

암호 플랫폼(Encryption Platform)의 시작, D'Amo

IT 보안은 암호화, 접근제어, 감사가 필수이며 키 관리가 핵심

암호화

- 검증필 암호모듈 탑재
- FIPS 인증 암호 알고리즘
- 국내외 표준 암호 알고리즘

접근 제어

- White/Black List 관리
- 컬럼별/사용자별 권한 부여
- 요일별, 날짜별, 시간별 정책

감사 로그

- 중앙 집중형 로그 관리
- 접근/정책/상태 로그
- 로그 자동 백업 및 조회

키 관리

핵심

- 국내 최초 CC인증 EAL3+ 획득 키 관리 서버
- 국내외 암호화 표준을 준수한 안전한 키 관리
- D'Amo, 외부 Application, TDE 키 관리 제공



D'Amo

I 주요기능 및 특징점

1 IT 시스템 규모와 특성에 알맞은 암호화 방식을 제공합니다.

- 6개 암호화 방식, 총 24종의 암호화 컴포넌트 보유
- SAP ERP와 같은 데이터의 속성 (길이, 형식, 데이터타입) 유지가 요구되는 환경에서도 안전한 암호화 적용 가능

2 검증된 암호모듈과 암호화 알고리즘을 사용합니다.

- 국정원으로부터 검증된 자체 개발 암호모듈 (CIS-CC 3.2)
- 국정원 정보보호제품 등록 D'Amo v3.0
- 미국국립 표준기술연구소의 FIPS 인증 암호화 알고리즘 (AES, TDES) 사용

3 국내 최초 CC인증을 획득한 키 관리 시스템으로 키를 관리합니다.

- 국내 최초 CC인증 EAL3+를 획득한 키 관리 시스템 (Key Management System) 보유
- DB암호화, 어플리케이션 암호화, POS/단말/ATM 암호화 등 전사적 키 관리 인프라 제공
- 양자 난수 생성기와 HSM(FIPS 140-2 Level 3)을 통한 보안성 강화 패키지 제공

4 국내외 고객들로부터 제품 우수성과 기술을 인정받았습니다.

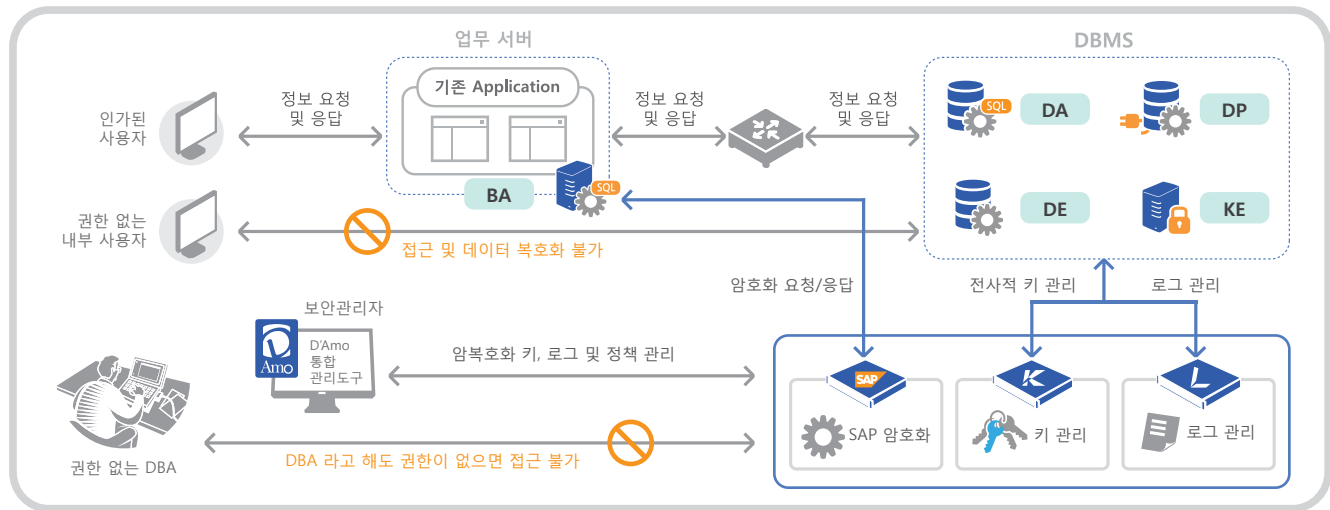
- D'Amo는 국내외 3,200 여 고객에게 인정받은 제품
- 빠른 성능과 대용량처리를 요구하는 금융권 점유율 1위 제품

5 클라우드 환경에서도 데이터 보안을 완성합니다.

