



윈도우 통합인증과 이 기종 SSO 구현

NETS*Single Sign On v3.0



- 1 Authentication**
- 2 NETS*Single Sign On**
- 3 Demonstration**

01 Authentication

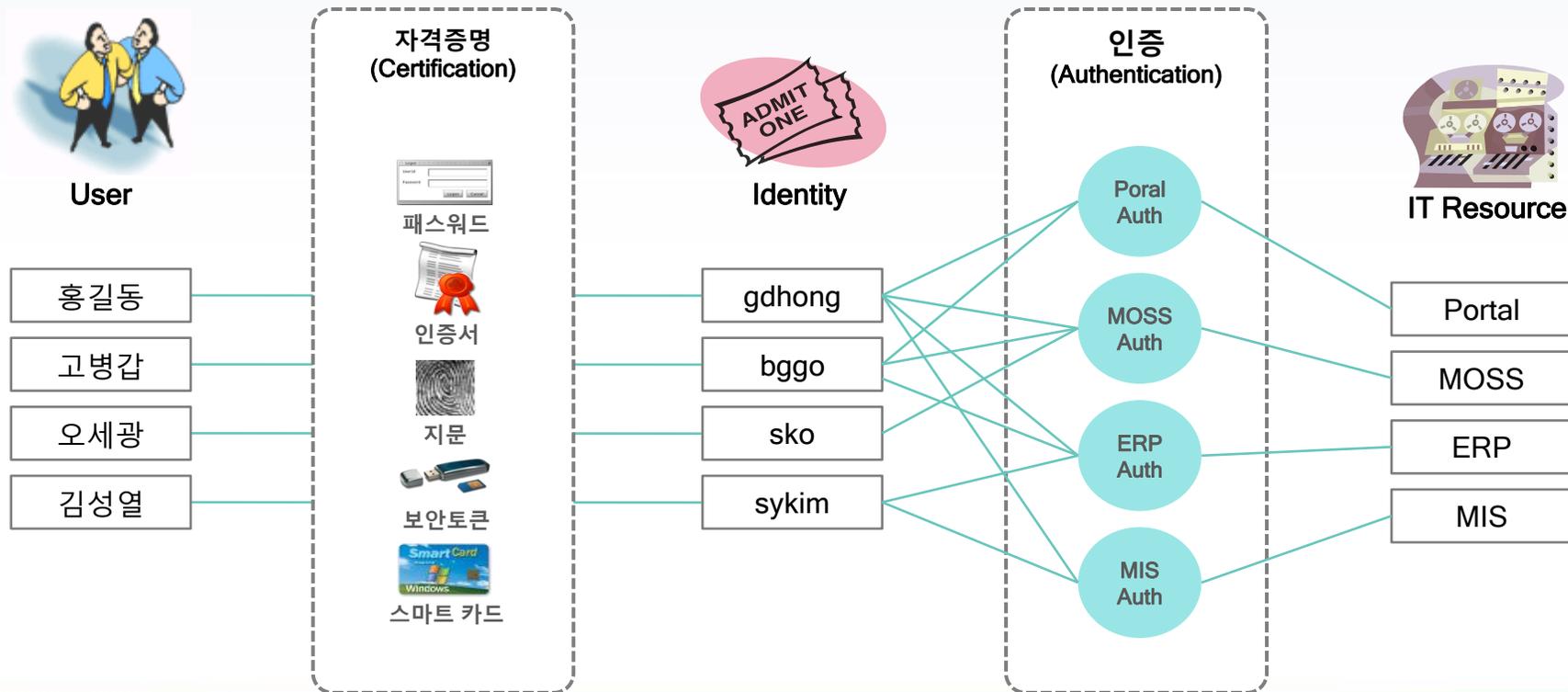
- 1) 개요
- 2) Microsoft의 인증
- 3) 기업의 인증
- 4) Issue

인증(Authentication)이란?

