USB Security key installation

This sheet describes how to install the security key used by the SPYRO® software This Installation should be executed at the computer where the Aladdin TimeHASP Security USB key is physically inserted.
When the SPYRO® software uses the security key at the same computer as where the USB security key is inserted only the *local security key installation* is necessary. When the security key is used by SPYRO via a network a host service needs to be activated as well at the server, this is explained in the *network security key installation* section.

Local Security key installation

Do not insert the USB security key before the driver is installed, and the PC is rebooted.

It is necessary to be logged in with administrator rights to install the driver program. Execute `HASPINST4116.EXE` with the argument /i to install the driver program that allows for the communication with the security key.

```
HASPINST4116 /i
```

A window will be displayed when the installation is successful, this may take a few minutes. Before inserting the USB security key, it is necessary to reboot the PC. Only after the PC is rebooted, and completely restarted, the USB security key may be inserted into one of the designated slots. Failure to do so may hinder MS Windows in properly recognizing the security key and assigning the right driver functionality to it.
A red led will illuminate on the key when inserted.

Copy the PYROTEC.INI file anywhere in the PATH, or into the directory designated by the SPYRO environment variable.

Verification

Proper installation of the security key and the driver of the security key can be verified using the program `KEYTEST.EXE`.

```
KEYTEST
```

Upon successful installation the following messages will be displayed:

```
KEYTEST 2.6 - COPYRIGHT 2009
TECHNIP BENELUX B.V. / PYROTEC DIVISION

PYROTEC SUPPLIED LOCAL SECURITY KEY DETECTED
LOCAL PYROTEC SECURITY KEY PY0001 FOUND
```

Upon unsuccessful installation the following messages will be displayed:

```
KEYTEST 2.6 - COPYRIGHT 2009
TECHNIP BENELUX B.V. / PYROTEC DIVISION

NO PYROTEC SUPPLIED LOCAL SECURITY KEY DETECTED
NO PYROTEC SUPPLIED NETWORK SECURITY KEY DETECTED
CANNOT IDENTIFY VALID LOCAL OR NETWORK SECURITY KEY
```

If the security key cannot be found, please verify the proper installation of the HASP device driver. To query the status of the HASP driver execute HASPINST4116.EXE with the /info argument.

```
HASPINST4116 /info
```

A window with status information will then be shown.

Removal

To remove the driver program for the security key execute `HASPINST4116.EXE` with the /r argument, again using administrator rights.

```
HASPINST4116 /r
```

A window will be displayed when the removal is successful.

Network Security key installation

This part describes how to install the security key used by SPYRO® in a network. The installation procedure for a PC with network security support is separated into two stages:

- Installation of the network support on the host computer;
- Installation of the SPYRO® executable on the application computer.

The "*host computer*" is the computer that holds the security key. This must be a PC operating Windows NT, 2000 or XP, but it does not necessarily need to be the network server.
The "*application computer*" is a different computer on which the user runs the SPYRO® software. This can be a PC operating either Windows 95 / 98 or Windows NT, 2000 or XP.

Host computer Installation

The following steps should be taken to install the network support for SPYRO®.

- To install the drivers for the security key first execute the *local security key installation*.
- To install the "KeyHostservice" use the `KeyHost24Installer.exe`. After successful installation of the service the computer will have to be restarted.

```
KeyHost24Installer
```

Take a note of the network name of the PC. This name can be found in the "network" section of the "control panel". In the "identification" section, the name is listed in the "computer name" field. This name is needed in the local executable installation, for instance "PC_KEYHOST".

Application computer Installation

Now the SPYRO® software can be installed on the application computer. Installation of the SPYRO® SAPC, SRTO or SPSL software is described in another document. For the installation of the offline SPYRO® program, the *local security key installation* is not necessary on the application computer.

