

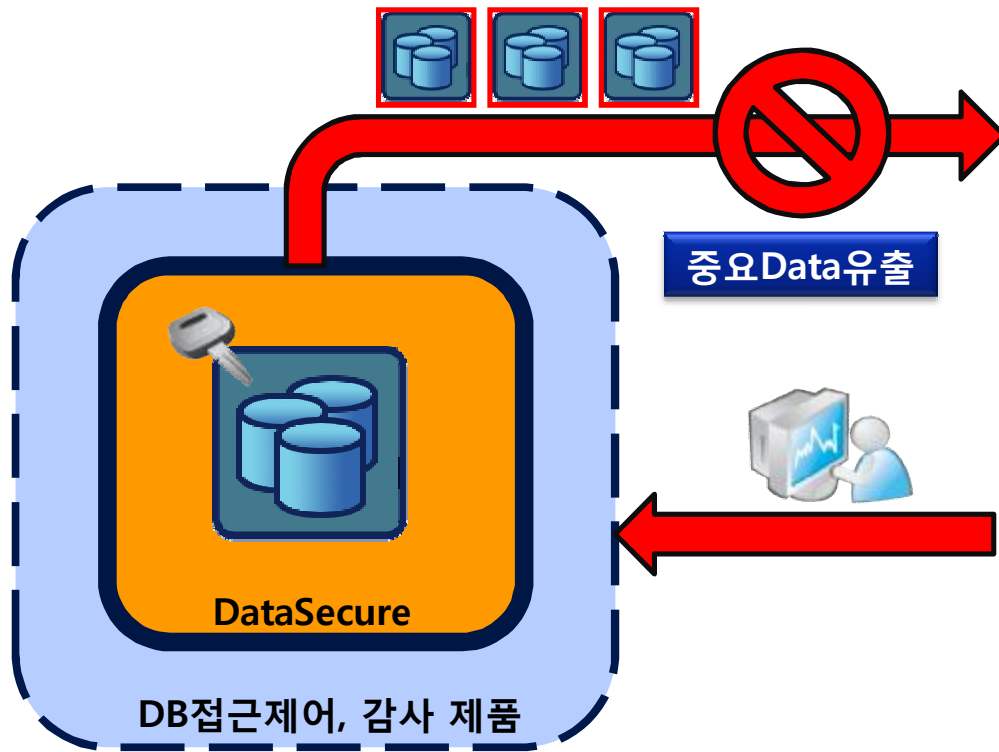


DataSecure™ Platform

최적의 데이터베이스, 파일 암호화 솔루션



● DB보안 제품의 종류



- DB암호화 제품(DataSecure)
 - 중요Data, 기밀Data의 암호화
 - 외부 또는 내부자에 의한 중요 Data의 유출피해 봉쇄
 - 유출된 Data는 암호화 키가 없으면 복호화 불가
- DB접근제어, 감사제품
 - 중요Data의 접근을 감시, 모니터링의 주 기능
 - 외부 또는 내부자에 의한 중요 Data의 유출 감시



● DB암호화의 필요성

- 정보유출은 언제 어디서나 발생할 수 있으며, 최근 중요 DB유출사고가 급증하면서 사회문제화 됨
- 유출경로의 차단 및 감시가 중요하지만 네트워크 경로상의 100%의 보안은 현실적으로 어려움
- PCI DSS를 비롯한 각종 법규 준수
(Payment Card Industry Data Security Standards)
- 기업 또는 브랜드 이미지 손실의 예방