- 클라우드 및 하이브리드 환경에서도 적용 가능
- 국내 최초 AWS (Amazon Web Service) Standard Technology Partner



구성도



D'Amo 컴포넌트 소개

> BA (Business Application)

- 어플리케이션에서 암호화를 수행하여 DBMS에 영향이 없는 API 방식 (BA-SCP, BA-JPF)
- ※ BA-JPF는 Java Platform에 최적화된 API

> DA (DBMS Application)

- DBMS API 방식으로 추가 패키지를 설치하지 않고 DBMS 내부에서 암호화를 수행하는 API 방식 (DBMS 함수/프로시저 이용)
- ※ 지원 DBMS: DB2, PostgreSQL, CUBRID, TIBERO, Sybase ASE, Sybase IQ, Informix, Cache

> DP (DBMS Packages)

- DBMS에 패키지를 설치하여 어플리케이션 수정 없이 암호화를 수행하고 간단하게 적용하는 방식
- ※ 지원 DBMS : Oracle, MS-SQL

> DE (DBMS Engine Level Encryption)

- DBMS 엔진에 직접 개입하여 어플리케이션 수정 없이 뛰어난 성능과 안전성을 제공
- ※ 지원 DBMS : MySQL/MariaDB, ALTIBASE, PostgreSQL (지원 예정)

> KE (Kernel Level Encryption)

- OS 커널 레벨 암호화 기술을 이용해 파일, 폴더 단위 암호화 수행
- ※ 이미지, 동영상, 녹취록, 의료 기록 등 개인 민감정보에 대한 가장 쉬운 보호 방식

> SP (System Processor facility)

- 자체 암호화 엔진과 메인프레임(M/F)에서 제공하는 암호화 프로세스를 이용하여 하드웨어 레벨에서 암호화를 수행
- ※ IBM M/F 전용 : C, PL/1, COBOL, RPG 지원

> SG (Security Gateway)

- 강력한 키 관리, 통합 로그 관리 등을 통하여 안전한 암호화 시스템을 구축하는 핵심 하드웨어 일체형 Appliance 서버
- ※ KMS : 암호화 키를 별도의 장비에 저장, 관리하여 PCI-DSS, ISMS, PIMS 등 국제 수준의 보안성 제공
- ※ LMS : 로그 저장, 분석, 백업 등 관련된 모든 기능을 GUI 관리도구로 통합 관리
- ※ SAP : SAP ERP 전용 암호화 제품으로 데이터의 속성 및 길이를 유지하며 암호화하는 NIST 표준 FPE (형태 보존 암호화) 운영모드 제공
- ※ POS : POS/CAT 등 신용카드 단말기 인증 암호화 솔루션 (여신금융협회 신용카드 단말기 정보보호 기술기준 적합)

주요 특허 (출원년도)

- > 특성유지 암호화를 이용한 데이터 보안 방법 및 장치 (2011년)
- > 평문의 확률적 분포특성을 고려한 순위 보존 암호화 방법 (2011년)
- > 데이터베이스 엔진을 이용한 데이터 보안 방법 (2011년)
- > 암호화된 데이터베이스에서의 쿼리 처리 장치 및 방법 (2007년)
- > 인덱스 컬럼 암호화 방법 (2005년)

주요 인증 및 수상

- > D'Amo KMS CC인증 EAL3+ 획득
- > 자체개발 국정원 검증필 암호모듈 (CIS-CC 3.2)
- > 미국국립 표준기술연구소 FIPS 인증 획득
- > 정보통신기술협회 (TTA) GS 인증 획득
- > 제2회 대한민국 소프트웨어 품질대상 최우수상

