HiPKI SafGuard 1000 Hardware Security Module User Guide

Ver 1.0

Chunghwa Telecom Co., Ltd.
Telecommunication Lab

April, 2008

Table of Contents

1. Introduction

HiPKI SafGuard 1000 Hardware Security Module and Key management program transmit data each other via USB. In this way, we are able to transfer and receive information more efficiently.

There are 3 entities in HiPKI SafGuard 1000 environment; (1) HiPKI SafGuard 1000 hardware security Module; (2) a CA server which requests HiPKI SafGuard 1000 for cryptographic operations; (3) Smartcards;

For security consideration, the Initialization process for HiPKI SafGuard 1000 has to meet the following purposes;

1. There must be a unique relationship between HiPKI SafGuard 1000 and CA server. HiPKI SafGuard 1000 can only provide services to the CA servers which have participated in the initialization process. This CA server can only request HiPKI SafGuard 1000 which has participated in this initialization process to provide cryptographic operation services。

2. HiPKI SafGuard 1000 provides the cryptographic service which depends on the identity of the smartcard; certain identity can only request certain services from HiPKI SafGuard 1000; this is decided while an smartcard is generated, HiPKI SafGuard 1000 will store the services which could be requested by this identity into the hardware.

3. This CA server requests that HiPKI SafGuard 1000 to insert an Smartcard while providing some cryptographic services; in such a way, this HiPKI SafGuard 1000 can ensure that the identity of this Smartcard having the authorization to execute this cryptographic service.

2. Instructions for HiPKI SafGuard 1000 Hardware Secure Module

In order to reach the above goals, we set the following HiPKI SafGuard 1000 Initialization process.

2.1. Initialization Process

2.1.1 Before left the Factory (before HiPKI SafGuard

1000 handed to customers)

While Customers obtain HiPKI SafGuard 1000, they will obtain several empty Smartcards and the files used for installing a CA server; at this moment HiPKI SafGuard 1000 firmware already exists without key stored in it.

2.1.2 After Left the Factory (Customers obtain HiPKI SafGuard 1000)

When HiPKI SafGuard 1000 is handed to a customer, all services related to cryptographic modules are disable. HiPKI SafGuard 1000 state is at Initialization state; customers can return it to the original factory, if it is not at the Initialization state.

Before initializing any service, customers have to execute initialization process (Key Management Program). After HiPKI SafGuard 1000 left the factory, Initialization process can be divided into the following two stages, customers have to execute these stages by order.

2.1.2.1. Generating Smartcards for different identities

The process is as follows: generating MK (Master Key) and storing it to the Smartcard marked as “MASTER 1” and “MASTER 2” . The results that HiPKI SafGuard 1000 generates MK are stored in HiPKI SafGuard 1000 itself and also Smartcards. Once generating MK, HiPKI SafGuard 1000 will store MK forever, until SO needs to restore a new MK or this HiPKI SafGuard 1000 is damaged.. If MK is changed, then all keys related to cryptographic modules have to be regenerated again by using this new MK.

There are 3 Security Officer Key Pair being generated, HiPKI SafGuard 1000 encrypts Private Key using MK, then stored it to the Smartcard marked as Security Officer. On the other hand, HiPKI SafGuard 1000 will store its Public Key in its interior.

While generating HK, Key Pair (RSA key pair with 1024-bit key length) will be stored in HiPKI SafGuard 1000, and the Public Key is transferred back for key management program to use.

After completion of the above activities, HiPKI SafGuard 1000 system state will be configured as Authentication State. Rebooting HiPKI SafGuard 1000 is necessary for entering the Authentication State for normal operations.

2.1.2.2. Generating Application Key

Generating an Application Key (APK) and stored it in HSM and Smartcards used by differently authorized personnel.

System administrators (Secuity Officer) can generate User key pair by their needs and store them to the Smartcard marked as “user” (or “operator”).

System administrators then use HiPKI SafGuard 1000 to generate APKs for different authorized users. The generated APK is a Public-key/Private-key key pair, 3DES or AES, which is stored in the HiPKI SafGuard 1000 and held by different Smartcards. Then they configure the ACL of APK. System administrators may configure system state of HiPKI SafGuard 1000 as Initialization State; however, this activity will erase any key stored in HiPKI SafGuard 1000.

Every Application Key has its corresponding ACL and Status. While generating APK, Status is “0x00”; once ACL is set, Status is enabled.

2.2. Key Usage

The keys generated above and their usages are as figure 2-1.

Type of Key	**Role of Key holder**	**Methods of storing to Smartcard**	**Number of Smartcards**	**Methods of Storing to HSM**
Security Officer Key	Security Officer, System Officer	CA pvk plaintext (signature only)	3	RSA public key
MK	Security Officer, System Administrator	Plaintext, split by 2		Key Splits
User Key	User1, System Operators	CA pvk Plaintext (signature only)	3	RSA public key
AP Key	User2, Key Holders		1	Plaintext

Table 2-1: Key Usage

According to the above analysis, one HiPKI SafGuard 1000 needs at most twelve Smartcard holders, at least four holders, three combinations are as follows.

(1) 12 persons

(2) 9 person (if Security officer and User1 are in the same group)

(3) 3 persons (if Security officer and User1, User2 are in the same group)

Two types of Smartcards are as follows.

(1) First type is for Security officer and User1.

(2) Second type is for User2. Because HiPKI SafGuard 1000 may store more than one key, this type of Smartcard is for saving more memory, and satisfies the separation principle of operation Smartcards and backup Smartcards.

2.3. Environments for Smartcards Control

CA is under a 12-person control, and RA is suitable for a 9-person or 3-person control. Standard ID-based control is feasible.

3. Instructions for Key Management Program

This chapter is for more details about the Authentication State for the hardware HiPKI SafGuard 1000.

3.1. Service Types

When the system is at the Authentication State, there are three types of Authentication Services, namely, Security Officer Service, User Service and Normal Service.

3.1.1 Security Officer Services

When executing the Security Officer Service, security officers need to do **S**ecurity **O**fficer Logon (**SO**Logon). Two Smartcards, called SO Smartcards, are also needed in this activity. This will generate a SessionKey, using this SessionKey for MAC to ensure that one can execute this service. There is only one SessionKey for Security Officer at a time.

- Change smart card PIN
- Export Master Key to smart cards
- Generate Module RSA Key
- Create User smart card

- Generate Application Keys (AP Key)
- Set AP Key ACL
- Backup AP Keys to smart cards
- Erase AP Key
- Erase All AP key
- Erase Back up Smart Card
- Import AP Keys
- Create Security Officers (COs)
- Set Real Time Clock
- Send self-test command to module
- Switch to Initialization state (zeroization of module)
- Write Application data

3.1.2 User Services

When executing the User Service, a User needs to do User Logon (UserLogon). User Logon is mainly for AP Keys; the key management program needs to transfer APK-keyType and APK-keyID to HiPKI SafGuard 1000. There are at least n different User Smartcards according to the Limit_auth_num “n” in ACL of AP Key. HiPKI SafGuard 1000 will also compare User ID in the Smartcard and that in the ACL.

Every UserLogon generates a SessionKey for MAC to ensure whether this service is executable. Every AP Key has only one SessionKey at a time.

- Change smart card PIN
- Use symmetric AP Keys for encryption and decryption
- Use asymmetric AP keys for generating and verifying signatures

3.1.3 Unauthenticated Services:

Unauthenticated Services :

- View Status
- View Serial No. and Version of Firmware
- View AP RSA public key
- View AP key status
- Do Hash function
- Generate random number
- Get Application data
- Verify signature
- Send self-test command to module

4. Setting Up the HiPKI SafGuard 1000

Fig. 4 -1 HiPKI SafGuard 1000 setting up screen

4.1. Initialization of HiPKI SafGuard 1000

Selecting “Start” buttons to initialize the HiPKI SafGuard 1000

4.1.1. Setting the identification name of HiPKI SafGuard 1000

Give an identification name for the HiPKI safGuard 1000.

