

# HANA DB 암호화

## - 개인정보보호법 관점 포함

Digital Transformation / Emerging Tech, SAP KOREA  
March 2017

# Agenda

---

- 개요
- 적용절차
- Summary/부록
- 추가 정보 링크



# SAP HANA Data/Log Volume Encryption

## - 개요

# 개인 정보 암호화

## 적용 대상

- 고유식별정보 : 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호 등
- 비밀번호
- 바이오정보 : 지문, 얼굴, 홍채, 정맥, 음성, 필적 등

## 암호화 적용 범위 및 대상

- 데이터 송/수신 및 저장
- 공공기관, 법인, 단체 및 개인을 포함한 모든 개인정보처리자를 적용 대상으로 한다.

## 데이터 암호화 방식

- 데이터 저장 시 암호화 : 저장소에 저장된 데이터 암호화 – Data Encryption 적용
- 데이터 전송 시 암호화 : 서버와 클라이언트 사이의 보안 – SSL (Secure Sockets Layer)를 적용하여 데이터 암호화 송수신



### 행정안전부 개인정보 암호화 조치 안내서



#### 개인정보처리 시스템 암호화

현재 운영 중이거나 향후 개발 예정인 개인정보처리시스템의 목적 및 환경에 맞게 쉽게 구현이 가능한 암호화 방식을 선택해야 한다.  
**응용프로그램 및 DB 스키마 수정 등을 최소화하고 개발 환경에 맞게 성능을 최대화할 수 있도록 해야 한다.**

# 데이터 암호화 구분

개인정보 암호화 조치 안내서 Ver 1.0 (행안부) 인용

방식	암 · 복호화 모듈 위치	암 · 복호화 요청 위치	주요 내용
응용 프로그램 자체 암호화	어플리케이션 서버	응용 프로그램	<ul style="list-style-type: none"> <li>암 · 복호화 모듈이 API 라이브러리 형태로 각 어플리케이션 서버에 설치되고, 응용 프로그램에서 해당 암 · 복호화 모듈을 호출하는 방식</li> <li>DB 서버에 영향을 주지 않아 DB 서버의 성능 저하가 적은 편이지만 구축시 응용프로그램 전체 또는 일부 수정 필요</li> <li>기존 API 방식과 유사</li> </ul>
운영체제 암호화	파일 서버	운영체제 (OS)	<ul style="list-style-type: none"> <li>OS에서 발생하는 물리적인 입출력(I/O)을 이용한 암 · 복호화 방식으로 DBMS의 데이터파일 암호화</li> <li>DB 서버의 성능 저하가 상대적으로 적으나 OS, DBMS, 저장장치와의 호환성 검토 필요</li> <li>기존 DB 파일암호화 방식과 유사</li> </ul>

## HANA에 적용 가능한 데이터 암호화

행안부 개인정보 암호화 조치 안내서 기준 HANA에 적용 가능한 Option

- 응용 프로그램 자체 암호화 : 어플리케이션에서 데이터 암호화 후 HANA에 저장, 데이터를 읽을 때 복호화
  - 암호화 적용 시 암/복호화 대상 프로그램을 모두 수정해야 함, 일반 Tool등에 대한 암/복호화가 어려움, 성능저하 최소화
- 운영체제(DBMS) 암호화 : HANA로 데이터 저장 시 암호화하여 저장, 메모리로 데이터 읽을 때 복호화
  - 프로그램 수정 불필요, 성능, 적용, 데이터 사이즈 등 측면에서 우수

