

D'Amo DA-MYQ

개발자 교육자료

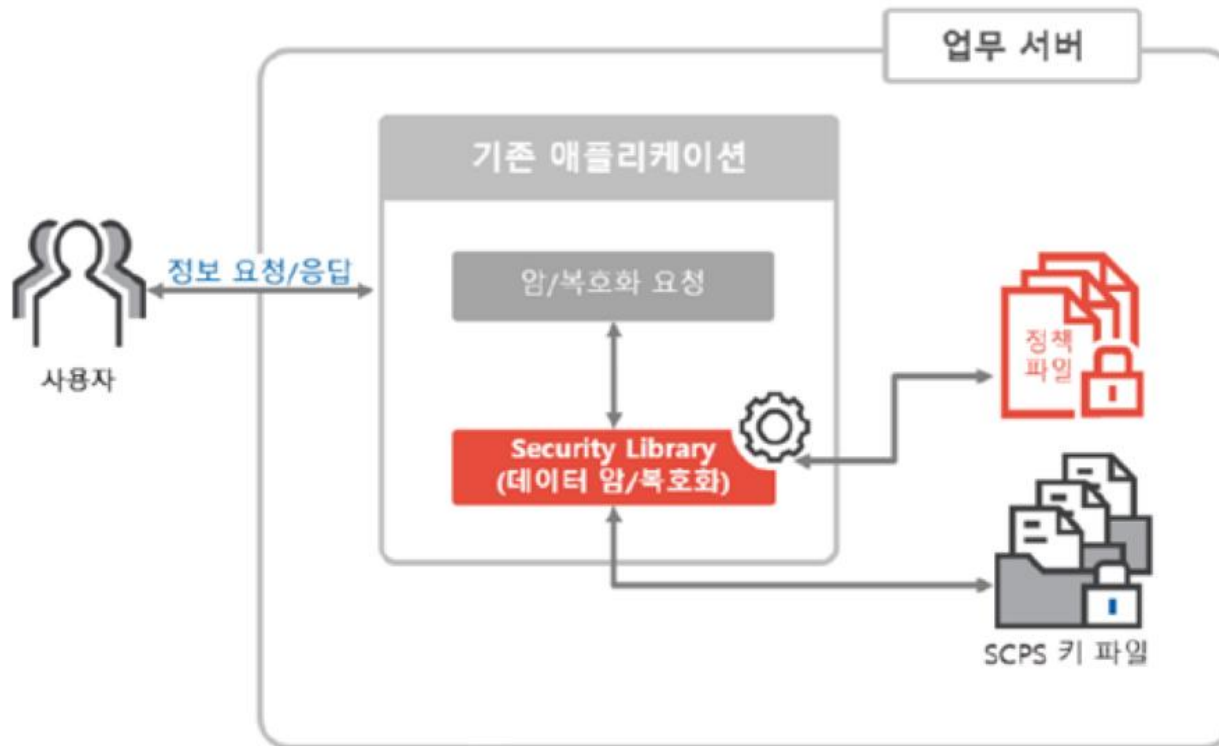
펜타링크(주)

목차

- I. 개요
- II. 동작과정
- III. 파라미터 설명
- IV. 함수

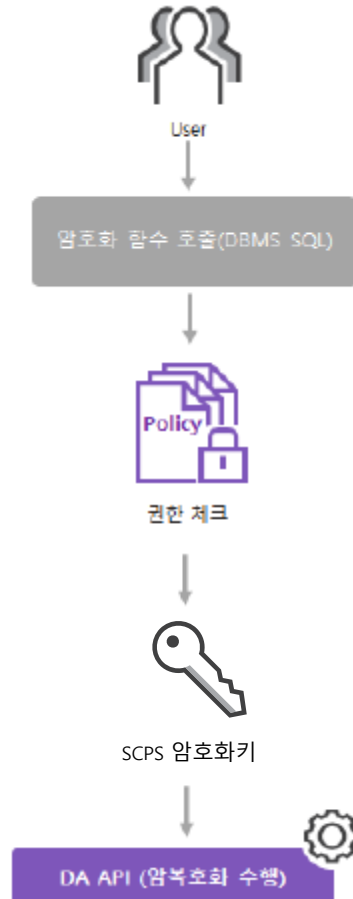
I. 개요

◆ DA-MYQ는 DBMS Application Encryption의 약자로 API 형태의 DB 서버 암호화 제품.