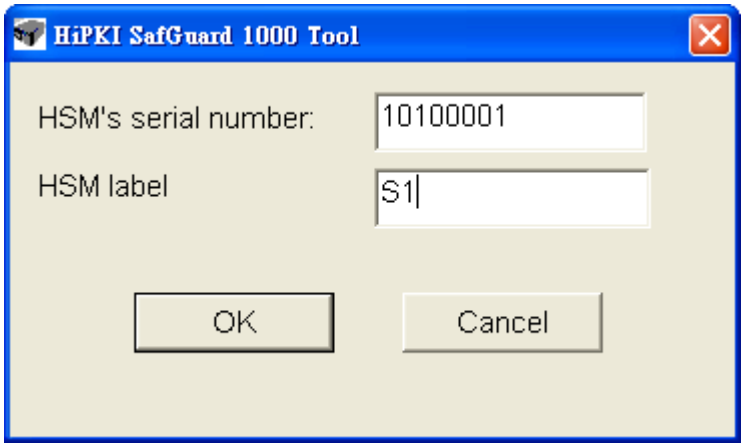


Fig. 4-2 Setting the identification name

4.1.2. Setting up the Real Time Clock of HiPKI SafGuard 1000

The program will show the time of HiPKI SafGuard 1000 “Real Time Clock” on screen , Setting up the HiPKI SafGuard 1000 “Real Time Clock”.

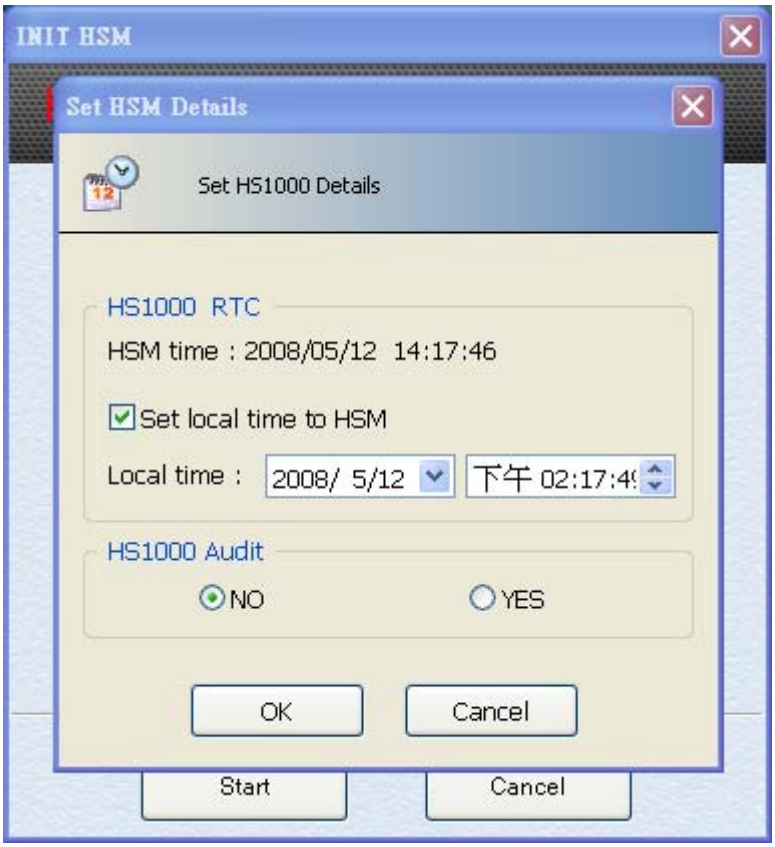


Fig. 4-3 Setting upHiPKI SafGuard 1000 Real Time Clock

4.1.3. Instialitation of Master Key

4.1.4.1. Produce Master Key

Two Backup Master IC card are required to produce Master Key.

Fig. 4-4 Generate Master Key

Push the “Start” botton ， start

Fig. 4-5 Insert the first Master Key IC card

Fig. 4-6 Insert the second Master Key IC card

4.1.4.2. Impose Master Key

Two Backup Master IC card are required to impose the Master Key。

Fig. 4-7 Import Master Key

Fig. 4-8 Insert the first Master Key IC card

Fig. 4-9 Insert the second Master Key IC card

4.1.4. Installing Security Officer Key

4.1.5.1. Produce Security Officer Key

Three **S**ecurity **O**ffices are required to produce Security Officer Keys.

4.1.5.2. Impose Security Officer Key

If selecting impose Security Officer Keys，the key-pair of SO IC card needed to be encoded by the HiPKI SafGuard 1000 MK such that the SOLogon can be used.

Fig. 4-10 Produce、Impose Security Officer Key

4.1.5. Produce the Key-Pair of HiPKI SafGuard 1000

The Key-Pair of HiPKI SafGuard 1000 are required for the usage of UserLogon and SOLogon.

Fig. 4-11 Produce HiPKI SafGuard 1000 Key-Pair

4.1.6. Complete HiPKI SafGuard 1000 initialization

(1) If previous steps all complete without any error, the initialization can be completed

Fig. 4-12 Initialization complete

If there is any error or the button “Cancle” was pressed, the initialization will be stop. If you want to initialiaze HiPKI SafGuard 1000 again, you need to go step 1 .

4.2. Key Management functions

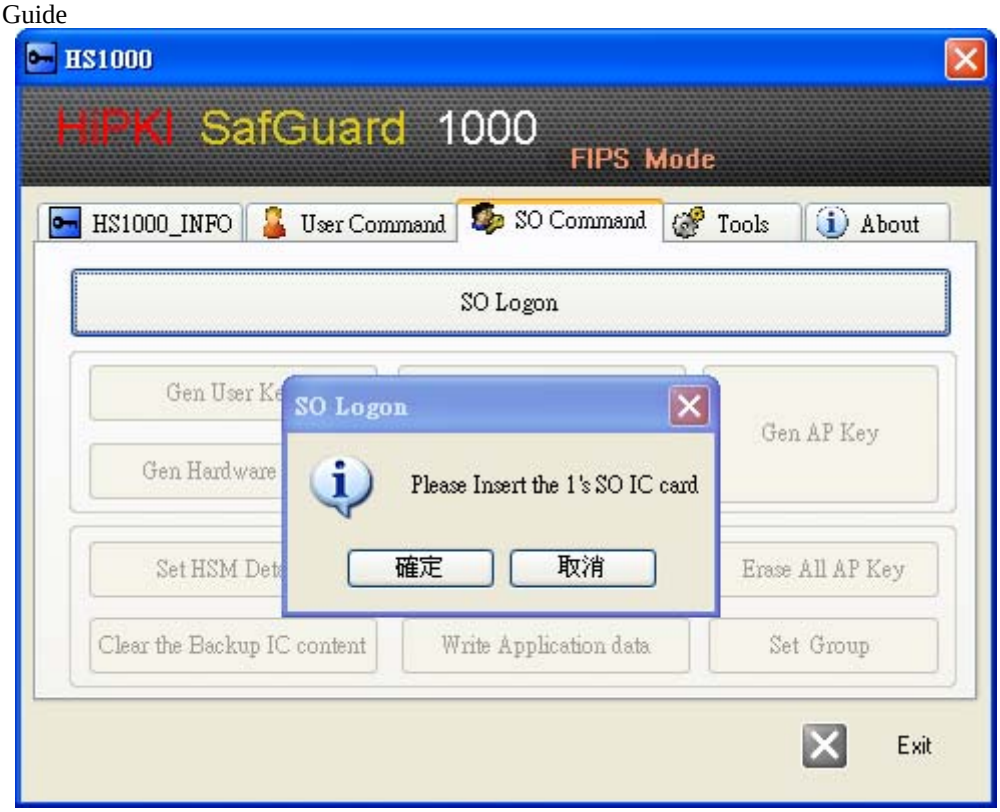
Two Security Officers are required to generate key pairs.