# HANA Data Encryption은 안전한가 ?

개인정보 암호화 조치 안내서 Ver 1.0 (행안부) 인용

**안전한 암호 알고리즘**

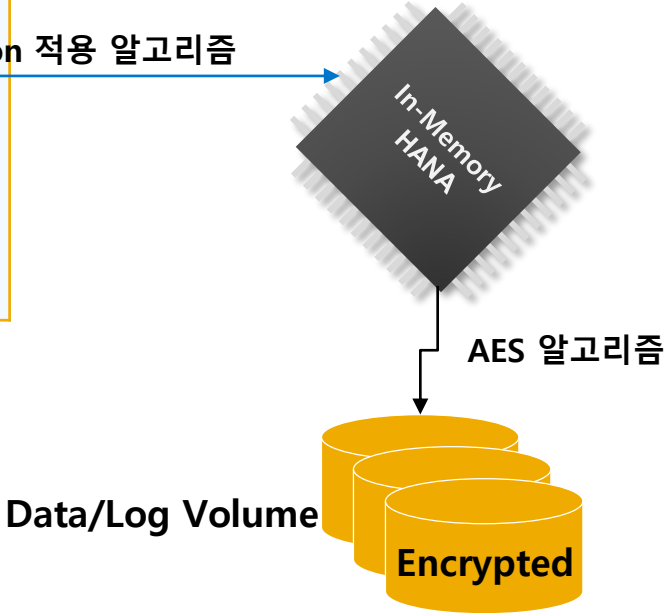
- 개인정보의 안전성 확보조치 기준 제7조제6항의 '안전한 암호알고리즘'이란 국내의 전문기관에서 권고하는 알고리즘을 의미한다.
- 국내외 전문기관(KISA, NIST, ECRYPT, CRYPTREC 등)의 권고를 중심으로 구성하고 있으며 이에 따른 암호 알고리즘은 표와 같다.

구분	알고리즘 명칭
대칭키 암호 알고리즘	SEED
	ARIA-128/192/256
	AES-128/192/256
	Blowfish
	Camelia-128/192/256
	MISTY1
	KASUMI 등

부록) 안전한 알고리즘과 개인정보보호법 참조

- AES(Advanced Encryption Standard) 256-CBC 알고리즘 적용
- HANA는 개인정보 암호화 조치 안내서에서 권고한 안전한 암호알고리즘 적용
- AES 알고리즘은 미국 NIST에서 사용 중