The following additional steps should be taken after the SPYRO® software is successfully installed.
Go to the installation directory and edit the PYROTEC.INI file to reflect the computer name of the host computer with the security key. The name "PyrotecServer" is the name of the property. The value should be the name of the PC holding the security key, in this case "PC_KEYHOST" is given as example. The line should look like:

```
PyrotecServer = PC_KEYHOST
```

Copy the PYROTEC.INI file into one of the following three directories. They are searched in this order:
1. The directory indicated by the SPYRO environment variable.
2. The directory in which the main calling module is placed.
3. The Windows directory, i.e. the directory indicated by the WINDIR environment variable
Specifically for the SPYRO® SAPC, SRTO or SPSL software there are additional environment variables.

In the rare case that another Aladdin HASP key is connected to the application computer, whereas the network key should be queried, then change also the property "NetworkOnly" in the PYROTEC.INI file to 1. This will force the SPYRO software to ignore a local inserted key.

```
NetworkOnly = 1
```

Verification

Proper installation of the security key at the host computer and the driver of the security key can be verified using the program `KEYTEST.EXE` at the application computer.

```
KEYTEST
```

Upon successful installation the following messages will be displayed:

```
KEYTEST 2.6 - COPYRIGHT 2009
TECHNIP BENELUX B.V. / PYROTEC DIVISION

NO PYROTEC SUPPLIED LOCAL SECURITY KEY DETECTED
PYROTEC SUPPLIED NETWORK SECURITY KEY DETECTED
NETWORK SECURITY KEY PY0001 FOUND
```

Installing HASP Drivers on newer operating systems

The HASP drivers v 4.116 as described above are valid for the next Microsoft operating systems.

- 32-bit: Windows 98SE, Windows ME, Windows NT, Windows 2000
- 32- and 64-bit: Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008

To install the drivers also on newer Microsoft operating systems we advise to use the latest HASP driver, currently this is v6.22 and can be used also on

- 32-bit: Windows 2000,
- 32-bit and 64-bit: Windows XP, Windows Server 2003, Windows Vista, Windows 2008, Windows 7
- 64-bit: Windows 2008 R2

Find the latest HASP drivers also at: http://www.spyrosuite.com/download

Running EFPS and SPYRO on 64 bit systems (Security error -2013)

It is very likely that EFPS and SPYRO will not run on 64 bit systems using a local attached key for security. This is caused by the security communication between the EFPS or SPYRO program and the HASP drivers. Still the key is successfully detected when using the KeyTest tool.
The solution is to divert the security communication via the network as is provided by the Pyrotec Keyhost service.

- Install the Pyrotec Keyhost service
- Edit the Pyrotec.ini to divert the Pyrotec software to check the key over the network protocol.
  ```
  PyrotecServer = PC_KEYHOST
  NetworkOnly = 1
  ```
- Check the key with keytest, the key should now be successfully detected as a network key.

Issue with local key use via remote desktop

Amongst other Windows 2003 Server causes a problem with the local use of the key when the user is logged on via remote desktop. This is caused by the HASP drivers that do not allow access to the key via a remote desktop session. This is true for Windows 2003 Server, for other non Server Windows versions this is no problem as with those Windows versions it is not possible to have multiple concurrent logins. For other Windows Server versions this has not been tested.
When the user is local logged on, then the Pyrotec Keytest will successfully detect the key. When the user is remotely logged on, then the Pyrotec Keytest will fail.

Also the above described Aladdin DiagnostiX tool will fail and show (in red) the message: "Terminal Server was found"

The solution to bypass this remote desktop protocol check is to force the network use as provided by Pyrotec service Keyhost.

- Install the Pyrotec Keyhost service at the Windows 2003 Server.
- Edit the Pyrotec.ini to force the Pyrotec software to check the key over the network protocol.
  ```
  PyrotecServer = PC_KEYHOST
  NetworkOnly = 1
  ```
- Check the key with keytest, the key should now be successfully detected as a network key.

Network key Issues

In some cases the verification with the KEYTEST.EXE program might be unsuccessful. One of the next messages might be issued after running the keytest program.

```
CreateFile returned: 123.
```

The filename, directory name, or volume label syntax is incorrect.

```
CreateFile returned: 1326.
```

Logon failure: unknown username or bad password.

