



beyond
payment

Software Authentication Tool (SAT)

For ICT220 Terminals



CONTENTS

1. Introduction	6
1.1. Purpose	6
1.2. Terminology and abbreviations	6
2. Environment	7
3. Installation process	8
3.1. Software installation	8
3.2. Terminal Tool configuration	8
4. General information on tool	16
4.1. Mockup version	16
4.2. Launching the tool	16
4.3. Main functions	17
4.4. Communication Port selection	18
5. Generating a downloadable file	20
5.1. Environment	20
5.2. Signing a scheme	20
5.3. Deleting a signed scheme	23
5.4. Creating the parameter file	24
5.5. Signing and authenticating an application	24
5.6. Checking a signed application	27
5.7. Selecting the default used certificate	27
6. Tool management	28
6.1. Modifying card PIN CODE	28
6.2. Changing your own password	28
6.3. Event log	29

6.4. Changing the tool language	29
6.5. Defining a new translation language	29
7. Using SAT in command mode	30
7.1. Command mode requirements	30
7.2. Example of configuration file	31
7.3. Running SAT in command mode	32
8. Tool un-installation	32
9. Parameter file description	33
10. Appendices	34
10.1. List of shortcut keys	34
10.2. Installing signature tool terminal driver	34
10.3. Network connection Troubleshooting	47

1. Introduction

1.1. Purpose

This document describes the manner in which to install and use the Software Authentication Tool (**SAT**). This tool allows the VAR to compute in a first step a local software signature and in a second step to get a remote authentication by INGENICO server. This application software, signed and authenticated, can be downloaded in ICT220 terminals.