Selecting Security Officr command on the key management screen.

Fig. 4-13 Selecting Security Officer button

4.2.1. Security Officer Logon

(1) To Logon Security Officer, Security Office will be required to insert his/her IC card。


HS1000
HiPKI SafGuard 1000
FIPS Mode
HS1000_INFO
User Command
SO Command
Tools
About
SO Logon
Gen User Ke
Gen Hardware
Gen AP Key
Set HSM Det
Erase All AP Key
Clear the Backup IC content
Write Application data
Set Group
Exit
SO Logon
Please Insert the 1's SO IC card
確定
取消

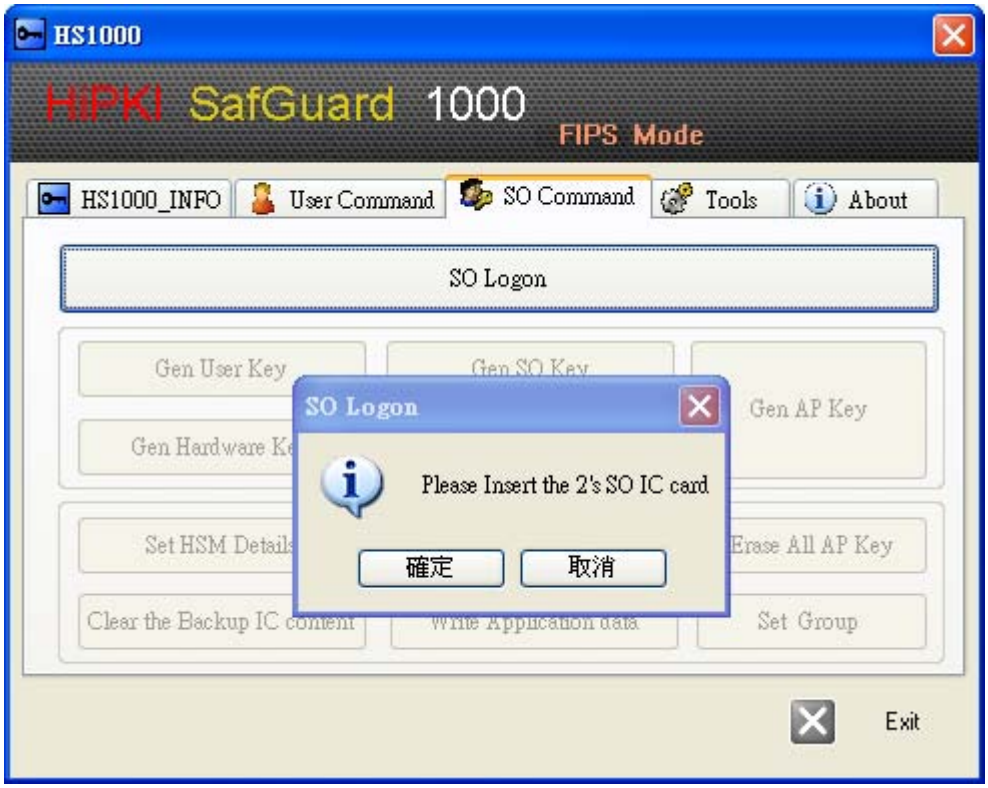

HS1000
HiPKI SafGuard 1000
FIPS Mode
HS1000_INFO
User Command
SO Command
Tools
About
SO Logon
Gen User Key
Gen SO Key
Gen AP Key
Gen Hardware Ke
Set HSM Details
Erase All AP Key
Clear the Backup IC content
Write Application data
Set Group
Exit
SO Logon
Please Insert the 2's SO IC card
確定
取消

Fig.4-14 Message of Security Officer Logon

(2) After SO Logon successfully, the window of selecting will show up as following

Fig. 4-15. The window of Security Officer function

4.2.2. Produce User Key

Ther are two ways to produce User Key』:

4.2.2.1. Produce User Key

【Produce】, a user(system operator) is required to generate a new key-pair.

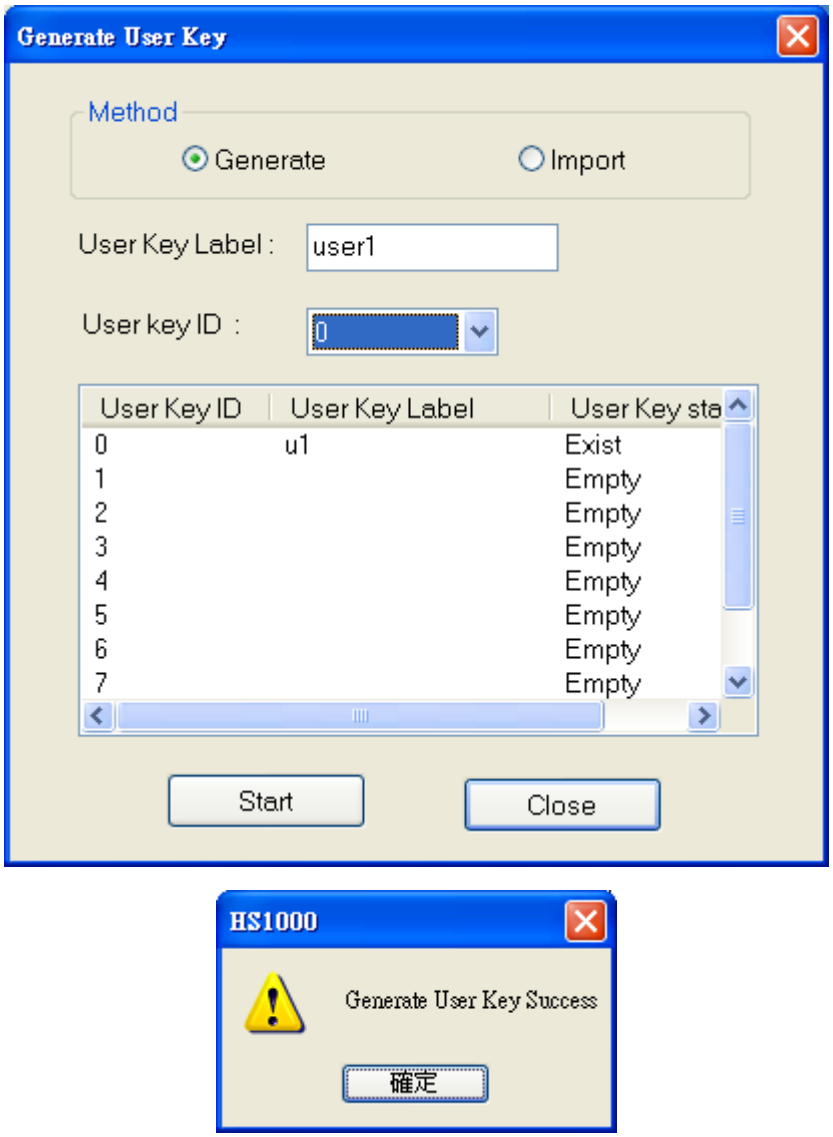


Fig. 4-16 the window of generate User Key

4.2.2.2. Impose User Key

【Impose】 User Key， make sure that the key of IC card is encoded by the MK of HiPKI SafGuard 1000.