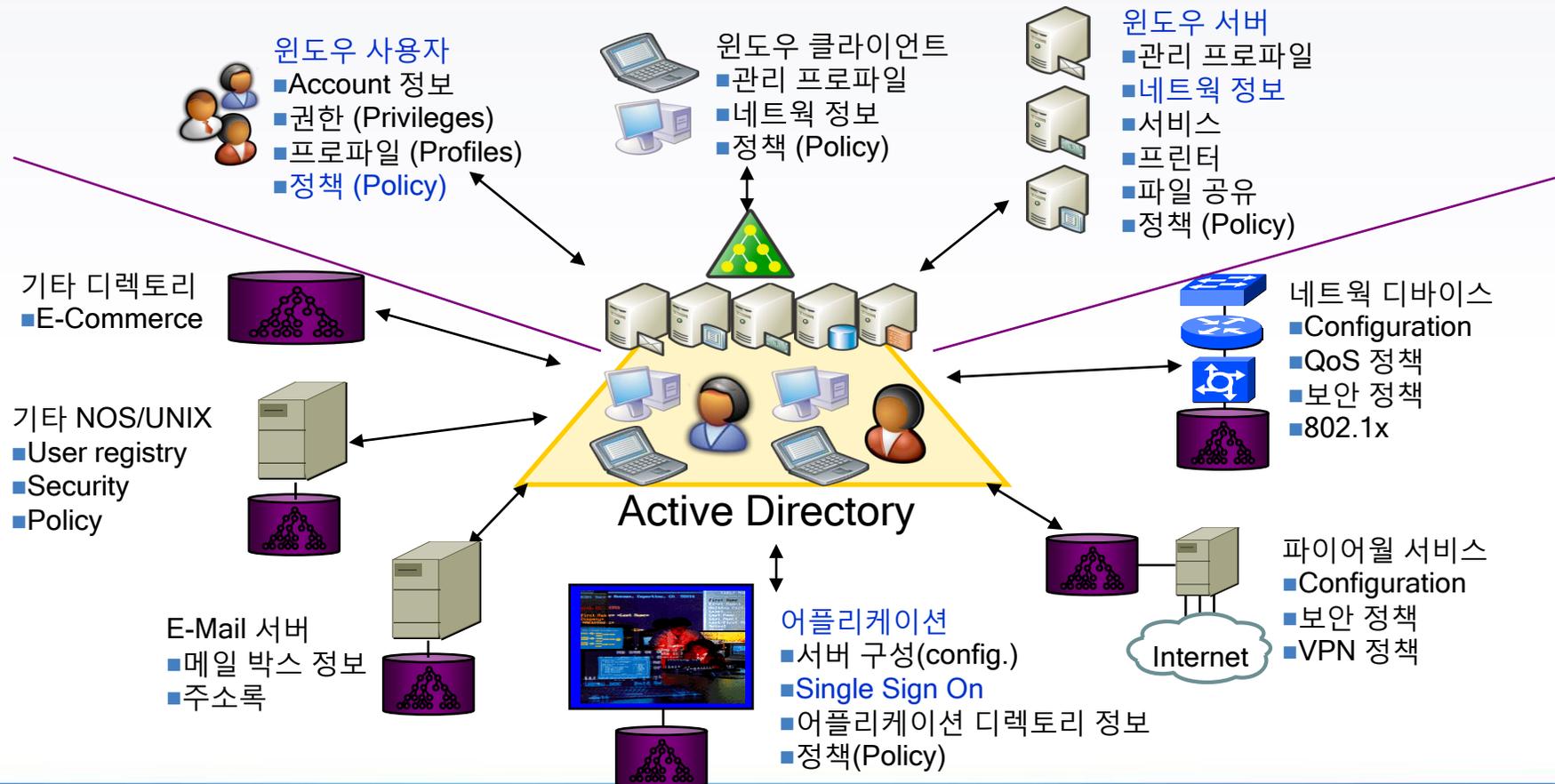
컴퓨터 보안에서 인증은 로그인 요청 등을 통해 통신 상에서 보내는 사람의 디지털 정체성을 확인하는 시도의 과정이다.

암호>Password)란?