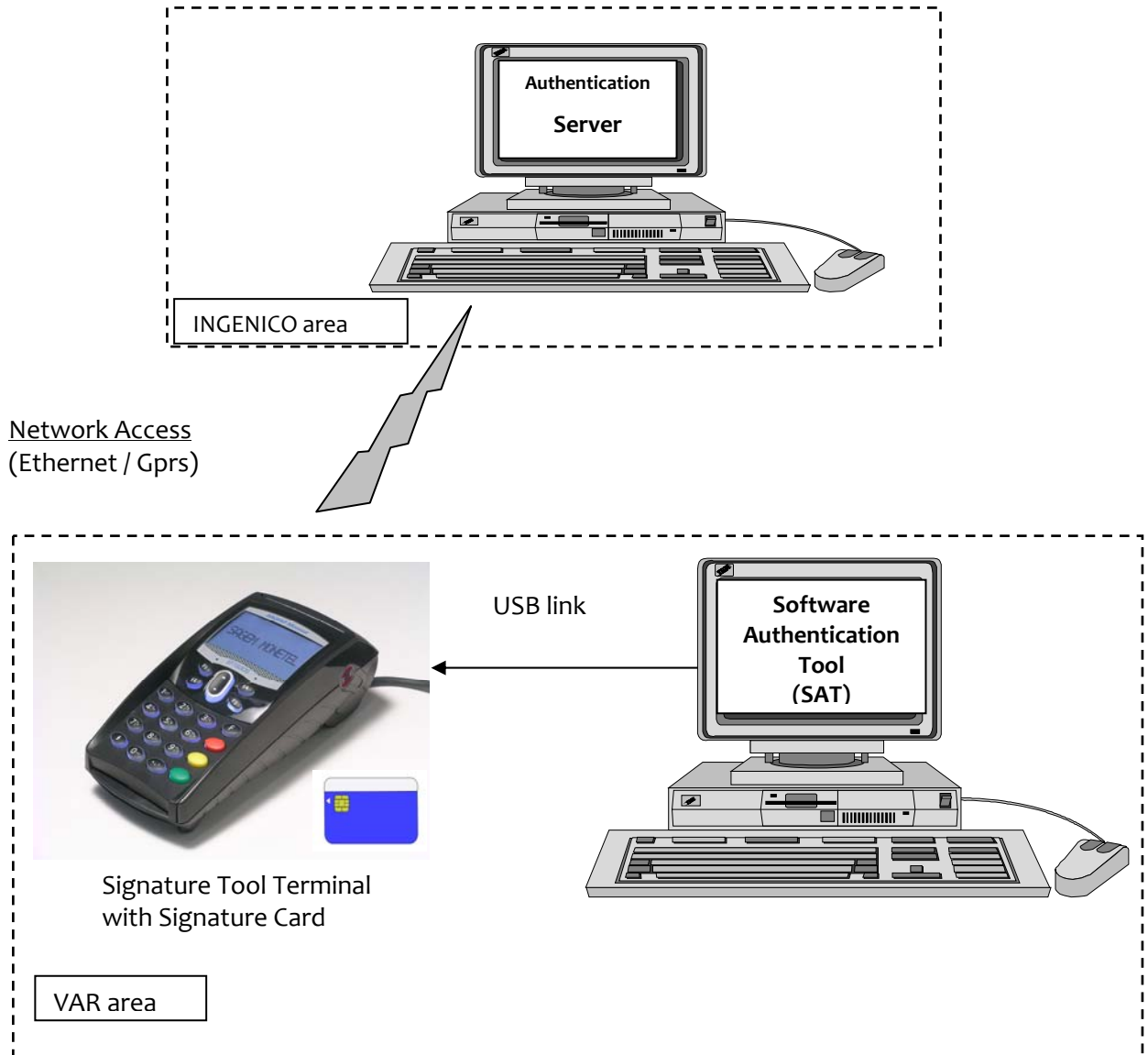
1.2. Terminology and abbreviations

- **Application software :**
Software component to be downloaded in the main processor of the terminal.
- **Certification authority:**
Entity personalizing cryptographic cards including VAR ciphering key. This entity is also named "Trusted Third Party" for the definition of certification keys.
- **Signature card :**
Card used by the banker or by the VAR containing cryptographic algorithms allowing signature generation.
- **Certificate:**
Message including VAR's ciphering key used to sign application software. This message is signed by a certification key.
- **Certification key:**
Key provided by the certification authority used to certificate the VAR's ciphering key.
- **Ciphering key :**
Key provided by the certification authority for the VAR. This key is used by the VAR to sign its schemes or/and its applications.
- **PC :**
Computer
- **Scheme :**
Software module to be downloaded in the cryptographic microprocessor of the ICT220 terminals.
- **Signature :**
Ciphered message used to authenticate the software issuer.
- **VAR :**
Value Added Reseller : Entity who develops software for the terminals.

2. Environment

The Software Authentication Tool is an application running under Windows ® 2000, Windows ® XP, Windows ® Vista platform and Windows ® Seven platform.

Software and hardware equipment are the following:



VAR area :

- A PC with a CD-ROM drive, with USB ports
- Microsoft ® Windows ® 2000, Windows ® XP, Windows ® Vista or Windows ® Seven **with 128 Mb RAM minimum**
- SAT software on a CD-ROM.
- A signature card and an individual certificate to sign terminal software.
- Signature Tool Terminal (Ethernet+Gprs) with signature application (SGNSMO).

3. Installation process

You must have administrative privileges to install and uninstall this program. This includes having administrative privileges the first time you start your computer after installing or uninstalling.

Before installing the SAT application, make sure that all applications are closed.

3.1. Software installation

- Insert the CD-ROM containing the SAT software,
- If your PC doesn't run the setup automatically, from the task bar, start button, choose run, then browse CD drive and take "SAT_setup.exe" with open button,
- Follow instructions on the screen. You can install this software in another directory than the one proposed by default.

3.2. Terminal Tool configuration

3.2.1. Terminal Tool/PC connection

Before launching the SAT software, the Signature Tool Terminal must be connected to your PC with an USB cable. See the chapter 10.2 to install the USB driver.

3.2.2. Network Configuration

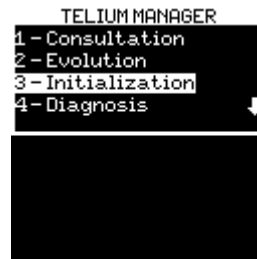
In order to sign and authenticate your application, your Signature Tool Terminal needs to be connected to Authentication Server by Ethernet or by GPRS.

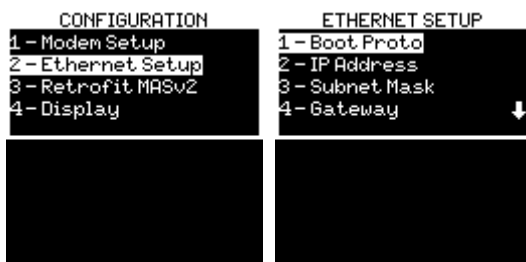
3.2.2.1. Ethernet Configuration

1. If you want to use an Ethernet connection, make sure you have an Ethernet link with a full access to Internet. Check if your Firewall allows your terminal to connect to server 83.206.130.148 on port 25000. By default Signature Tool Terminal is configured to use network with DHCP. Ask your network administrator if you need a static IP address.

If necessary, configure the signature Tool terminal Manager as following :

- Connect the terminal with your Ethernet cable before starting it.
- Go to the Manager Ethernet configuration : F → 0 → 3 → 3 → 2 → 1.





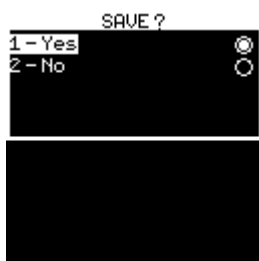
- Choose static address and press green key to confirm your choice.



- Under the same Ethernet conf menu, type your IP address, Network mask and gateway.

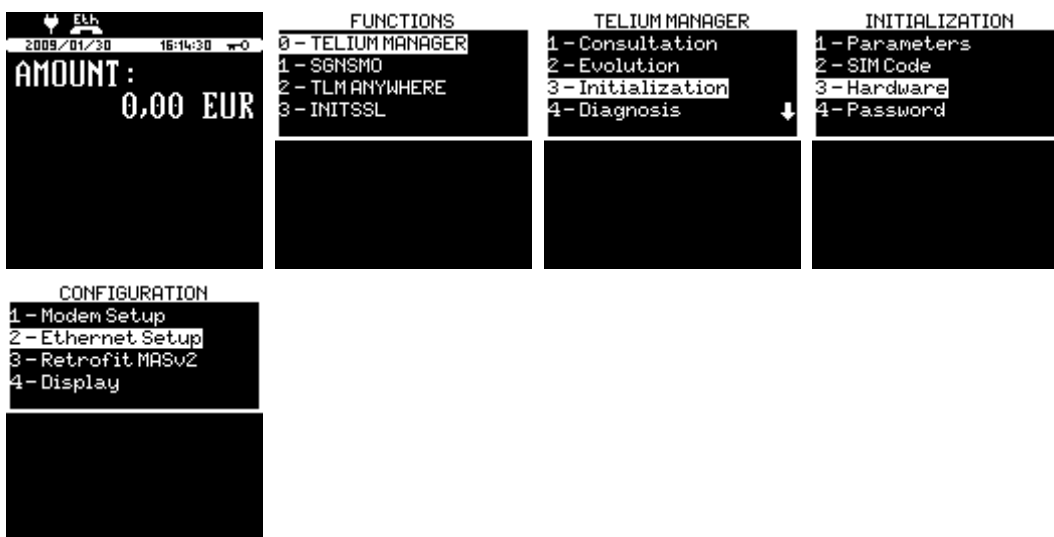


- Save your configuration and restart the terminal.

