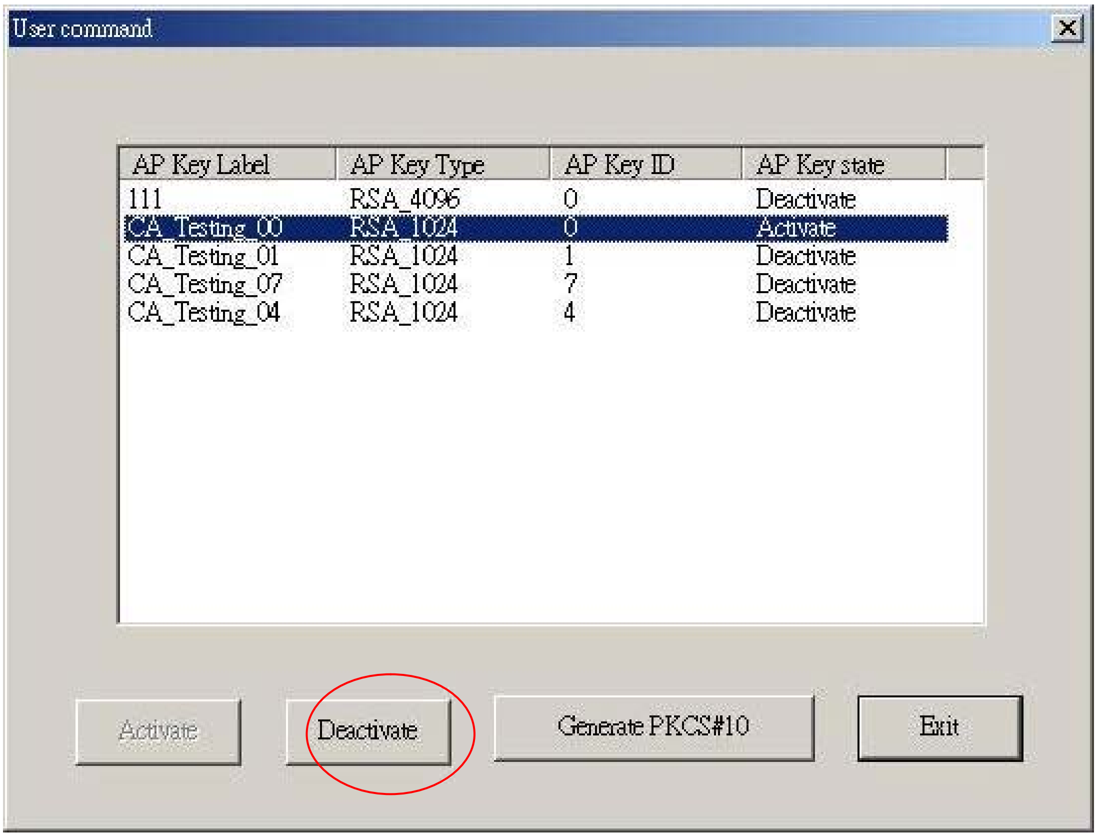
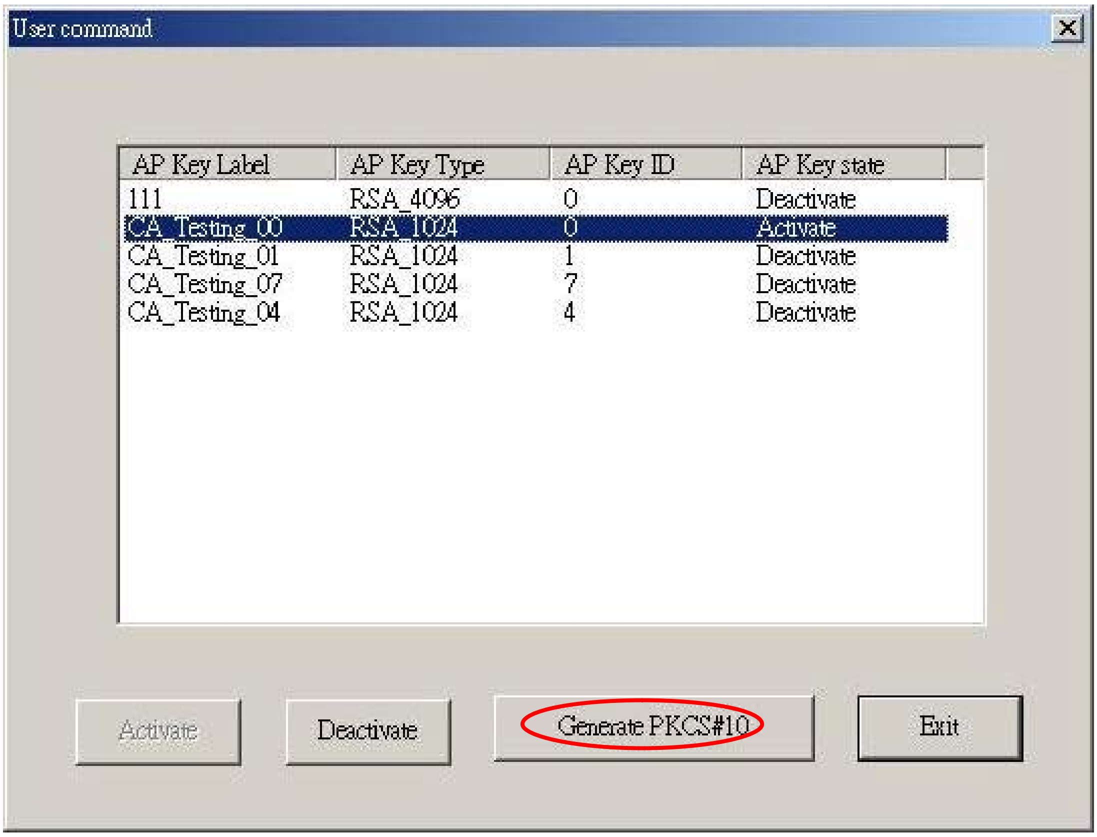


AP Key Label	AP Key Type	AP Key ID	AP Key state
111	RSA_4096	0	Deactivate
CA_Testing_00	RSA_1024	0	Activate
CA_Testing_01	RSA_1024	1	Deactivate
CA_Testing_07	RSA_1024	7	Deactivate
CA_Testing_04	RSA_1024	4	Deactivate

Fig.　4-32 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】。



User command

AP Key Label	AP Key Type	AP Key ID	AP Key state
111	RSA_4096	0	Deactivate
CA_Testing_00	RSA_1024	0	Activate
CA_Testing_01	RSA_1024	1	Deactivate
CA_Testing_07	RSA_1024	7	Deactivate
CA_Testing_04	RSA_1024	4	Deactivate

Figure 4-33 Produce PKCS10 Request File

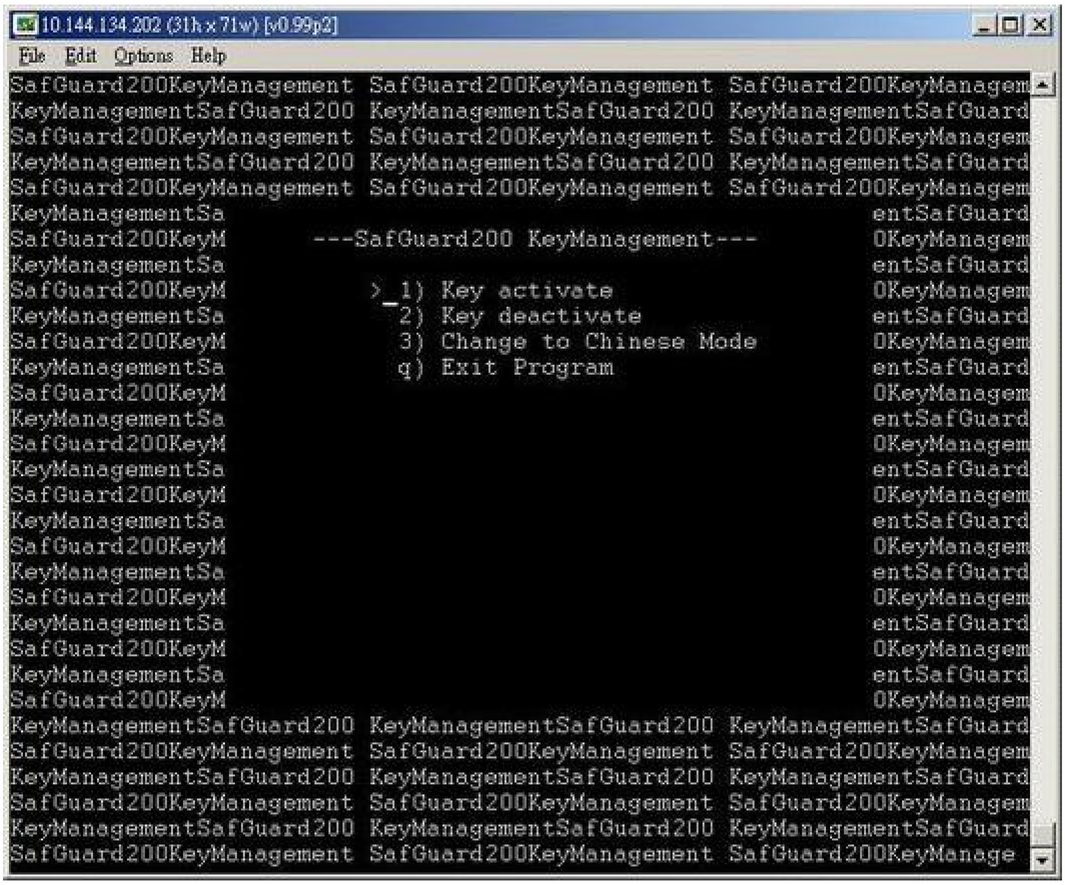
4.2.8 Enable or Disable Key (UNIX_LIKE)

You need toexecute the SafGuard200service program (Reference5.2 Solaris/Linux driver installation manual), then the UNIX KeyManagement Toolcan be executed.

The execute file of UNIX KeyManagement Tool is *KeyMng* which has two operation mode.

1. KeyMng –w： Frame/Win mode

In this mode, the program can be operated by using the key (↑ ↓ ← →), or directly press “1”, ”2” ,”3”…and so on.