The reason is most probably the failing authorization of the user on the *host computer*. The user of the SPYRO® software on the *application computer* must also be authenticated on the *host computer*. Technically spoken, for the license network communication the Named Pipes functionality of Microsoft Windows is used. This means that the User Credentials of the user who runs SPYRO® must be known and have sufficient rights to access the key host interface on the *host computer*.
To verify if the use has file access to the *host computer* browse to the hostname using Windows Explorer: \\hostname. If this fails then the access permissions or firewall have to be changed such that access for the user is granted. A possible solution is to define on the *host computer* a username with access to share one of its folders; the user should map this shared folder with the username.

Another message that can be issued by the Keytest program is:

```
CreateFile returned: 5.
```

Access Denied error.

This is caused by the local system identity running the SPYRO software (through RTO or APC) trying to find the remote Pyrotec Security Key. For most current Windows systems this is initially restricted for security reasons, the local sytem should be allowed access to the Named Pipe “PyrotecPipe” by adding this Pipe Name to the registry key
`\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\NullSessionPipes`
More information on this topic is found in the next Microsoft Know-How article:
http://support.microsoft.com/kb/126645 (Access Denied When Opening a Named Pipe from a Service)

Another reason can be the firewall preventing the Named Pipes protocol. This protocol as part of the inter process communication (IPC) over the SMB protocol requires the following ports to be open

- Ports 135 through 139 and 445 for both the TCP and UDP protocol

More information on this topic is found in the next Microsoft Know-How article:
http://support.microsoft.com/kb/298804 (Internet firewalls can prevent browsing and file sharing)

Keyhost Service Interruption Issue

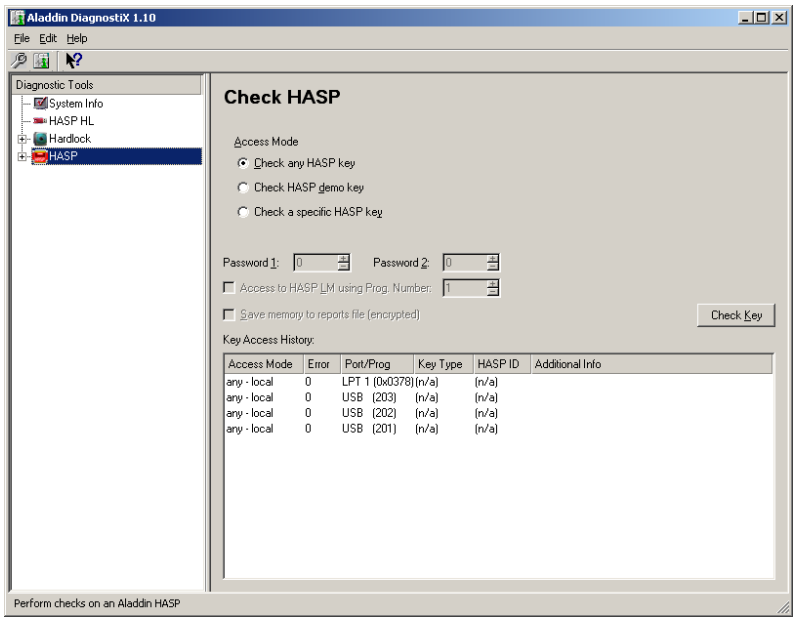
The Microsoft Data Execution Prevention settings may cause the keyhost service to be interrupted and stop the service from running. It will then not be able for remote clients to use the key to validate the security of the SPYRO® program.
The Data Execution Preventionshould be disabled for the program *keyhost.exe* . The settings for Data Execution Preventioncan be found via Control Panel > System > Advanced > Performance Settings > Data Execution Prevention tab. Select the option ‘Turn on DEP for all programs and services except those I select’ and add the keyhost.exe program.