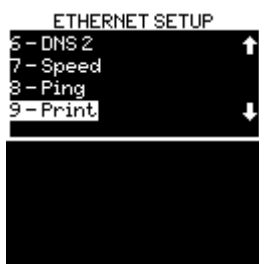


- Now, DHCP is deactivated and your terminal is configured with static IP on static boot proto.

2. To check if your terminal is properly configured, print your network configuration as following :
 - Start your terminal.
 - Go to the Manager Ethernet configuration : F → 0 (Telium manager) → 3 (Initialization) → 2 or 3 (Hardware) → 2 (Ethernet Setup).



- Press 9 to print the ticket.



3. In default DHCP mode, Check your terminal is properly initialized with not null IP, MASK and GATEWAY :

```

HWADDR=00:1E:74:DD:88:70
BOOTPROTO=dhcp
IPADDR=134.100.33.64
NETMASK=255.255.255.0
GATEWAY=192.168.1.1
DNS1=192.168.1.1
DNS2=192.168.1.1
PPP_LOCAL_ADDR=172.20.187.1
PPP_REMOTE_ADDR=172.20.187.2
DHCP_GATEWAY=on
DHCP_DNS=on

```

```

IP = 192.168.1.162
MASK = 255.255.255.0
GATEWAY = 192.168.1.1
DNS1 = 192.168.1.1
DNS2 = 0.0.0.0

```

```

ICMP_ECHO_REPLY=on
ICMP_REDIRECT=on

```

DHCP CONF OK

```

HWADDR=00:1E:74:DD:88:70
BOOTPROTO=dhcp
IPADDR=134.100.33.64
NETMASK=255.255.255.0
GATEWAY=192.168.1.1
DNS1=192.168.1.1
DNS2=192.168.1.1
PPP_LOCAL_ADDR=172.20.187.1
PPP_REMOTE_ADDR=172.20.187.2
DHCP_GATEWAY=on
DHCP_DNS=on

```

```

IP = 0.0.0.0
MASK = 0.0.0.0
GATEWAY = 0.0.0.0
DNS1 = 80.10.246.3
DNS2 = 80.10.246.30

```

```

ICMP_ECHO_REPLY=on
ICMP_REDIRECT=on

```

DHCP CONF KO

4. In static IP configuration, you should have a ticket like following

```

HWADDR=00:1E:74:DD:88:70

```

```

BOOTPROTO=static
IPADDR=134.100.33.64
NETMASK=255.255.255.0
GATEWAY=192.168.1.1
DNS1=192.168.1.1
DNS2=192.168.1.1

```

```

PPP_LOCAL_ADDR=172.20.187.1
PPP_REMOTE_ADDR=172.20.187.2
DHCP_GATEWAY=on
DHCP_DNS=on
ICMP_ECHO_REPLY=on
ICMP_REDIRECT=on

```

STATIC IP CONF OK

3.2.2.2. GPRS configuration

If you want to use a GPRS connexion, insert your SIM card into the Signature Tool Terminal and configure it like following :

- Start your Signature Tool Terminal and start SGNSMO application. After a while , check on the top right of the screen if can see the name of your provider and if you receive a sufficient GPRS signal.



- Go to the Manager Network Access Menu : F → 0 (Telium Manager) → 3 (Initialization) → 1 (Parameters) and enter Network Access menu.



- Choose GPRS mode and press green key.



- Enter your APN and press green key.



- Enter your password (if necessary) and press green key.



- Enter gateway address (if necessary) and press green key.



- Choose 'No Fallback network'.



Your terminal is now configured to connect by GPRS mode.

3.2.3. 'SGNSMO' application

To sign and authenticate an application, it is necessary to launch the '**SGNSMO**' application on the Signature Tool Terminal. Press on 'F' key and select 'SGNSMO' application.



First, you must check 'Authentication Server' parameters ('Param'):

```
SGN TOOL
1-Param
2-Start
3-Ticket
```

- Check IP Address (format: xx.xx.xx.xx),

```
ADRESSE IP SERV
83.206.130.148
```

- Check Port number,

```
NUM PORT SERV
25000
```

- Configure GPRS hang-up time-out (99999 no time-out).

```
GPRS TO
99999
```

It's possible to print a parameters report ('Ticket').



When the Signature Tool Terminal is configured, launch the 'SGNSMO' application ('Start').



Press 'RED' key to stop SGNSMO application.