*** 침해사고 발생시에도 정보유출을 방지하고, DB유출로 인한 피해를 원천 봉쇄하기 위해서는 최상위 레벨 또는 최종 단의 Data보안으로써 DB 암호화가 필수입니다**

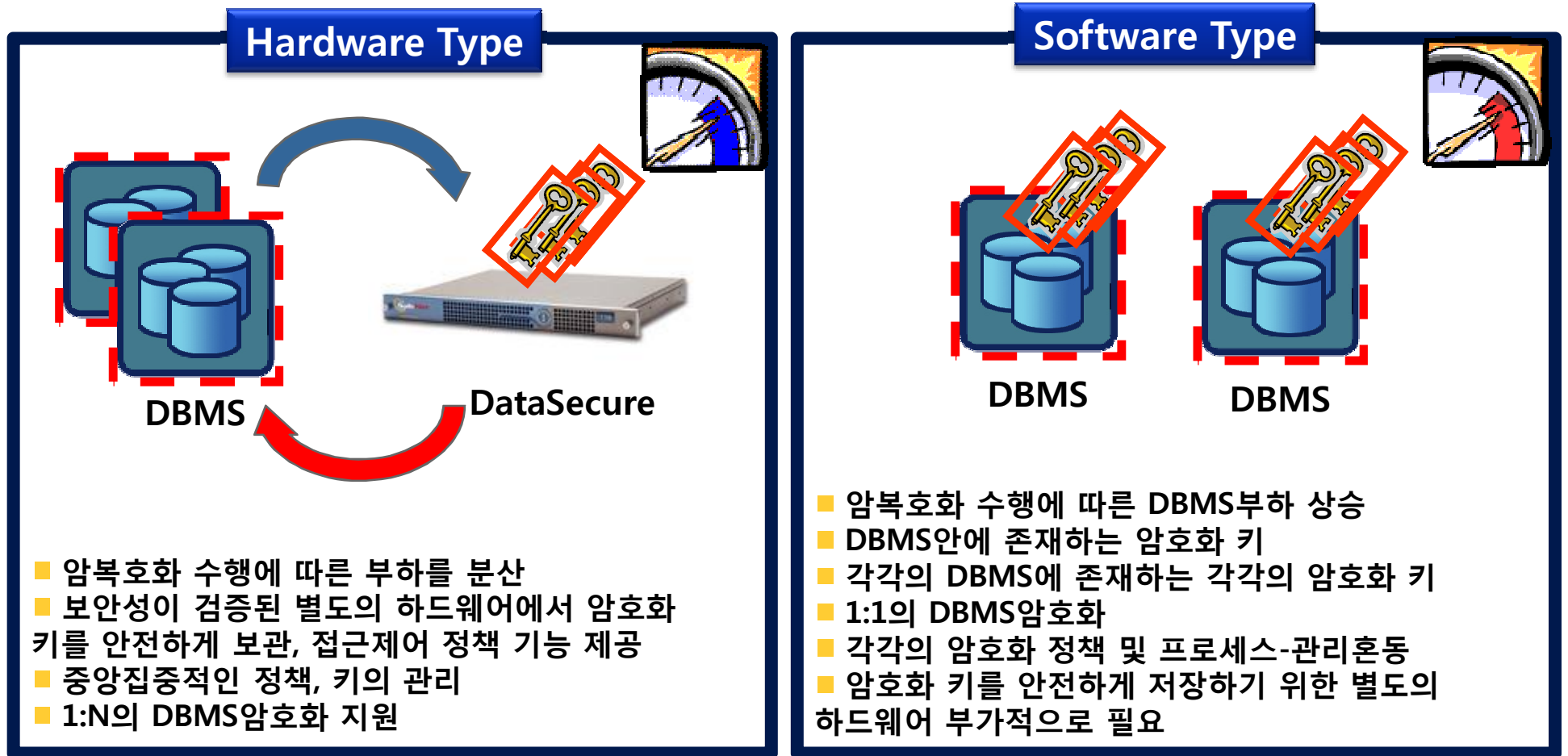


● 암호화 관련 기타 국내 개인정보보호 관련법규

법령/고시/표준	조항	내용
“정보통신망 이용촉진 및 정보 보호 등에 관한 법률”에 의한 대통령 및 방통위 고시 (개인정보의 기술적,관리적 보호조치 기준)	대통령령 제20756호 제 15조 (개인정보의 보호조치)	① 법 제28조에 따른 개인정보의 안전성 확보에 필요한 기술적, 관리적 조치는 다음 각 호와 같다. 4. 개인정보를 안전하게 저장, 전송할 수 있는 암호화 기술 등을 이용한 보안조치
	방통위 고시 제2008-3호 제5조 1~2항 (개인정보의 암호화)	① 정보통신서비스제공자 등은 패스워드, 생체정보 등 본인임을 인증하는 정보에 대해서는 복호되지 아니하도록 일방향 암호화 하여 저장한다. ③ 정보통신서비스제공자등은 이용자의 개인정보를 PC에 저장할 때에는 이를 암호화 해야 한다
공공기관의 개인정보보호에 관한 법률	제9조 (개인정보의 안정성 확보)	② 공공기관의 장은 개인정보 처리에 관한 사무를 다른 공공기관 또는 관련 전문기관에 위탁할 수 있으며, 이 경우 개인정보가 분실, 도난, 유출, 변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 조치를 취하여야 한다
	행정정보 데이터베이스의 보안관리 기준 제8장, 제40조	① 보안담당자는 제33조 제1항의 보안 1등급 및 보안 2등급 이외의 행정정보에 대하여 보안이 필요하다고 판단한 정보에 대하여 암호화 하여 관리할 수 있다.
금감원 전자금융거래 보안종합 대책		VAN사 저장 정보 중 거래일로부터 3개월이 경과되지 않은 정보는 카드번호를 암호화 하여 저장
PCI DSS	3.4, 3.4.1, 3.5, 3.5.1, 3.5.2	PAN을 암호화 할 것. 암호화 키의 보호 안전한 암호화 키의 관리