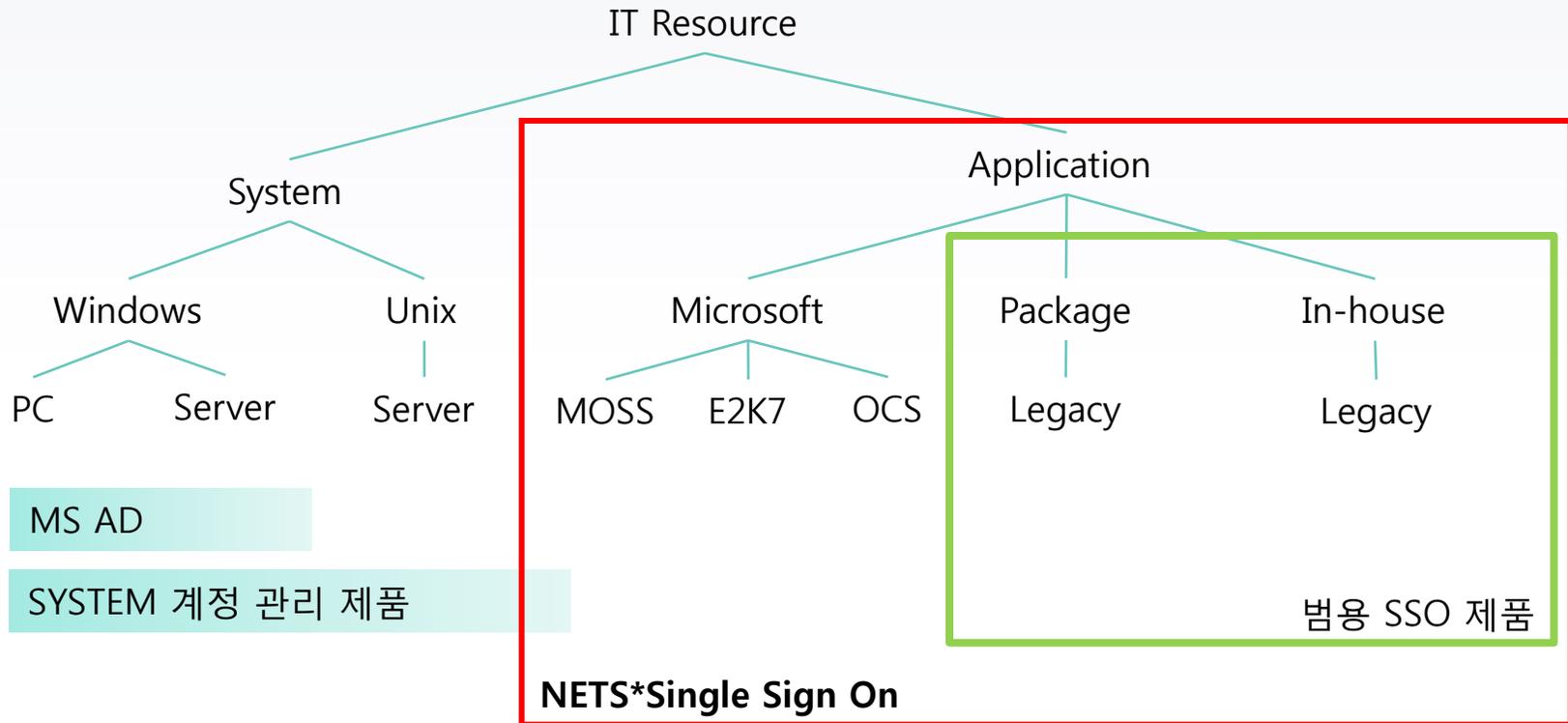
암호(暗號)는 비밀 인증 데이터의 한 형식으로 어떠한 자원에 대한 접근을 제어하는 데에 사용된다. 암호는 허용되지 않는 접근으로부터 비밀을 보호하며, 접근을 얻으려는 사람들에게 암호를 물어서 접근 여부를 결정한다.



- 기업의 주요 인프라를 Active Directory를 중심으로 설계한다.
- 구성원은 Active Directory의 사용자 계정으로 사용자 인증을 받아야 한다.
- 사용자의 PC는 Active Directory에 Join되어 관리 되어야 한다.(1인 1PC 정책)
- 기업 내 모든 Application은 Windows 통합 인증을 수용한다.



- 기업 인프라는 Windows와 Unix가 혼재된 환경
- 개발 도구 또한 .NET Framework과 Java Environment를 함께 사용
- 사용자에 대한 인증 방식도 윈도우 통합 인증, DB나 LDAP 기반의 ID/PWD 인증, 인증서와 물리적 인증 장치 등을 활용