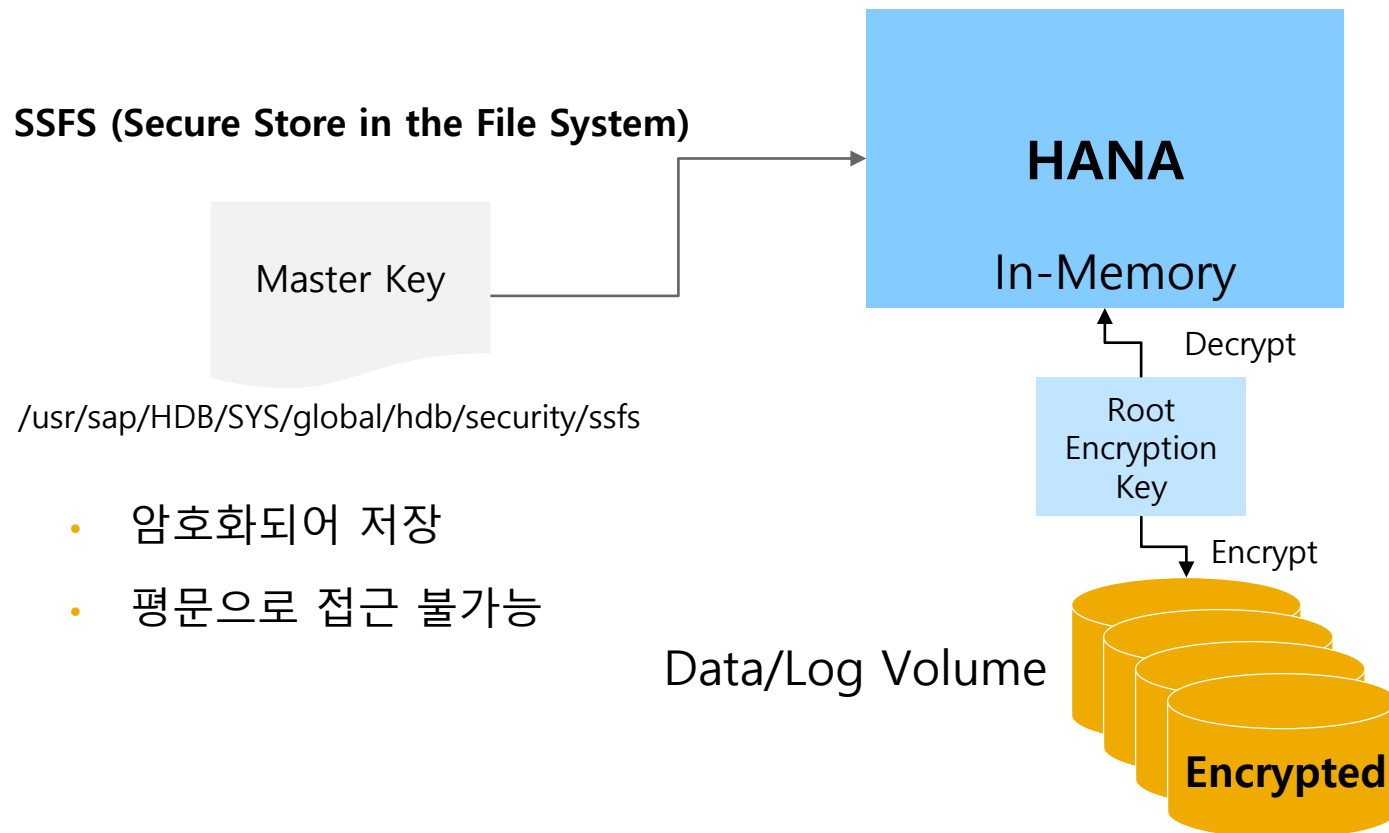
HANA Data Encryption 적용 알고리즘





# HANA Data/Log Volume Encryption 구성

## HANA Data Volume Encryption 구성도



- 암호화되어 저장
- 평문으로 접근 불가능

- AES(Advanced Encryption Standard - 256-CBC 알고리즘 채택
- 미 NIST (National Institute of Standards and Technology)에서 승인된 알고리즘
- 강력한 암호화 – 256 Byte Key
- 프로그램 수정 불필요
- 암호화 적용 간편
- 성능 저하 없음
- 기본 기능 – Free
- 키 2중 관리 – Master Key (SSFS 저장) , Root Encryption Key (HANA DB)
- 키는 암호화되어 접근 불가능

