

Настройка HSM для работы KDH с блочными ключами

Инструкция

Версия 3.0.4

История изменений документа

Версия	Дата	Перечень изменений
1.0	12.08.2019	Первоначальная версия

Содержание

1. Введение	4
2. Подключение к HSM через COM/USB.....	5
2.1. Проверка текущего состояния HSM с VARIANT ключами	5
2.2. Порядок настройки “HSM”	5
2.3. Перевод в «Secure Mode»	5
3. Настройка HSM	6
3.1. Установка основных настроек с удалением всех ключей	6
3.2. Загрузка «Keyblock LMK» в ячейку «1».....	7
3.3. Авторизация команд «Keyblock LMK».....	7
3.4. Загрузка «Variant LMK» в ячейку «1» Key change storage table.....	9
3.5. Загрузка «Variant LMK» в ячейку «0»	10
3.6. Авторизация команд «Variant LMK»	10
4. Проверка настройки ячеек HSM.....	11

1. Введение

В данном документе описана настройка “HSM” для перевода “KDH” на хранение и обработку ключей в формате «**keyblock**».

2. Подключение к HSM через COM/USB

Физически подключить “HSM” к компьютеру через COM/USB.

В командной строке компьютера ввести:

```
ssh  
sudo putty /dev/ttyUSB0 -serial -sercfg 9600,8,n,1,N
```

Откроется консоль для выполнения команд на “HSM”.

```
Online-AUTH>
```

2.1. Проверка текущего состояния HSM с VARIANT ключами

В консоли ввести команду «vt», которая показывает какие ключи загружены в “HSM”.

```
Online-AUTH>vt  
  
LMK table:  
  
ID Authorized Scheme Algorithm Status Check Comments  
00 Yes(11H,11C)Variant 3DES(2key) Test 268604 variant lmk  
  
Key change storage table:  
No keys loaded in key change storage  
  
Online-AUTH>
```

2.2. Порядок настройки “HSM”

ВАЖНО!!! Порядок настройки “HSM” крайне важен, т.к. при настройке не в правильном порядке может привести к некорректной работе “HSM”.

1. Установить основные настройки с удалением всех ключей;
2. Загрузить «**Keyblock LMK**» в ячейку «1»;
3. Авторизовать команды «**Keyblock LMK**»;
4. Загрузить «**Variant LMK**» в ячейку «1» Key change storage table;
5. Загрузить «**Variant LMK**» в ячейку «0»;
6. Авторизовать команды «**Variant LMK**».

2.3. Перевод в «Secure Mode»

Перевести “HSM” в «**Secure Mode**» с помощью поворота 2-х физических ключей офицеров безопасности.

В консоли отобразится что “HSM” перешел в «**Secure Mode**».

```
Online-AUTH>HSM now in OFFLINE mode.  
  
Offline-AUTH>HSM now in SECURE mode.  
Master Key loading facilities now available.
```

3. Настройка HSM

3.1. Установка основных настроек с удалением всех ключей

В консоли ввести команду «CS» и ввести следующие значения:

- Default LMK identifier – 1;
- Management LMK identifier – 1;
- Erase LMK's – Y;

ВАЖНО!!! Действие «Erase LMK's – Y», которое удаляет все «LMK» в «HSM», выполняется если на «HSM» нет других «LMK» используемых в других системах, кроме «KDH». Выполняется по согласованию (на усмотрение) офицера безопасности «HSM».

