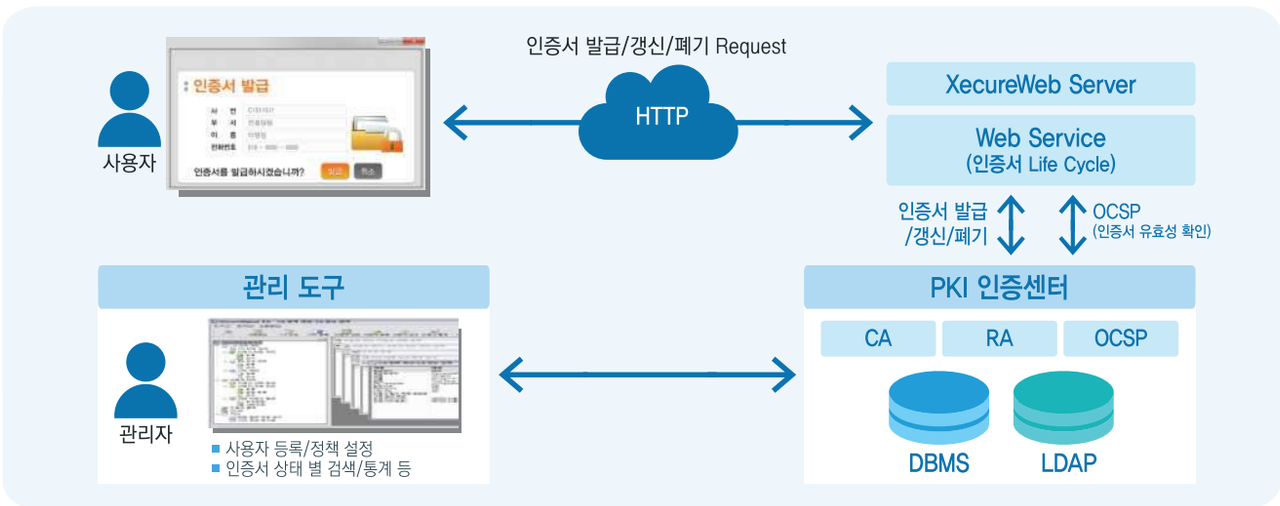
XecurePKI

인증 체계 구축 솔루션

PKI 인프라 구축을 통해 사용자 인증 체계를 확립하여 사용자 인증 보안 강화, 구간 데이터 암호화, 단일화된 인증서 관리 체계 확보 등의 편리한 보안 시스템 환경을 구현하는 제품입니다.



주요 제품 구성

XecureCA
인증서 발급 솔루션

- 인증서 발급 기관
- 인증서 발급/폐기/갱신 등 수행
- 국정원 암호 검증 필 모듈 탑재
- 기술 표준(PKIX, PKCS, ITU-T 등) 준수
- 암호체계 고도화 반영
  (RSA 2048, SHA-2 등)

XecureRA
가입자 등록 솔루션

- 인증서 등록 기관
- 가입자 정보 등록 및 관리
- 인증관리(CA)와의 정보 동기화
- 인증기관과 보안 통신 수행
- 암호체계 고도화 반영
  (RSA 2048, SHA-2 등)

XecureOCSP
유효성 검증 솔루션

- 실시간 인증서 유효성 검증 솔루션
- 국내외 표준 알고리즘 지원
- 기술표준(PKIX, PKCS, ITU-T 등) 준수
- 암호체계 고도화 반영
  (RSA 2048, SHA-2 등)

주요 특징

다양한 기능의 인증서 발급 및 관리

- 개인용, 기기용, 서버용 등 다양한 용도의 인증서 발급
- 확장 필드에 다양한 정보 삽입 지원
- 독자적인 사설인증시스템을 구축하여 사설인증서 발급, 갱신 및 폐기까지의 인증서 관리

안전성 및 호환성

- PKCS #5 v2.0 이상의 개인 키 암호화 지원
- 암호 키 쌍에 대한 키 복구 시스템(KMI) 연동 지원
- 인증서 유효기간, 알고리즘 크기, 인증서 타입 등의 인증서 정책 관리
  국내 최초로 국제 B2B 인증 네트워크 '아이덴트러스(Identrus)' 호환 인증 획득