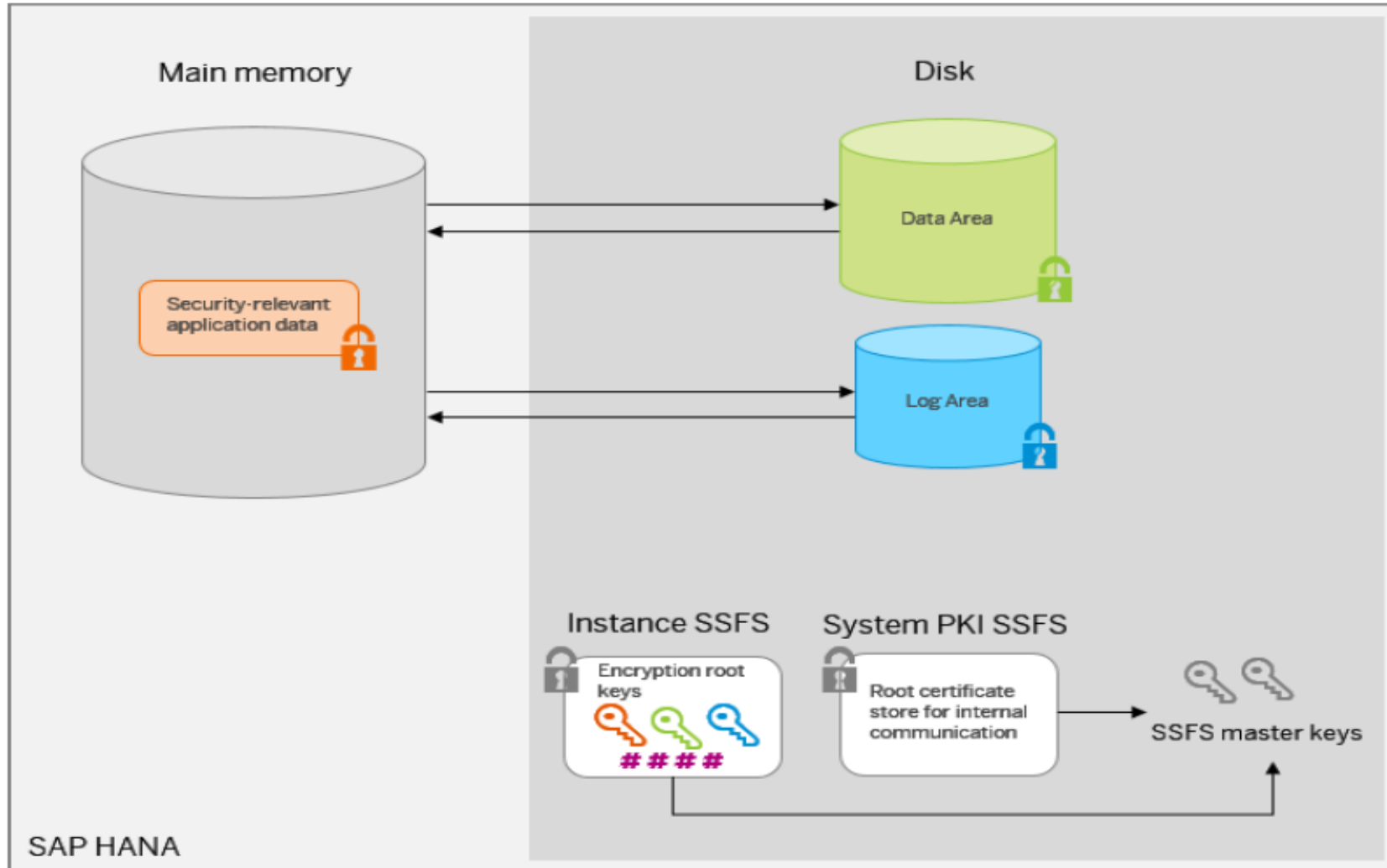


# SAP HANA Data/Log Volume Encryption

## - 적용 절차



# Key 관리

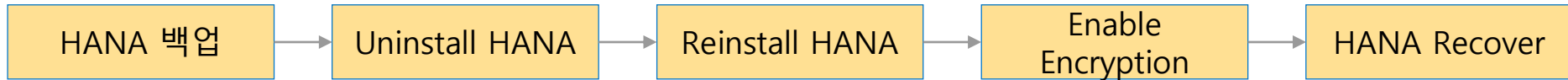


- 패스워드는 암호화되어 안전한 저장소에 저장
- SSFS(Secure Store in the File System)에 Instance SSFS와 System PKI SSFS를 관리
- Instance SSFS는 HANA Data Encryption을 위한 Root Key 보호
- System PKI SSFS는 System- Internal Root certificate(SSL 통신 등)
- 패스워드는 Hash 알고리즘 SHA-256 사용



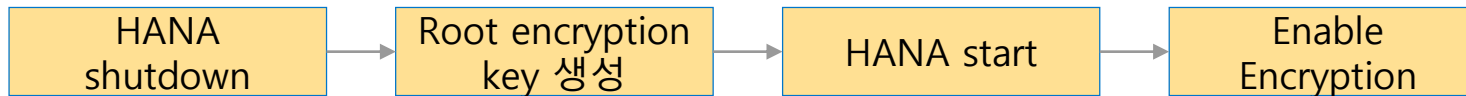
# 적용 절차 개요

## HANA 재설치 후 암호화 적용



- SAP에서 추천하는 방법
- 적용에 따른 Downtime 발생
- 완벽한 암호화

## HANA 재설치 없이 암호화 적용



- 빠른 암호화 적용
- 적용에 따른 Downtime 최소화
- 일부 Savepoint를 수행하지 않은 데이터의 경우 암호화되지 않을 수 있음

# Instance SSFS 마스터 키 수정 (생성)

- H/W 양도 즉시 Instance SSFS와 System PKI SSFS 수정을 추천 (설치 시 자동적으로 생성)
- Root Encryption Key는 SSFS에 안전하게 저장 (protected by file system permissions).