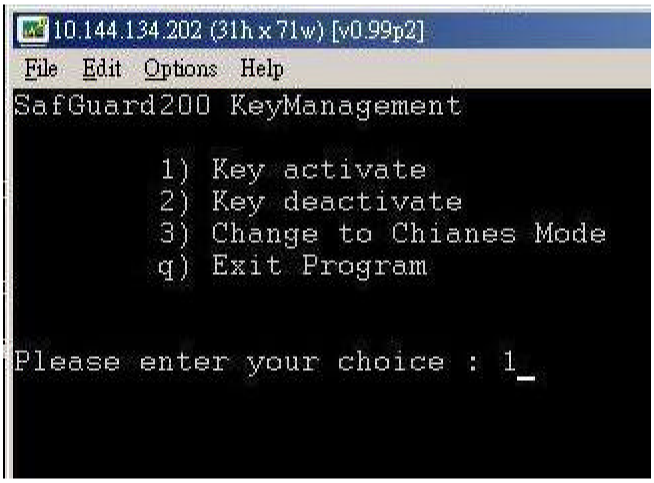


```
SafGuard200KeyManagement SafGuard200KeyManagement SafGuard200KeyManagem
KeyManagementSafGuard200 KeyManagementSafGuard200 KeyManagementSafGuard
SafGuard200KeyManagement SafGuard200KeyManagement SafGuard200KeyManagem
KeyManagementSafGuard200 KeyManagementSafGuard200 KeyManagementSafGuard
SafGuard200KeyManagement SafGuard200KeyManagement SafGuard200KeyManagem
KeyManagementSa                                             entSafGuard
SafGuard200KeyM      ---SafGuard200 KeyManagement---        0KeyManagem
KeyManagementSa                                             entSafGuard
SafGuard200KeyM          >_1) Key activate                  0KeyManagem
KeyManagementSa            2) Key deactivate                entSafGuard
SafGuard200KeyM            3) Change to Chinese Mode        0KeyManagem
KeyManagementSa            q) Exit Program                  entSafGuard
SafGuard200KeyM                                             0KeyManagem
KeyManagementSa                                             entSafGuard
SafGuard200KeyM                                             0KeyManagem
KeyManagementSa                                             entSafGuard
SafGuard200KeyM                                             0KeyManagem
KeyManagementSa                                             entSafGuard
SafGuard200KeyM                                             0KeyManagem
KeyManagementSa                                             entSafGuard
SafGuard200KeyM                                             0KeyManagem
KeyManagementSa                                             entSafGuard
SafGuard200KeyM                                             0KeyManagem
KeyManagementSa                                             entSafGuard
SafGuard200KeyM                                             0KeyManagem
KeyManagementSafGuard200 KeyManagementSafGuard200 KeyManagementSafGuard
SafGuard200KeyManagement SafGuard200KeyManagement SafGuard200KeyManagem
KeyManagementSafGuard200 KeyManagementSafGuard200 KeyManagementSafGuard
SafGuard200KeyManagement SafGuard200KeyManagement SafGuard200KeyManagem
KeyManagementSafGuard200 KeyManagementSafGuard200 KeyManagementSafGuard
SafGuard200KeyManagement SafGuard200KeyManagement SafGuard200KeyManage
```

Fig. 4-34 The screen of Frame Mode operation

2. KeyMng –c：Command line mode

In this mode its operatoion is like mode 1, and the only difference is that mode 2 can not be operated by using the key (↑ ↓ ← →)



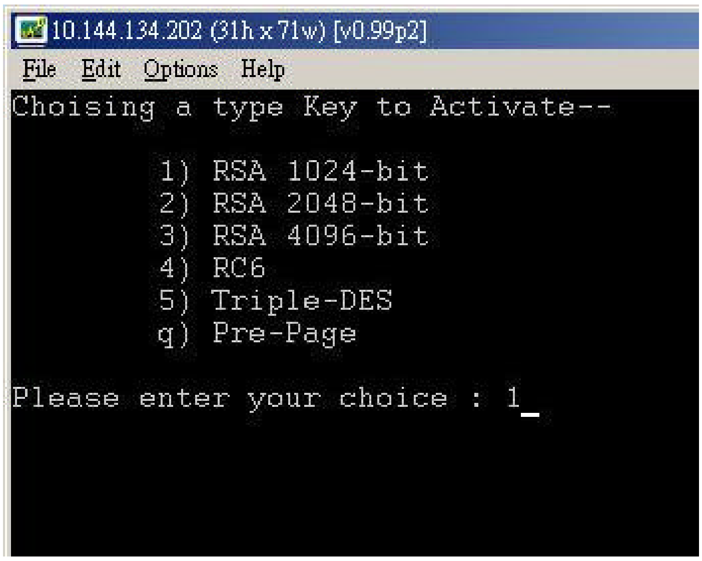
```
SafGuard200 KeyManagement

        1) Key activate
        2) Key deactivate
        3) Change to Chianes Mode
        q) Exit Program


Please enter your choice : 1_
```

Figure 4-35 the screen of Command mode operation

The screen of UNIX KeyManagement Tool is explained by Command mode.

4.2.8.1 Enable Key

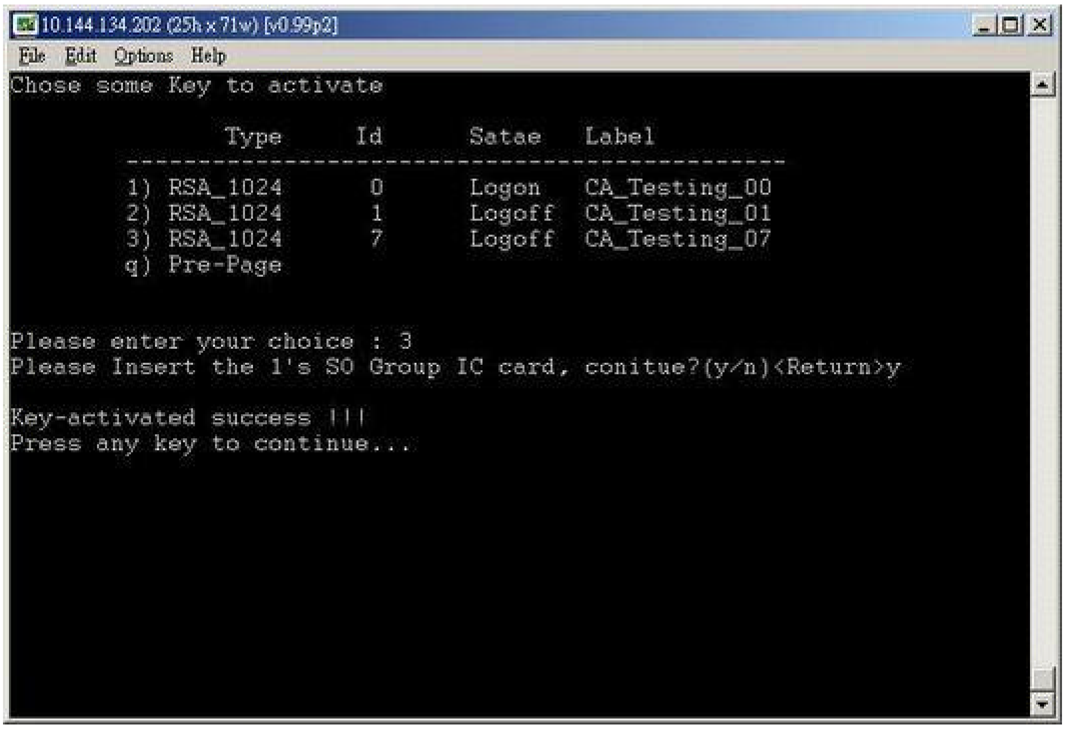
1. Selecting 1)Enable Key on the main screen (Reference Figure 4-35)。
2. Selecting the type of the key you want to enable



```
Choising a type Key to Activate--

        1) RSA 1024-bit
        2) RSA 2048-bit
        3) RSA 4096-bit
        4) RC6
        5) Triple-DES
        q) Pre-Page

Please enter your choice : 1_
```

Fig. 4-36 Selecting the type of key

3. Selecting the key you want to enable, and displaying the key information according to .ini file. You need to make sure that apkfile.ini file has been updated.



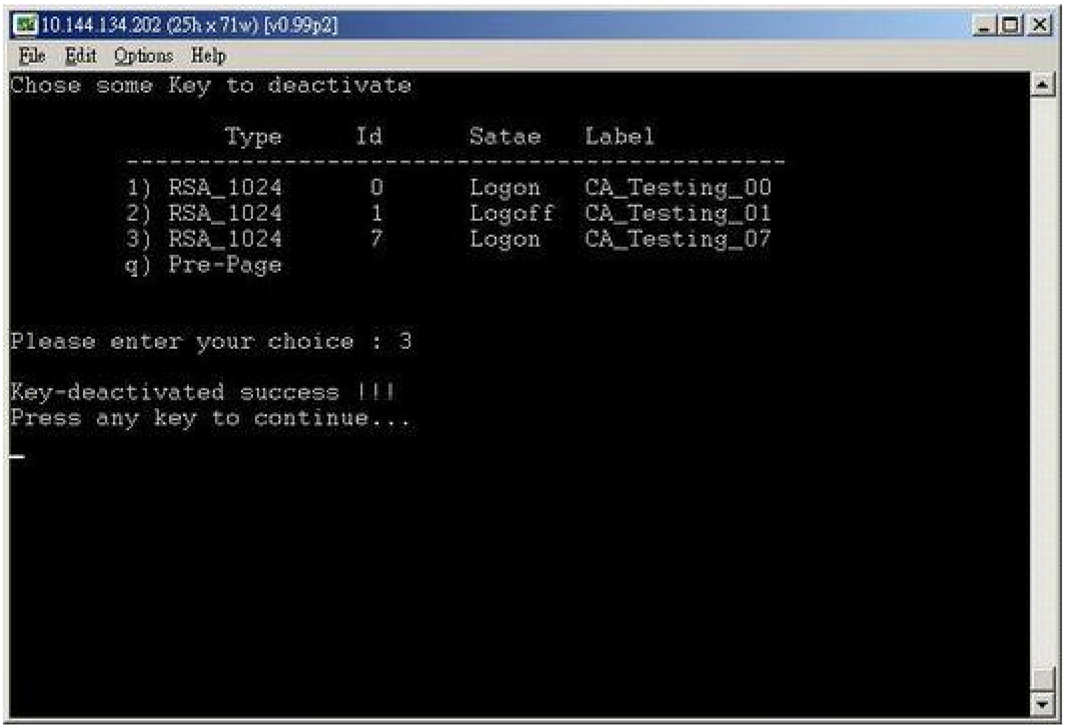
```
Chose some Key to activate

               Type      Id       Satae    Label
        ---------------------------------------------
        1) RSA_1024      0       Logon    CA_Testing_00
        2) RSA_1024      1       Logoff   CA_Testing_01
        3) RSA_1024      7       Logoff   CA_Testing_07
        q) Pre-Page


Please enter your choice : 3
Please Insert the 1's SO Group IC card, conitue?(y/n)<Return>y

Key-activated success !!!
Press any key to continue...
```

Fig. 4-37 Enable Key

4.2.8.2 Disable Key

In this section, disable key is also called key Logout

1. Selecting 2)Key Logout (Reference Figure 4-35)。
2. Selecting the type of the key, reference Figure 4-36。
3. Selecting the key



```
Chose some Key to deactivate

               Type      Id       Satae    Label
        ------------------------------------------------
        1) RSA_1024       0       Logon    CA_Testing_00
        2) RSA_1024       1       Logoff   CA_Testing_01
        3) RSA_1024       7       Logon    CA_Testing_07
        q) Pre-Page


Please enter your choice : 3

Key-deactivated success !!!
Press any key to continue...
_
```

Fig. 4-38 Key Logout

5. SafGuard200 Installation

5.1 Installation of Windows2000 Driver

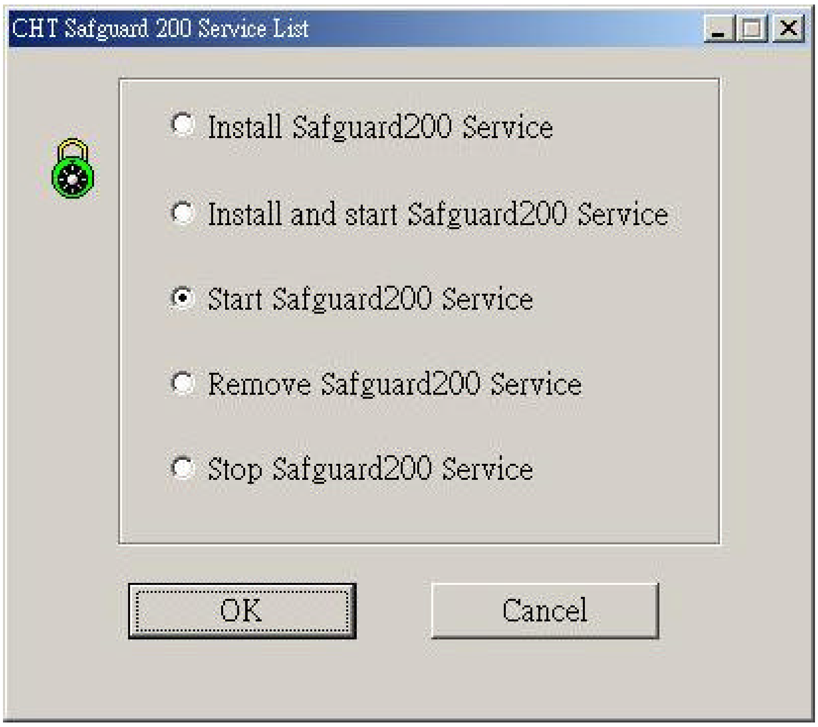
5.1.1 Installation

First, install SafGuard200 driver and key management tool to Win2000：

The program for SafGuard200 driver
Hsm_Server.exe: Win2000 Service program, SafGuard200 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



CHT Safguard 200 Service List

○ Install Safguard200 Service
○ Install and start Safguard200 Service
● Start Safguard200 Service
○ Remove Safguard200 Service
○ Stop Safguard200 Service

Fig. 5-1 The screen for executing Hsm_Service.exe

Function details：

Installing service program ：

installing SafGuard200 service programs

Installing and enable service program：

Installing service program in the system and execute the service program.