● Hardware Type VS Software Type



*** 암호화에 있어서 가장 중요한 것은 암호화 키의 보관과 관리입니다**



● DataSecure Models

DataSecure i116 Model

- 초당 11,000건의 암호호화 성능
- Single Power Supply
- Single Network Interface

DataSecure i426/i430 Model

- 초당 100,000건의 암호호화 성능
- Dual Power Supply
- Dual Network Interface

- 국내외 표준 암호화 알고리즘 지원

3DES, DES, AES, RSA (signatures and encryption), RC4, SHA-1, HMACSHA-1, SEED

- 비대칭Key Size: 512, 1024, 2048

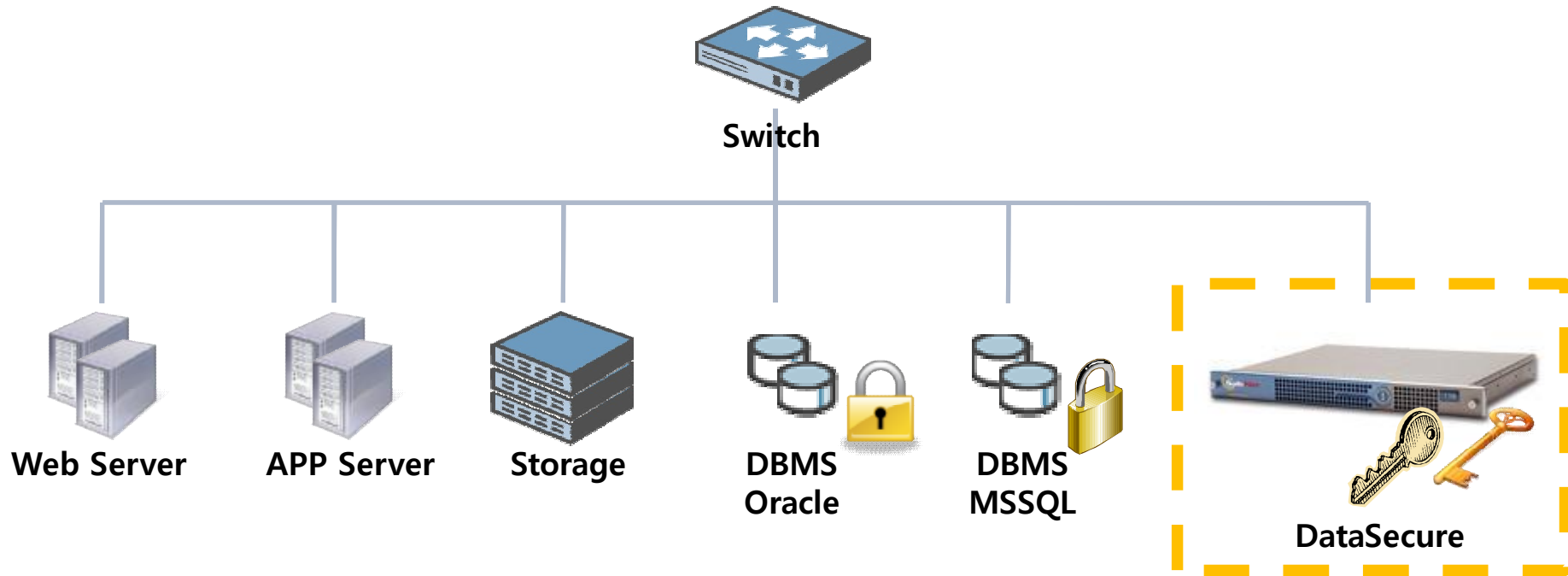
- 대칭Key Size: 40, 56, 128, 168, 192, 256