## (1) Instance SSFS의 마스터 키 수정

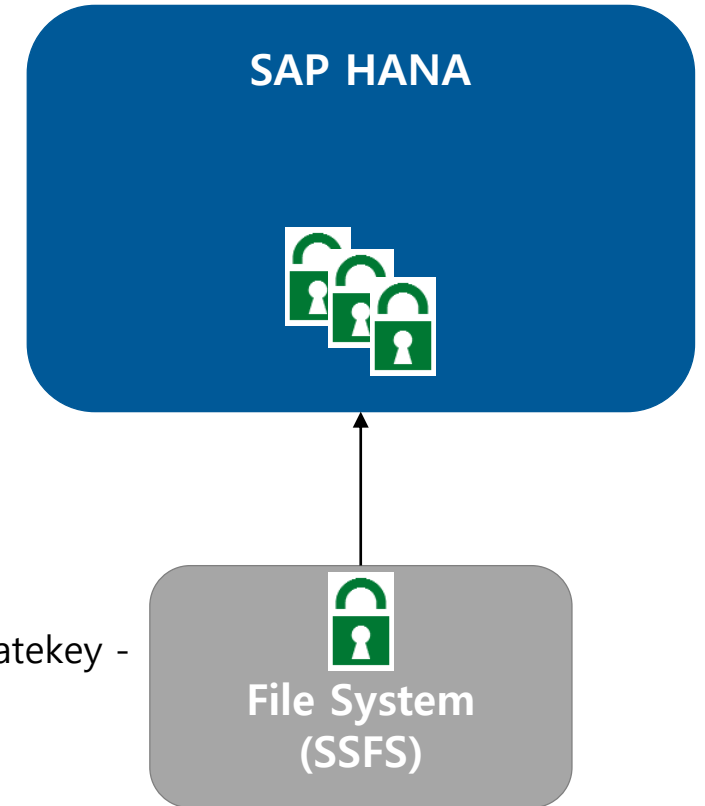
**rsecssfx** command line program을 이용하여 instance SSFS 수정 (part of the SAP HANA installation).

```
export RSEC_SSFS_DATAPATH=/usr/sap/HDB/SYS/global/hdb/security/ssfs
export RSEC_SSFS_KEYPATH=/usr/sap/HDB/SYS/global/hdb/security/ssfs
hdbadm@poc1db2:/usr/sap/HDB/SYS/global/hdb/security/ssfs> rsecssfx changekey $(rsecssfx generatekey -
getPlainValueToConsole)
```

Record Statistics

```
=====
Encrypted and readable           : 3
Encrypted and not readable       : 0
Plaintext                       : 1
Removed by compacting            : 0
```

- HANA System Replication을 구성 및 운영 중 Instance SSFS가 수정되었다면 패스워드 수정을 위해 Secondary HANA를 Restart해야 함



