cube One™

eGlobal
Global Technology, Make IT easy

(주)이글로벌시스템 서울특별시 강남구 역삼동 703-5 일환빌딩 9층
TEL. 02-6447-6988 FAX. 02-6447-6989 E-Mail. sales@cubeone.co.kr
www.cubeone.co.kr

cube One™

색인 검색을 지원하는 대용량 DB 암호화 솔루션

An Ideal “Data-at-rest Column Level Encryption Solution”
specialized for High Transaction and No Downtime Database

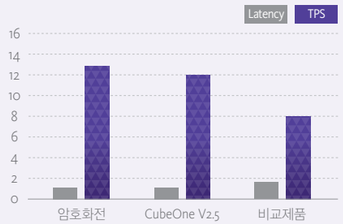
Premium DBMS 암호화 솔루션

CubeOne™은 중요정보(개인정보)가 저장된 대용량 DB에 적용하기에 알맞은 매우 독창적인 구조를 가지고 있습니다. 이러한 기술은 NEP(우수신제품인증) 및 국내외 특허로 그 독창성과 기술력이 입증된 바 있습니다. 또한 DBMS 암호화를 적용한 대형 시스템 구축사업에서 비교할 수 없는 우수성이 입증 되고 있습니다.

Why CubeOne™

BMT 마다 경이적인 성능 기록

CubeOne™ 은 많은 대형 BMT에서 비교할 수 없는 막강한 성능을 기록하고 있습니다. 기존의 제품들에서 나타났던 성능저하 문제는 CubeOne™에서는 더 이상 문제가 되지 않습니다. 중요한 것은 OLTP 처리에 있어서 성능저하가 거의 느낄 수 없는 정도에 그친다는 점입니다.



개인정보 보호관련 법규에서 요구하는 암호화 기술적 보호조치 충족

CubeOne™은 FIPS-140 기준을 만족하며 국정원 암호모듈검증필 암호모듈 (KLIB V.1.x)이 탑재된 안전한 제품입니다. DB 또는 AP서버내의 디스크에 평문으로 된 키를 저장하지 않아 어떠한 경우에도 데이터와 키가 함께 유출될 가능성이 없는 매우 안전한 키 관리 체계를 가지고 있습니다.

기술적 보호조치 기준	만족 방법
▪ 중요 개인정보의 저장시 암호화	▪ 컬럼 단위 암호화
▪ 중요 개인정보에 대한 접근 기록은 별도저장 장치에 저장	▪ CubeOne™ Security Server에 저장 (DB와 분리된 별도의 서버에 저장)
▪ 중요 개인정보에 대한 접근기록은 위.변조 및 훼손을 방지하도록 저장	▪ 암호화하여 저장 (암호화는 위.변조가 불가능 함.)
▪ 접근통제 실시	▪ 암호화한 칼럼에 대한 접근제어 및 통제 (네트워 보안 장치와 더불어 요건 충족)
▪ 비밀번호 및 바이오정보는 일방향으로 암호화하여 저장	▪ SHA-1/256/384/512 알고리즘 적용

CubeOne™ 인증 사항
※국정원 인증 : 국가용 암호 제품 인증 (NCPL-2009-030, NCPL-2011-004)
※암호모듈검증 : KLIB V1.6 인증번호 (CM-29-2015.01)
※행정안전부 : 행안부 행정정보 보호제품 등록

What's CubeOne™

고성능

- 암호화된 컬럼 색인검색
- 가장 빠른 암,복호화 성능

대용량

- 수억~수십억건에 대한 암호화 지원
- 대량의 트랜잭션 환경 지원

무중단

- 무장애 운영 구조
- 암호화 작업 시 무 중단 서비스 가능 (Oracle Only)