Enable SafGuard200 service program ：

Execute service program

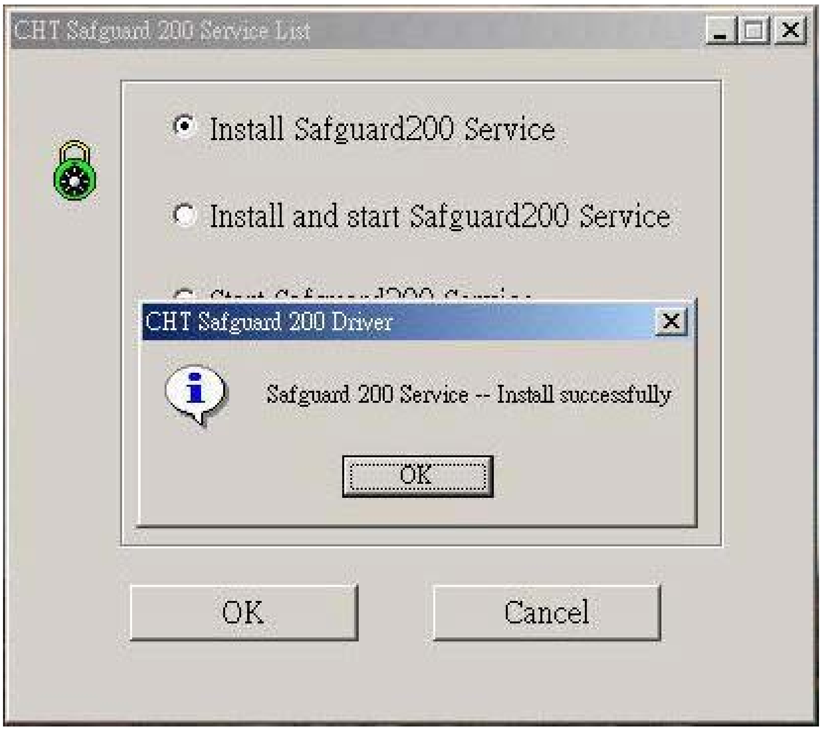
Remove Service program ：

Remove the service program from the system.

Shut down service program ：

Shut down the service program

After executing Hsm_Server.exe, click [Installing SafGuard200 service program] or [Installing and enable SafGuard200 service program], then press ok button, as shown in the following Figure. If you click[Installing and enableSafeGuard200 service program], the service program will be executed after installion.



CHT Safguard 200 Service List

● Install Safguard200 Service

○ Install and start Safguard200 Service

○ Start Safguard200 Service

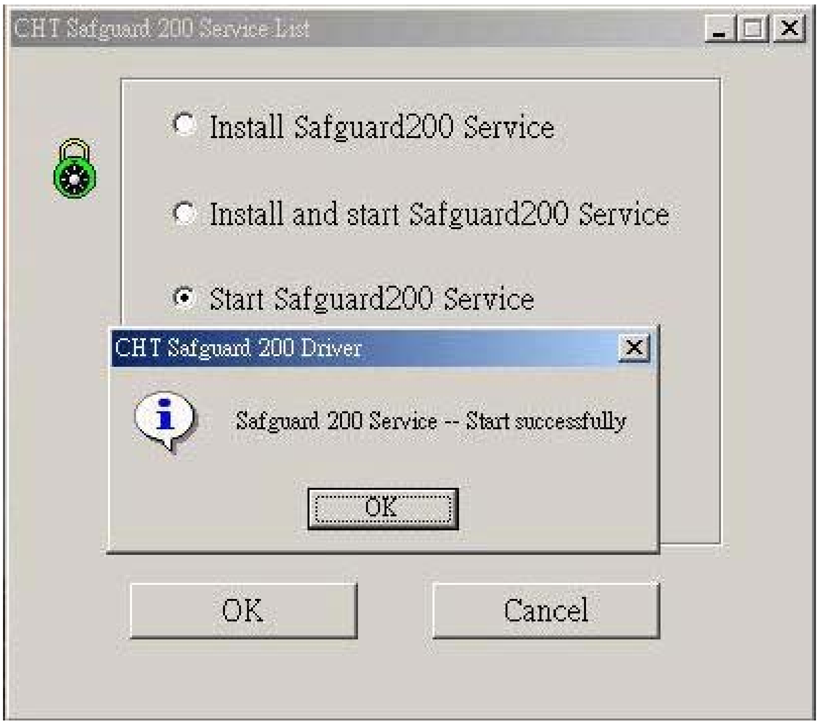
CHT Safguard 200 Driver

Safguard 200 Service -- Install successfully

Fig. 5-2 The screen of installing service program

5.1.2 Enable Service Program

After installition, click [EnableSafGuard200 service program] , then click ok button, the service program can be enabled.



CHT Safguard 200 Service List

○ Install Safguard200 Service

○ Install and start Safguard200 Service

● Start Safguard200 Service

CHT Safguard 200 Driver

Safguard 200 Service -- Start successfully

Fig. 5-3 The screen of enable the service program

After completing all previous tasks, you can find the icon of running HSM_Server at right bottom corner of Win2000. If the color of this icon is green, like 🔒, it means that the SafGuard200 has been connected, otherwise the color of the icon will be red like 🔒. At this point, you can press right button of the mouse to quit HSM_Server. Its function as shown in the following

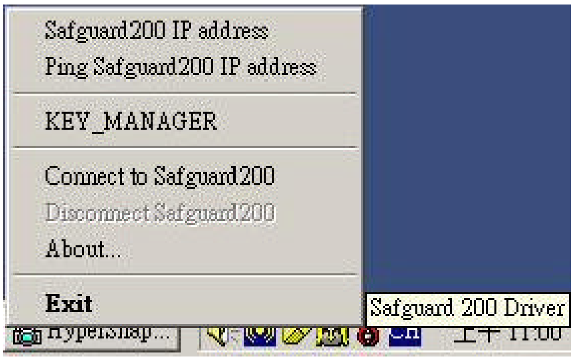
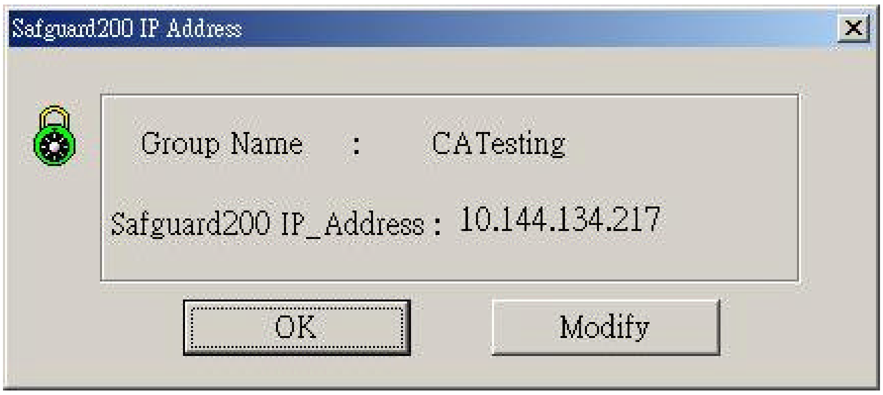


Fig. 5-4 The Screen fo enabling HSM_Server

Function details:

SafGuard IP Address : Displaying theGroup name and IP address of SafGuard200 as shown in the following：



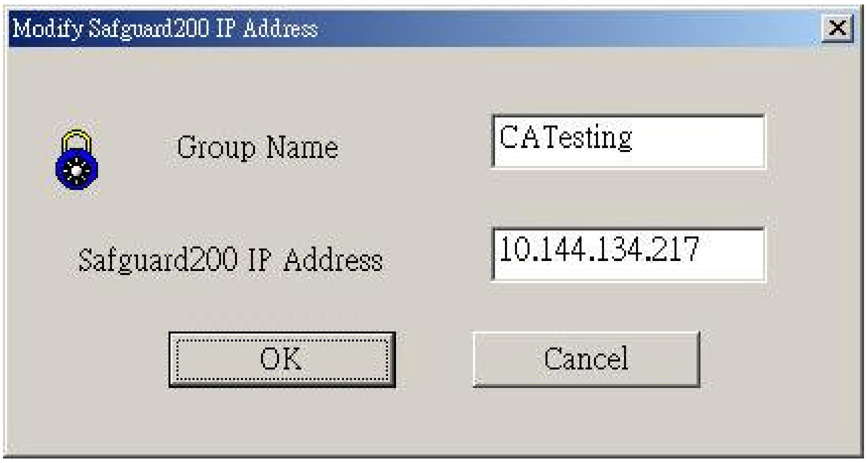
Safguard200 IP Address

Group Name : CATesting

Safguard200 IP_Address : 10.144.134.217

Fig. 5-5 SafGuard IP Address

The modifyingbutton can only be used when the SafGuard200 is disconnected. The screen is given as the following:



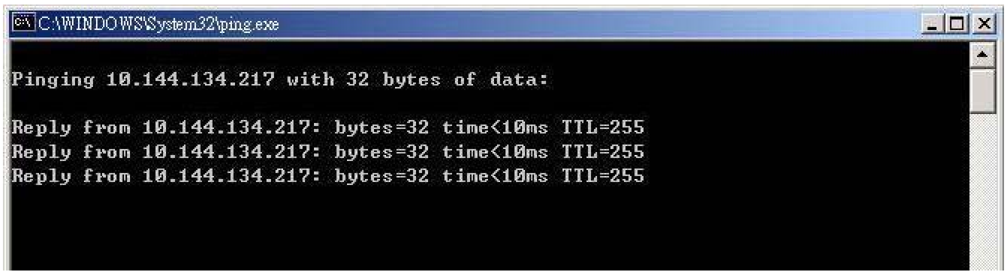
Modify Safguard200 IP Address

Group Name CATesting

Safguard200 IP Address 10.144.134.217

Fig. 5-6 Modifying the SafGuard200 IP Address

Ping HSM_IP : Executing ping program as the following



```
C:\WINDOWS\System32\ping.exe

Pinging 10.144.134.217 with 32 bytes of data:

Reply from 10.144.134.217: bytes=32 time<10ms TTL=255
Reply from 10.144.134.217: bytes=32 time<10ms TTL=255
Reply from 10.144.134.217: bytes=32 time<10ms TTL=255
```