# Encryption Root 키 백업을 위한 비밀번호 세팅

## (2) Encryption Root Key 백업을 위한 비밀번호 세팅

안전한 Encryption Root Keys 백업을 위해 비밀번호가 필요

이 비밀번호는 Instance SSFS에 저장되고 Encryption Root Keys 백업을 위해 생성

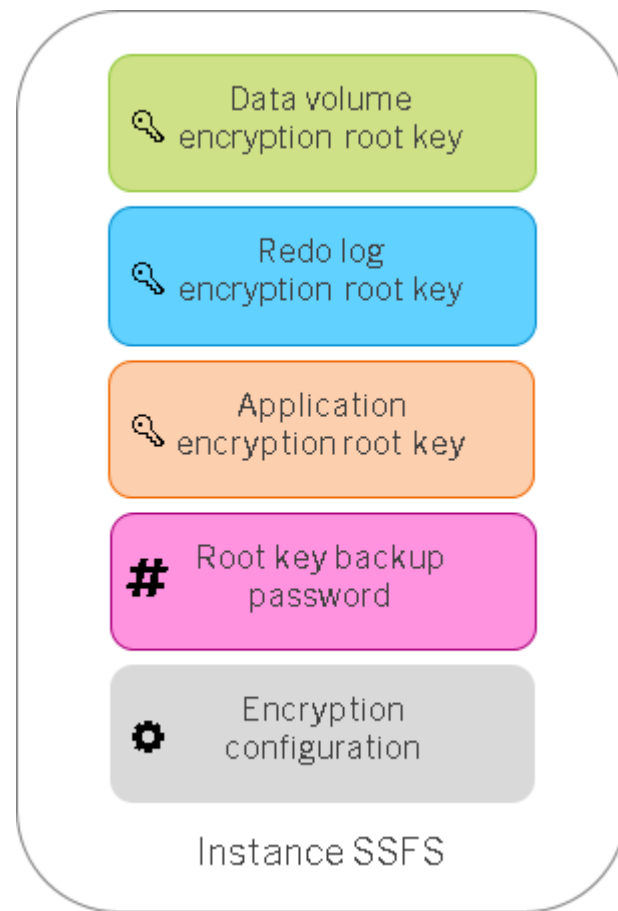
### i. SQL문을 이용하여 비밀번호 세팅

**ALTER SYSTEM SET ENCRYPTION ROOT KEYS BACKUP PASSWORD <passphrase>;**

Root 키 비밀번호가 이미 있다면, Overwrite 됨

### ii. Instance SSFS가 아닌 분리된 안전한 곳에 위 비밀번호 저장

Instance SSFS 복구 전에 비밀번호가 필요함. 만일 비밀번호를 잃어버리면 DB 복구가 불가능



# Encryption Root Key 생성

## (3) 새로운 Encryption Root Keys 생성

### i. Data volume encryption

`ALTER SYSTEM PERSISTENCE ENCRYPTION CREATE NEW ROOT KEY WITHOUT ACTIVATE;`

### ii. Redo log encryption

`ALTER SYSTEM LOG ENCRYPTION CREATE NEW ROOT KEY WITHOUT ACTIVATE;`

### iii. Application encryption

`ALTER SYSTEM APPLICATION ENCRYPTION CREATE NEW ROOT KEY WITHOUT ACTIVATE;`

## ENCRYPTION\_ROOT\_KEYS 시스템 뷰의

Root키 버전/Timestamps 확인

- "DPAPI": Application Encryption
- "PREACTIVE": Root Key는 생성되었으나 아직 WITHOUT ACTIVATE

SQL

Result

select \* from ENCRYPTION\_ROOT\_KEYS

	ROOT_KEY_TYPE	ROOT_KEY_VERSION	CREATE_TIMESTAMP	IS_CONSISTENT	RESET_COUNT	IS_USED	ROOT_KEY_STATUS
1	PERSISTENCE	0	2017. 1. 31 오전 7:30:17.0	TRUE	0	FALSE	ACTIVE
2	PERSISTENCE	1	2017. 1. 31 오전 10:49:18.0	TRUE	0	FALSE	PREACTIVE
3	DPAPI	0	2017. 1. 31 오전 7:30:18.0	TRUE	0	TRUE	ACTIVE
4	DPAPI	1	2017. 1. 31 오전 10:49:35.0	TRUE	0	FALSE	PREACTIVE
5	LOG	0	2017. 1. 31 오전 7:30:19.0	TRUE	0	FALSE	ACTIVE
6	LOG	1	2017. 1. 31 오전 10:49:27.0	TRUE	0	FALSE	PREACTIVE

# 백업 Root Encryption Keys

## (4) Root Encryption Keys 백업

**주의 :** 키를 잃어 버리면 DBMS를 복구할 수 없음

백업을 원하는 Root Encryption Key를 선택할 수 있음

- **hdbnsutil 명령어**

`/usr/sap/<sid>/<HDBinst_no>/exe/hdbnsutil -backupRootKeys <file>.rkb -type='ALL'`

hdbadm@poc1db2:/usr/sap/HDB/SYS/global/hdb/security/ssfs> hdbnsutil -backupRootKeys backup.rkb -type='ALL'

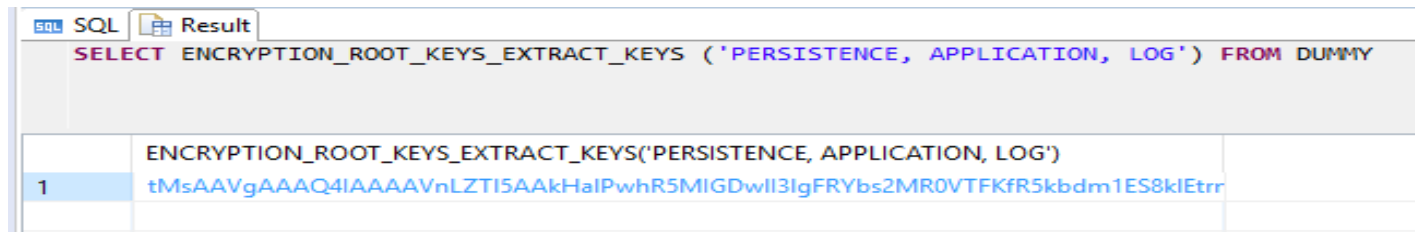
Exporting root keys to /hana/shared/HDB/global/hdb/security/ssfs/backup.rkb

Successfully exported root keys to /hana/shared/HDB/global/hdb/security/ssfs/backup.rkb

done.