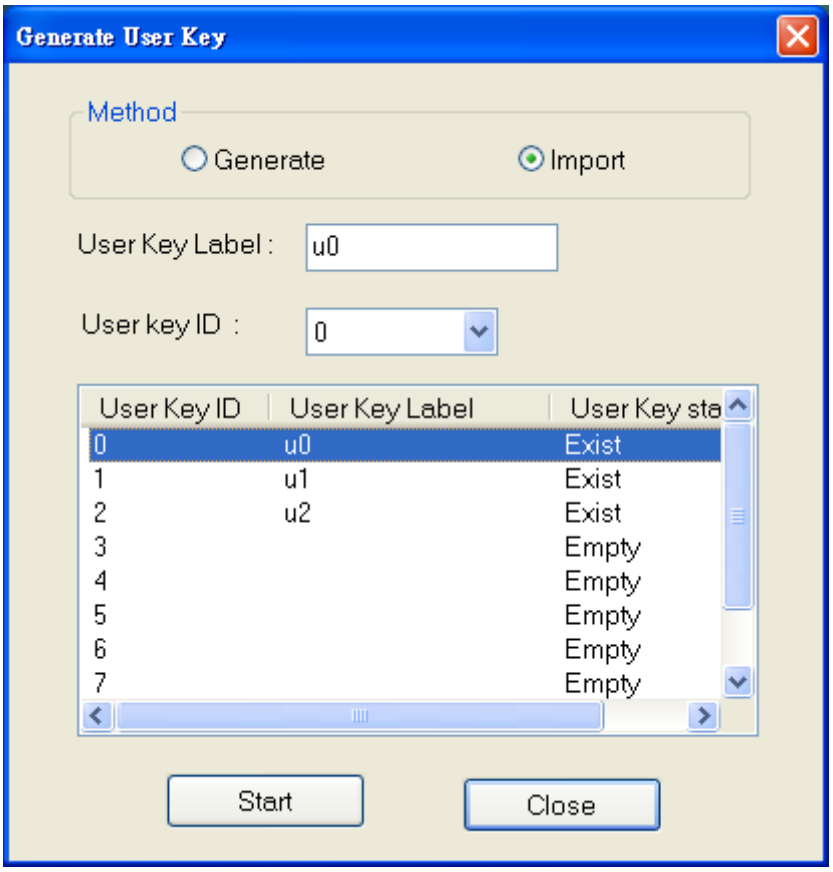


Fig. 4-17 the window of import User Key

4.2.3. Setting up user group

After the User Key has been generated, please select 『set up Group』 on 【Security Officer function table】。 This function can classify Security Officer and User which can be used by Application Key(APK).

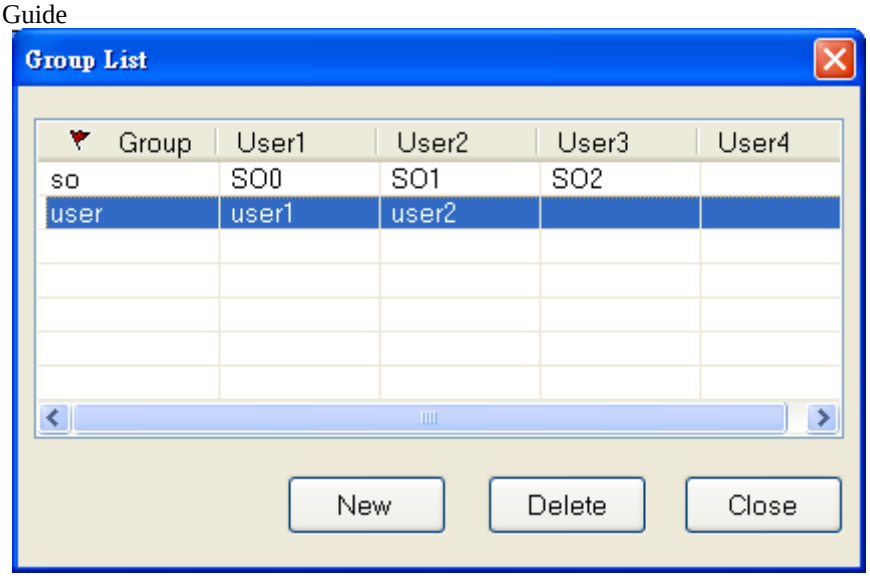


Fig. 4-18 Setting User-Group

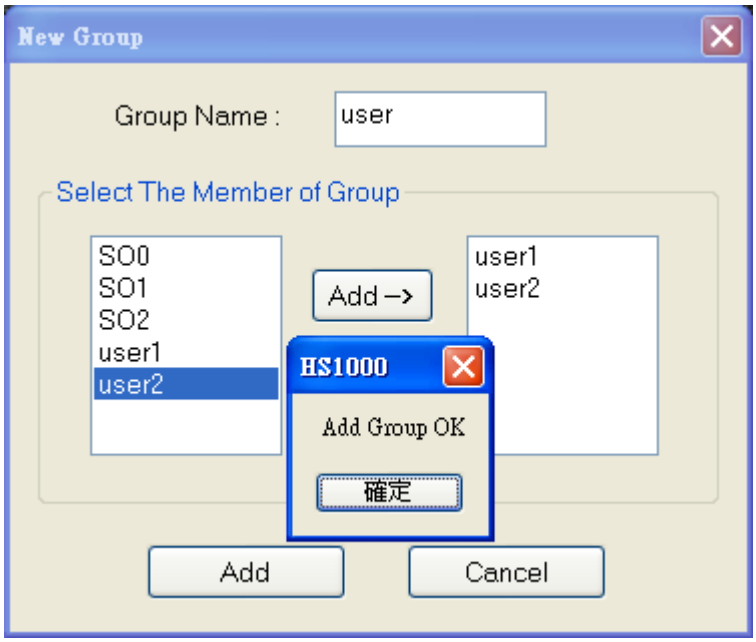


Fig. 4-19 Add User-Group

4.2.4 Produce AP Key

From Security Officer function window, click【Produce AP Key】 and go to the window of producing AP Key.