- Enable X9.17 for import – YES.
- Additional padding to disguise key length – YES;
- Key export and import in trusted format only – NO;

```

/dev/ttyUSB0 - PuTTY
Secure-AUTH>cs

Please make a selection. The current setting is in parentheses.
Press ENTER to keep the current setting.
PIN length [4-12](4):
Echo [oN/off](OFF):
Atalla ZMK variant support [oN/off](OFF):
Transaction key scheme: Racal, Australian or None? [R/A/N](N):
User storage key length [S/D/T/V](DOUBLE):
Default LMK identifier [0-1](1): 1
Management LMK identifier [0-1](1): 1

LMKs must be erased before remaining parameters can be set
Erase LMKs? [Y/N]: y

Select clear PINs? [Y/N](YES):
Enable ZMK translate command? [Y/N](YES):
Enable X9.17 for import? [Y/N](YES): YES
Enable X9.17 for export? [Y/N](YES):
Solicitation batch size [1-1024](1024):

Enable Single-DES? [Y/N](NO):
Prevent single-DES keys masquerading
as double or triple-length key? [Y/N](YES):
Making default length for ZMKs: Double
Decimalization table Encrypted/Plaintext [E/P](E):
Enable Decimalization Table Checks? [Y/N](YES):

PIN encryption algorithm [A/B](A):
Use default card issuer password [Y/N](YES):
Authorized State required when importing DES key under RSA key? [Y/N](NO):
Minimum HMAC length in bytes [5-64](10):
Enable PKCS#11 import and export for HMAC keys [Y/N](YES):
Enable ANSI X9.17 import and export for HMAC keys [Y/N](YES):
Enable ZEK/TEK encryption of ASCII data or Binary data or None [A/B/N](B):
Restrict Key Check Values to 6 hex chars [Y/N](YES):
Enable multiple authorized activities [Y/N](YES):
Allow persistent authorized activities [Y/N](YES):
Enable support for variable length PIN offset [Y/N](NO):
Enable weak PIN checking [Y/N](NO):
Enable PIN Block Format 34 as output format
for PIN Translations to ZPK [Y/N](YES):
Enable translation of account number for LMK encrypted PINs [Y/N](NO):
Use HSM clock for date/time validation? [Y/N](YES):
Additional padding to disguise key length? [Y/N](YES): YES
Key export and import in trusted format only? [Y/N](NO): NO
Secure Link password (local) [ENTER = no change]:
Protect MULTOS cipher data checksums? [Y/N](YES):

The next 5 settings affect PCI HSM compliance - see Console Reference Manual:
Card/password authorization (local) [C/P](C):

The following setting is not PCI HSM compliant:
Restrict PIN block usage for PCI HSM compliance? [Y/N](NO):

The following setting is not PCI HSM compliant:
Enforce key type 002 separation for PCI HSM compliance? [Y/N](NO):
Enforce Authorization Time Limit? [Y/N](YES):

The following setting is not PCI HSM compliant:
Enforce Multiple Key Components? [Y/N](NO):
Save SECURITY settings to smartcard? [Y/N]: N
  
```

3.2. Загрузка «Keyblock LMK» в ячейку «1»

Для загрузки необходима карточка с «**Keyblock LMK**» и PIN от неё.
В консоли ввести команду «lk».

```
Secure-AUTH>lk
Enter LMK id [0-1]: 1
Enter comments: keyblock lmk

Load LMK from components

Insert card and enter PIN: ****
Check: 165126

Load more components? [Y/N]: n

LMK Check: 165126
LMK id: 01
LMK key scheme: KeyBlock
LMK algorithm: 3DES(3key)
LMK status: Test
Comments: keyblock lmk

Confirm Details? [Y/N]: y

Use the L0 command to load LMKs into key change storage.

Secure-AUTH>
```

3.3. Авторизация команд «Keyblock LMK»

Для загрузки необходима карточка с «**Keyblock LMK**» и PIN от неё.
В консоли ввести команду «a».
Ввести номер ячейки «1» куда загружен «**Keyblock LMK**».

```
Secure-AUTH>a
Enter LMK id [0-1]: 1

The following activities are authorized for LMK id 01:

admin..console:720 (658 mins remaining)
admin..host:persistent
audit..console:720 (658 mins remaining)
audit..host:persistent
command..console:720 (658 mins remaining)
command..host:persistent
component..console:720 (658 mins remaining)
component..host:persistent
diagnostic..console:720 (658 mins remaining)
diagnostic..host:persistent
export..console:720 (658 mins remaining)
export..host:persistent
generate..console:720 (658 mins remaining)
generate..host:persistent
genprint..console:720 (658 mins remaining)
genprint..host:persistent
import..console:720 (658 mins remaining)
import..host:persistent
misc..console:720 (658 mins remaining)
misc..host:persistent
pin..console:720 (658 mins remaining)
pin..host:persistent

List of authorizable activities:
generate  genprint  component  import
export    pin         audit      admin
diagnostic misc        command

Select category: 
```