- **SQL 명령 (시스템 권한 ENCRYPTION ROOT KEY ADMIN 필요)**

`SELECT ENCRYPTION_ROOT_KEYS_EXTRACT_KEYS ('PERSISTENCE, APPLICATION, LOG') FROM DUMMY;`



SQL	Result
<code>SELECT ENCRYPTION_ROOT_KEYS_EXTRACT_KEYS ('PERSISTENCE, APPLICATION, LOG') FROM DUMMY</code>	
1	<code>tMsAAVgAAQ4IAAAVnLZTI5AAkHalPwhR5MIGDwII3IgFRYbs2MR0VTFKfR5kbdm1ES8klEtrr</code>



# 새로운 Root 키 활성화

## (5) 새로운 root encryption key 활성화

### 1. Data volume encryption

**ALTER SYSTEM PERSISTENCE ENCRYPTION ACTIVATE NEW ROOT KEY;**

### 2. Redo log encryption

**ALTER SYSTEM LOG ENCRYPTION ACTIVATE NEW ROOT KEY;**

### 3. Application encryption

**ALTER SYSTEM APPLICATION ENCRYPTION ACTIVATE NEW ROOT KEY;**

Encryption이 액티브 되면, 새로운 키와 함께 새로운 데이터는 Encryption 됨

- ROOT\_KEY\_STATUS
- 이전 PREACTIVE에서 ACTIVE

- 시스템 뷰에서 Key 및 Encryption 정보 Display

**SELECT \* FROM  
ENCRYPTION\_ROOT\_KEYS;**

SQL

Result

select \* from ENCRYPTION\_ROOT\_KEYS

	ROOT_KEY_TYPE	ROOT_KEY_VERSION	CREATE_TIMESTAMP	IS_CONSISTENT	RESET_COUNT	IS_USED	ROOT_KEY_STATUS
1	PERSISTENCE	0	2017. 1. 31 오전 7:30:17.0	TRUE	0	FALSE	DEACTIVATED
2	PERSISTENCE	1	2017. 1. 31 오전 10:49:18.0	TRUE	0	FALSE	ACTIVE
3	DPAPI	0	2017. 1. 31 오전 7:30:18.0	TRUE	0	FALSE	DEACTIVATED
4	DPAPI	1	2017. 1. 31 오전 10:49:35.0	TRUE	0	TRUE	ACTIVE
5	LOG	0	2017. 1. 31 오전 7:30:19.0	TRUE	0	FALSE	DEACTIVATED
6	LOG	1	2017. 1. 31 오전 10:49:27.0	TRUE	0	FALSE	ACTIVE

# Data Encryption 활성화

## (6) Data Encryption On

### 1. Data Volume Encryption

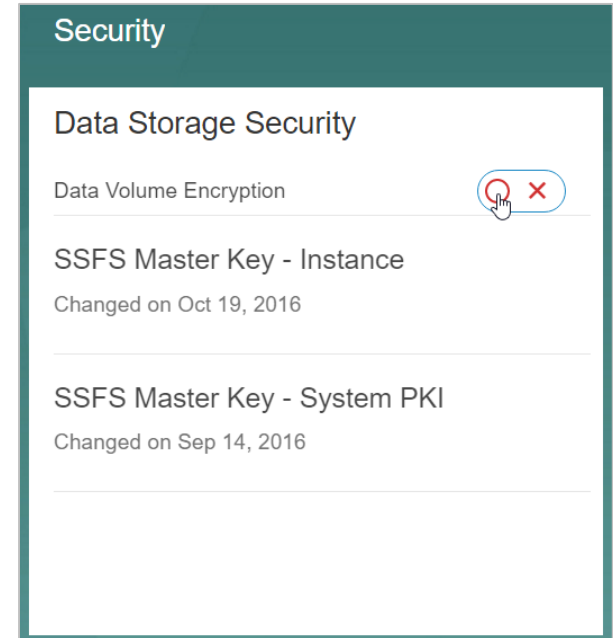
SAP HANA Cockpit를 이용하거나, 또는 SQL문 이용  
**ALTER SYSTEM PERSISTENCE ENCRYPTION ON;**

### 2. Redo Log Encryption

**ALTER SYSTEM LOG ENCRYPTION ON;**

SELECT \* FROM M\_ENCRYPTION\_OVERVIEW;

SAVEPOINT 수행 후 ENCRYPTION  
ALTER SYSTEM SAVEPOINT;



SQL

Result

SELECT \* FROM M\_ENCRYPTION\_OVERVIEW

	SCOPE	IS_ENCRYPTION_ACTIVE	LAST_CHANGE_TIME
1	LOG	TRUE	2017. 1. 31 오후 8:13:31.0
2	PERSISTENCE	TRUE	2017. 1. 31 오후 8:13:21.0

ENCRYPTION 된 정보와 일자

## Data Encryption Off



SAP HANA Studio를 이용하거나, 또는 SQL문 이용  
**ALTER SYSTEM PERSISTENCE ENCRYPTION OFF;**