4. General information on tool

4.1. Mockup version

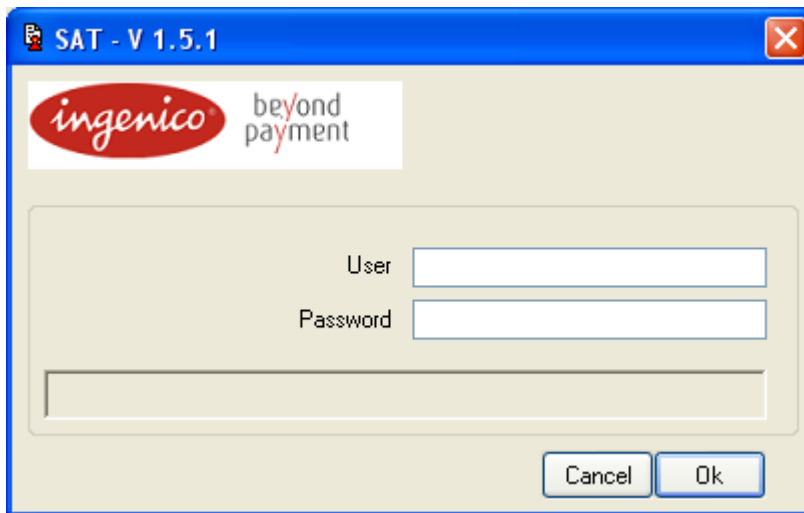
If the key 'Mockup=yes' in the section [Options] is present in the SAT.INI file, the SAT will be started in mock-up mode. In this mode you don't need to have a signature card and a card reader to generate a downloadable component. In this case the label Mockup version is displayed on the SAT login window.

Note: This “mockup” component can be downloaded only in a terminal with mockup system.

4.2. Launching the tool

To log on to the SAT, you have to enter your user name and your password. You will be able to change your password later.

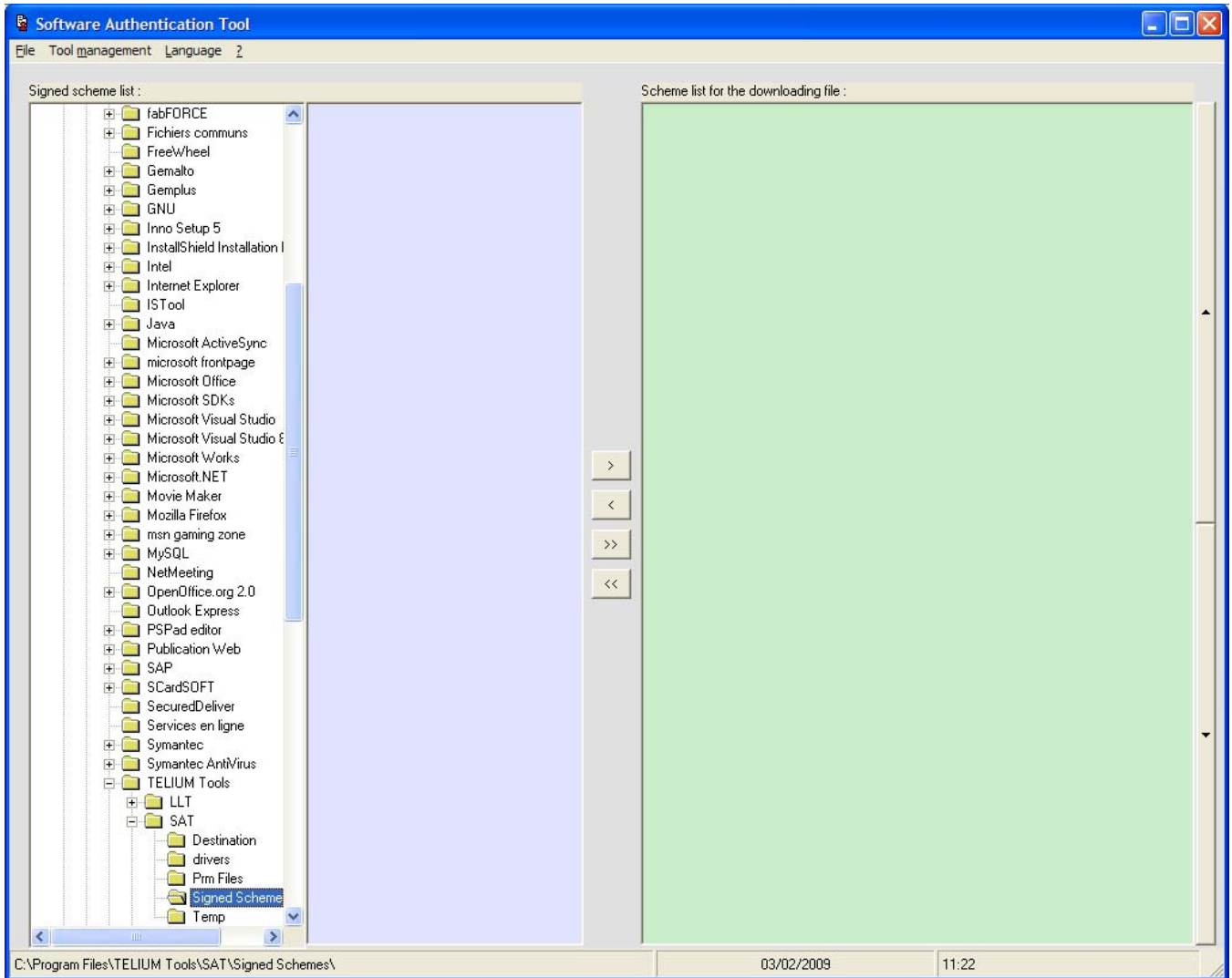
Through this procedure, only an authorized person can access the tool.



After confirmation, the main screen is displayed.

4.3. Main functions

You can have access to all the functions of the SAT from the main screen:



- sign a scheme,
- delete a signed scheme,
- open / create a parameter file,²
- sign and authenticate an application,
- check a signed and authenticated application,
- select the default certificate,
- tool management :
 - communication port selection,
 - terminal tool connexion test,
 - signature card pin code update,
 - password,
 - event log display.
- language selection.