Далее авторизуем команды из списка «**List of authorizable activities**». Для этого в строке «**Select category**» указать сокращенное название команды и нажать «**Enter**».

Для следующих шагов нужно нажать кнопку «**Enter**»:

- **Select sub-category or <Return> for all;**
- **Select interface or <Return> for all;**
- **Enter time limit for [сокращенное название команды], or <Return> for permanent;**
- **Console authorization will expire in 720 minutes (12 hours).**

Для шагов «**Make host activity persistent**» и «**Enter additional activities to authorize**» указывается значение «**Y**».

```
List of authorizable activities:
generate  genprint  component  import
export    pin      audit      admin
diagnostic misc     command

Select category: genp

b0        c0        d0        e0
e1        e2        e3        e4
e5        e6        k0        m0
m1        m2        m3        m4
m5        p0        v0        v1
v2        01        11        12
13        21        22        31
32        51        52        71
72        73

Select sub-category or <Return> for all:
host      console

Select interface or <Return> for all:

Enter time limit for genprint, or <Return> for permanent:

Console authorizations will expire in 720 minutes (12 hours).

Make host activity persistent? [Y/N]: y

Enter additional activities to authorize? [Y/N]: y

List of authorizable activities:
generate  genprint  component  import
export    pin      audit      admin
diagnostic misc     command

Select category: █
```

Необходимо повторить действия для каждой из команд.

При авторизации последней команды на шаге «**Enter additional activities to authorize**» нужно указать значение «**N**», после чего вставить карточки 2-х офицеров безопасности и ввести PIN'ы (поочерёдно).

```
First officer:
Insert card and enter PIN: *****

Second officer:
Insert card and enter PIN: *****

The following activities are authorized for LMK id 01:

admin..console:720 (720 mins remaining)
admin..host:persistent
audit..console:720 (720 mins remaining)
audit..host:persistent
command..console:720 (720 mins remaining)
command..host:persistent
component..console:720 (720 mins remaining)
component..host:persistent
diagnostic..console:720 (720 mins remaining)
diagnostic..host:persistent
export..console:720 (720 mins remaining)
export..host:persistent
generate..console:720 (720 mins remaining)
generate..host:persistent
genprint..console:720 (720 mins remaining)
genprint..host:persistent
import..console:720 (720 mins remaining)
import..host:persistent
misc..console:720 (720 mins remaining)
misc..host:persistent
pin..console:720 (720 mins remaining)
pin..host:persistent

Secure-AUTH>
```

3.4. Загрузка «Variant LMK» в ячейку «1» Key change storage table

Для загрузки необходима карточка с «Variant LMK» и PIN от неё.

Загрузить «Variant LMK» в ячейку «1» Key change storage table возможно введя в консоль команду «LO».

```
Secure-AUTH>lo
Enter LMK id [0-1]: 1
Enter comments: variant old lmk
Load old LMK from components
Insert card and enter PIN: *****
Check: 268604
Load more components? [Y/N]: n
LMK Check: 268604
LMK id: 01
LMK key scheme: Variant
LMK algorithm: 3DES(2key)
LMK status: Test
Comments: variant old lmk
Confirm Details? [Y/N]: y
```

3.5. Загрузка «Variant LMK» в ячейку «0»

Для загрузки необходима карточка с «Variant LMK» и PIN от неё.