## ALTER SYSTEM LOG ENCRYPTION OFF;

[illegible]

## ENCRYPTION Disable된 정보와 일자

# Import 백업 Root Keys

## 이전 백업한 Root Key가 필요한 경우 Import

- **Root Key Import Validate**

**`/usr/sap/<sid>/<HDBinst_no>/exe/hdbnsutil -validateRootKeysBackups <file>.rkb`**

```
hdbadm@poc1db2:/usr/sap/HDB/SYS/global/hdb/security/ssfs> hdbnsutil -validateRootKeysBackup ./temp/backup.rkb
```

Please Enter the password:

Successfully validated the backup file /hana/shared/HDB/global/hdb/security/ssfs/temp/backup.rkb  
done.

- **Root Key Import**

**`/usr/sap/<sid>/<HDBinst_no>/exe/hdbnsutil -recoverRootKeys <file>.rkb --password=<password> --type=ALL`**

```
hdbadm@poc1db2:/usr/sap/HDB/SYS/global/hdb/security/ssfs> hdbnsutil -recoverRootKeys ./temp/backup.rkb --password=Sap12345  
--type=ALL
```

Importing root keys from /hana/shared/HDB/global/hdb/security/ssfs/temp/backup.rkb

Checking for inactive nameserver

nameserver poc1db2:30301 not responding.

Successfully imported root keys from /hana/shared/HDB/global/hdb/security/ssfs/temp/backup.rkb  
done.



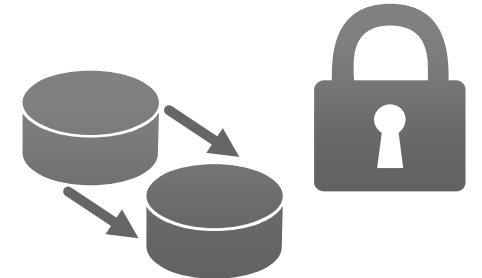
# Summary

# Summary

SAP HANA Data Encryption는 기본 기능으로 Cost-effective하고 적용에 따른 어플리케이션 수정이 불필요하여 다른 솔루션과 대비 됨

- ✓ 비용 효율적 – 라이선스, 적용, 관리 등
- ✓ 간편한 Data Encryption 적용
- ✓ 다른 HANA Security 기능과 상호 보완하여 강력한 보안 제공

**Data Encryption**  
Protect data at rest



**Data Encryption**

**【Q1】** 공공기관이 아닌 일반기업입니다. 개인정보처리시스템의 DBMS (DataBase Management System)에서 제공하는 TDE(Transparent Data Encryption) 방식을 사용한 암호화가 개인정보보호법에 위배될까요?

개인정보의 안전성 확보조치 기준(고시) 제 7조에 따라 고유식별정보 암호화시 안전한 알고리즘을 사용하도록 하고 있습니다. TDE 방식에서 안전한 알고리즘을 사용하여 암호화 한다면 법 위반 사항이 아닙니다.

개인정보 암호화 조치 안내서 Ver 1.0 (행안부) 인용





# 추가 정보

# Need more information on SAP HANA security?

Read the **SAP HANA security** whitepaper!



## SAP HANA Security Whitepaper

SAP HANA SP511  
Andrea Kristen, Holger Mack, Tom Schröder (SAP SE)  
February 2016

<b>3</b>	<b>Scenarios .....</b>	
3.1	3-tier application.....	
3.2	Application on SAP HANA extended application se.....	
3.3	Application on SAP HANA extended application se.....	
3.4	Integrated scenario: reporting on ERP data in SAP.....	
3.5	Integrated scenario: reporting on BW data in SAP.....	
3.6	Data mart: customer-specific analytic reporting on.....	
<b>4</b>	<b>Security functions .....</b>	
4.1	Access control .....	
4.2	Secure configuration and encryption .....	
4.3	Tools and data center integration .....	
<b>5</b>	<b>Security in the software lifecycle .....</b>	<b>14</b>
5.1	Secure development .....	14
5.2	Security patches .....	14

Want to know more? Check out  
the **SAP HANA security page**  
<http://hana.sap.com/security>

**SAP HANA platform Security**

**Manage secure data access and keep your SAP HANA systems protected**

Protecting corporate information is one of the most important topics for you as an SAP HANA customer. You need to meet the increasing business challenges by ensuring...



**Thank you**