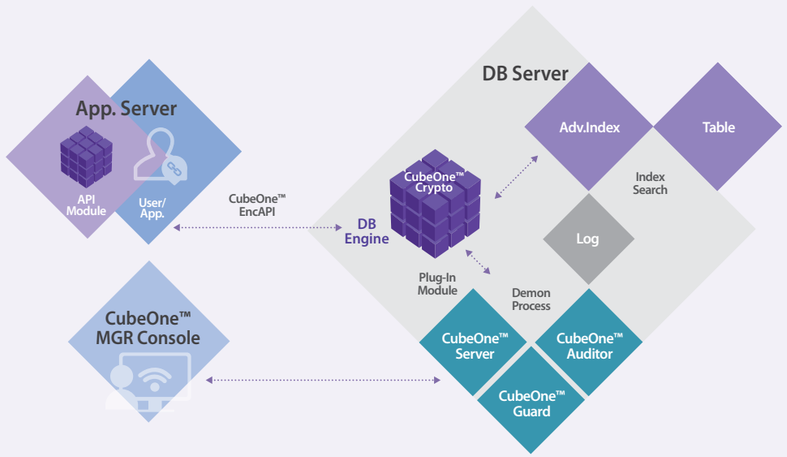
CubeOne™ 제품군

- CubeOne™ Plug-In : Oracle, MS-SQL, DB2, Tibero, Informix, MySQL, GreenPlum, TeraData, Sybase IQ, Altibase 등
- CubeOne™ API : Any DBMS, SAM/TXT File
- CubeOne™ for SAP
- CubeOne™ Options : Security Server, API Handler, BeaCon, SQL Converter

Architecture

분산처리가 가능한 Hybrid 지원

CubeOne™ 은 보안관리자용 Manager Console에서 다수의 DB서버 또는 AP서버를 통합 관리하며, 모든 작업이 GUI를 통해 자동으로 처리되어 DB를 잘 모르는 보안관리자가 운영하기에 적합 합니다.
또한, DB서버 내에 Plug-In 및 AP서버에서 동작하는 API를 동시에 사용할 수 있는 Hybrid 형태의 S/W로서 Plug-In 과 API의 장점을 모두 지원하는 구성을 지원 합니다.



CubeOne™ Plug-In

진정한 Application 독립성 확보

CubeOne™ Plug-In 은 Application과 독립적이므로, Application을 개발하고 관리하는 사람이 암호화에 대해 어떠한 관심도 기울일 필요가 없습니다. 즉 기존에 사용하던 SQL문을 그대로 사용할 수 있습니다.
특히 DB관리자가 신경을 써야 하는 Dependency (예, Trigger등) 관련 작업들도 CubeOne™에서 관리해 주므로 별도 수작업이 필요치 않습니다.

업계 유일의 암호화된 Index를 통한 색인 검색

CubeOne™ 은 테이블과 Index 모두를 완벽히 암호화 하고, 이 Index를 통한 색인검색을 지원하는 유일한 제품 입니다(특허 등록). CubeOne™으로 암호화하면 Full Table Scan 발생으로 인한 심각한 성능 저하가 없습니다.

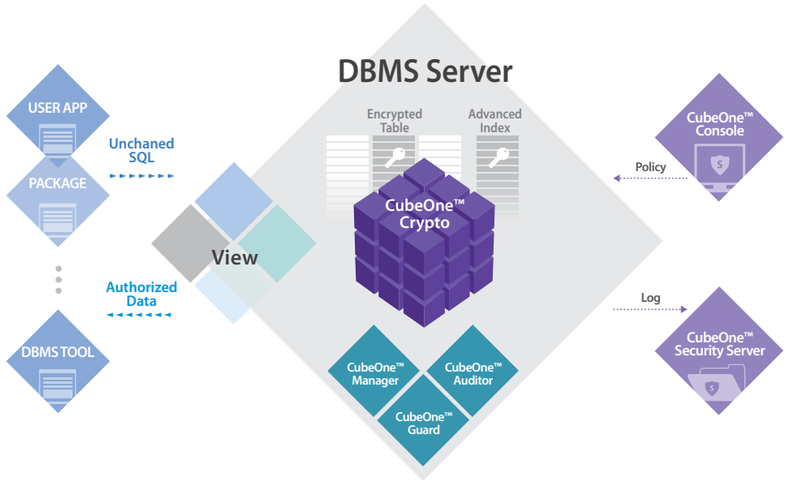
최고의 운영성 및 내 장애성 구조

CubeOne™의 API 및 Plug-In은 모든 데몬프로세스의 장애시에도 정상작동 하는 구조를 제공 합니다.
또한 기밀성을 위해 DB/App. 서버의 메모리에 로딩된 키가, 재부팅시 자동 로딩될 수 있도록 키 분배 서버(CubeOne™ Security Server)를 제공 합니다. 이러한 구조들로 인해 CubeOne™의 내 장애성은 업계 최고 입니다.