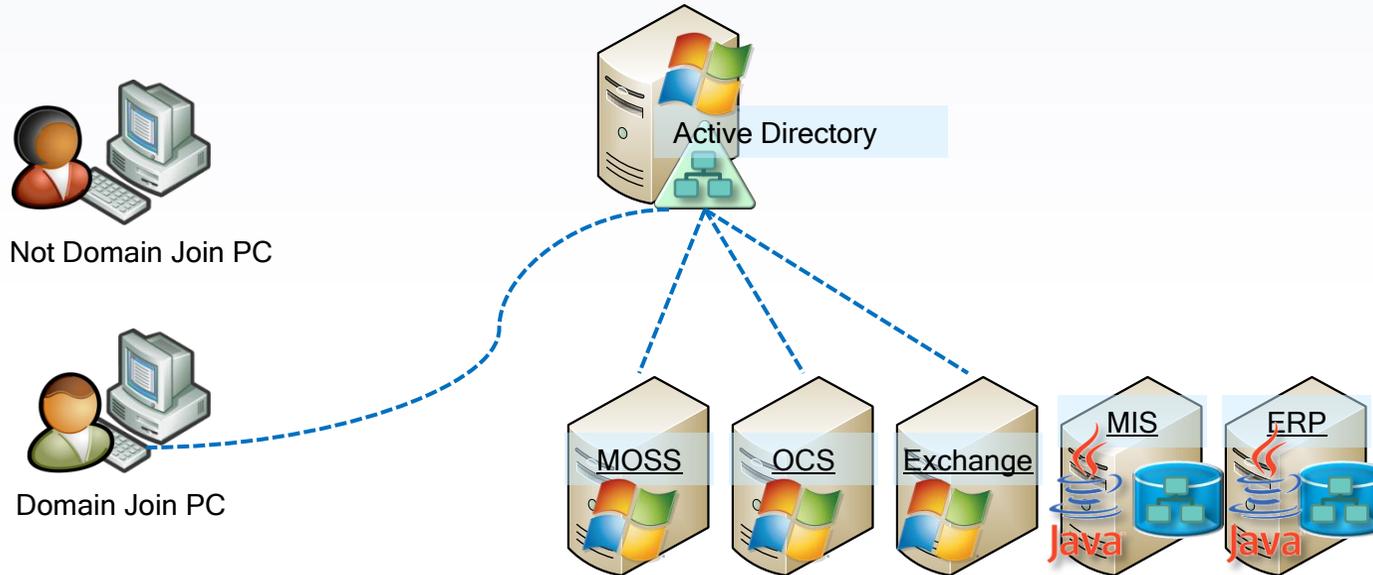


- 또 다른 LDAP 및 SSO 서버 구축에 대한 부담 없이 단일하고 일관성 있는 “윈도우 표준 플랫폼” 환경에서 조직의 다양한 인증 요구사항을 통합하고 이 기존 서버 및 애플리케이션에 대한 SSO 시스템을 구현할 수 없는가?
- 모든 사용자 PC를 도메인 조인할 것인가?
- 도메인 조인을 할 수 없는 환경 하에서 MS의 MOSS와 같은 제품을 사용할 수 없는가?
- 도메인 조인된 PC이지만 다수의 사용자가 이용해야 하는데 어떻게 해야 하나?
- 한번의 인증으로 메일(OWA)과 메신저(OCS)등을 이용할 수 있는 방안은?
- 다양한 운영체제(UNIX, LINUX 등) 및 개발환경 (JAVA, .NET 등)에 적용되는 윈도우 기술 기반의 SSO 시스템 구현 방안은?
- 윈도우 핵심 인증 기술인 Kerberos와 연동하여 표준 지향의 보안 인증 처리와 SSO 처리 방안은 무엇인가?
- 웹 APP SSO연동 시에는 HTTP 표준 기술 적용으로 다양한 Client 환경에 적용 가능하고 ActiveX 다운로드 및 설치 없이 SSO 구현이 가능한가?