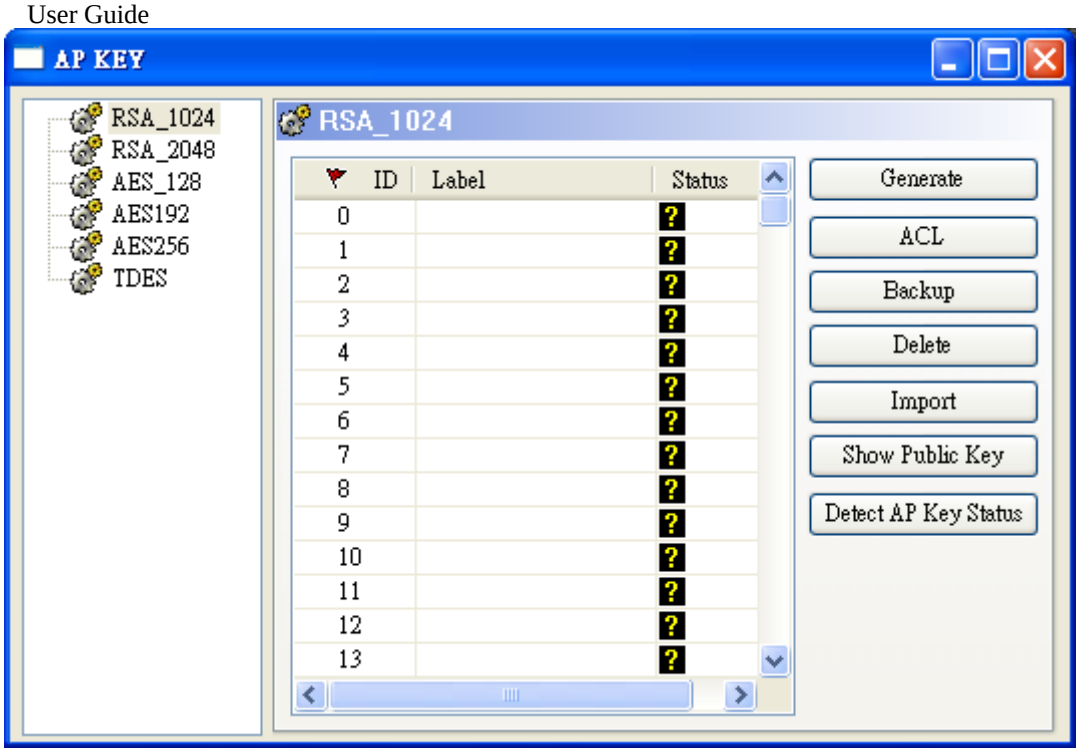


Fig. 4-20 the window of producing AP Key

4.2.4.1. Generating Keys

Click 『Generating key』 on 【producing AP Key】window。

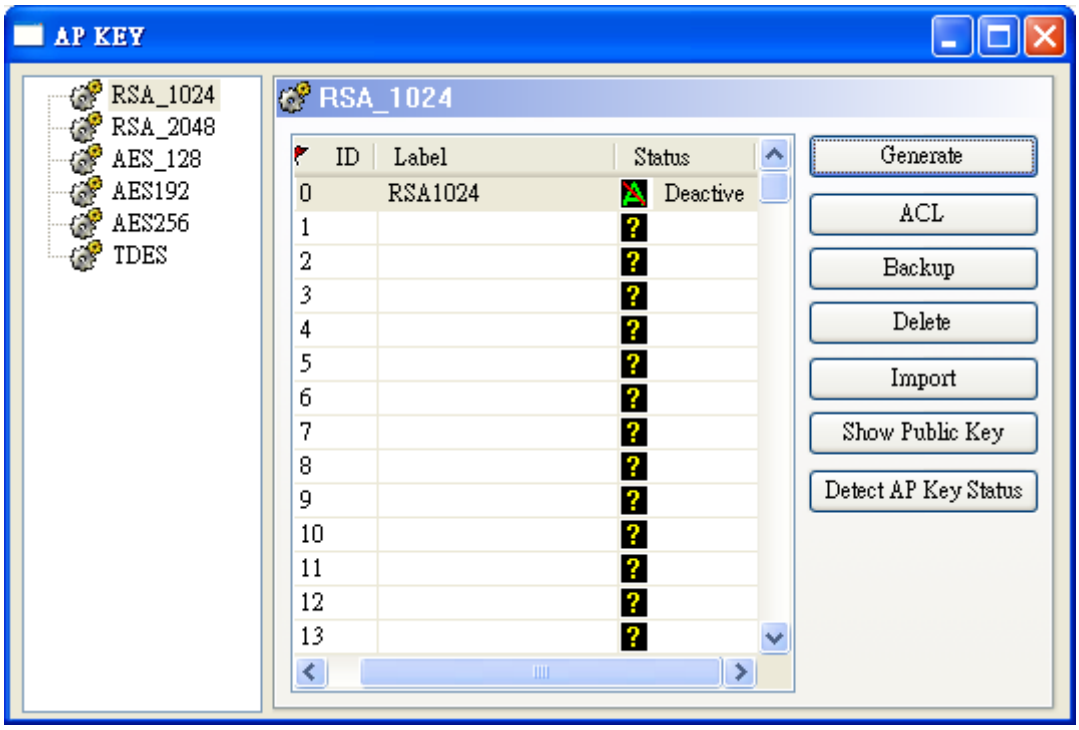


Fig. 4-21 the complete of producing AP Key

Then you will be asked to set up the ACL(Access Control Limit) of the Application Key.

4.2.4.2. Setting up the ACL of Key

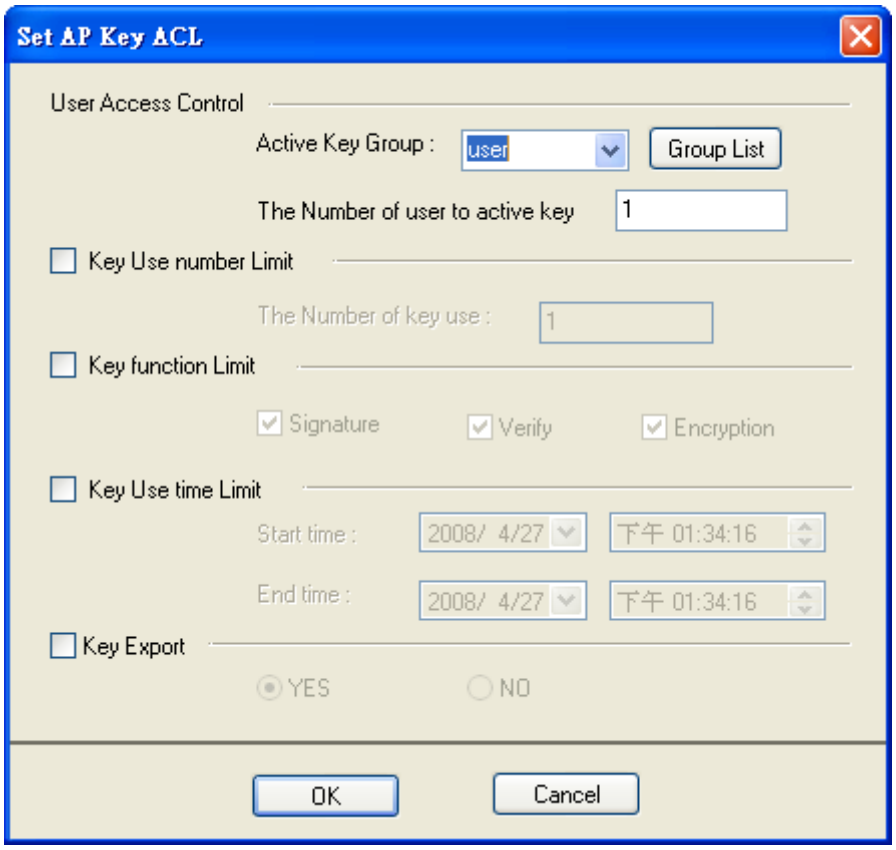


Fig. 4-22 Set the ACL of AP Key

4.2.5 Key Recovery and Key Backup

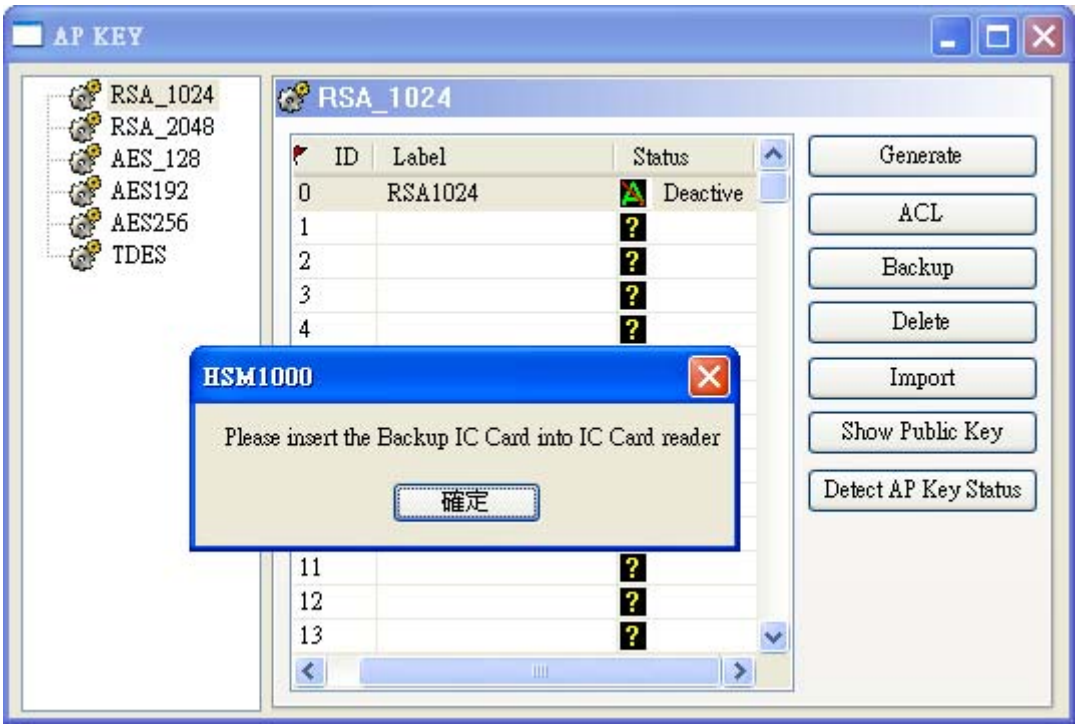


Fig. 4-23 the screen of AP Key Backup and Recovery

4.2.5.1. Key BackUp

Click on『BackUp』 of 【producing AP Key screen】. Make sure the APK has been generated and HiPKI SafGuard 1000 already has the key-pair of AP Key.