그 밖의 한발 앞선 신 기술들

그 외에도 CubeOne™에는 실제 구축 경험에서 비롯된 업계 최초로 구현한 Dual Sync Mode 기능, 복호화를 하지 않고 추가 암호화가 가능한 기능, 연결된 세션에도 즉시 적용되는 Realtime Sync. 기능, 다중 모니터링 콘솔, Triple-Depth 패스워드 인증 기능, 변경된 패스워드 및 Application명 탐지 및 통제 기능 등 경쟁제품들이 가지지 못한 다양한 기능들이 가득 합니다.

Architecture



Key Features

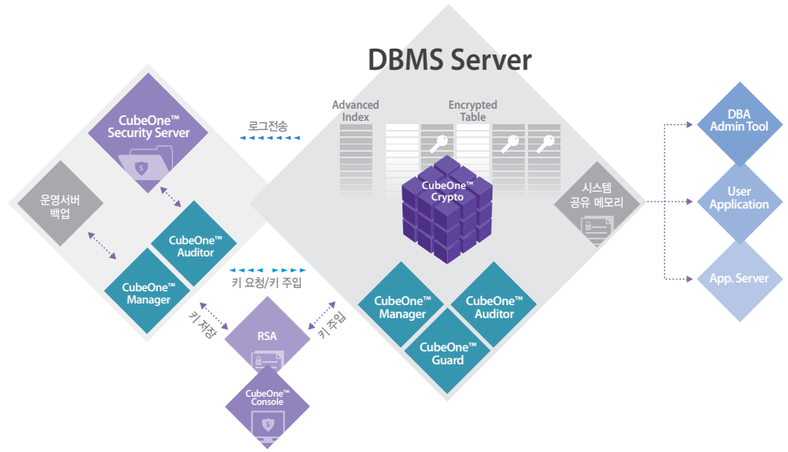
CubeOne™ Plug-In

암호화 컬럼 Index 색인 검색

CubeOne™ 은 색인 검색이 지원됨에도 불구하고 암호화 데이터의 일부, 혹은 전부에 대한 복호화된 정보를 보관하지 않습니다. CubeOne™ 만의 암호화된 색인(Advanced Index)을 사용하여 암호화 적용된 컬럼에 대하여 일치 검색은 물론 Like검색과 같은 범위 검색을 지원 합니다. (특허기술 : Advanced Index Searching.)

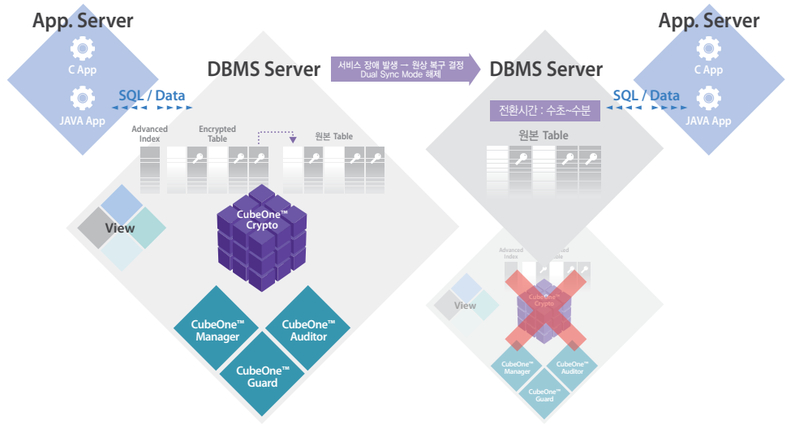
암복호화 키 기밀성 유지

암복호화 키와 Master키는 분리되어 있으며, 암복호화 키는 운영서버의 File이나 DBMS에 저장하지 않습니다. DBMS 암호화 운영에 필요한 암복호화 키는 변조된 상태로 메모리에 상주시키며, 사용 후 모듈 종료 시 키가 제로화 됩니다.