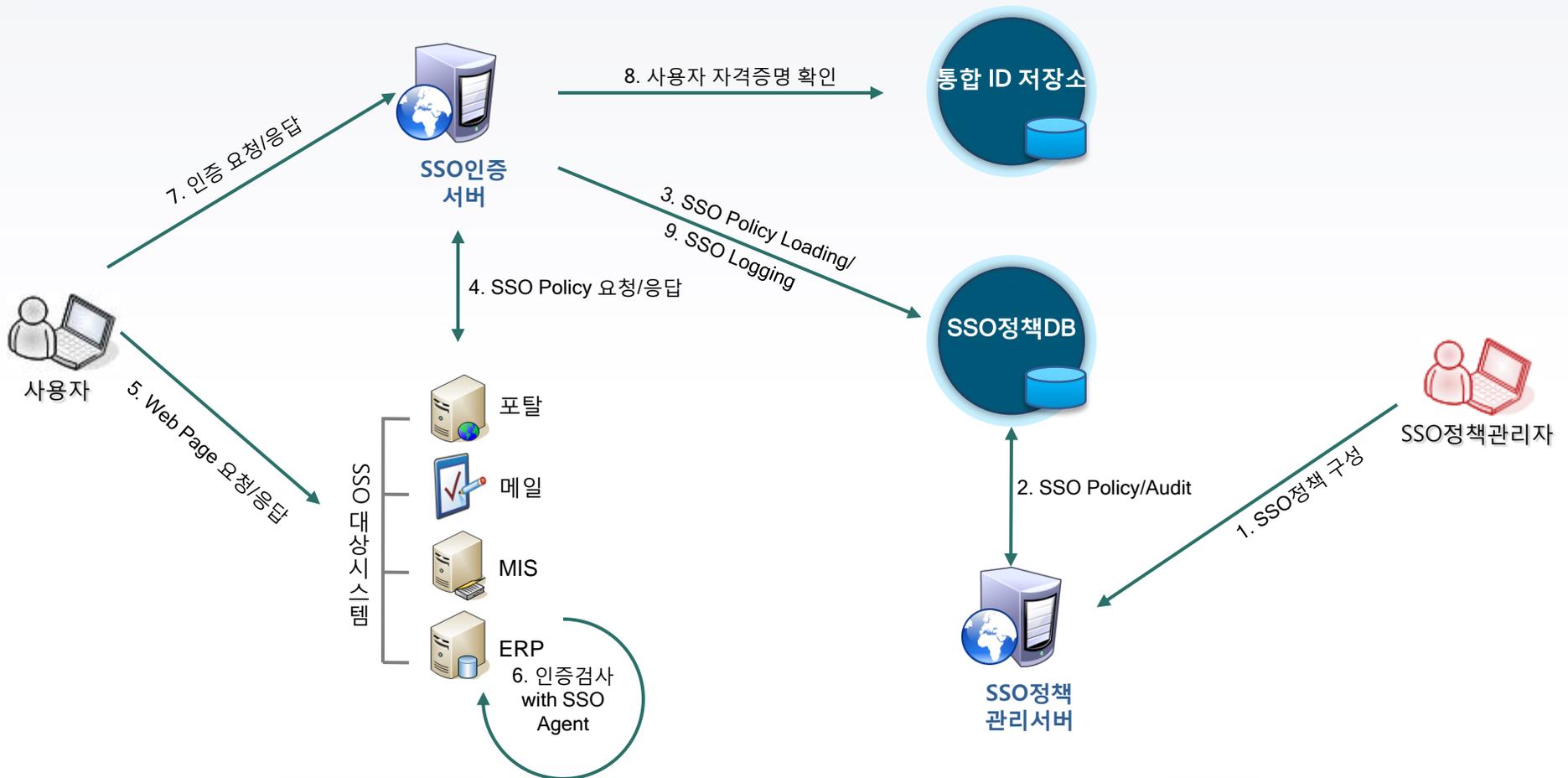
02 **NETS*Single Sign On**

- 1) 기업 인프라 현황
- 2) SSO Architecture
- 3) MOSS 통합 인증
- 4) AD 기반의 SSO 구축
- 5) NETS*Single Sing On 기능
- 6) 특•장점
- 7) SSO 도입 이점

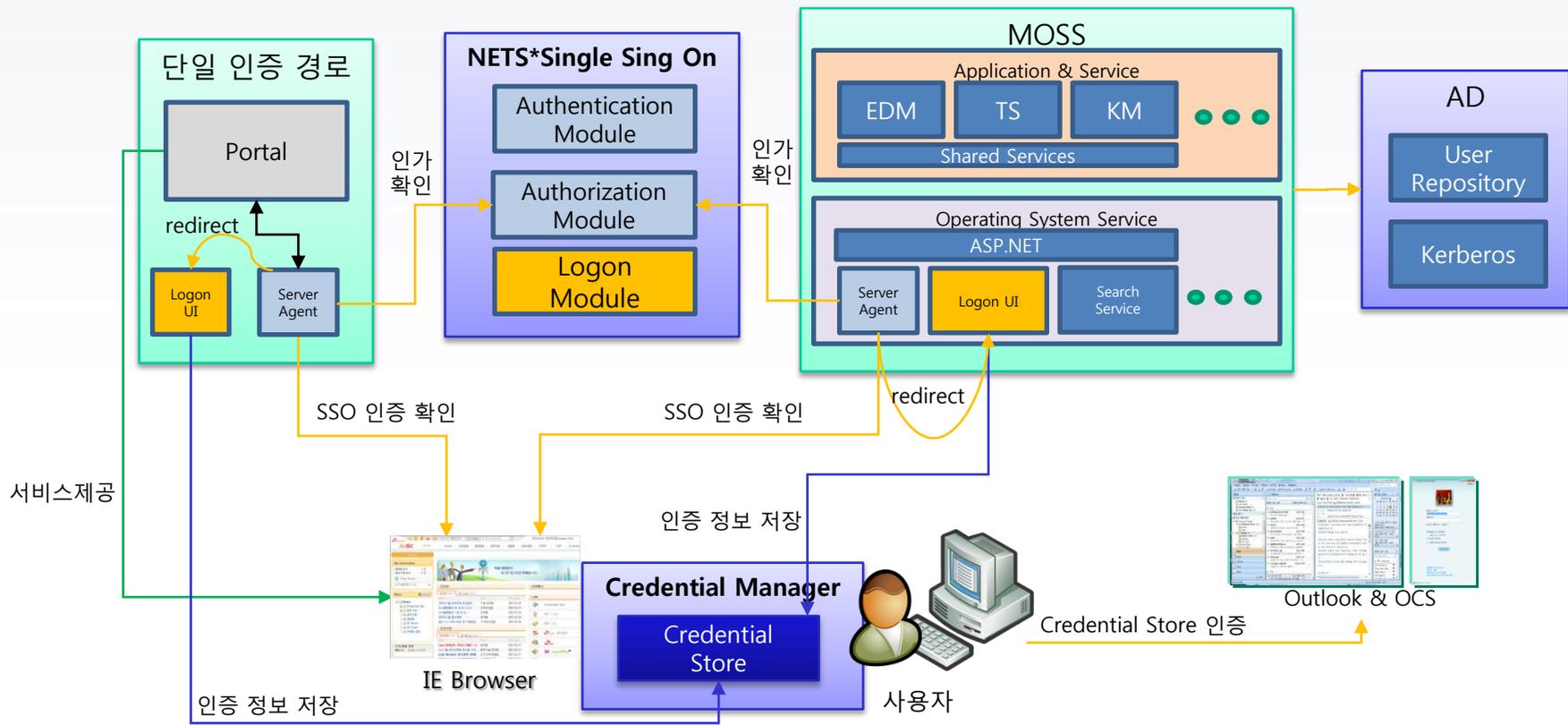
- 일반적인 기업의 업무 지원 인프라
 - 각 Application 접근 시마다 인증 요청 대응
 - MOSS의 경우 도메인 조인된 PC가 아니면 사용상의 불편함 초래
 - Windows 통합 인증을 요구하는 Application에 대한 대응 필요