4.4. Communication Port selection

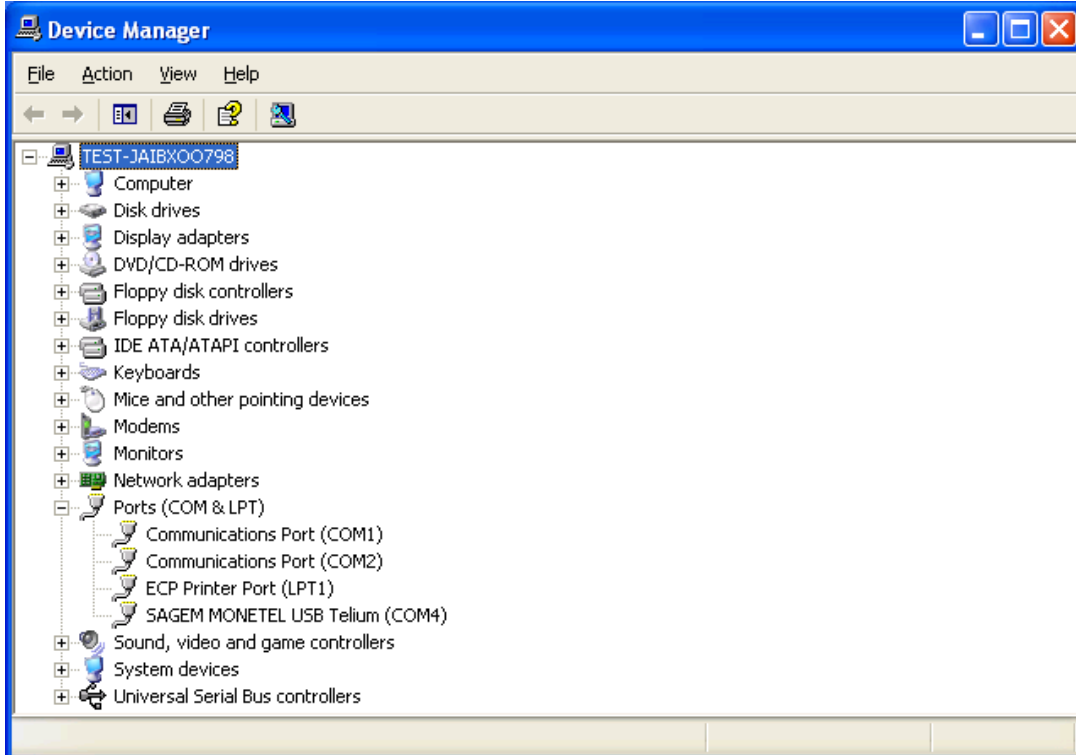
Before launching the SAT software, the terminal tool must be connected to your PC with an USB cable.

The USB driver must be installed first (see chapter 10.2)

The 'SGNSMO' application must be launched on the terminal tool to select the communication port number in use (see chapter 3.2)

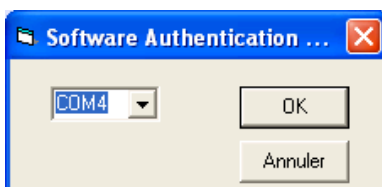
4.4.1. Display the communication port number

Display the 'Device manager' panel via the menu "Tools management | Device manager ...".



4.4.2. Communication port selection

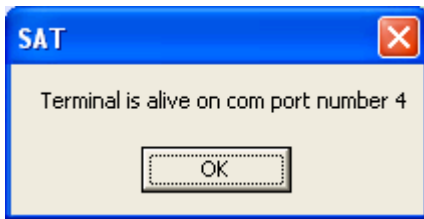
Select the communication port number via the menu "Tools management | Comm port selection".



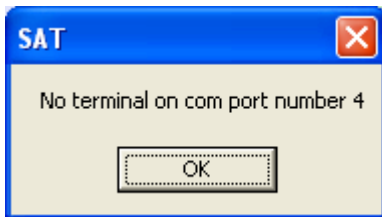
4.4.3. Communication port test

Warning : first start sign application (SGNSMO) on the terminal tool,.

Test the communication port number via the menu “Tools management | Test Connexion to terminal”.



Communication port OK



Error detected (see chapter [10.2](#))

5. Generating a downloadable file

5.1. Environment

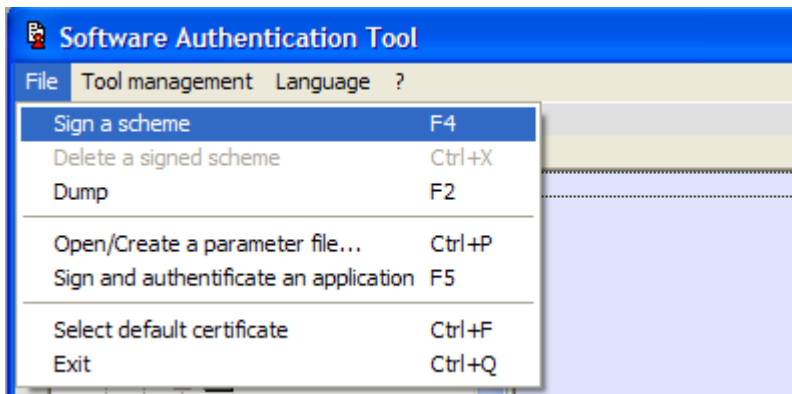
To generate a downloadable file, the SAT software needs:

1. The signature tool terminal with the application 'SGNSMO' running.
2. A signature card
3. A card certificate
4. Binary files of the scheme, signed or not signed (optional)
5. Binary files of the application file.