암호화 적용 후 장애발생 시 신속한 원상복구 (Dual Sync Mode)

운영서버에 암호화 적용 이후 혹시 발생 할 수 있는 장애로 인해 암호화 이전의 상태로 서비스 전환 시, 시간이 많이 소요되는 Rollback이 필요 없습니다.



CubeOne™ API

타 API 보다 월등히 빠른 성능의 간결한 구조

CubeOne™ API 는 접근제어 → 암복호 처리 → 로그저장 으로 이어지는 전 과정이 별도 프로세스의 개입 없이 Encryption_API내에서 처리 됩니다. 이러한 보기 드문 간결한 구조는 빠른 성능과 함께 고도의 내 장애성을 함께 제공합니다. (BMT결과 타사 API보다 약 50% 정도의 빠른 성능을 제공 합니다.)

이기종 DBMS 지원

CubeOne™ API 는 DBMS 종속적이지 않으므로 모든 DBMS에 대해 암호화 기능을 제공할 뿐 아니라, 작업시간이 많이 걸려 암호화 적용이 어려웠던 Batch 업무에 대한 암호화 적용을 가능하게 합니다. 또한, CubeOne™ Plug-In 제품과 동시 적용 시 암호화된 Index의 색인 검색을 지원 합니다.

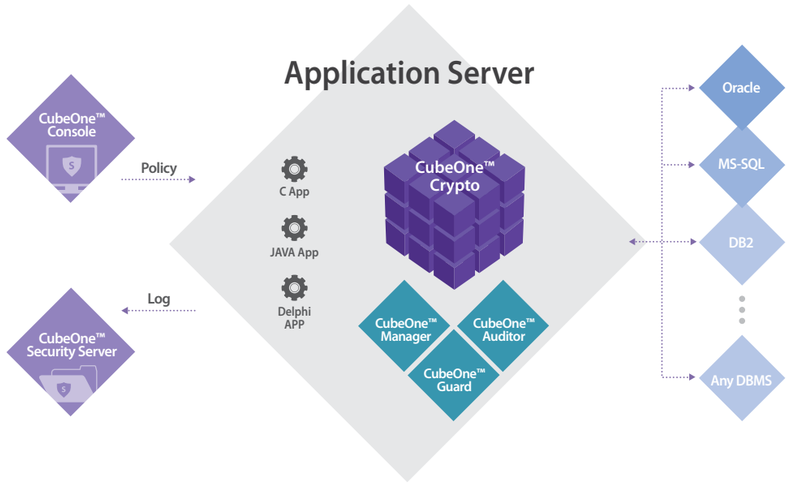
대용량 Batch 성능 확보

CubeOne™ API 는 DBMS 암호화 적용 시 서비스 성능저하 문제는 더 이상 문제 되지 않습니다. DBMS 암호화 적용 이후 목표 처리 시간 이내에 서비스 완료를 하지 못하는 대용량 Batch 업무의 경우 DBMS Local 서버에서 CubeOne™ API를 적용하여 Batch 업무를 수행함으로써 암호화 적용 후 서비스 완료시간을 획기적으로 단축시킬 수 있습니다.

그 밖의 한발 앞선 신 기술들

그 외에도 CubeOne™ API 에는 실제 구축 경험에서 비롯된 부분암호화 기능, 다중 모니터링 콘솔, Triple-Depth 패스워드 인증 기능, 변경된 패스워드 및 Application명 탐지 및 통제 기능 등 경쟁제품들이 가지지 못한 다양한 기능들이 가득합니다.

Architecture



CubeOne™ API Handler

API의 단점 보완

CubeOne™ API Handler 는 암호화 대상 DBMS에 설치 되며, API 만을 Application 서버에 설치 되는 경우 발생할 수 있는 암호화 DB 운영 및 관리상의 단점을 보완해 주는 CubeOne™ API용 전용 Option 입니다.

암호화 적용된 컬럼의 색인검색

CubeOne™ API Handler 는 암호화된 컬럼에 대한 색인 검색 (Index Search) 지원 함으로써 일치 검색은 물론, 전방 일치 (LIKE, BETWEEN, >, <, >=, <=등 모든 전방 일치 검색) 검색 시 Index Search를 지원합니다. 색인 검색이 지원됨에도 불구하고 암호화 데이터의 일부, 혹은 전부에 대한 복호화된 정보를 보관하지 않음으로써 보안성을 확보 합니다.