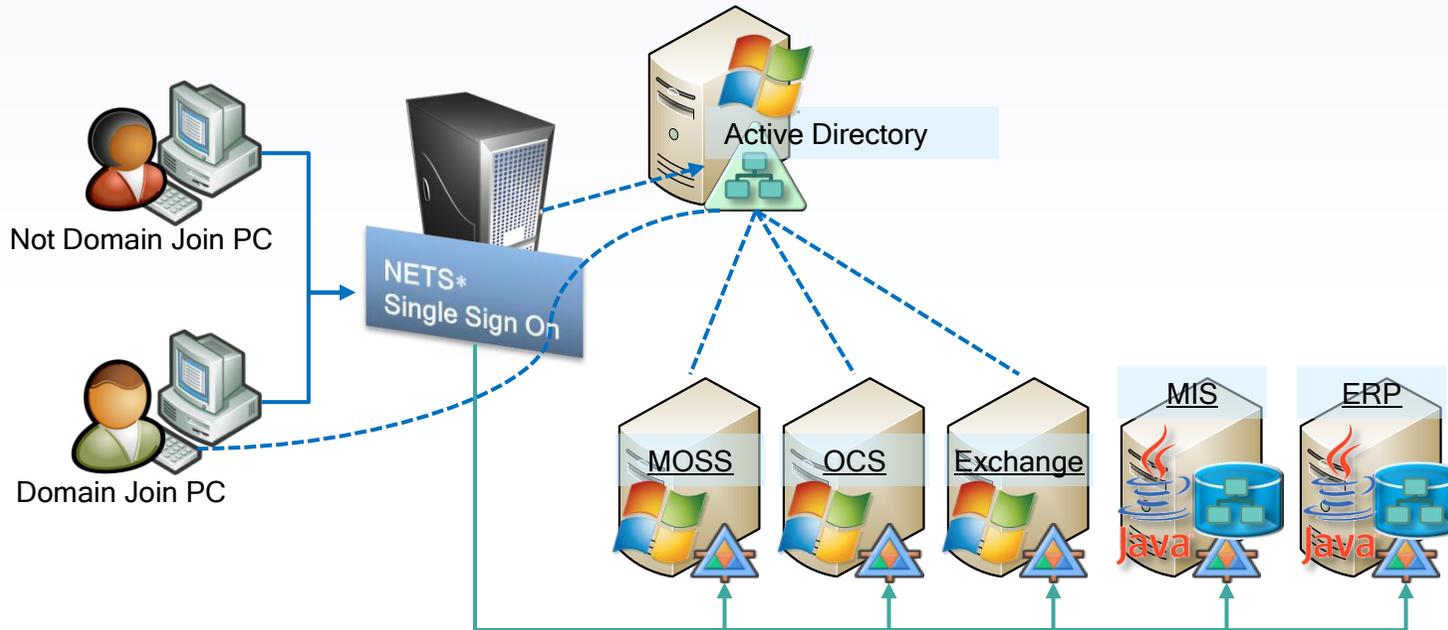
- 단일 인증을 통해 모든 애플리케이션 접속을 자동화함으로써 사용자의 애플리케이션 이용을 단순화하고 보안을 강화