Fig. 5-7 Ping HSM_IP

KEY_MANAGER : Executing Key_Managerprogram

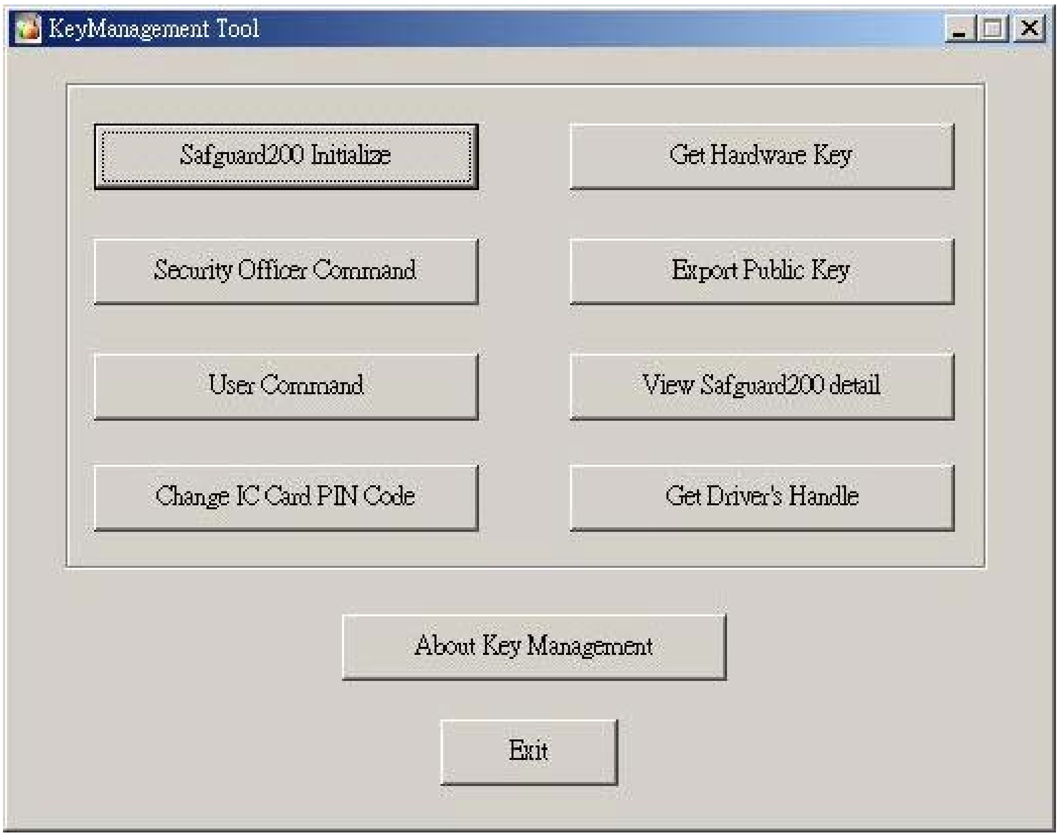
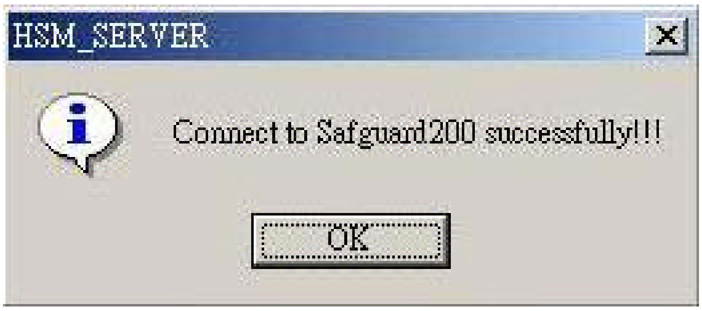


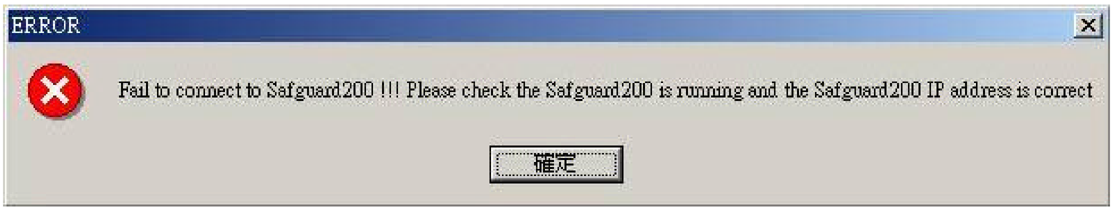
Figure 5-8 KeyManager

Connecting SafGuard200 : connecting to SafGuard200



Connect to Safguard200 successfully!!!

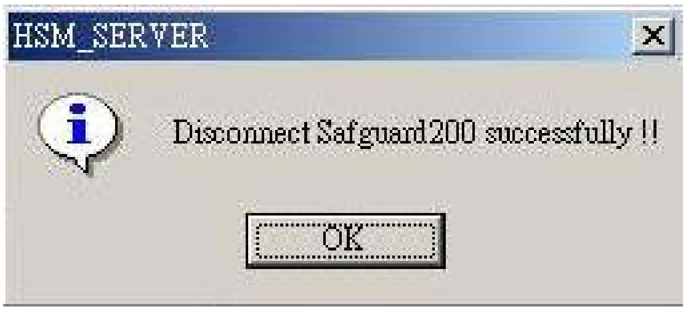
Fig. 5-9 Connecting Successfully



Fail to connect to Safguard200 !!! Please check the Safguard200 is running and the Safguard200 IP address is correct

Fig. 5-10 Connecting fail

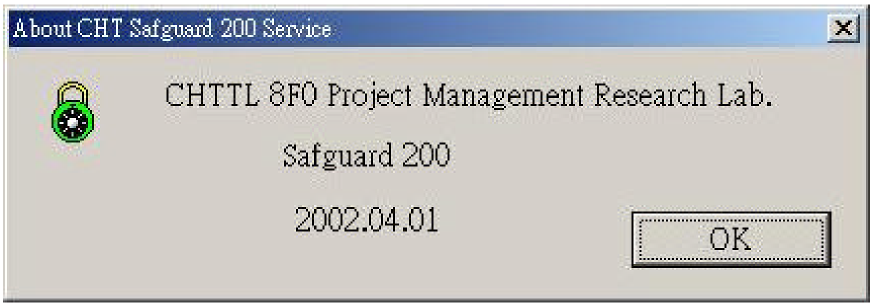
Disconnect SafGuard200 : disconnecting SafGuard200



Disconnect Safguard200 successfully !!

Fig. 5-11 Disconnecting Successfully

About : Displaying the version and date of HSM_Sever program



About CHT Safguard 200 Service

CHTTL 8F0 Project Management Research Lab.

Safguard 200

2002.04.01

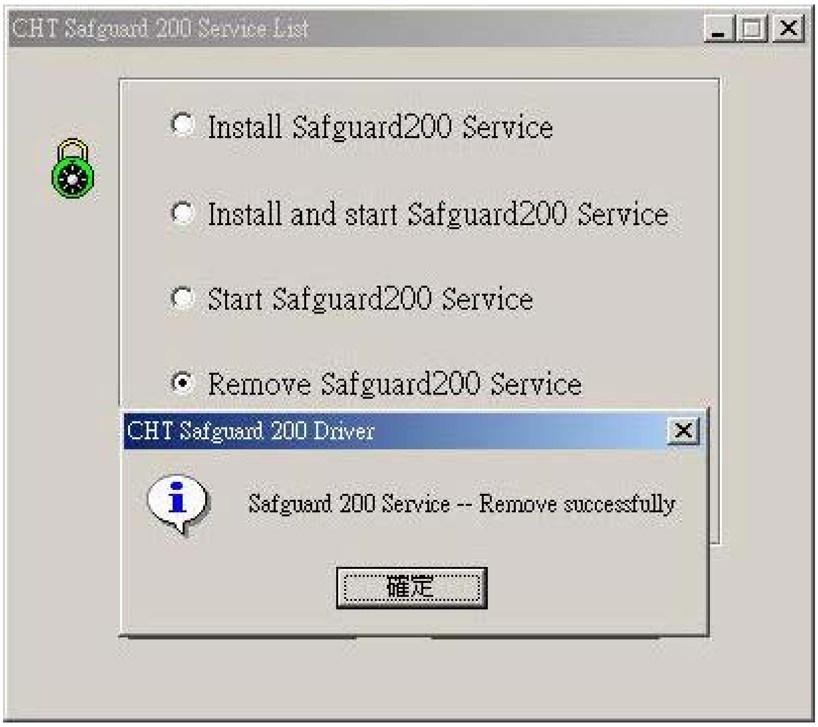
Figure 5-12 About

Eixt : Quit the HSM_Server program.

5.1.3 Remove Service Program

(1)

Executing HSM_Server.exe in the installing directory, click [Remove service program] and then click ok button. the service program, HSM_Server, will be removed from the system.



CHT Safguard 200 Service List
○ Install Safguard200 Service
○ Install and start Safguard200 Service
○ Start Safguard200 Service
● Remove Safguard200 Service
CHT Safguard 200 Driver
確定

Safguard 200 Service -- Remove successfully

Fig. 5-13 The screen of removing service program

(2) After remove all file in the installing directory, the operation of removing is completed.

5.2 Installation of Solaris/Linux driver

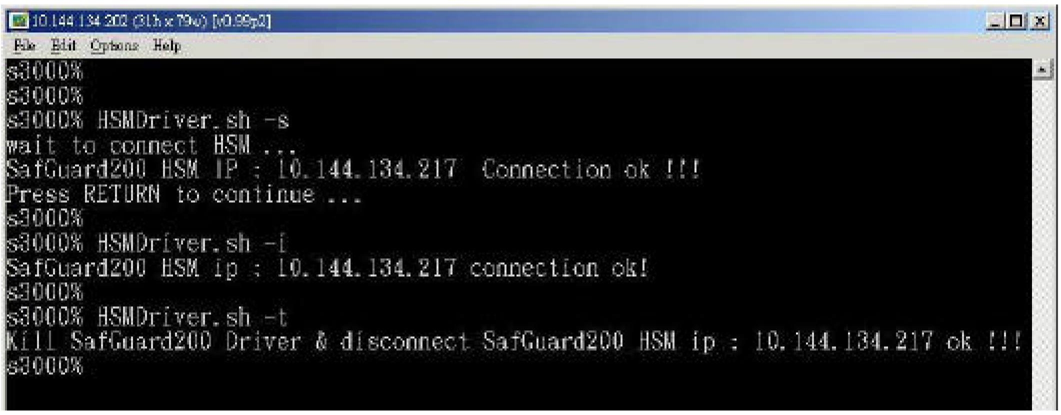
(1) First copy the SafGuard200 drivre to UNIX-like system, including：

1. HSMDriver.sh (batch file, start/stop command file)
2. server (main program)
3. SafeGuardStop (stoping running executing file)
4. safeguard.ini (information about SafGuard200)

Safeguard.ini need to be replaced by safeguard.ini generatred by previous key management tool.

(2) Exectuing in the installation directory

HSMDriver.sh –s : Start SafGarud200 driver program
HSMDriver.sh –stop SafGurad200 driver program
HSMDriver.sh –i : check the state of connecting betwenSafGuard200 ad driver.



```
s3000%
s3000%
s3000% HSMDriver.sh -s
wait to connect HSM ...
SafGuard200 HSM IP : 10.144.134.217  Connection ok !!!
Press RETURN to continue ...
s3000%
s3000% HSMDriver.sh -i
SafGuard200 HSM ip : 10.144.134.217 connection ok!
s3000%
s3000% HSMDriver.sh -t
Kill SafGuard200 Driver & disconnect SafGuard200 HSM ip : 10.144.134.217 ok !!!
s3000%
```

Fig. 5-14 The service program on UNIX-Like system

5.3 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 SafGuard200).ini。Therefore, if AP_KEY is RSA4096, and it is stored at location 1 of SafGuard200, 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

5.4 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

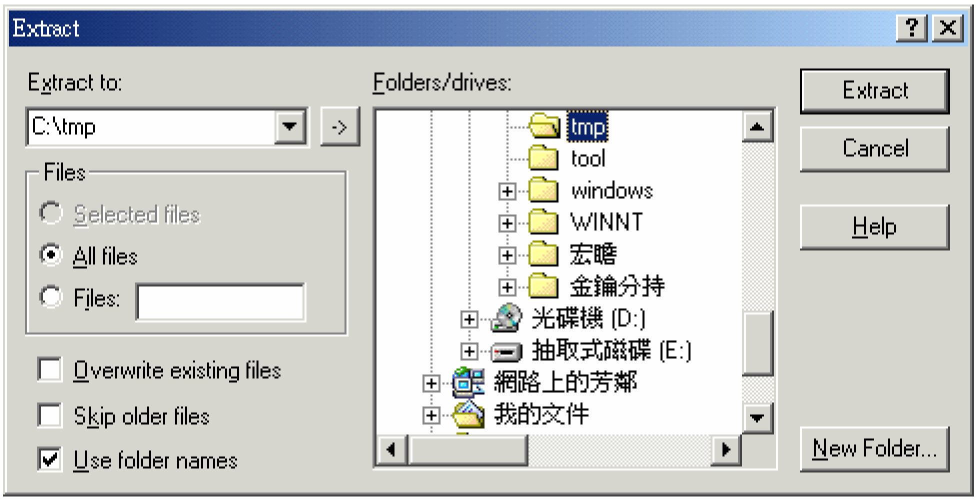
Note : This directory can be created only when KeyManagerTool has been executed. About the way to generation please reference to manual 4.2Key management function。