*** DataSecure는 FIPS 140-2와 CC인증을 취득한 국내 유일의 하드웨어 타입의 Database 암호화 제품입니다**



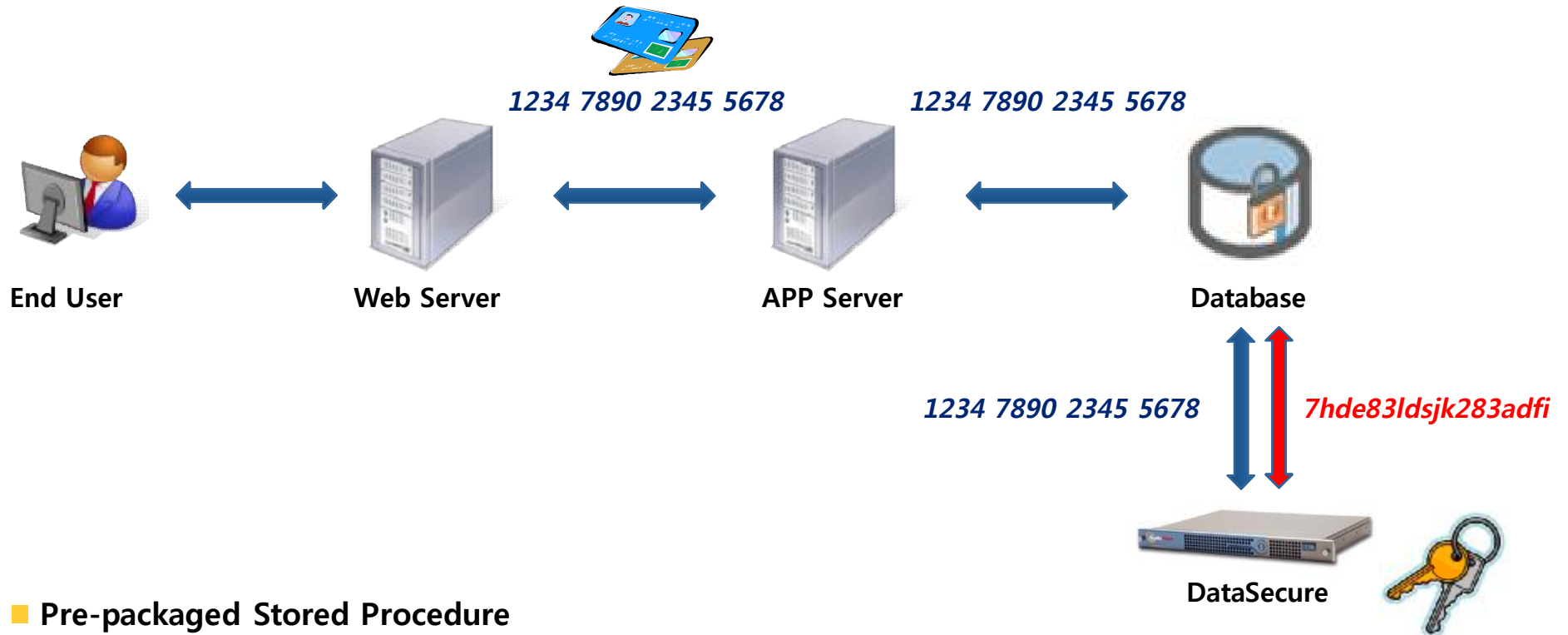
● DataSecure 연동



	AES-256		Oracle DBMS 암호화 Key
	TDES-128		MSSQL DBMS 암호화 Key



● DataSecure 연동방식-DB Integration

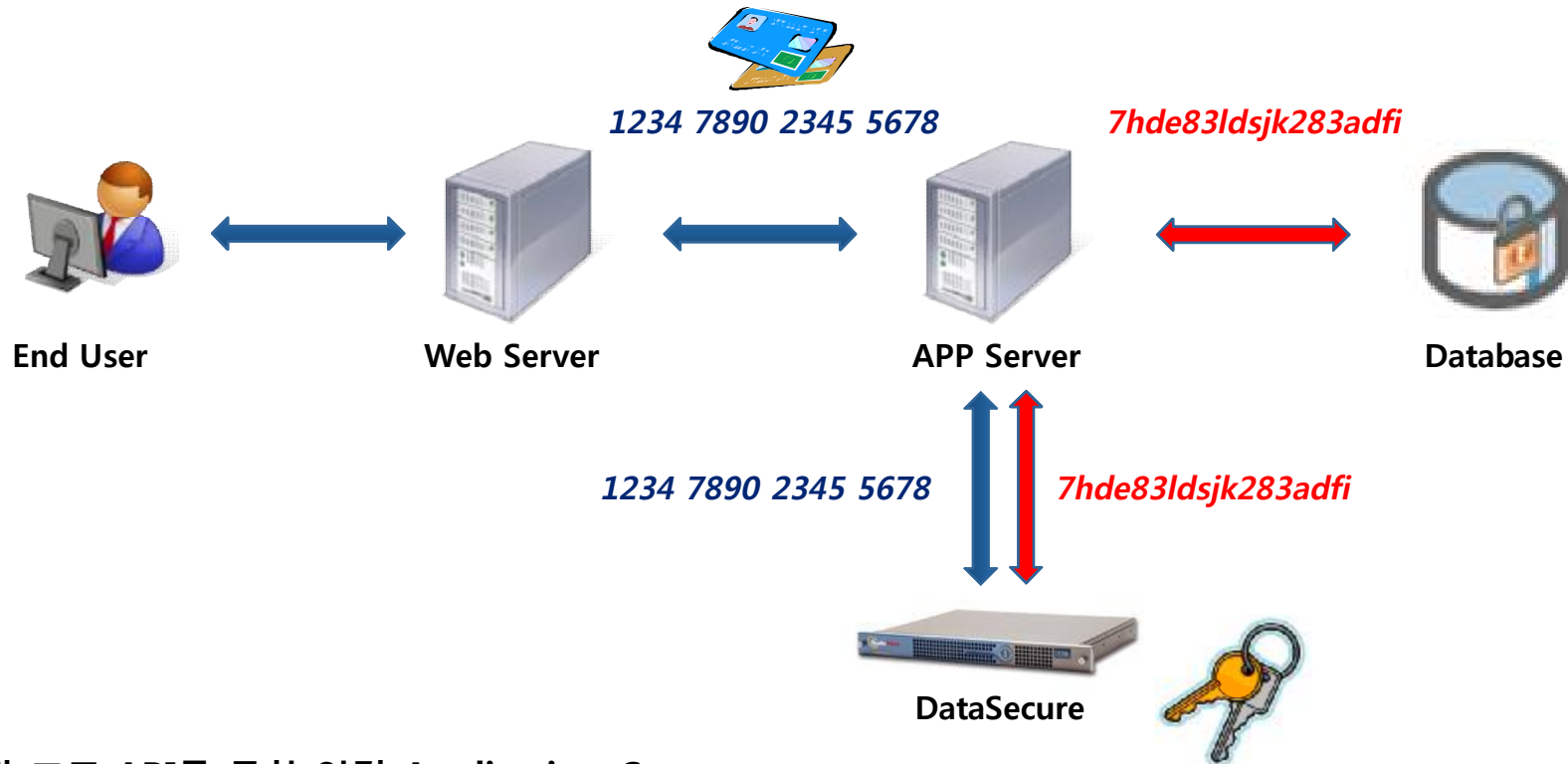


- Pre-packaged Stored Procedure
- 구성이 간결하고 용이함
- DB 및 Application의 수정 없음
- APP 서버의 환경 및 구성 방식에 전혀 영향을 받지 않음
- 사용자에게 투명한 암복호화 기능 제공
- 인증서를 통한 DataSecure장비와 DBMS와의 SSL 설정 가능
- Oracle, MSSQL, DB2, Teradata지원