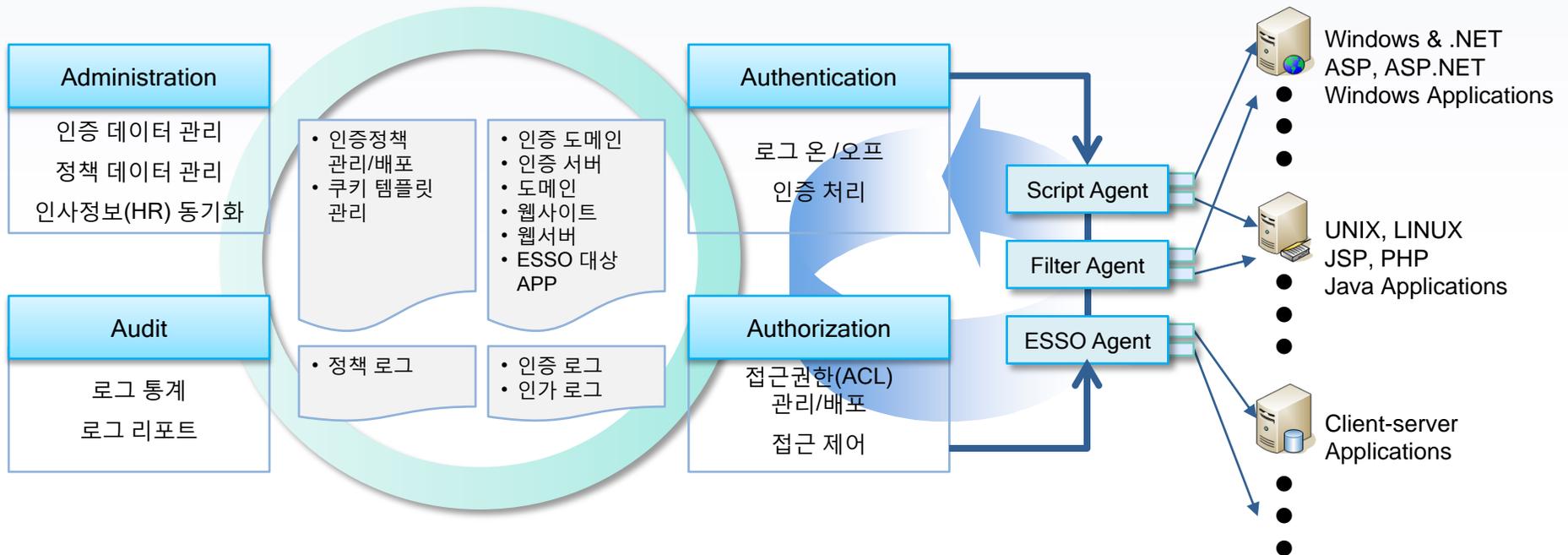
- MOSS 등의 윈도우 통합 인증이 필요한 Application 지원
- MOSS(포탈) 로그인 시 인증 정보는 Credential Manager(CM)에서 관리하고, Legacy 시스템에 대한 인증 정보는 NETS*Single Sign On에서 관리



- 한번의 인증으로 기업 내 다양한 IT 자원 접근
- Microsoft의 다양한 솔루션에 대한 표준 인증 지원
- 비 MS 계열의 개발 솔루션에 대한 표준 인증 체계 구축



- 폭넓은 로그-인 프로세스 지원
 - 유연한 로그-인 프로세스 제공으로 어떤 자원의 로그-인 요청도 포괄적으로 지원
- 강력한 유관 솔루션 연동
 - 인증강화(PKI, Token, Smart Card 등) 솔루션 연동, 공유 PC 환경, 계정•권한관리(IAM) 솔루션 연동
- 기능 개념도



NETS*Single Sign On 특·장점

다양한 이기종 OS 지원

- SSO Agent가 설치되는 인증 대상시스템은 유닉스, 윈도우, 리눅스 등의 다양한 이기종 OS에 설치 가능
- 대상시스템에 SSO Agent가 설치되더라도 서버 운영 시 영향을 최소화

IM 기반의 완전한 SSO 구현

- NSSO는 NETS 통합계정권한관리(IAM) 솔루션의 일부로써 NIM과 완전한 통합을 제공함
- 사용자(계정, 권한 등) 프로비저닝 시스템 기반의 진정한 SSO 서비스 제공

MOSS 통합 인증

- 윈도우 클라이언트가 도메인 조인이 되지 않은 환경 즉, AD 이행이 되지 않은 윈도우 전산 환경에서도 도메인 로그인 절차 없이 AD 기반의 윈도우 통합 인증을 지원함

PKI 기반의 SSO 지원

- PKI 기반의 SSO 처리를 통하여 더욱 강화된 보안 인증 체계를 제공함
- MS CA/AD 기반의 사설인증 SSO 처리를 지원함으로써 기존 윈도우 서버 전산 환경을 그대로 이용한 PKI 환경 구현

다양한 이중인증 체계 지원

- ID/Password 방식의 보안 취약성을 강화하기 위한 보안 Token , SmartCard, USB 등의 물리적 장치를 이용한 다양한 이중인증 체계 지원

풍부한 SSO 프로젝트 수행 경험

- 2004년 제품 개발 이후, 현장 경험이 지속적으로 반영된 제품 출시 (v3.0)
- 다양한 IT 환경에 적용할 수 있는 자체 SSO 구축 방법론 보유