초기 암호화 적용 기능

초기 암호화 구축 작업을 GUI를 통해 자동화 해주므로 매우 편리하게 데이터 마이그레이션을 수행할 수 있습니다.

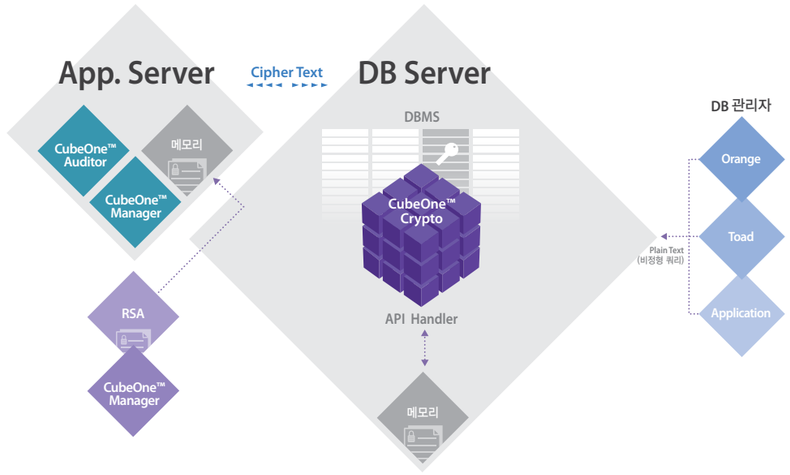
DB 직접 접속 시 암복호화 기능

SQL*plus, Toad, Orange, Golden 등의 툴을 이용하여 인가자가 DB로 직접 접속하여 암호화된 데이터를 조회/처리할 수 있도록 해 줍니다.

CubeOne™ API Handler 지원 환경

항목	설명
적용 가능 DBMS	Oracle 8.1.6 이상
	MS-SQL 2000, 2005, 2008
	DB2 7.x 이상
	Informix 9.x 이상
	Tibero 4.0 SPI 이상

Architecture



CubeOne™ BeaCon

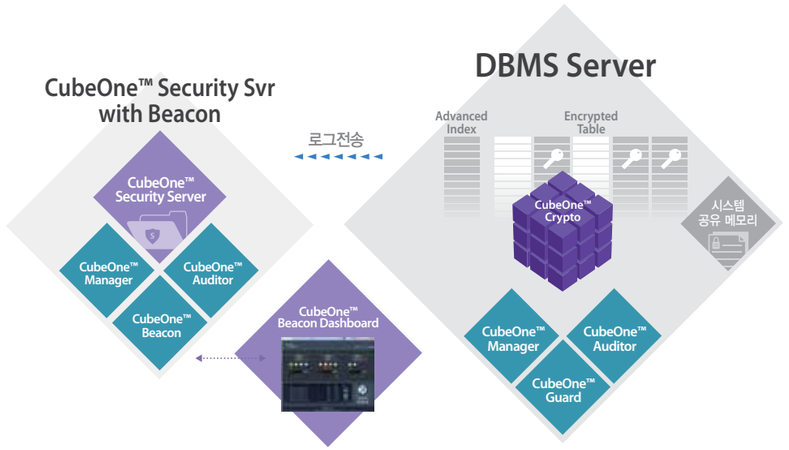
암호화 상태 통합 모니터링

CubeOne™ BeaCon 은 전용 Dashboard를 통하여 CubeOne™이 적용된 시스템의 암복호화 처리상태의 통합 모니터링을 지원 합니다.
※ CubeOne™ Security Server에 Add On 하여 구성 됩니다.

대량 복호화 방지 기능

암호화 인가자를 통하여 발생할 수 있는 임계치를 넘는 인가된 복호화 요구를 차단 또는 보안관리자에게 통지를 함으로써 대량의 개인정보 유출 상황을 방지 합니다.