Multiple HASP keys

Only a single HASP security key should be connected to the computer for validation of the Pyrotec software. Any additional HASP key of any kind will interfere. Successful use of the key for validation of Pyrotec software will very likely fail.
To check if multiple HASP keys are connected to the computer we advise the use of the Aladdin HASP DiagnostiX tool (version 1.10)

ftp://ftp.aladdin.com/pub/hasp/hl/windows/installed/redistribute/Aladdin_Diagnostics.zip

This HASP diagnotics tool can check any connected HASP key. Select in the tree in the left pane ‘HASP’. The right pane will then show the ‘Check HASP’ option, click on the ‘Check key’ button, while ‘Check any key’ is selected. In the report history at the bottom the detected keys will be indicated.



An extensive test procedure
Security errors (-2001, -2012, -2013, -2014, -3004, -3005, 03006)

In any kind of security error we advise to follow the next procedure to make sure that all required settings are correct. The next procedure will verify that the Pyrotec Security Key is properly installed and can be detected both local and via a remote computer client. Also the SPYRO environment variable is verified.

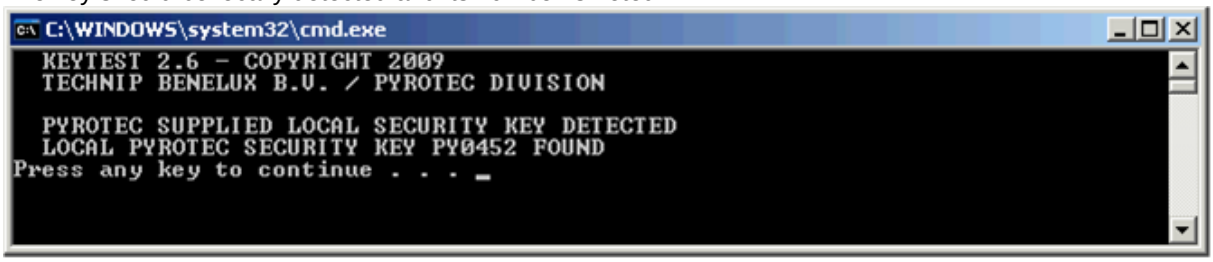
The first target is to verify that the Pyrotec Security Key is properly installed and can be detected at the local computer to which it is physically connected. Before proceeding with this test make sure that the HASP drivers are installed with the command

```
HASPINST4116 /info
```

A confirmation window with status information will then be shown.

This verification of the HASP driver also works with the more recent versions of the HASP drivers.

LOCAL KEY TEST
Verify if if the key can be detected with the *keytest* utility physically connected to the local machine. This test should not be executed through a remote desktop connection. Make sure that in the *Pyrotec.ini* file located in the same folder as the keytest utility that the line "NetworkOnly = 0" is present.
The key should be locally detected and its number is noted.



If the key is not detected, then

- Check if you are not working via remote desktop or any other remote connection
- Check if the key is connected to the computer and the red light is on
- Check if the HASP drivers are installed

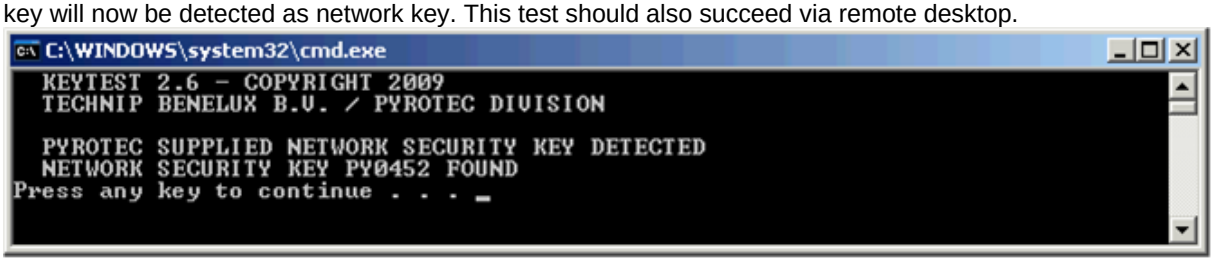
LOCAL NETWORK KEY TEST VIA LOOPBACK

If the key is to be used in a network environment at other remote computer, then proceed with the next steps. Else continue to the step where the SPYRO environment variable is verified and defined.