● DataSecure 연동방식-APP Integration



- 제공된 표준 API를 통한 연결-Application Connectors
Microsoft .NET, Microsoft CAPI, Java (JCE), PKCS#11 (C/C++),
Ingrian CAPI, XML Interface
- 연동 시 APP의 일부 수정과 모듈의 생성이 필요
- String의 부분 암호화 가능 - 성능향상
- APP서버와 DB서버간의 암호화된 데이터(보안성향상)





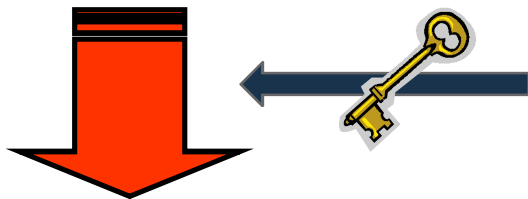
● DataSecure의 컬럼 암호화

CUSTOMER

ID	NAME	JUMIN1	JUMIN2
1	HONG	820127	1234567
2	KIM	790325	2345678
3	LEE	810724	3456789

- 각 Column별 각기 다른 다른 암호화 알고리즘과 암호화 키의 사용
- 암호화 키의 Rotation
- IV(Initial Vector)적용-Column별, Row별
- VIEW와 TRIGGER의 생성

JUMIN2 암호화



Key and Algorithm: AES 256
 Mode: CBC
 Padding: PKCS5Padding
 IV: 112335667788123344567788(Column)

CUSTOMER_NEW

ID	NAME	JUMIN1	JUMIN2	JUMIN2_NEW
1	HONG	820127	NULL	0x00D0EEE6C387235D5B4B1001774A5DCF
2	KIM	790325	NULL	0x00E8AB8E271DEB5FE96CBFAD20CC2454
3	LEE	810724	NULL	0x01CB8A834A9F866D20A058C8DDDC718



● DataSecure Admin

Key and Policy Configuration

NAE Keys

Filtered by where value

Items per page:

Key Name	Owner Username
<input type="radio"/> aes256_key	nae_user
<input type="radio"/> aes_key	nae_user
<input type="radio"/> des_key	nae_user2
<input checked="" type="radio"/> rsa_key	nae_user2

Database Configuration

Database List

Items per page:

Alias	Database Name/SID	Type	Description
<input checked="" type="radio"/> MSSQL2K	bmt2	SQLServer	
<input type="radio"/> Oracle10gr2	orcl	Oracle	

1 - 2 of 2

Add a Database

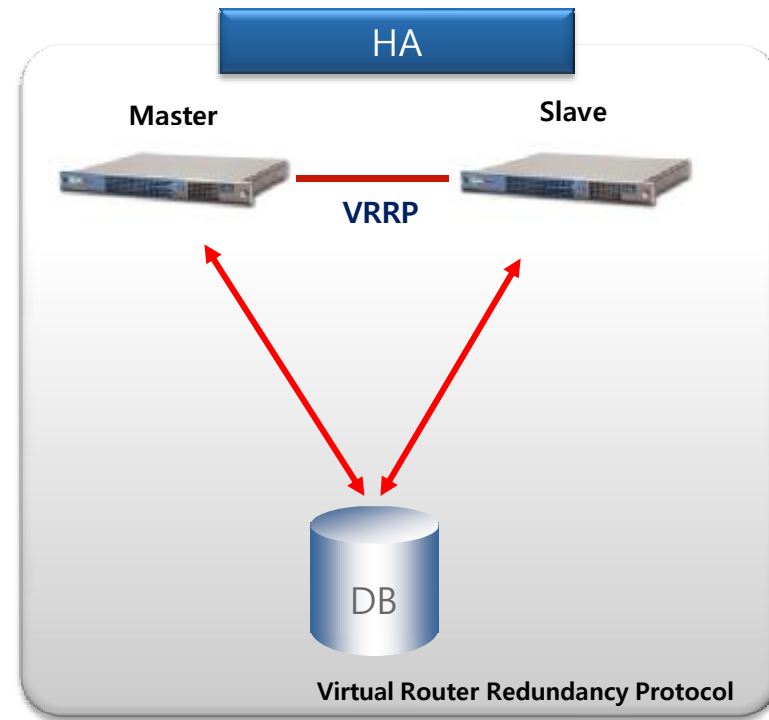
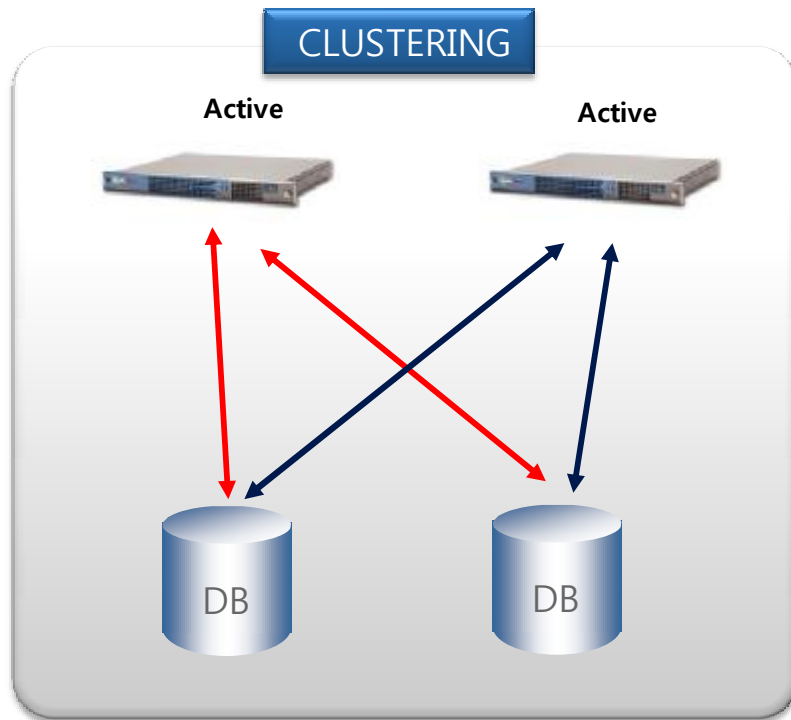
Database Type:

- Oracle 8i, 9i, 10g
- DB2 v8
- SQL Server 2000, 2005
- Teradata

- Web기반의 편리한 관리자 화면 제공
- Clear하고 투명한 암복호화 과정 확인
- 다수의 Database암호화 기능
- 다수의 Database암호화 Key의 중앙집중적인 관리
- 암복호화 관련 상세 log제공



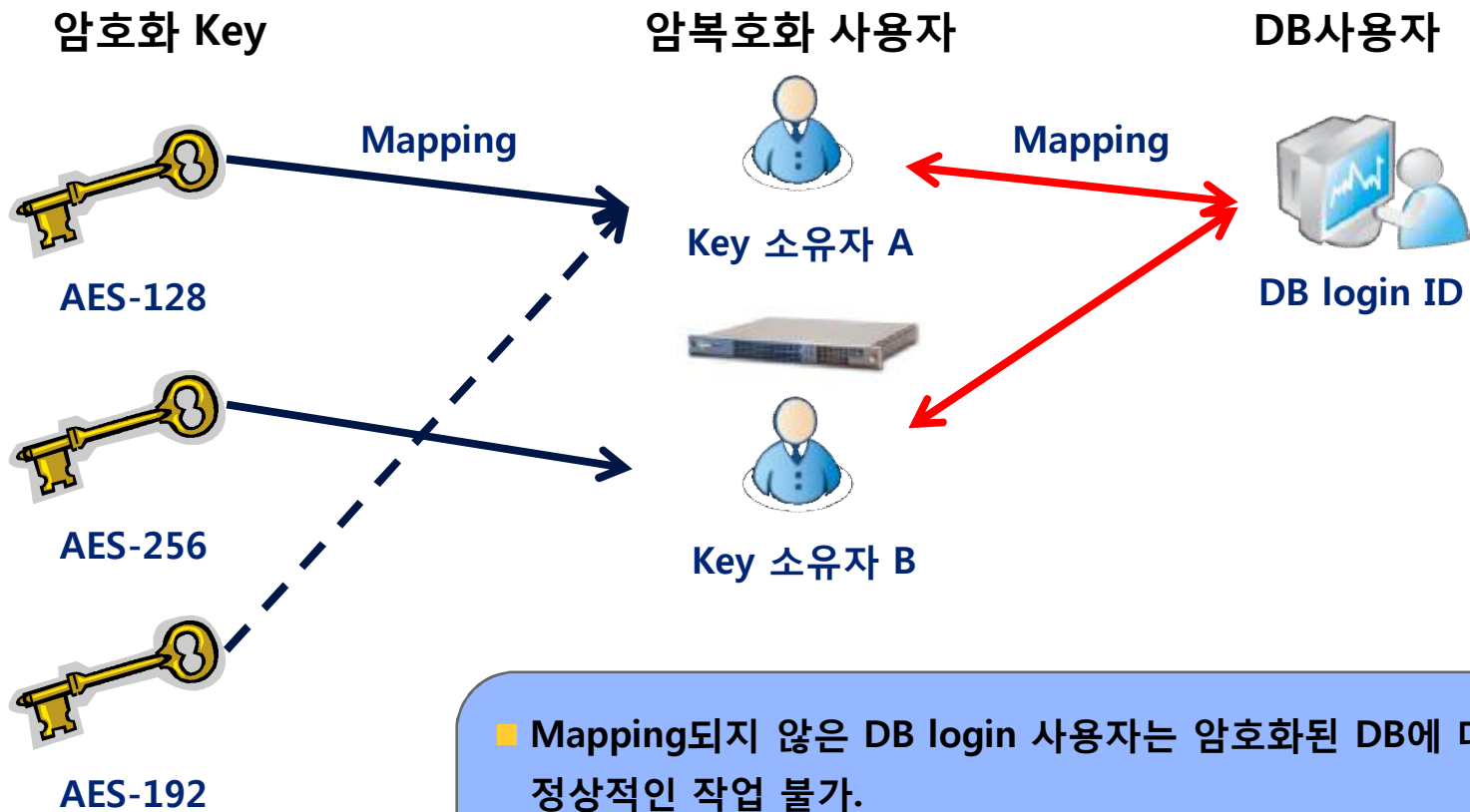
이중화



- Fail-Over와 Load Balancing을 위한 HA 및 Clustering 구성 지원
- 장비 내 두 개의 HDD Disk(RAID-1), Dual CPU, 두 개의 Gigabit 네트워크 카드, Dual Power, 6개의 팬으로 구성(i426 model)



● 사용자 Mapping



- Mapping되지 않은 DB login 사용자는 암호화된 DB에 대해서 정상적인 작업 불가.
- AES-128 키로 data암호화 한 경우, Key Owner A와 맵핑
- AES-256 키로 data암호화 한 경우, Key Owner B와 맵핑
- 한 컬럼에서 각각 다른 Key를 사용 data암호화한 경우