6. The Installation And Operation Of The Auditing Server

6.1 Installation

6.1.1 Step 1. :

Decompress the AuditingServer.zip file into a temporary directory, eg. C:\TMP。



Extract to: C:\tmp

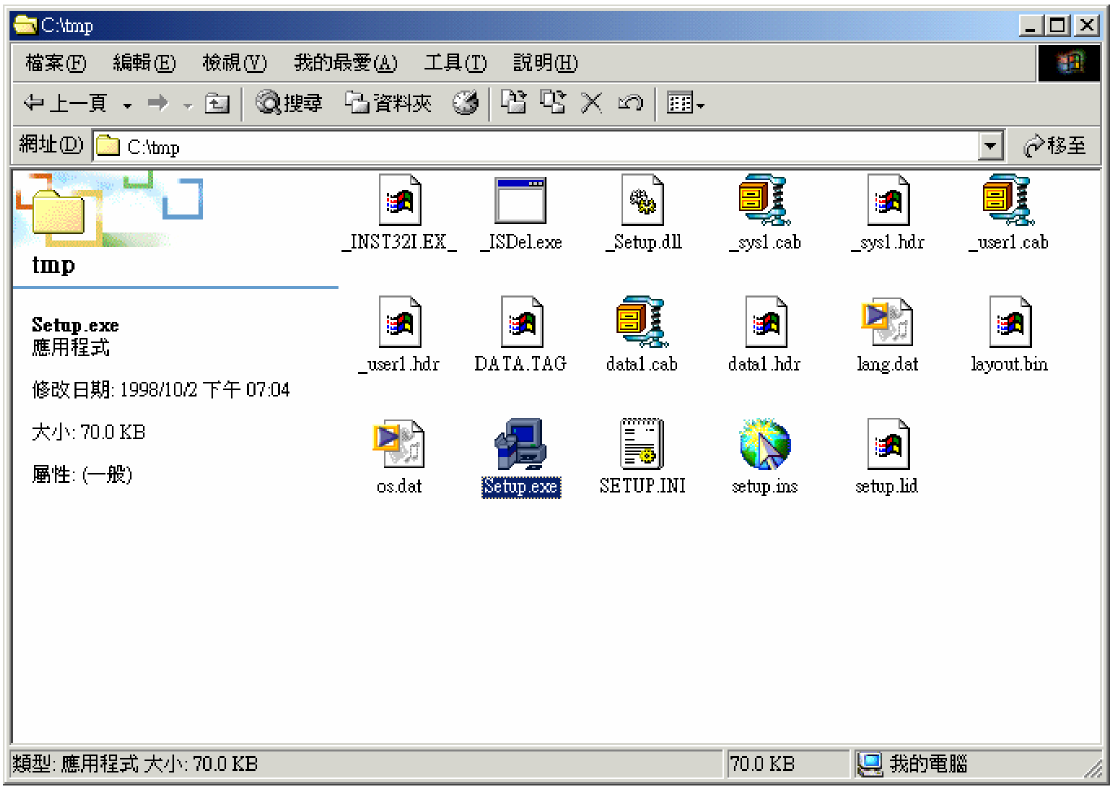
Files
○ Selected files
● All files
○ Files:

□ Overwrite existing files
□ Skip older files
☑ Use folder names

Folders/drives: tmp

6.1.2 Step 2. :

Change to the directory containing the decompressed files, and double click Setup.exe to start the installation procedure.



Setup.exe
應用程式

修改日期: 1998/10/2 下午 07:04

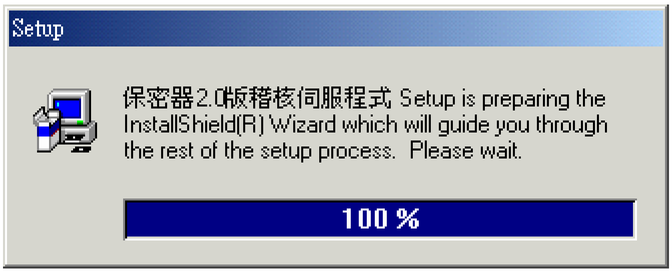
大小: 70.0 KB

屬性: (一般)

類型: 應用程式 大小: 70.0 KB 70.0 KB

6.1.3 Step 3. :

Follow the prompts and instructions of Setup.exe to install Auditing Server。



保密器2.0版稽核伺服程式 Setup is preparing the InstallShield(R) Wizard which will guide you through the rest of the setup process. Please wait.

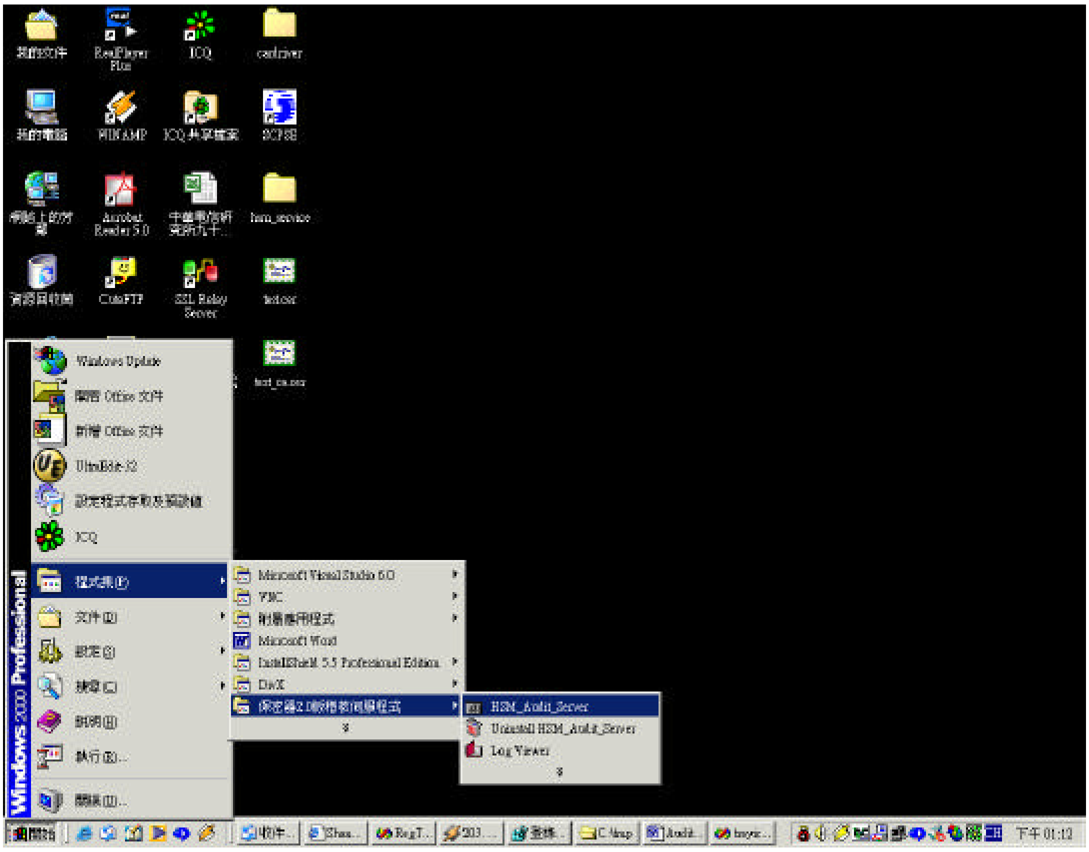
100 %

6.2 Activation

6.2.1 Step 1. :

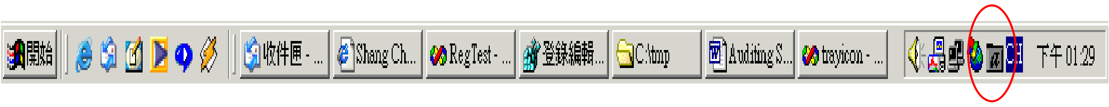
Click the ”Start” button of Windows and from the “Program” menu, select the

“HSM_Audit_Server “ item in the “Secure Hardware 2.0 Auditing Server” group to activate the Auditing Server.



6.2.2 Step 2. :

After the activation, an icon of the Auditing Server located on the right-lower corner of Windows task bar can be seen.



This represents that the Auditing Server has been successfully activated and is running well.

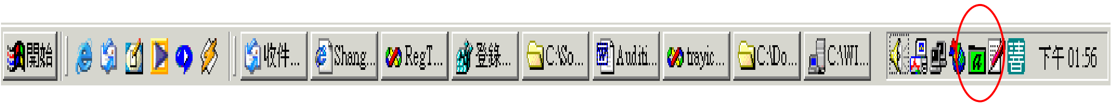
6.3 Install As A Service

Click the ”Start” button of Windows and from the “Program” menu, select the ”service” item inside the ”Install HSM_Audit_Server as a Service” of the “Secure Hardware 2.0 Auditing Server” group, this installs the Auditing Server as a service of Windows. Thereafter the Auditing Server will be activated each time Windows boots.

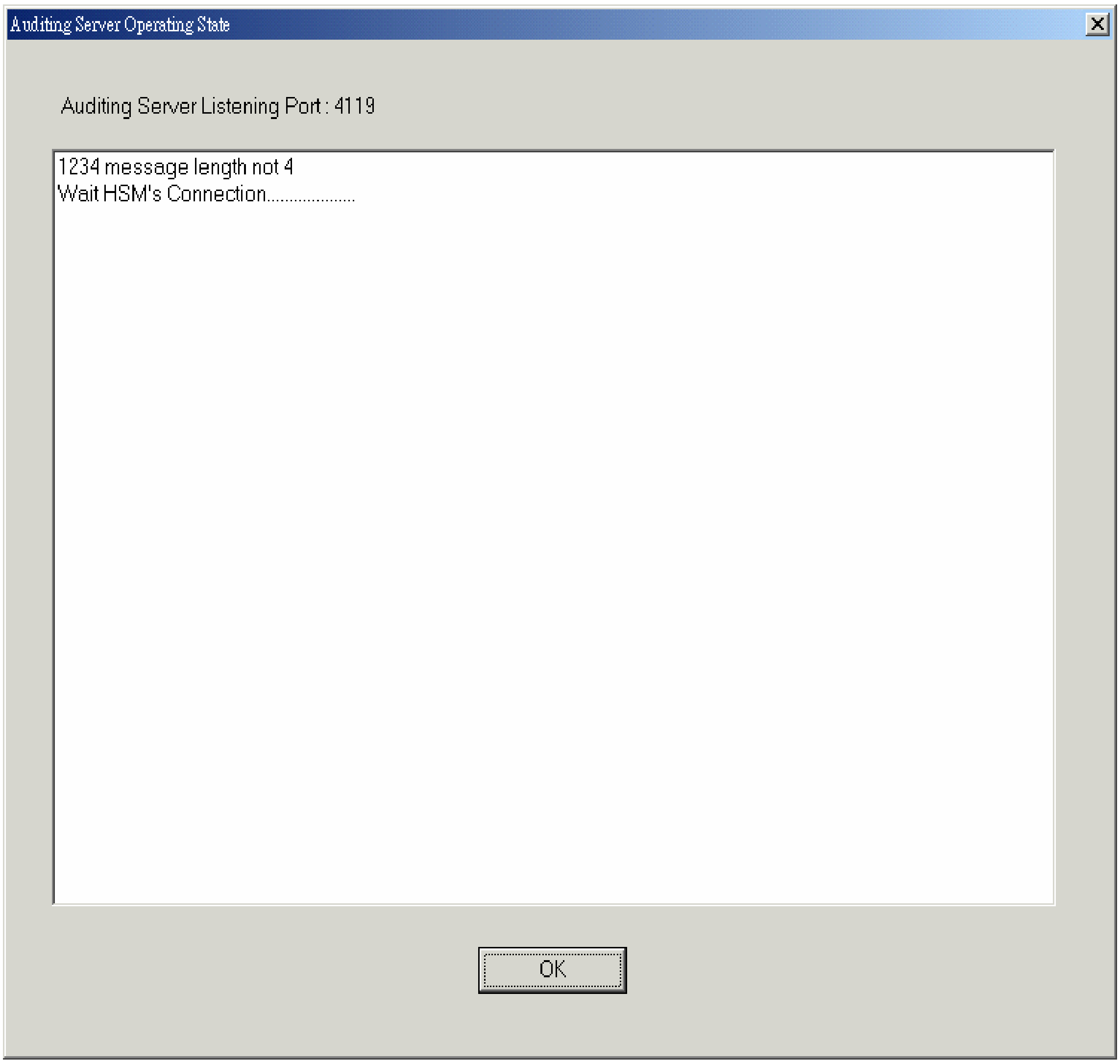
If an immediate activation of the Auditing Server is required, click “Run HSM_Audit_Server Service” item in the same group.