Для загрузки «Variant LMK» в ячейку «0» нужно в консоли ввести команду «LK».

```
Secure-AUTH>lk
Enter LMK id [0-1]: 0
Enter comments: variant lmk

Load LMK from components

Insert card and enter PIN: ****
```

3.6. Авторизация команд «Variant LMK»

Для загрузки необходима карточка с «Variant LMK» и PIN от неё.

В консоли ввести команду «a».

Ввести номер ячейки «1» куда загружен «Variant LMK».

```
Secure-AUTH>a
Enter LMK id [0-1]: 0

The following activities are authorized for LMK id 00:

admin..console:720 (662 mins remaining)
admin..host:persistent
audit..console:720 (662 mins remaining)
audit..host:persistent
command..console:720 (662 mins remaining)
command..host:persistent
component..console:720 (662 mins remaining)
component..host:persistent
diagnostic..console:720 (662 mins remaining)
diagnostic..host:persistent
export..console:720 (662 mins remaining)
export..host:persistent
generate..console:720 (662 mins remaining)
generate..host:persistent
genprint..console:720 (662 mins remaining)
genprint..host:persistent
import..console:720 (662 mins remaining)
import..host:persistent
misc..console:720 (662 mins remaining)
misc..host:persistent
pin..console:720 (662 mins remaining)
pin..host:persistent

List of authorizable activities:
generate  genprint  component  import
export    pin        audit      admin
diagnostic misc        command

Select category: █
```

Авторизация команд из списка «List of authorizable activities» выполняется по аналогии с авторизацией команд «Keyblock LMK».

4. Проверка настройки ячеек HSM

После выполненной настройки “HSM”, необходимо в консоли ввести команду «vt».

```
Secure-AUTH>vt

LMK table:

ID Authorized Scheme Algorithm Status Check Comments
00 Yes(11H,11C)Variant 3DES(2key) Test 268604 variant lmk
01 Yes(11H,11C)KeyBlock 3DES(3key) Test 165126 keyblock lmk

Key change storage table:

ID Scheme Algorithm Status Check Comments
01 Variant 3DES(2key) Test 268604 variant old lmk
```

Далее возвращаем “HSM” в «Online mode», для этого нужно повернуть и вытащить 2-а физических ключа офицеров безопасности.

Если “HSM” настроен не верно, то при генерации ключей «Keyblock» будет ошибка.

```
com.trsys.tm.kdh.core.exceptions.KdhRuntimeException: HSM response code: 33. LMK key change storage is corrupted
    at com.trsys.tm.kdh.impl.services.SecurityServiceImpl.translateVariantKeyToKeyBlock(SecurityServiceImpl.java:204)
    at com.trsys.tm.kdh.web.service.impl.ZMKServiceImpl.generateKeyBlockZMKFromVariantZMK(ZMKServiceImpl.java:133)
    at com.trsys.tm.kdh.web.controllers.api.APIZMKController.generateKeyBlockZMKFromVariantZMK(APIZMKController.java:
    at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
    at sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:62)
    at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43)
    at java.lang.reflect.Method.invoke(Method.java:498)
    at org.springframework.web.method.support.InvocableHandlerMethod.doInvoke(InvocableHandlerMethod.java:189)
    at org.springframework.web.method.support.InvocableHandlerMethod.invokeForRequest(InvocableHandlerMethod.java:13
    at org.springframework.web.servlet.mvc.method.annotation.ServletInvocableHandlerMethod.invokeAndHandle(ServletIn
    at org.springframework.web.servlet.mvc.method.annotation.RequestMappingHandlerAdapter.invokeHandlerMethod(Request
    at org.springframework.web.servlet.mvc.method.annotation.RequestMappingHandlerAdapter.handleInternal(RequestMapp
    at org.springframework.web.servlet.mvc.method.AbstractHandlerMethodAdapter.handle(AbstractHandlerMethodAdapter.j
    at org.springframework.web.servlet.DispatcherServlet.doDispatch(DispatcherServlet.java:1038)
```