● DataSecure 보안

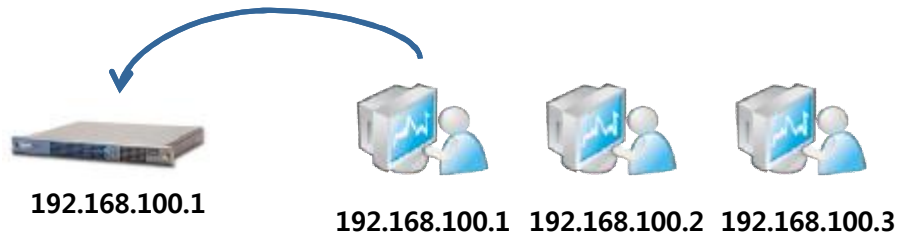
인증서 기반의 접근 제어



암호화 Key의 사용



IP 기반의 접근 제어



관리자 권한분리



중앙집중적 Key관리와
암호화된 Backup Data





● DataSecure 특징점

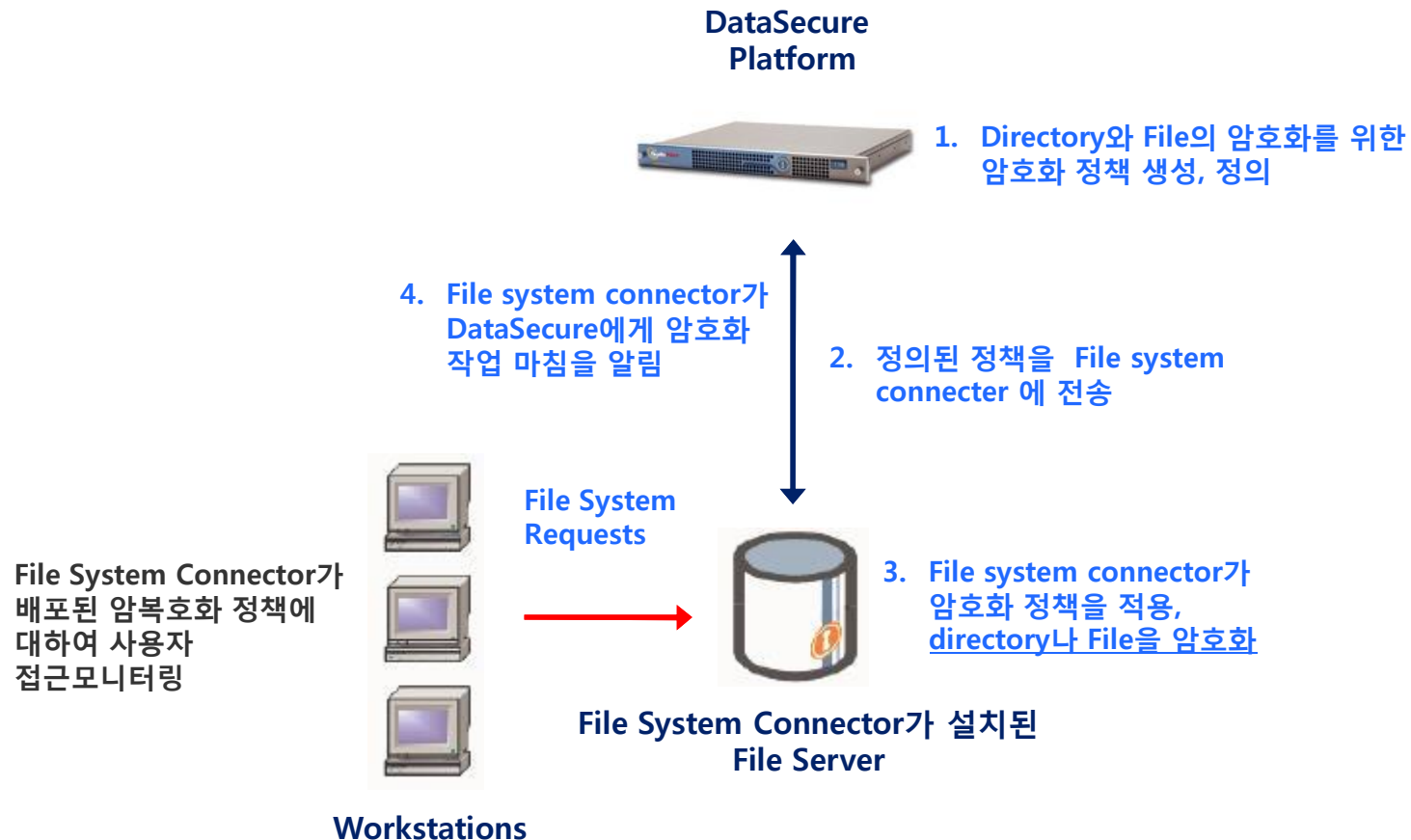
- 다양한 이기종의 O/S환경과 DBMS 지원
 - 다양한 O/S 계열 지원 (Windows, Linux, Solaris, HP, AIX, OS/400)
 - 다양한 DBMS 동시지원 (Oracle, SQL, DB2, Sybase, Informix, Teradata)
- 선택적인 암호화 구성
 - DB 서버 및 APP 서버와 선택적 또는 병합적으로 구성
- Failover와 Load Balancing를 위한 HA및 Clustering구성 가능
- 자체 제공되는 암호화 API을 통한 암복호화 성능 개선방안 제공
 - Encrypt, Decrypt function
- File Server 중요 Data의 암호화 기능(폴더, excel, word, dbf...)
- 1:N의 DBMS암호화 가능