Please note that this test is also possible through a remote desktop connection. Once the key is locally detected, then make sure that the Pyrotec Keyhost software is installed and running. Verify if the process called *keyhost.exe* is active. If keyhost is active then update the Pyrotec.ini in the same folder as the keytest utility contains the lines

"PyrotecServer = <hostname or ip address>"
"NetworkOnly = 1"

The <hostname or ip address> should be the hostname of this computer. Run the keytest utility again, the key will now be detected as network key. This test should also succeed via remote desktop.



If the key is not detected, then check the keyhost installation.

REMOTE NETWORK KEY TEST

If the key can be locally detected as network key, then the detection can be tested from a remote computer. Switch to another computer that is connected to the same network as the computer where the key is installed. The computers should be able to communicate to each other.
In this test the Pyrotec.ini (to be in the same folder as keytest.exe) should contain the lines

"PyrotecServer = <hostname or ip address>"
"NetworkOnly = 0"

The <hostname or ip address> should be the server/computer where the key is physically connected to as in the previous test. The key should again be detected as network key.

If the key is not detected, then

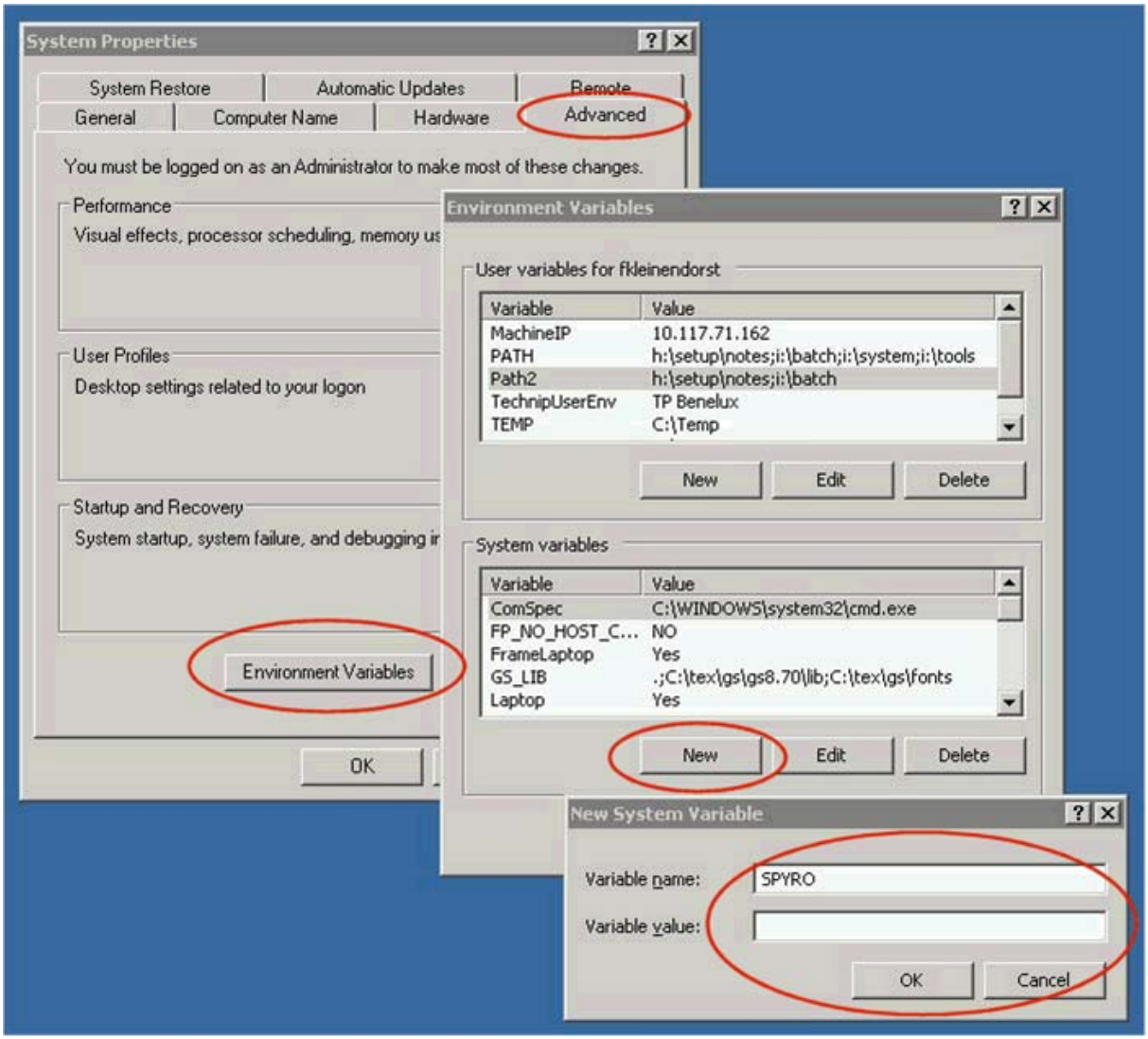
- Verify the hostname specification in the pyrotec.ini file.
- Verify the network connection to the key host server. Can the host be reached through a ping command?
- Verify if the user is authenticated on the keyhost server (see Network key Issue).