6.4 Show The Status Of the Auditing Server

1. When there is no Secure Hardware connected with the Auditing Server, the icon located on the right-lower corner of Windows is gray. The icon turns green while there is any Secure Hardware connection. Locate the mouse cursor above the icon, and the IP address of the connected Secure Hardware will be displayed accordingly.



2. Double click the icon, or click the right button of the mouse on the icon and select ”Show Operating State”, the Operating state information between Secure Hardware and Auditing Server will be shown.


Auditing Server Operating State
Auditing Server Listening Port : 4119
OK

```
1234 message length not 4
Wait HSM's Connection...................
```

3. On the icon click the right button of the mouse and select " Connected HSM IP" to display the IP address of the connected Secure Hardware.

4. On the icon click the right button of the mouse and select " LogViewer" to activate LogViewer and review the auditing logs. This can also be achieved by clicking the "Start" button of Windows, and from the "Program" menu select the "Logviewer" item in the "Secure Hardware 2.0 Auditing Server" group.

6.5 Stop The Auditing Server

On the icon click the right button of the mouse and select "Exit" to stop the Auditing Server.

6.6 Stop And Remove The Auditing Server Service

Click the ”Start” button of Windows, and from the “Program” menu select ”Stop HSM_Audit_Server Service” item in the “Secure Hardware 2.0 Auditing Server” group to stop the Auditing Server Service. Select ”Remove HSM_Audit_Server Service” item in the same group to remove the Auditing Server Service.

6.7 Uninstall The Auditing Server

Click the ”Start” button of Windows, and from the “Program” menu select ”Uninstall HSM_Audit_Server” item in the “Secure Hardware 2.0 Auditing Server” group to uninstall the Auditing Server.

7. The Log Viewer

7.1 System Requirements

- Hardware Requirement：
  x86 PC， 256MB RAM or above
- Operation System：
  MS Windows NT 4.0 or later.

7.2 Operation

7.2.1 Start The Log Viewer

Execute LogViewer.exe and a Windows menu is shown as the following picture depicts.

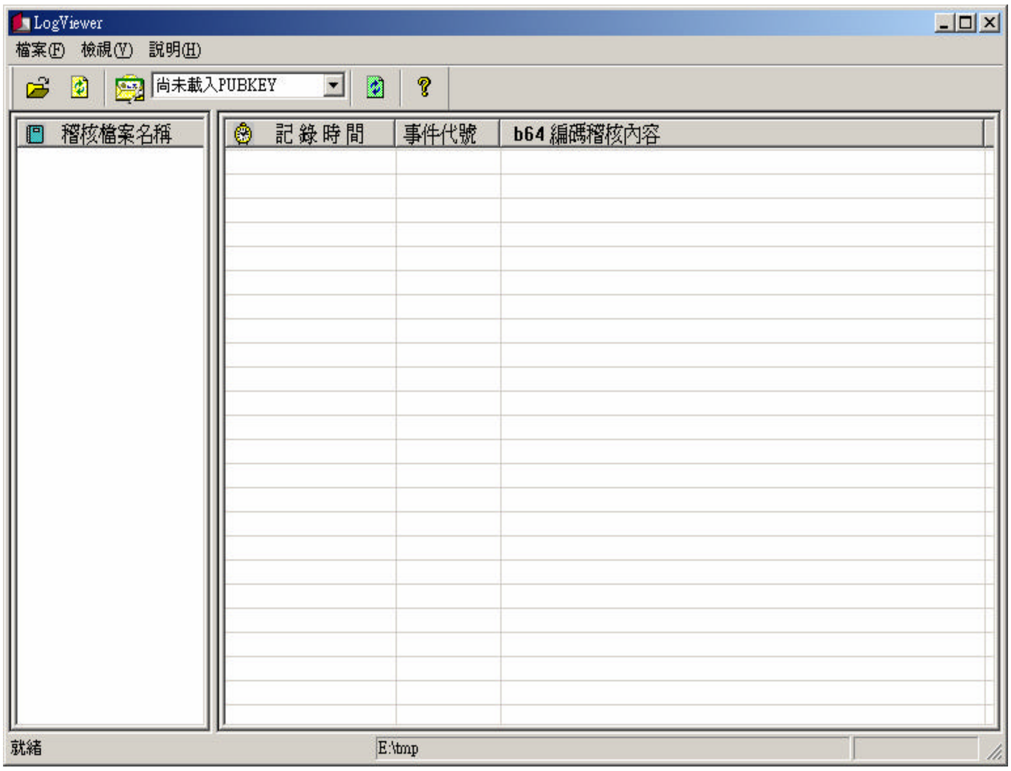
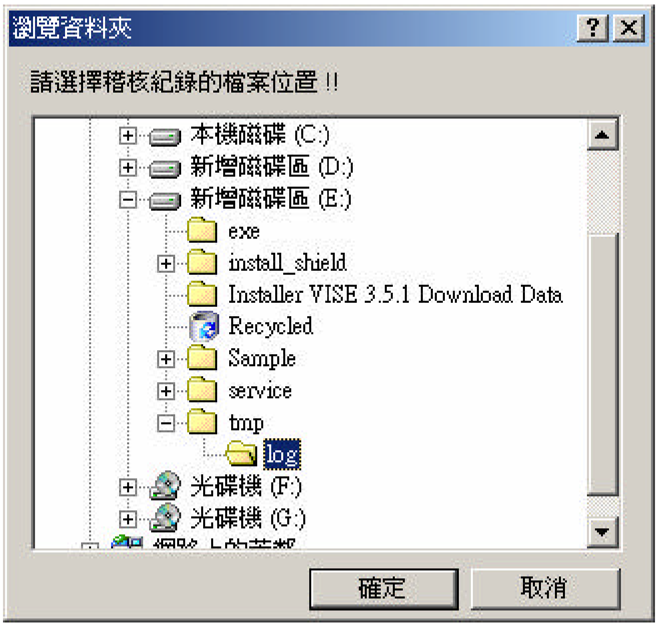


Fig. 7.1 LogViewer.exe

7.2.2 Function Description

Open a directory to store the audit files:

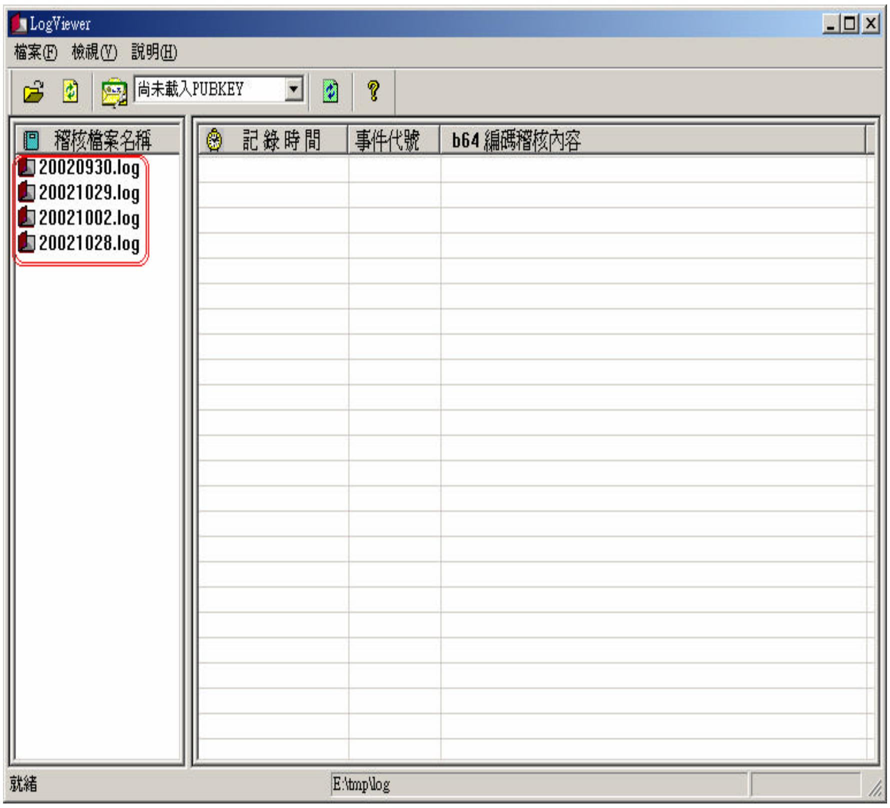
Select a proper directory that can store the audit files, as the following picture depicts:



請選擇稽核紀錄的檔案位置 !!

Fig. 7.2 Open a directory to store the audit files

And the audit files under that directory will be shown as the following picture depicts.

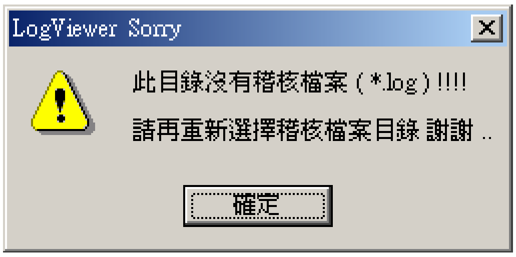


20020930.log
20021029.log
20021002.log
20021028.log

就緒 E:\tmp\log

Fig. 7.3 Showing audit files

If there is no audit file under the selected directory, a warning message is shown as the following picture depicts.



LogViewer Sorry

此目錄沒有稽核檔案 (*.log) !!!!

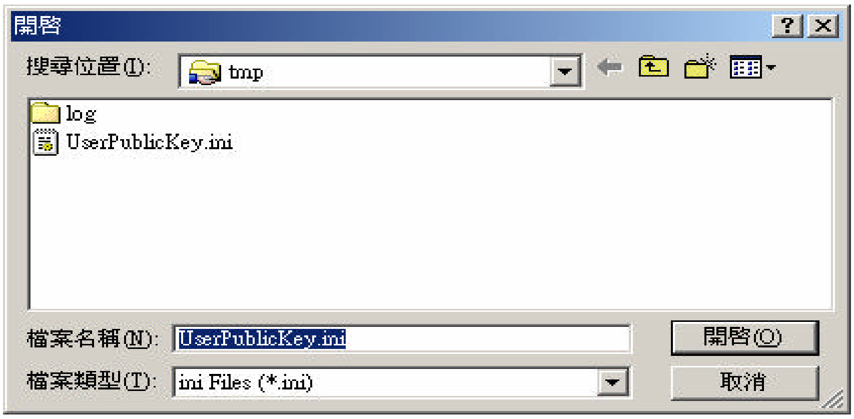
請再重新選擇稽核檔案目錄 謝謝 ..

Fig . 7.4 No audit file is found under that directory

Refresh the auditing directory.