Architecture



BeaCon 관리 화면

■ BeaCon 메인 화면

■ BeaCon 암호화 통계화면

■ BeaCon Access Log 조회

■ BeaCon 관련 SQL 상세 조회

■ BeaCon 암호화 Event 상세조회

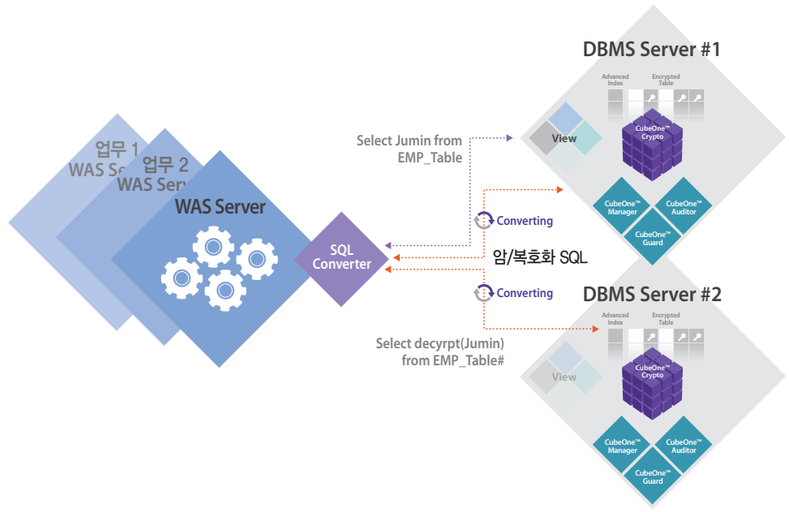
■ BeaCon 기능 설정

CubeOne™ SQL Converter

Application 소스코드 변경 최소화

CubeOne™ SQL Converter 는 JAVA(WAS) 환경에서 작성된 Application의 암복호화 관련 SQL을 CubeOne™ Plug-In 환경의 최적화된 SQL로 자동 변환을 지원함으로써 사용자의 Application 변경 요구를 최소한으로 유지 합니다. 암호화 성능 확보를 위하여 Plug-In을 적용하더라도 발생할 수 있는 SQL 변경사항을 직접 Application을 변경하여 반영 하지 않고 CubeOne™ SQL Converter에 등록하는 작업 만으로 최적의 암호화 성능을 확보할 수 있습니다.

Architecture



SQL Converter 관리 화면

1. 적용대상 시스템 등록

- SqlConverter를 적용 할 WAS를 등록함.

2. 변경대상 SQL 등록

- 변경이 필요한 SQL을 등록 함.
- 변경 전 SQL은 실행중인 WAS에서 자동으로 수집
- 변경 후 SQL은 담당자가 수동으로 입력

3. 변경대상 SQL 등록_상세

- 변경할 SQL을 등록

4. SQL실행결과 모니터링

- WAS를 통해서 실행되는 모든 SQL을 모니터링함
- 변경 대상으로 등록된 SQL은 SqlConverter에서 자동으로 변경되고 해당 정보는 Converted Query 에서 확인 가능

5. SQL실행결과 모니터링_상세.png

- SqlConverter를 통해서 자동으로 변경된 SQL정보 상세 화면
- 변경 전 SQL과 변경 후 SQL을 동시에 비교 가능
- 각종 필요정보 조회가능 : PreparedStatement의 인자로 들어온 정보 확인 가능, 실행시간, 성공/실패 여부

6. 정책변경이력

- 서버정보 변경 이력
- 변경대상 SQL 변경 이력

CubeOne™ for SAP

CubeOne™ for SAP 는 자유로운 SAP 업그레이드(Integrity 보장) 지원 하며, SAP Standard Object 수정 불필요, CBO 소스 자동수정 기능제공 등, 암호화 설정 및 적용에 필요한 조치를 자동화 하여 암호화로 인한 혼란 없이 편리하고 안전하게 SAP를 운영할 수 있습니다. 또한, 암호화 전체 과정과 암호화로 인한 변경내용을 기록/모니터링하고 SAP Upgrade시 변경내용 재활성화 기능 등이 자동화 되어있는 CubeOne™은 Upgrade시나 추가 암호화시에 최소의 컨설팅을 통하거나 사용자가 GUI를 통해 직접 수행할 수 있어 비용절감 효과가 매우 큽니다.