고객 응답 개선

- 웹 사이트 이용에 대한 만족도 향상
- ID & 패스워드 관련 불편사항에 대한 신속한 처리

사용자 만족 및 생산성 향상

- 사용자는 (대상 애플리케이션의 보완 및 수정 없이) 단일 인증을 통해 애플리케이션 또는 시스템에 접근할 수 있음
- 사용자는 자신의 업무를 효과적으로 수행하기 위해 필요한 애플리케이션에 빠르고 안전하게 접근

Single Sign-On 시스템 소개



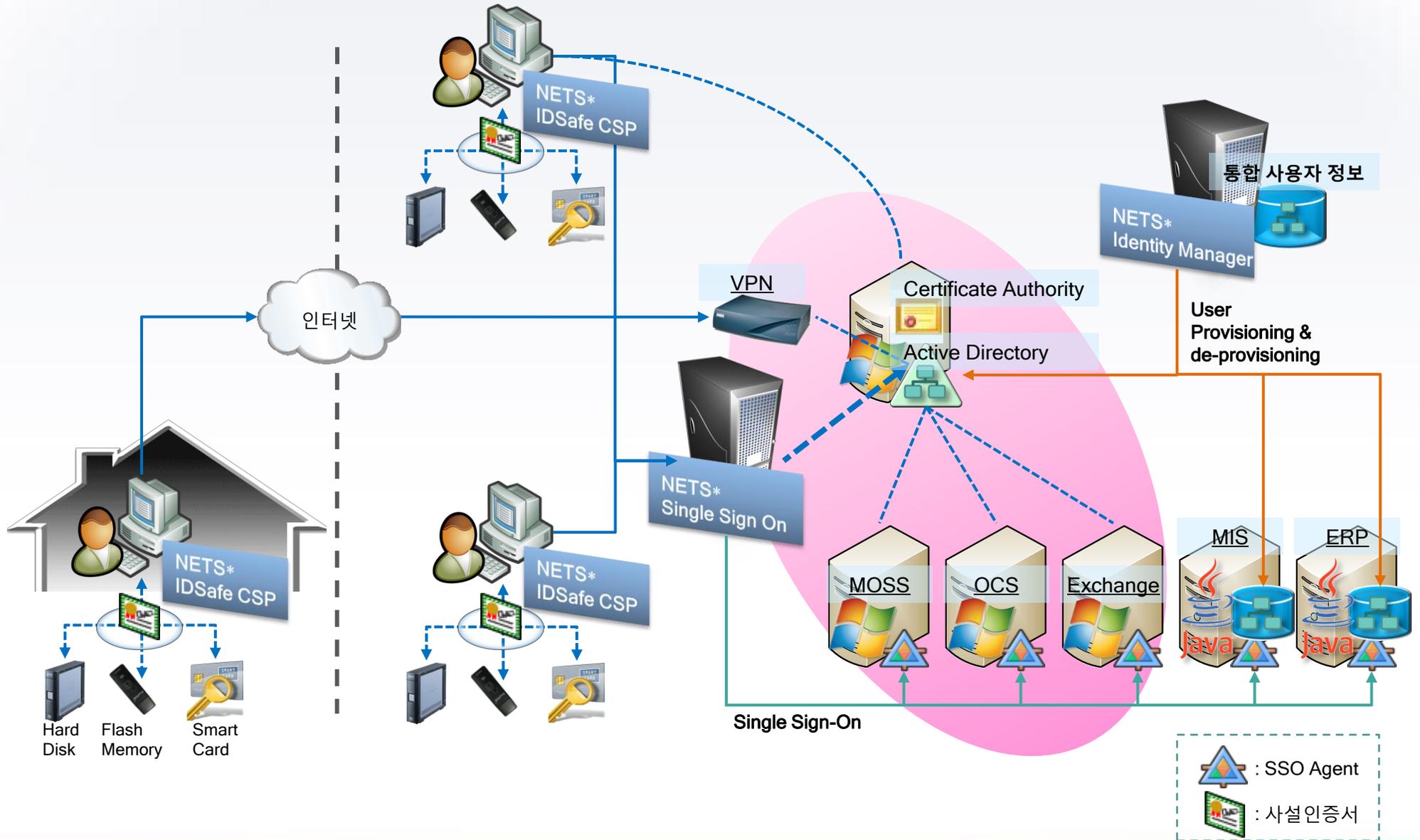
비용 절감

- 패스워드와 관련된 도움 데스크 비용 절감
- 조직의 IT 관리 일원화 및 단순화 기여

보안 강화 및 규제준수(Compliance)

- 애플리케이션 데이터에 대한 보호 강화
- 애플리케이션 접근 감사로 규제준수 지원
- SSO를 이용함으로써 기관 및 기업은 중앙집중적 사용자 애플리케이션 접근 권한 관리, 접근 기록 및 감사, 기존 애플리케이션에 대한 패스워드 정책 적용을 강화함으로써 전반적인 애플리케이션 접근 보안 개선

03 **Demonstration**



NETS*Single Sign On v3.0



질의 및 응답