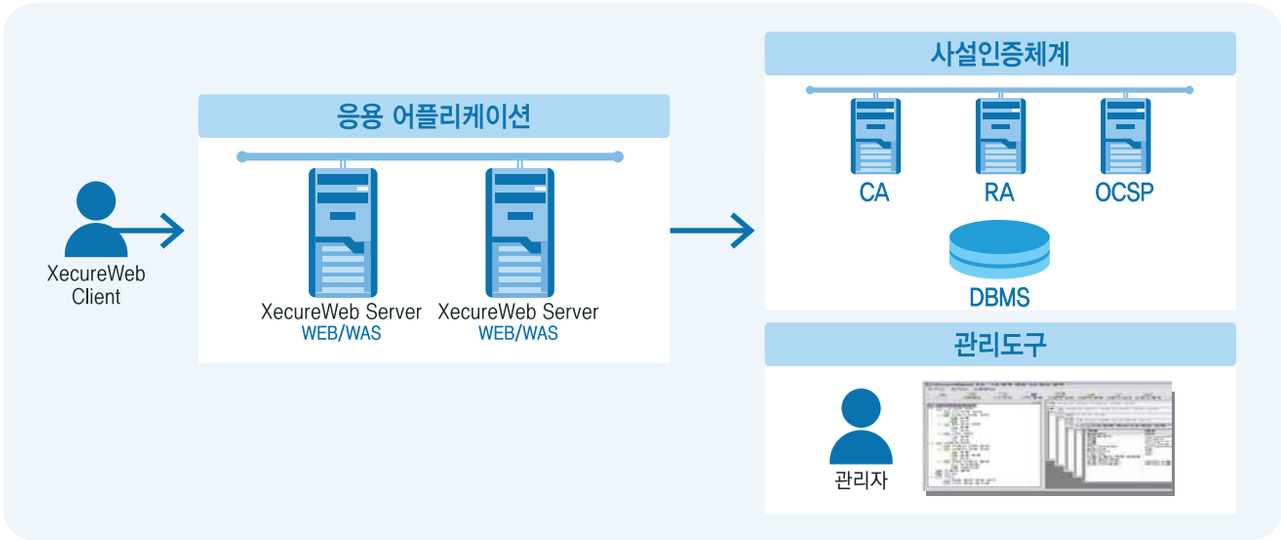
보안성 강화

- 암호체계 고도화 반영(RSA 2048bit, SHA-2 등)
- 국정원 검증필 암호모듈(CMVP) 탑재
- 등록기관 간의 통신 보호를 위해 암호화 프로토콜을 이용한 보안 절차 수행

유효성 검사

- 별도의 LDAP 구축으로 CRL 방식의 인증서 유효성 검증
- OCSP 모듈을 이용하여 인증서 발급 DB를 직접 참조하는 실시간 인증서 유효성 검사

구성도 및 수행기능



구분	구성 시스템	수행 기능	비고
인프라 시스템	XecureCA	■ 인증서 발급 기관	■ 인증서 유효성 확인을 OCSP 방식 지원 ■ CA/RA/OCSP는 RDB 별도 필요
	XecureRA	■ XecureCA 등록 기관 ■ 공인인증기관의 등록기관	
	XecureOCSP	■ 실시간 인증서 유효성 확인 기관	
관리 시스템	XecureCC	■ CA/RA/OCSP의 관리를 위한 서버 사이드 관리 데몬	
	관리도구	■ CA/RA/OCSP의 관리자 인터페이스	■ XecureCC와 통신하여 CA/RA/OCSP 제어
사용자 인터페이스	PKI Toolkit	■ Client – 사용자 PC에 설치되는 컨트롤로 인증서 관련 인터페이스 수행 ■ Server – WAS에 설치되어 인증서 Life Cycle 서비스를 위한 연동 인터페이스 제공	■ XecureWeb(ActiveX) or AnySign(Non-ActiveX) (별도 제공)

지원 환경

제품		기능	32Bit 지원현황	64Bit 지원현황
XecurePKI (CA/RA/OCSP/CC)	OS	■ Solaris 2.8 이상	지원	지원
		■ AIX 5.1 이상	지원	지원
		■ HP-UX 11.0 이상	지원	지원
		■ HP-IA(Itanium) 11.23 이상	지원	지원
		■ Windows : win2000 서버 이상	지원	지원
	DB	■ Oracle 9/10/11	해당 사항 없음	
		■ DB2 9.2/9.7		
		■ Informix 11.5		
		■ MS-SQL(windows only)		
		■ Sybase 12.5		

HANCOM SECURE
(우)13493 경기도 성남시 분당구 대왕판교로 644번길 49 한컴타워 9층 대표전화 : 031-622-6300 FAX : 031-622-6277
www.hsecure.co.kr