암호화 적용 시 SAP Upgrade 보장

기능 : SAP 시스템의 Standard 구조를 유지하여 SAP 버전 업그레이드 시 암호화 모니터링 기능을 이용하여 과거 적용내역을 쉽게 활성화 할 수 있습니다.
이점 : 암호화 적용 후에도 자유로운 SAP Upgrade 및 Patch 가능

운영 안정성 보장

기능 : CubeOne™ AI 서버의 네트워크 또는 시스템 장애로 인하여 암복호화 서비스 중단 시에도 SAP의 서비스는 정상적으로 진행 되며, 암호화가 미 적용된 Data는 추후 암호화 조치를 수행 합니다.
이점 : SAP 운영 안정성 확보

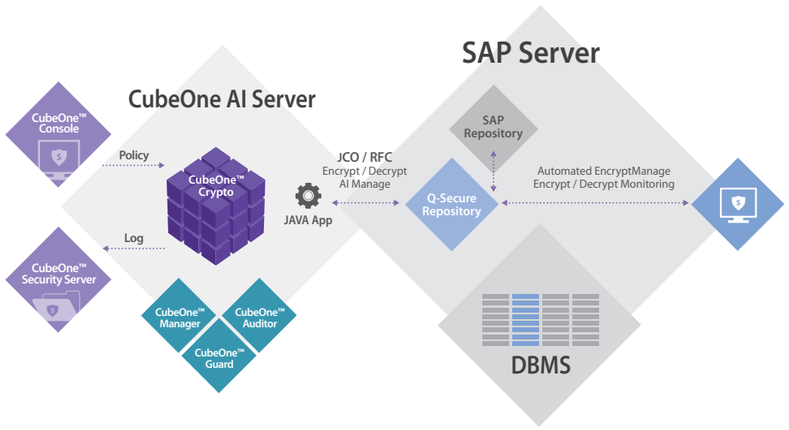
보안성 확보

기능 : 국정원에서 인증된 안전한 암,복호화 알고리즘 및 권한 통제 수준 확보, 안전한 암,복호화 키 관리체계 확보
이점 : 관련 법규 요구사항 충족

TCO 절감

기능 : 암호화 대상 도메인의 자동 반영 (설정방식) 및 암호화 해당 도메인 암,복호화 Function 자동생성 기능, 초기 마이그레이션 프로그램 자동생성 등
이점 : 도입 프로젝트 기간단축을 통한 비용 절감

Architecture



Key Features

CubeOne™ For SAP

SAP Integrate GUI

■ 암호화 GUI 메뉴

■ 암호화 설정

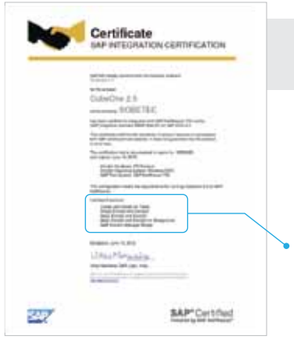
■ 암호화 설정 모니터링

■ USER-EXIT 설정

■ 암/복호화 일괄 마이그레이션

■ 유틸리티-CBO 조정

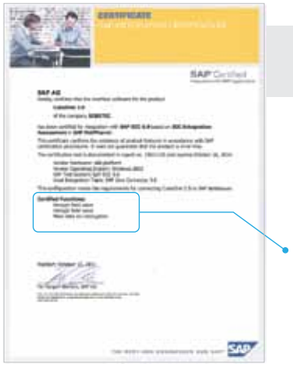
SAP 인증 (2-Level 인증)



Add-On 제품인증 (업계유일)
인증명 : ICC ABAP ADD-ONS Certificate

Certificate
SAP Integration Certification

Certified Functions :
Create and Delete A / I Table
Single Encrypt and Decrypt
Mass Encrypt and Decrypt
Mass Encrypt and Decrypt for Background
SAP Solution Manager Ready



연동 인증
인증명 : ICC Integration Assessment Certificate

Certificate
SAP Integration Certification

Certified Functions :
Encrypt field value
Decrypt field value
Mass data en-/decryption