On-Premise) 클라우드 서비스 입니다.

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

04 컴플라이언스 대응

국내 금융규제 샌드박스 기준에 따라, 설치형 클라우드 사용자 인증 서비스만 사용 가능한 환경에서도 설치형 형태로 제공하여 규제 조건을 충족합니다.
또한, 과학기술정보통신부의 제로 트러스트 보안 가이드라인을 준수합니다.