上圖中的 **AP Key 狀態** 非〔尚未寫入〕即可。之後進入備份 AP Key 的設定畫面。

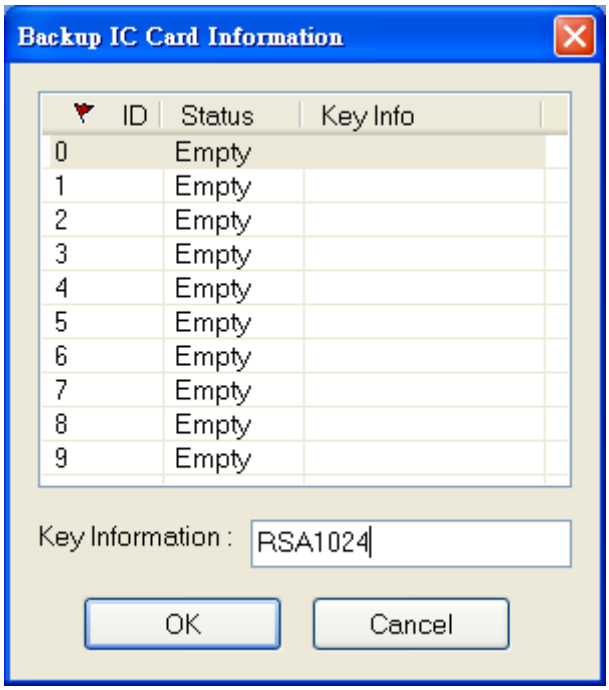


Fig. 4-24 the screen of setting up the AP Keybackup information

4.2.5.2. Key Recovery

Click 『import』on 【Producing AP Key screen】

User need to have the backup data in order to excute thekey recovery operation.The screen of setting up the AP Key

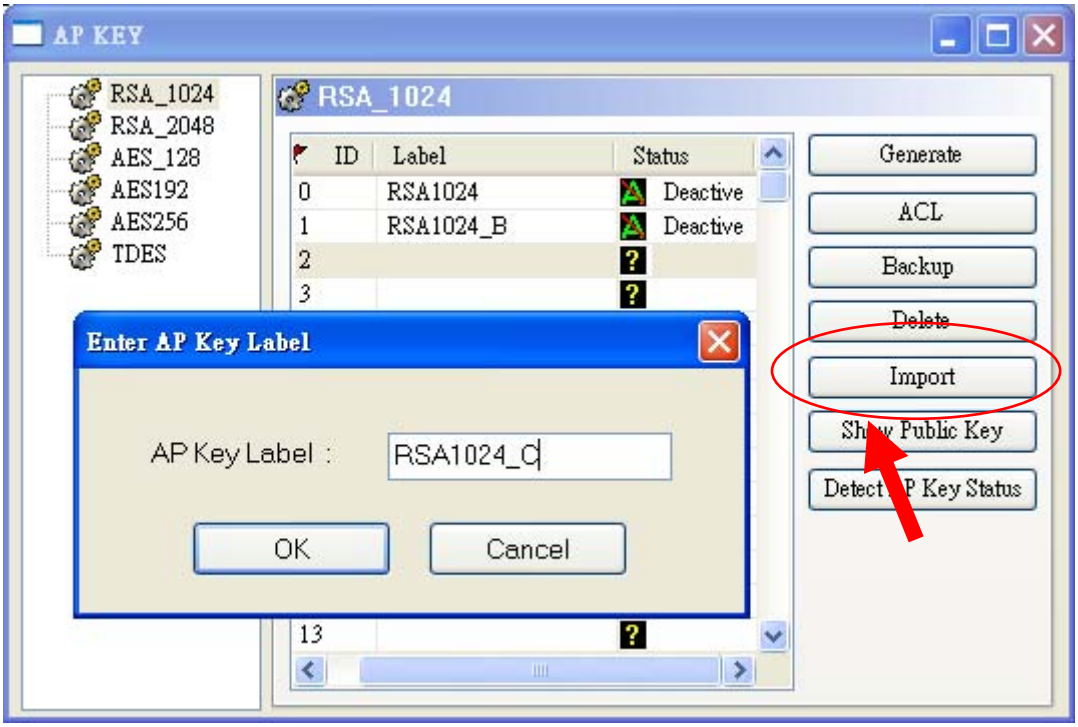


Fig. 4-25 the operation window of Import AP Key

After Key Recovery, you will be asked to set up the ACL of AP Key.

Please reference 〈Figure 4-22 Setting up the ACL of AP Key〉。

4.2.6 Key Destroy

4.2.6.1. HiPKI SafGuard 1000 Key Destroy

Selecting 『Delete』or『Delete All』 on the 【AP Keywindow】.

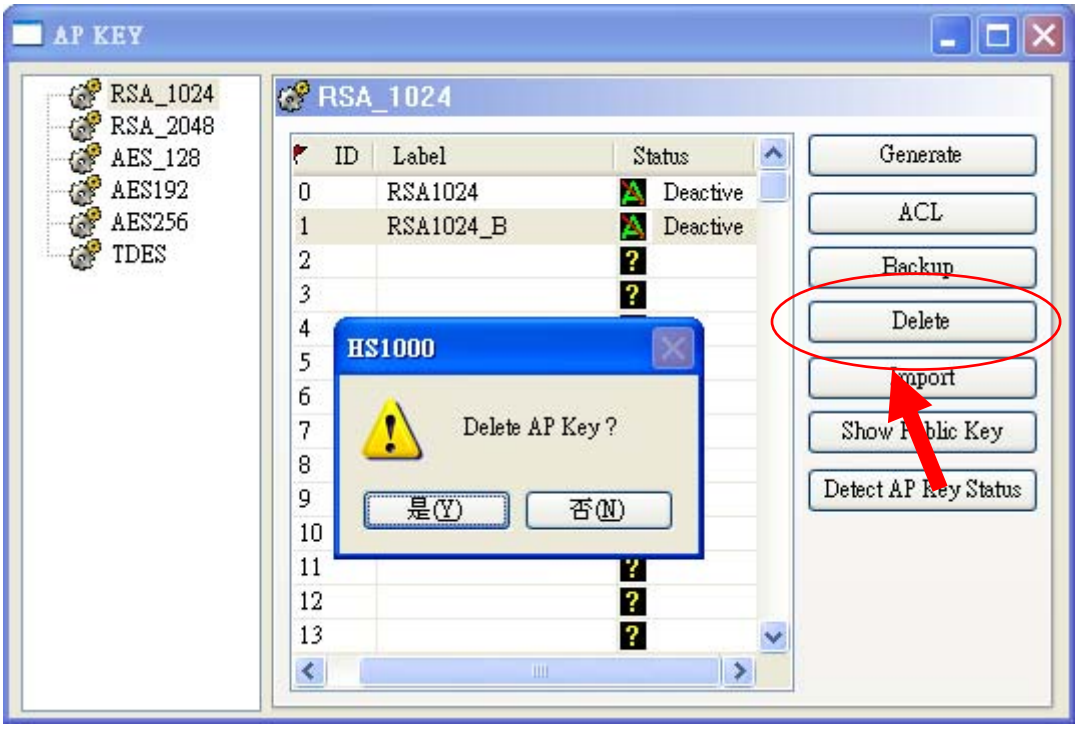


Fig .4-26 The screen of SafGuard Destroy

(1) 『Delete』the selected AP Key .