II. 동작과정

◆ DA-MYQ 동작 개념도



Ⅲ. 파라미터 설명

- I_KEY : 암호화/복호화 때 사용하는 암호화 키명
 - ✓ 설정 파일(scpdb_agent.ini)의 [KEYINFO] 중 ALIAS 값
 - ✓ ALIAS는 KEY1로 명시
- I_DATA : 평문(암호화 함수일 경우), 암호문(복호화 함수일 경우)

```
scpdb_agent.ini
[KEYINFO]
KEY1=/dbms_api/key/ARIA256.scps
```

-> scpdb_agent.ini 설정 내용

```
MariaDB [test]> SELECT ENC_B64('KEY1', 'abc') from dual;
+-----+
| ENC_B64('KEY1', 'abc') |
+-----+
| kp0OkVEc7g7Ndvf2SjrSxg== |
+-----+
1 row in set (0.11 sec)

MariaDB [test]> SELECT DEC_B64('KEY1', 'kp0OkVEc7g7Ndvf2SjrSxg==') from dual;
+-----+
| DEC_B64('KEY1', 'kp0OkVEc7g7Ndvf2SjrSxg==') |
+-----+
| abc |
+-----+
1 row in set (0.00 sec)
```

-> 함수 사용예제

IV. DB 함수

◆ 함수리스트

함수명	입력		출력
ENC_STR	I_KEY	IN 문자열	Hex String 암호문
	I_DATA	IN 문자열 (평문)	
ENC_B64	I_KEY	IN 문자열,	Base64 Encording 암호문
	I_DATA	IN 문자열 (평문)	
DEC_STR	I_KEY	IN 문자열,	평문
	I_DATA	IN 문자열 (Hex String 암호문)	
DEC_B64	I_KEY	IN 문자열,	평문
	I_DATA	IN 문자열 (base64 String 암호문)	

IV. DB 함수

◆ 함수리스트

함수명	입력			출력
HASH_STR	I_LOG	IN 숫자,	SHA1 =70	Hex String 해쉬 암호문
			SHA256 =71	
			SHA384 =72	
			SHA512 =73	
			HAS160 =74	
	I_DATA	IN 문자열		
HASH_B64	I_LOG	IN 숫자,	SHA1 =70	Base64 String 해쉬 암호문
			SHA256 =71	
			SHA384 =72	
			SHA512 =73	
			HAS160 =74	
	I_DATA	IN 문자열		
HEXTOB64	I_DATA	IN 문자열 (Hex String 암호문)		base64 Encording 암호문
B64TOHEX	I_DATA	IN 문자열 (base64 Encording 암호문)		Hex String 암호문

IV. DB 함수

◆ 함수리스트

구분		기존 SQL	SQL 수정
양방향	select	SELECT A, B, SSN FROM MEMBER WHERE SSN = '8104191111111'	SELECT A, B, DEC_B64('KEY1',SSN) as SSN FROM MEMBER WHERE SSN = ENC_B64('KEY1','8104191111111')
	insert	INSERT INTO MEMBER (A,B,SSN) VALUES ('1','2','8104191111111')	INSERT INTO MEMBER (A,B,SSN) VALUES ('1','2', ENC_B64('KEY1','8104191111111'))
	update	UPDATE MEMBER SET SSN = '8510191111111' WHERE SSN = '8104191111111'	UPDATE MEMBER SET SSN = ENC_B64('KEY1','8510191111111') WHERE SSN = ENC_B64('KEY1','8104191111111')
단방향	insert	INSERT INTO MEMBER (A,B,PASSWORD) VALUES ('1','2','damopassword')	INSERT INTO MEMBER (A,B,PASSWORD) VALUES ('1','2', HASH_B64('71',damopassword))
	update	UPDATE MEMBER SET PASSWORD = '1234' WHERE NAME = '펜타' AND ID = 'penta'	UPDATE MEMBER SET PASSWORD = HASH_B64('71','1234') WHERE NAME = '펜타' AND ID = 'penta'



KOREA www.pentalink.co.kr