Read the information of the Public Key:

Select the secure hardware SO and the user’s public key files.



檔案名稱(N): UserPublicKey.ini

檔案類型(T): ini Files (*.ini)

Fig. 7.5 Select the secure hardware SO and the user’s public key files

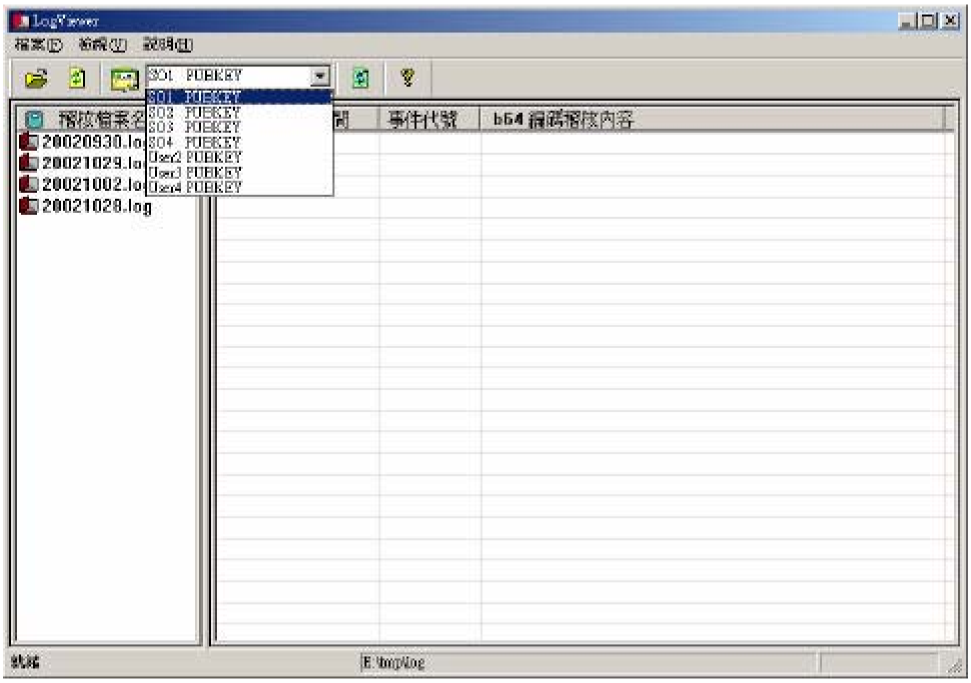
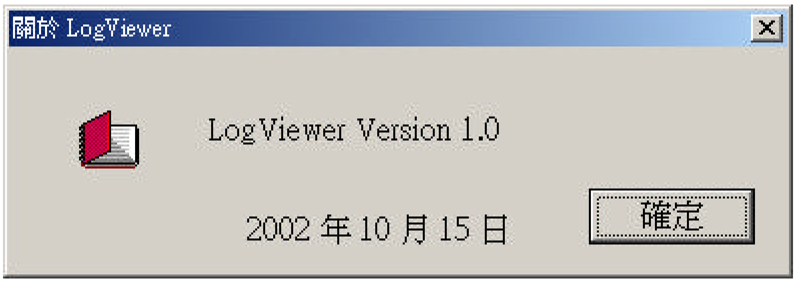


Fig. 7.6 List the secure hardware SO and the user’s public key

Reload the content of Audit files:

About:

LogViewer Copyright information.



LogViewer Version 1.0

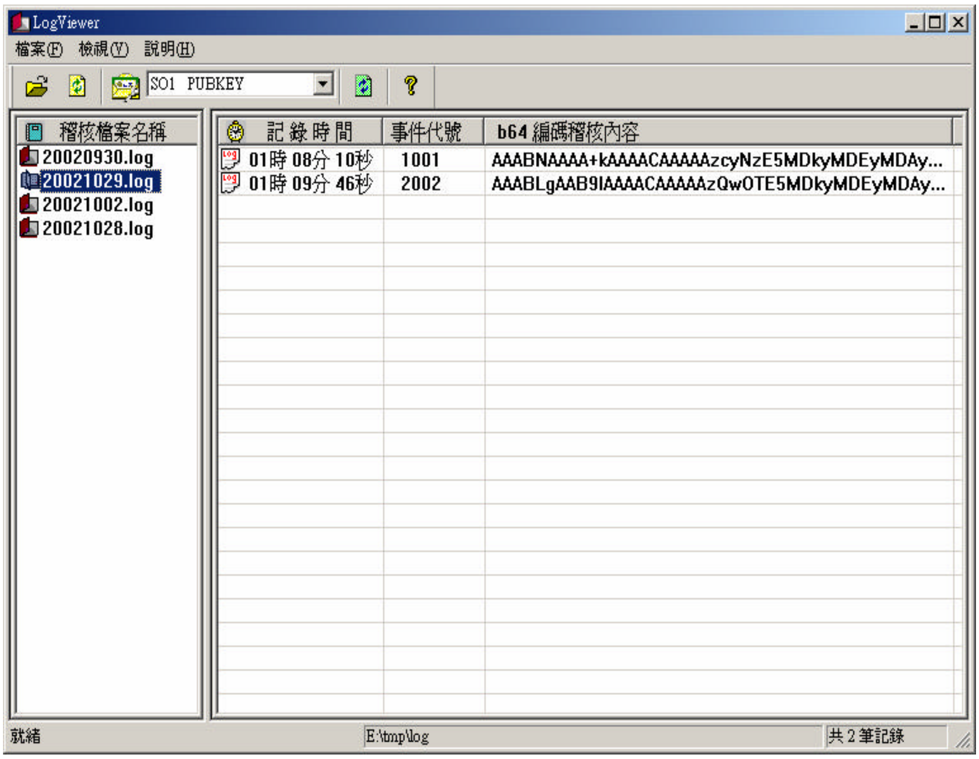
2002 年 10 月 15 日

Fig. 7.7 LogViewer Copyright information

7.3 View The Log

7.3.1 Select The Audit File To View:

Select the audit file of interest with the mouse, as the following picture depicts.



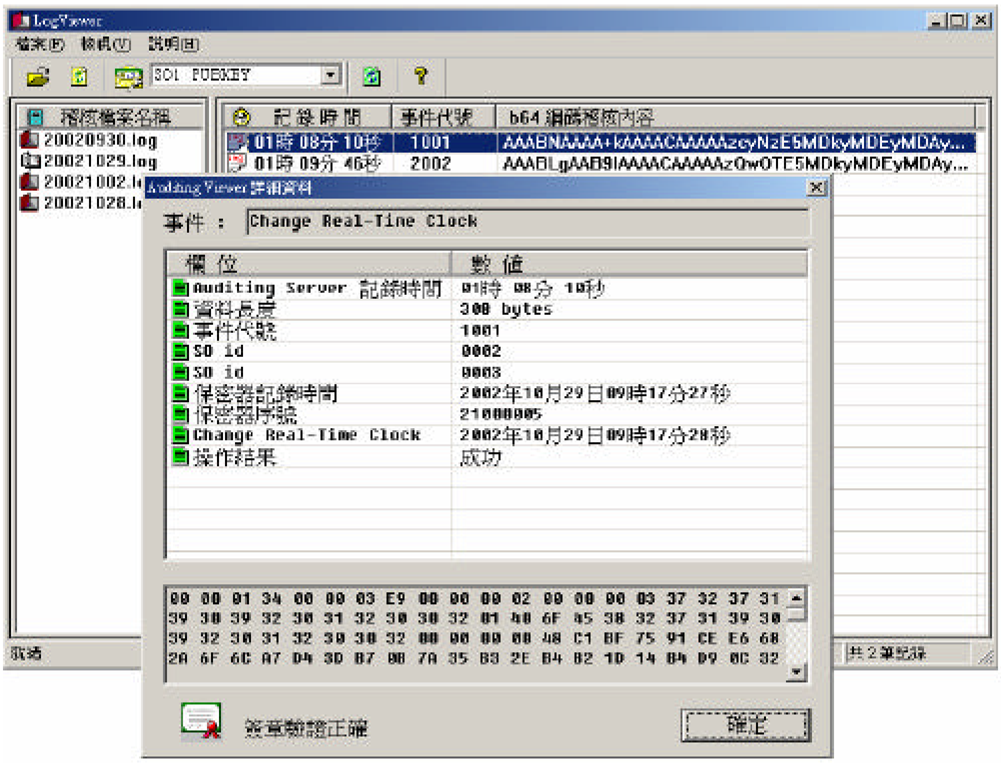
稽核檔案名稱
20020930.log
20021029.log
20021002.log
20021028.log

記 錄 時 間	事件代號	b64 編碼稽核內容
01時 08分 10秒	1001	AAABNAAAA+kAAAACAAAAAzcyNzE5MDkyMDEyMDAy...
01時 09分 46秒	2002	AAABLgAAB9IAAAACAAAAAzQwOTE5MDkyMDEyMDAy...

Fig. 7.8 Select the audit file to view

7.3.2 View The Detailed Record:

Click on the selected audit record to view the detailed information, as the following picture depicts.



記錄時間	事件代號	b64 編碼稽核內容
01時 08分 10秒	1001	AAABNAAAA+kAAAACAAAAAzcyNzE5MDkyMDEyMDAy...
01時 09分 46秒	2002	AAABLgAAB9IAAAACAAAAAzQwOTE5MDkyMDEyMDAy...

Auditing Viewer 詳細資料

事件 : Change Real-Time Clock

欄 位	數 值
Auditing Server 記錄時間	01時 08分 10秒
資料長度	308 bytes
事件代號	1001
SO id	0002
SO id	0003
保密器記錄時間	2002年10月29日09時17分27秒
保密器序號	21000005
Change Real-Time Clock	2002年10月29日09時17分28秒
操作結果	成功

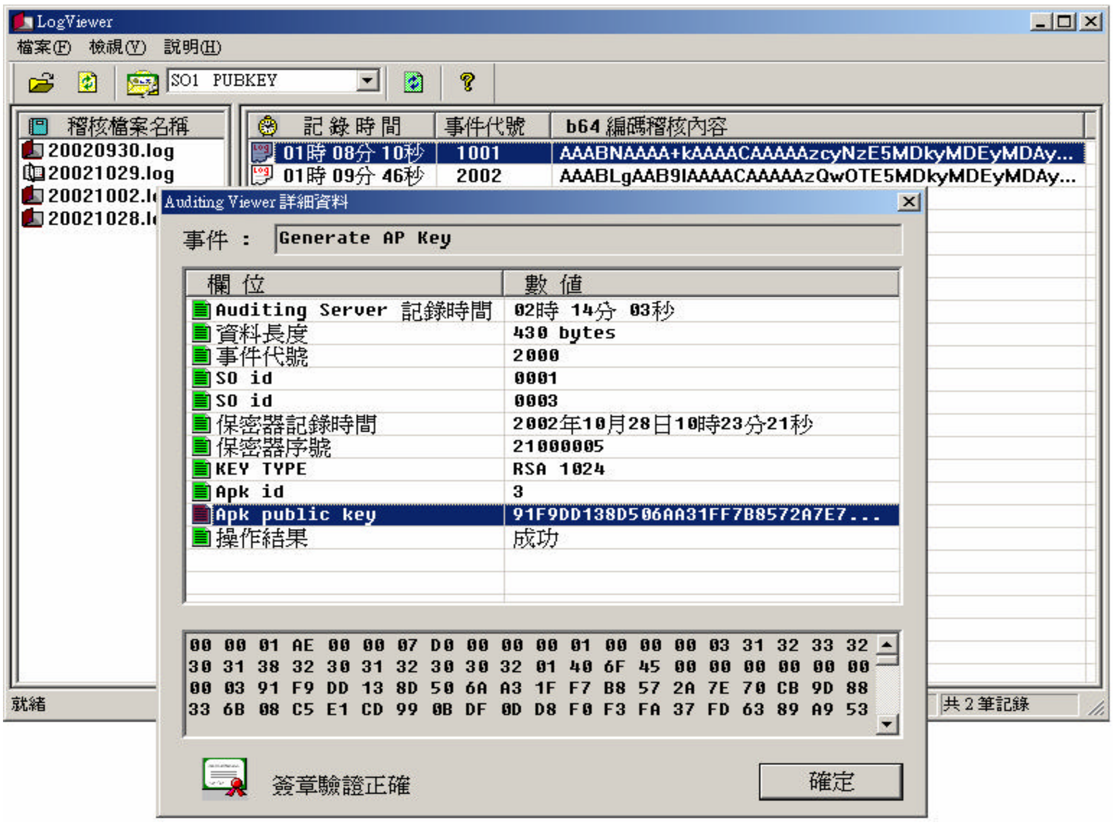
```
00 00 01 34 00 00 03 E9 00 00 00 02 00 00 00 03 37 32 37 31
39 30 39 32 30 31 32 30 30 32 01 40 6F 45 38 32 37 31 39 30
39 32 30 31 32 30 30 32 00 00 00 00 48 C1 BF 75 91 CE E6 68
2A 6F 6C A7 D4 3D B7 0B 7A 35 B3 2E B4 B2 1D 14 B4 D9 0C 32
```

簽章驗證正確

Fig. 7.9 View the detailed record

7.3.3 Display the Apk public key:

Select the Apk public key from the detailed record menu, and the key value is shown as the following picture depicts.