(2) or『Delete All』to delete all AP Key。

Fig. 4-26 key destroy

4.2.6.2. IC Card Backup Key Destroy

Selecting 【Delete the context of Backup ICcard】 on the Security Officer selecting window.

Delete the key on Backup IC Card.

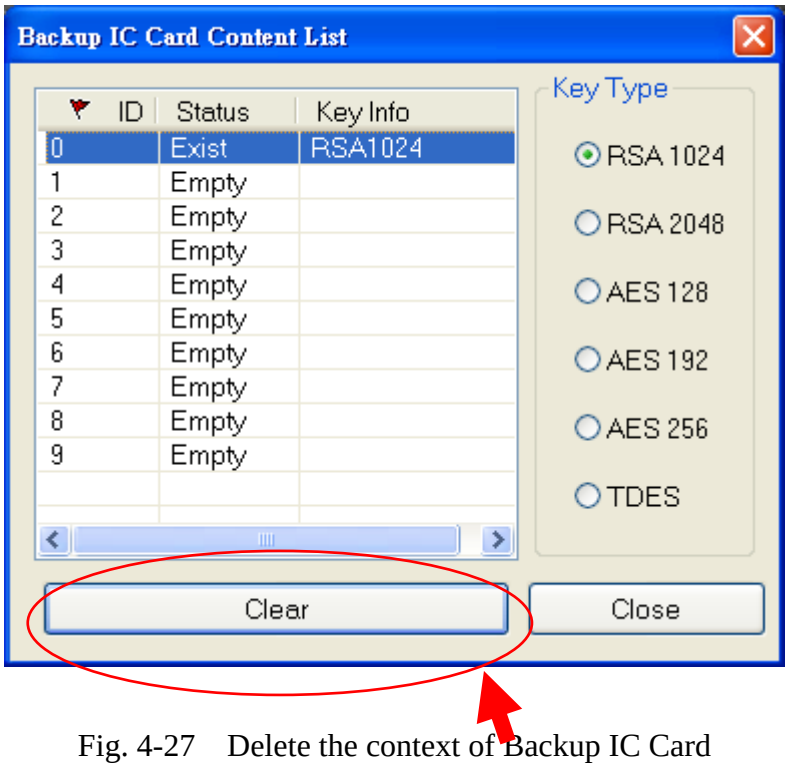


Fig. 4-27 Delete the context of Backup IC Card

4.2.7 Enable or Disable Key(WINDOWS)

Click 『User commands』 on the HiPKI SafGuard 1000 setting up screen

Fig. 4-28 Selecting the button of User commands

4.2.7.1. Enable Key

(1) Selecting the AP Key that you want to be enabledon on the List, than press 【Enable】。

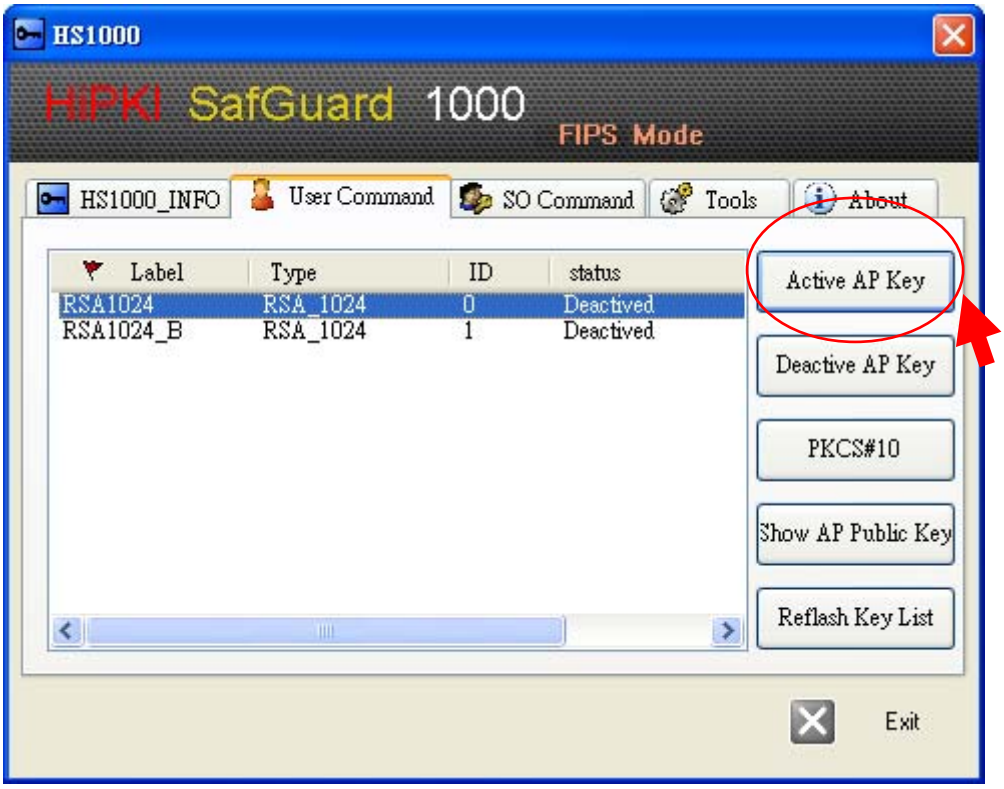


Fig. 4-29 The screen of key enable(User Logon)

(2) You will be asked to insert at least one User IC Card, according to Limist_auth_num of the ACL of eack AP Key(Reference Figure 4-20 Setting up the ACL of AP Key)。

Fig. 4-29 Enable AP Key。The message of inserting User IC Card

(3) After enable the key, set up the information about the AP Key

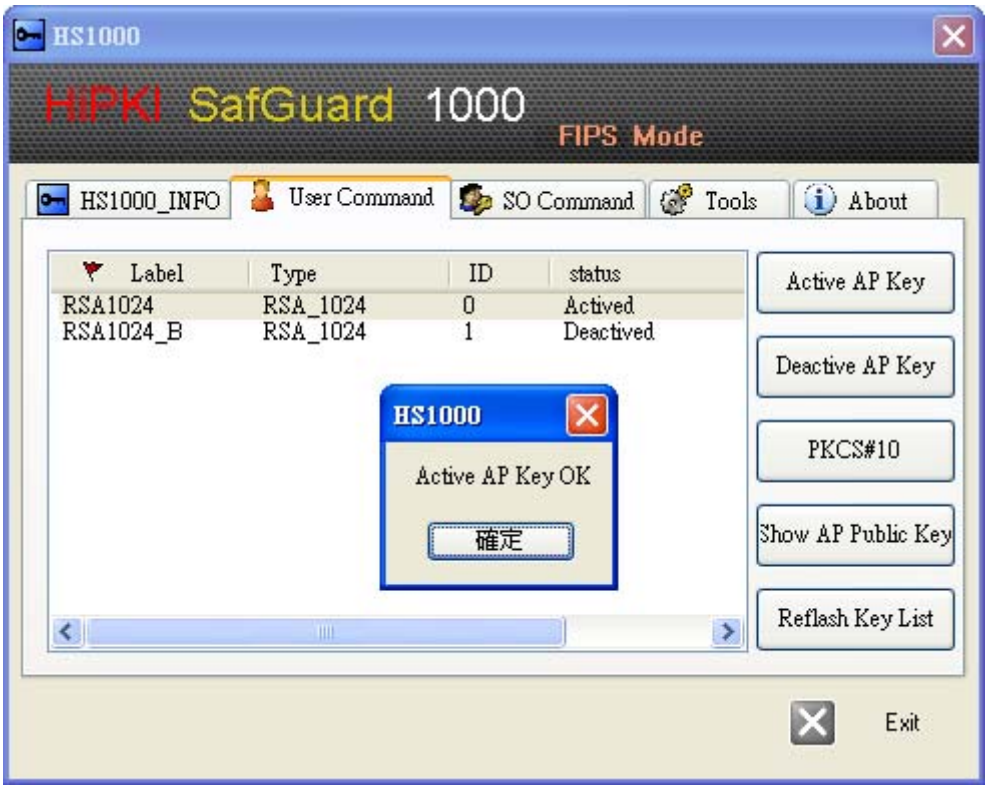


Fig. 4-30 Enable AP Key complete

4.2.7.2. Disable a using Key

Selecting the AP key you want to be disabled on the List, then press【Deactivate】。