* DataSecure는 국내 유일의 하드웨어타입의 암복호화 제품인 동시에 가장 많은 O/S와 DBMS를 동시에 지원 가능한 제품입니다.



● 파일 암호화 기능

■ DataSecure장비의 File System Tool 과 File Server의 File System Connector로 구성



* 암호화 정책: 암호화를 위해 사용할 키와 암호화를 적용 할 Directory나 File등을 정의

* File System connector는 DataSecure와 통신을 위해 File Server에 설치되는 요소



● DataSecure 파일서버 암호화 특징

- DataSecure의 새로운 암호화 기능(i116, i430)
- MSWord, Excel 등 비구조적인 data의 암호화 가능
- Database file 암호화 가능
- 암복호화를 위한 추가적인 사용자 작업 없이 암복호화 사용
- 백업 수행 시 암호화 된 백업으로 기밀성 보장
- 사용자들에게 투명한 암호화 프로세스 제공
- 기존 data의 downtime이 없는 암호화 수행
- Windows 2003 platform 지원(추후 Unix, Linux지원)



● 국내구축사례





● 해외구축사례





구축사례-Wells Fargo

Company background

- 다양한 금융서비스 제공
- 세계 Rank # 4
- 6000개 이상의 지점
- 146,000명 이상의 직원



Encryption Requirements

- 고객 정보 도난으로 인한 고객정보의 암호화 필요성
 - 200,000명의 고객정보 도난, 약 15-18 million 의 비용 손실발생
- 다양한 이 기종 DBMS환경 지원가능
- 250개 이상의 Database Table
- 10개 Column이 민감한 data로 분류되며 암호화가 필요
- Credit card번호 와 고객 account 정보를 우선적으로 암호화
- 보안상 암호화key는 반드시 software가 아니 hardware에 저장되어야 하는 전제 조건
- 성능저하가 없고 Load Balancing 기능 지원

Solution

- DataSecure를 통한 위의 요구 사항 해결
- 50개의 i221 model(8000tps for Encrypt and Decrypt) 사용
- 100개 이상의 DBMS에 적용
- 보안상 암호화key는 반드시 software가 아니 hardware에 저장되어야 하는 전제 조건



● DataSecure 도입 기대 효과

- 관련법규의 충실한 이행으로 고객 정보가 해킹 및 사기로부터 좀 더 안전하게 보호
- 브랜드 인지도 증대 및 소비자 신뢰도 증가에 따른 매출증대
- 잠재적 손실 최소화에 따른 운용 비용 절감
- 원치 않는 언론 노출에 따른 이미지 실추로부터의 위험 감소
- 기업 신뢰도 증대



“DataSecure DB Encryption Solution”



감사합니다

(주) 한국전자증명원

152-780, 서울 구로구 구로동 191-7 에이스테크노타워8차 710호
솔루션사업부 보안사업팀 류문형 팀장 016-495-6355
솔루션사업부 보안사업팀 한정환 과장 010-3893-5188
TEL:02-2025-7566 / FAX:02-2025-7584

(주) 한국전자증명원은 고객만족을 위해 최선을 다하겠습니다.