記錄時間	事件代號	b64 編碼稽核內容
01時 08分 10秒	1001	AAABNAAAA+kAAAACAAAAAzcyNzE5MDkyMDEyMDAy...
01時 09分 46秒	2002	AAABLgAAB9IAAAACAAAAAzQwOTE5MDkyMDEyMDAy...

事件 ： Generate AP Key

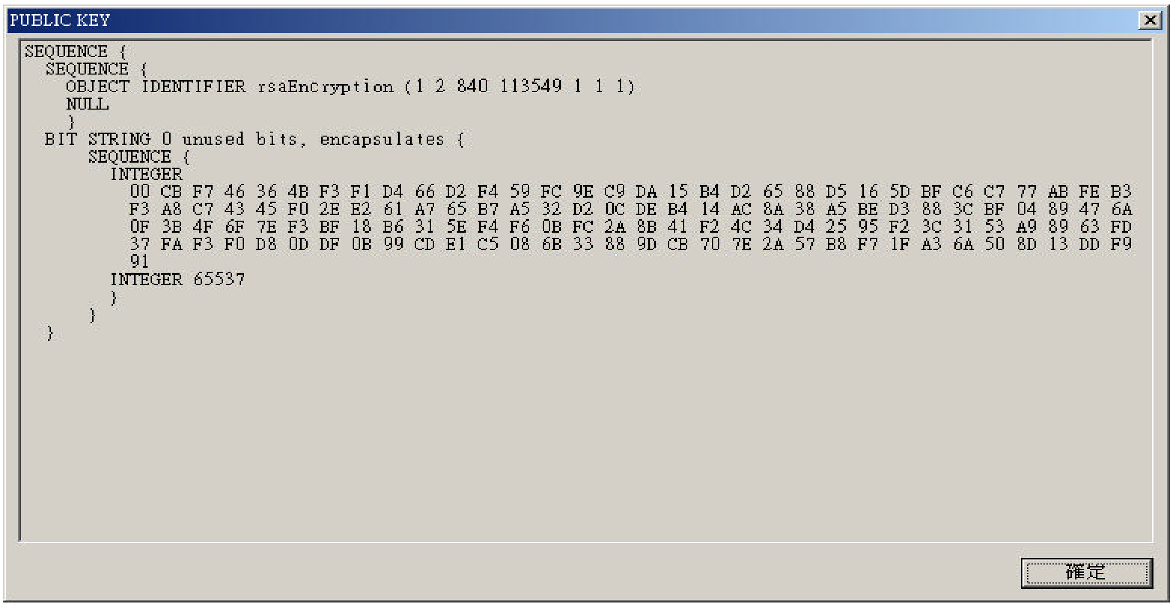
欄 位	數 值
Auditing Server 記錄時間	02時 14分 03秒
資料長度	430 bytes
事件代號	2000
SO id	0001
SO id	0003
保密器記錄時間	2002年10月28日10時23分21秒
保密器序號	21000005
KEY TYPE	RSA 1024
Apk id	3
Apk public key	91F9DD138D506AA31FF7B8572A7E7...
操作結果	成功

```
00 00 01 AE 00 00 07 D0 00 00 00 01 00 00 00 03 31 32 33 32
30 31 38 32 30 31 32 30 30 32 01 40 6F 45 00 00 00 00 00 00
00 03 91 F9 DD 13 8D 50 6A A3 1F F7 B8 57 2A 7E 70 CB 9D 88
33 6B 08 C5 E1 CD 99 0B DF 0D D8 F0 F3 FA 37 FD 63 89 A9 53
```

簽章驗證正確

Fig. 7.10 Display the Apk public key

Click on the Apk public key to view its value, as the following picture depicts.



```
SEQUENCE {
  SEQUENCE {
    OBJECT IDENTIFIER rsaEncryption (1 2 840 113549 1 1 1)
    NULL
    }
  BIT STRING 0 unused bits, encapsulates {
      SEQUENCE {
        INTEGER
          00 CB F7 46 36 4B F3 F1 D4 66 D2 F4 59 FC 9E C9 DA 15 B4 D2 65 88 D5 16 5D BF C6 C7 77 AB FE B3
          F3 A8 C7 43 45 F0 2E E2 61 A7 65 B7 A5 32 D2 0C DE B4 14 AC 8A 38 A5 BE D3 88 3C BF 04 89 47 6A
          0F 3B 4F 6F 7E F3 BF 18 B6 31 5E F4 F6 0B FC 2A 8B 41 F2 4C 34 D4 25 95 F2 3C 31 53 A9 89 63 FD
          37 FA F3 F0 D8 0D DF 0B 99 CD E1 C5 08 6B 33 88 9D CB 70 7E 2A 57 B8 F7 1F A3 6A 50 8D 13 DD F9
          91
        INTEGER 65537
        }
      }
  }
```

Fig. 7.11 Apk public key

7.4 The Event Code Of Audit Records

Table 7.1 The data type and length of auditing records

Label	Type	Length (byte)
Length	Int	4
Event ID	Int	4
Audit Time	Char	14
HSM serial number	Int	4
HSM IP address	Char	4
Audit flag	Int	4
Audit server IP	Char	4
Audit server Port	Int	4
SO ID	Int (0-3)	4
SO public key	Char	128
User ID	Int (4-12)	4
User Public Key	Char	128
User Count	Int	4
AP key type	Int	4
AP key ID	Int	4
AP key ACL	Char	45
Ap key public key	Char	128,256,512
Hash (MK)	Char	20
HK public key	Char	128
Result	Int	4
Signature	Char	128

Table 7.2 Initial states of audit events

Event	Event code	Data
Configure Real-Time Clock	0001	Length+ Event ID+ Audit Time+ HSM serial number+ Result
Generate Master Key	0002	Length+ Event ID+ Audit Time+ HSM serial number+ Hash(MK)+ Result
Import Master Key	0003	Length+ Event ID+ Audit Time+ HSM serial number+ Hash(MK)+ Result
Create Security Officer key	0004	Length+ Event ID+ Audit Time+ HSM serial number+ SO ID+ Result
Import Security Officer key	0005	Length+ Event ID+ Audit Time+ HSM serial number+ SO ID+ SO public key+ Result
Generate Hardware key	0006	Length+ Event ID+ Audit Time+ HSM serial number+ HK public key+

		Result
Configure HSM IP, Audit flag, Audit server IP & port	0007	Length+ Event ID+ Audit Time+ HSM IP+ HSM serial number+ Audit flag+ Audit IP+ Audit Port+ Result

Since there’s no operator ID for the initial state, the events on table 7.2 just send the event code and data to the audit server, no signature attached.

Table 7.3 operational state audit events

Event	Event code	Data
Configure Real-Time Clock	0001	Length+ Event ID+ Audit Time+ HSM serial number+ Result
Generate Master Key	0002	Length+ Event ID+ Audit Time+ HSM serial number+ Hash(MK)+ Result
Import Master Key	0003	Length+ Event ID+ Audit Time+ HSM serial number+ Hash(MK)+ Result
Create Security Officer key	0004	Length+ Event ID+ Audit Time+ HSM serial number+ SO ID+ Result
Import Security Officer key	0005	Length+ Event ID+ Audit Time+ HSM serial number+ SO ID+ SO public key+ Result
Generate Hardware key	0006	Length+ Event ID+ Audit Time+ HSM serial number+ HK public key+ Result
Configure HSM IP, Audit flag, Audit server IP & port	0007	Length+ Event ID+ Audit Time+ HSM IP+ HSM serial number+ Audit flag+ Audit IP+ Audit Port+ Result
Set Network Configuration	1000	Length+ Event ID+ SO ID+ SO ID+ Audit Time+ HSM serial number+ HSM IP+ HSM Port+ Result+ Signature (so id 1)+ Signature (so id 2)
Change Real-Time Clock	1001	Length+ Event ID+ SO ID+ SO ID+ Audit Time+ HSM serial number+ Change Time+ Result+ Signature (so id 1)+ Signature (so id 2)
Create SO	1002	Length+ Event ID+ SO ID+ SO ID+ Audit Time+ HSM serial number+ Create SO ID+ Result+ Signature (so id 1)+ Signature (so id 2)
Generate Hardare key	1004	Length+ Event ID+ SO ID+ SO ID+ Audit Time+ HSM serial number+ HK public key+ Result+ Signature (so id 1)+ Signature (so id 2)
Create User	1006	Length+ Event ID+ SO ID+ SO ID+ Audit Time+ HSM serial number+

		User ID+ User Public key+ Result+ Signature (so id 1)+ Signature (so id 2)
Import User key	1007	Length+ Event ID+ SO ID+ SO ID+ Audit Time+ HSM serial number+ Import User ID+ User Public Key+ Result+ Signature (so id 1)+ Signature (so id 2)
Erase ALL AP key	1008	Length+ Event ID+ SO ID+ SO ID+ Audit Time+ HSM serial number+ Result+ Signature (so id 1)+ Signature (so id 2)
Switch to Initialization state & Erase ALL keys	1009	Length+ Event ID+ SO ID+ SO ID+ Audit Time+ HSM serial number+ Result+ Signature (so id 1)+ Signature (so id 2)
Generate AP Key	2000	Length+ Event ID+ SO ID+ SO ID+ Audit Time+ HSM serial number+ AP Key Type+ AP Key ID+ AP Key Public Key+ Result+ Signature (so id 1)+ Signature (so id 2)
Import AP key	2001	Length+ Event ID+ SO ID+ SO ID+ Audit Time+ HSM serial number+ AP Key Type+ AP Key ID+ Import APK Public key+ Result+ Signature (so id 1)+ Signature (so id 2)
Delete AP Key	2002	Length+ Event ID+ SO ID+ SO ID+ Audit Time+ HSM serial number+ AP Key Type+ AP Key ID+ Result+ Signature (so id 1)+ Signature (so id 2)
Backup APK shares onto IC Card	2003	Length+ Event ID+ SO ID+ SO ID+ Audit Time+ HSM serial number+ AP Key Type+ AP Key ID+ Result+ Signature (so id 1)+ Signature (so id 2)
Set APK ACL	2004	Length+ Event ID+ SO ID+ SO ID+ Audit Time+ HSM serial number+ AP Key Type+ AP Key ID+ ACL+ Result+ Signature (so id 1)+ Signature (so id 2)
Set APK active (User)	2005	Length+ Event ID+ User Count+ User ID…. + Audit Time+ HSM serial number+ AP Key Type+ AP Key ID+ Result+ Signature (user id 1….)

The events on table 7.3 require HSM to compute a SHA1 hash of the data (from Event ID to Result), and then use the operator's private key to sign the hash.