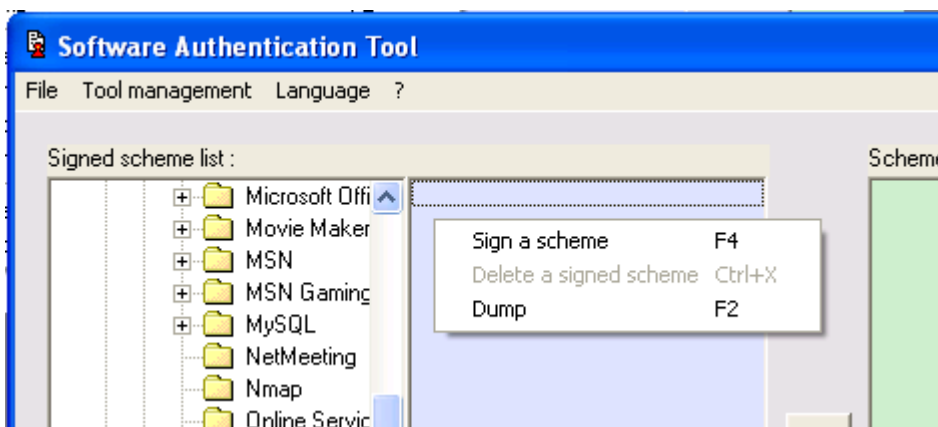
5.2. Signing a scheme

This function is needed when a scheme must be downloaded in the cryptographic microprocessor. To sign and add a scheme in the "Signed scheme list", you have several ways:

- From the main menu "File | Sign a scheme"



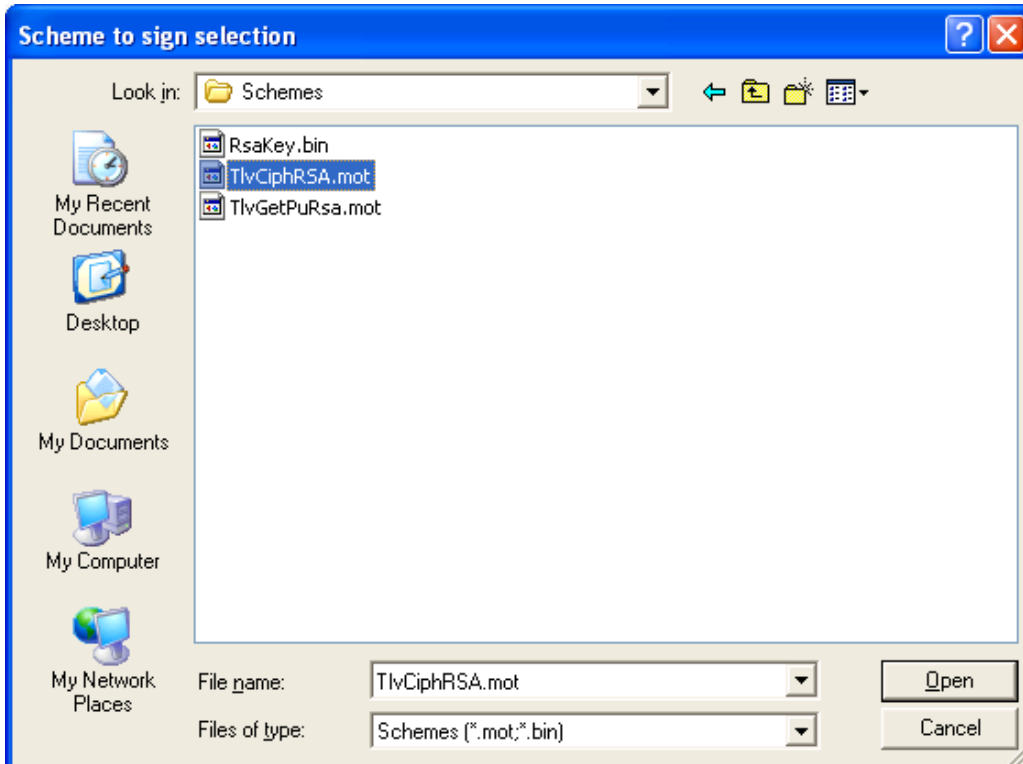
- From the popup menu (with right mouse button) "Sign a scheme".



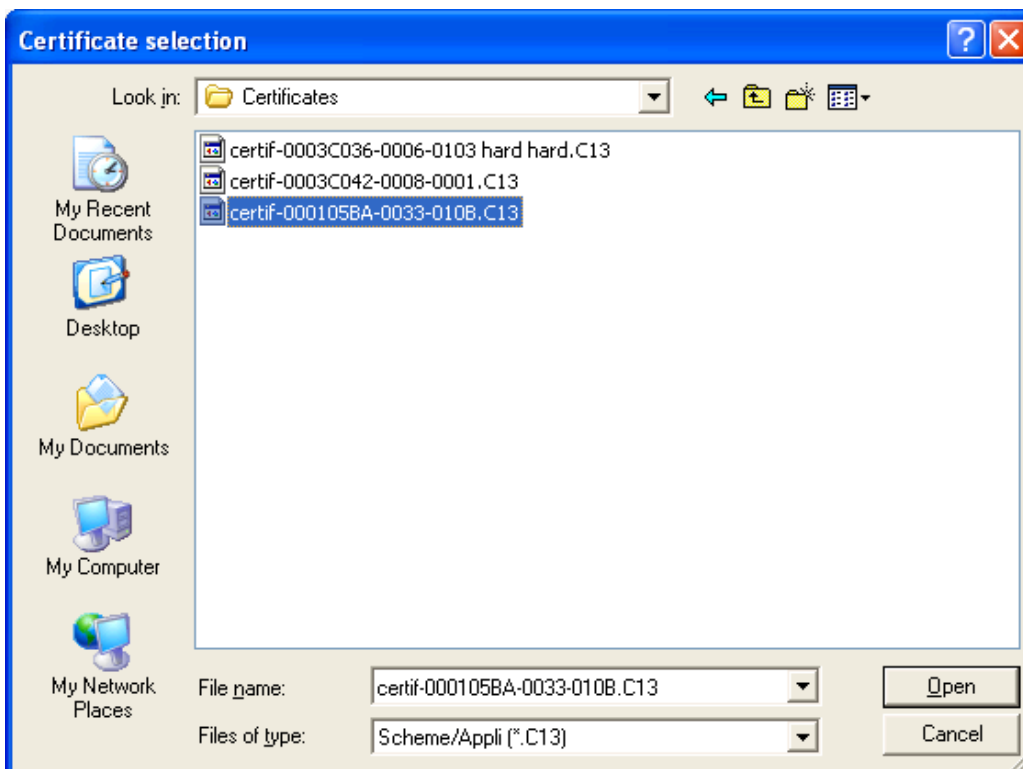
- From the shortcut key F4.