If this last test is successful, then it is possible to run the SPYRO software on the remote machine. It might be necessary to define the SPYRO environment variable to identify the folder where the SPYRO dll is located and the security files (PRTC, PRTYPR and Pyrotec.ini). Of course the Pyrotec.ini residing in the same folder as the SPYRO dll should be updated accordingly.

SPYRO ENVIRONMENT VARIABLE

When the key can be detected, but SPYRO fails due to security errors then it is most likely that the SPYRO environment variable is undefined. This environment variable defines for the SPYRO program where to find the security files (PRTPYR and PRTC) and the Pyrotec.ini. Once defined it should be possible to run the program using the SPYRO dll.

To verify and define the SPYRO environment variable go to the *System Properties*, select the *Advanced tab* and click the *Environment Variables* button. Here the SPYRO environment variable can be verified and if necessary be (re)defined. The SPYRO environment variable can be defined as user or system variable, we strongly advise to apply it as a system variable. Create a new, define or redefine the system variable named "SPYRO". The value of the SPYRO environment variable should be the folder where the SPYRO program is installed.



RUNNING DIFFERENT SPYRO PROGRAMS ON ONE COMPUTER

Pyrotec's online software for embedding the SPYRO model in third party applications (eg Excel, Aspen, Honeywell or Invensys software) require as a prerequisite the definition of the SPYRO environment variable. In special cases it can be necessary to run both the offline SPYRO program as well as one or more online SPYRO models on the same computer. It will then be necessary to apply multiple environment variables, one for each program.

The next program specific environment variables can be additionally used. These environment variables overrule the default SPYRO environment variable, which can be used for the offline SPYRO/EFPS software.

- SPYRO_RTO (only to be used with EFML, online SPYRO, SRTO software)
- SPYRO_SAPC (only to be used with SAPC software)
- SPYRO_SPSL (only to be used with SPSL software)

These program specific environment variables may co-exist with the SPYRO environment variable.

Please do note that the delivered security files for the each program cannot be exchanged with security files of other Pyrotec software.

TABLE OF LICENSE RELATED ERROR CODES

Error code	Error description
-2001	CPU ID not valid (or wrong security key inserted).
-2002	License expiration date exceeded
-2003	File integrity error. The PRTC file is corrupted (or for another project)
-2004	The password in the PRTPYR is not correct. The combination PRTC and PRTPYR may be wrong, or typo in the password.
-2006	Last used date and time incorrect.
-2008	Cannot open Pyrotec file (PRTC.DAT)
-2009	User file (PRTPYR.DAT) not found.
-2012	Cannot locate a security key (either locally or on the network).
-2013	Cannot locate a security key (on the network).
-2014	Network settings file (PYROTEC.INI) not found.
-3004	The binary license file (PRTC) cannot be accessed
-3005	The ASCII password file (PRTPYR) cannot be accessed
-3006	The geometry file (*.KTI) cannot be found / accessed.