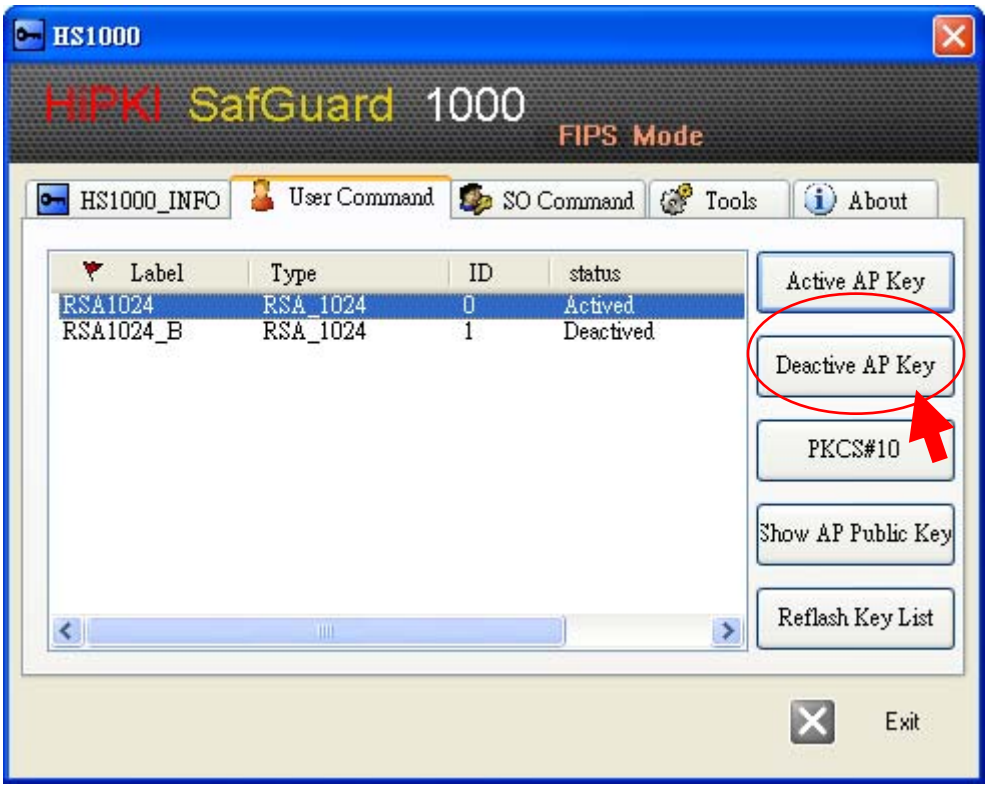


Fig. 4-31 Deactivate an APKey(User Logout)

4.2.7.3. Produce PKCS10 Request File

Selecting the AP Key from the List to produce its PKCS10 request file, then press【produce PKCS10 request file】。

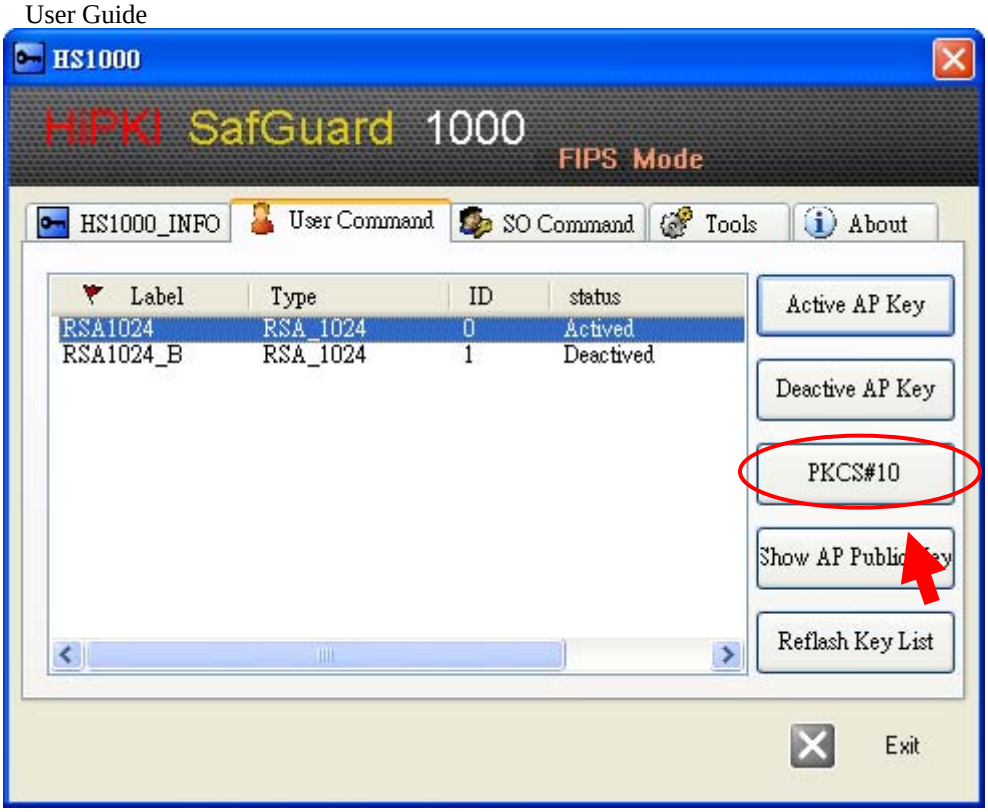


Figure 4-32 Produce PKCS10 Request File

5. HiPKI SafGuard 1000 Installation

5.1 Installation of Windows Driver

5.1.1 Installation

First, install HiPKI SafGuard 1000 driver and key management tool to Win2000：

The program for HiPKI SafGuard 1000 driver
Hsm_Server.exe:　Win2000 Service program, HiPKI SafGuard 1000 driver

The program for Key management:
KeyManage.exe: Key Management Tool
Findptrs.avi: pictures for key management program
BfiveUcs.dll 與 Mfc42.dll: Programs used for dynamic linking

Execute the Hsm_Server.exe in the installation directory

5.2 Active_Ap_Key_file Directory

The Active_Ap_Key_file directory is used to store parameters for enabling key, the file name is assigned as the following

AP_UseKey_ (the type of the Key: RSA_1024o r RSA_4096)_(store in HiPKI SafGuard 1000).ini。Therefore, if AP_KEY is RSA4096, and it is stored at location 1 of HiPKI SafGuard 1000, then its parameter file name is AP_UseKey_RSA_4096_1.ini. Besides ，this file will be fail whenever the hardware is reset. So you need to check the parameter file and make sure it is the latest version. (Please copy the parameter file to your AP directory.

Note : this directory can be created only after the key management tool has beenexecuted. About how to enable the keys, please reference to manual 4.2key management tool

5.3 The Directory PubKey_file

PubKey_file: the directory for storing public key

Pubkey_file*.inf	sub publickey info
Pubkey_file*_CertReq.PKCS10	PKCS10 Certification Request
Pubkey_file*_CertReqSign.b64	B64 encoded PKCS10 Certification Request file (with digital signature)
Pubkey_file*_CertReqSign.PKCS10	PKCS10 Certification Request with digital signature
Pubkey_file*_dn.hex	The necessary DN hex values to enable CA

Table 5-1 Filesabout public keys

Note * represents the name of AP_KEY

Note : This directory can be created only when KeyManagerTool has been executed. About the way to generation please reference to manual 4.2Key management function。

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.