Then follow the instructions given by SAT :

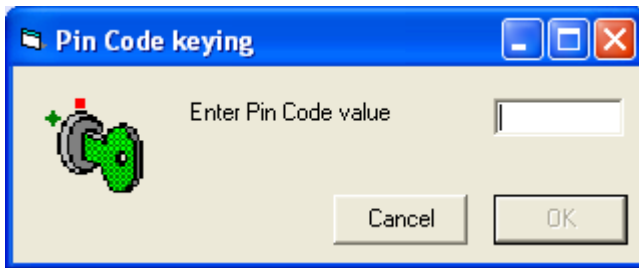
- Select the scheme (Motorola format or binary file) to be signed with the dialogue box,



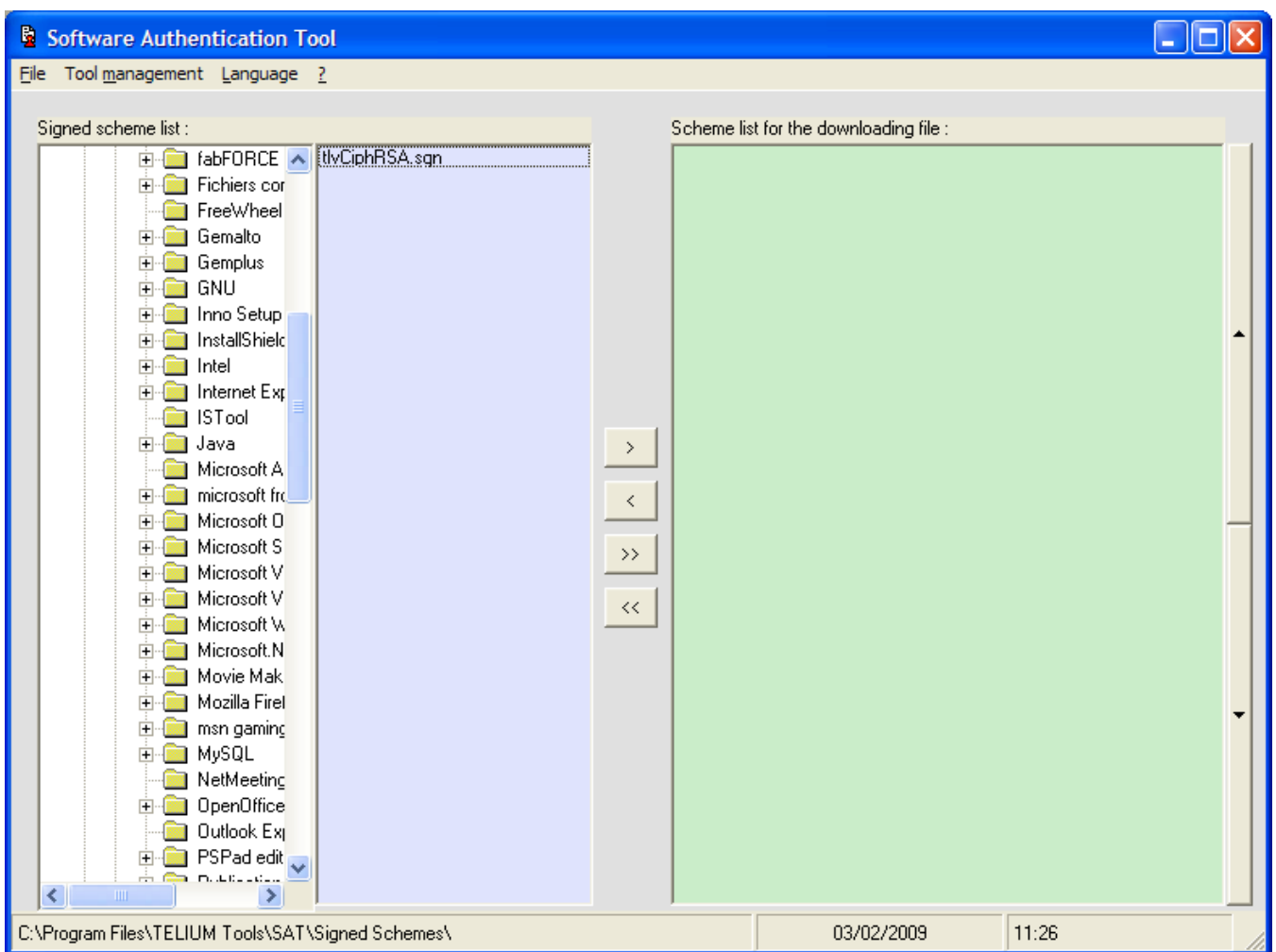
- Insert a signature card (with the module facing down) in the signature tool terminal card reader and select the directory and then the certificate file (file name "certif-xxxxxxx-yyyy-zz.C13") in the dialogue box to sign scheme software:



- Couple Card/Certificate is checked.
- Enter the card Pin Code:



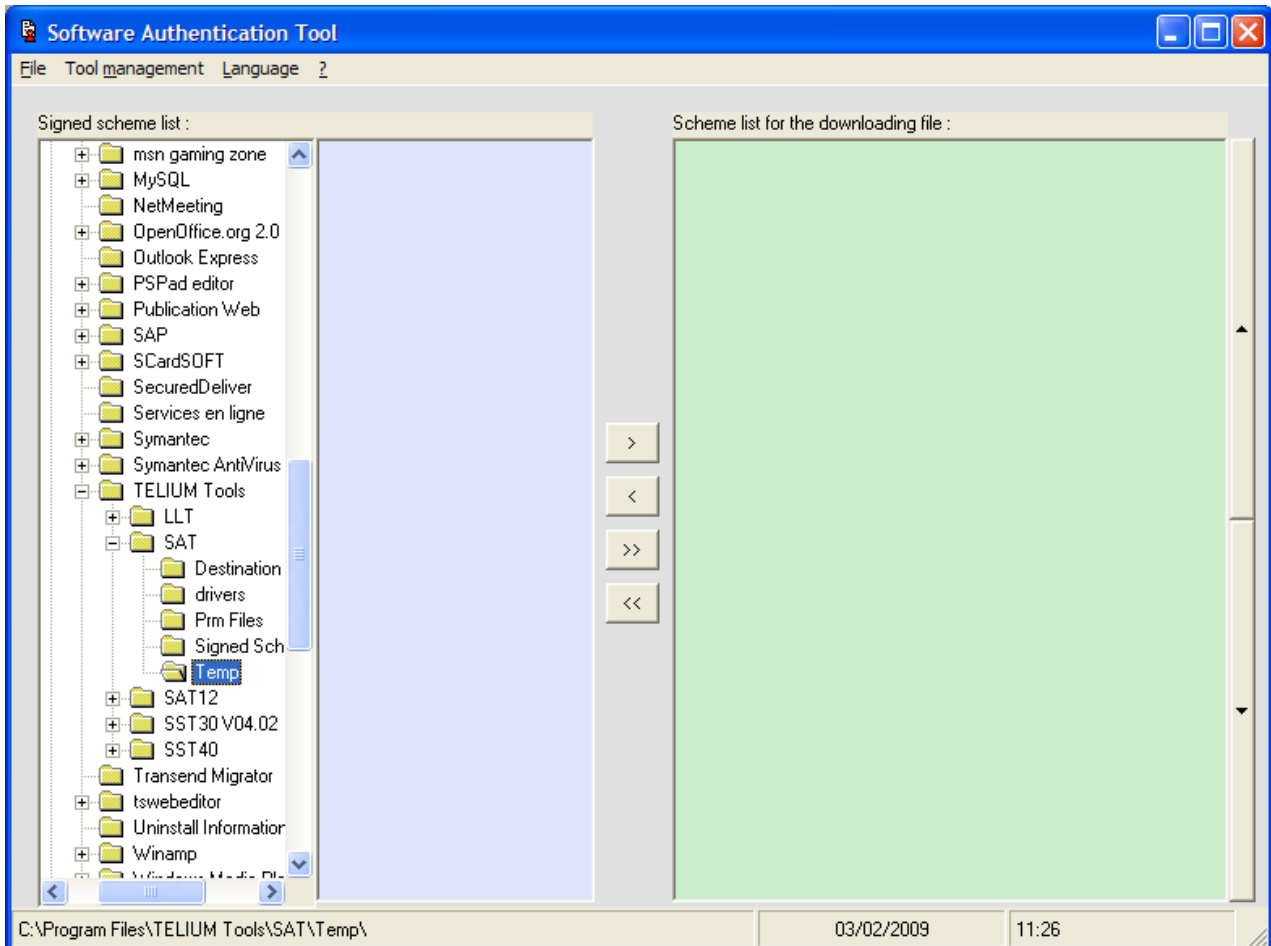
After that, the signed scheme is added to the list in the directory selected (by default in the "Signed Schemes" directory of the SAT application):



5.2.1. Selecting the default signed scheme directory

It is possible to change directory where the signed scheme are or will be located (at the first SAT launching the "Signed Schemes" directory of the SAT application is selected). To change directory, select the directory in the tree view.

For example, in this case "Temp" directory:



5.3. Deleting a signed scheme

It is possible to delete a scheme in the signed scheme list. The scheme will be deleted of the default scheme directory.

After selecting a signed scheme in the list, you have several ways to delete the file:

- from the menu **"File | Delete a signed scheme"**.
- from the popup menu (with right mouse button) **"Delete a signed scheme"**.
- from the shortcut key **CTRL + X**.

5.4. Creating the parameter file

In order to define the application characteristics, you must define a parameter file used during the creating of the final files (see next chapter). Creation of this parameter file will be proposed during the process "Sign an application", but it is possible to create or modify this file before one from the menu **"File | Open/Create a parameter file ..."** or from the shortcut key **CTRL + P**.

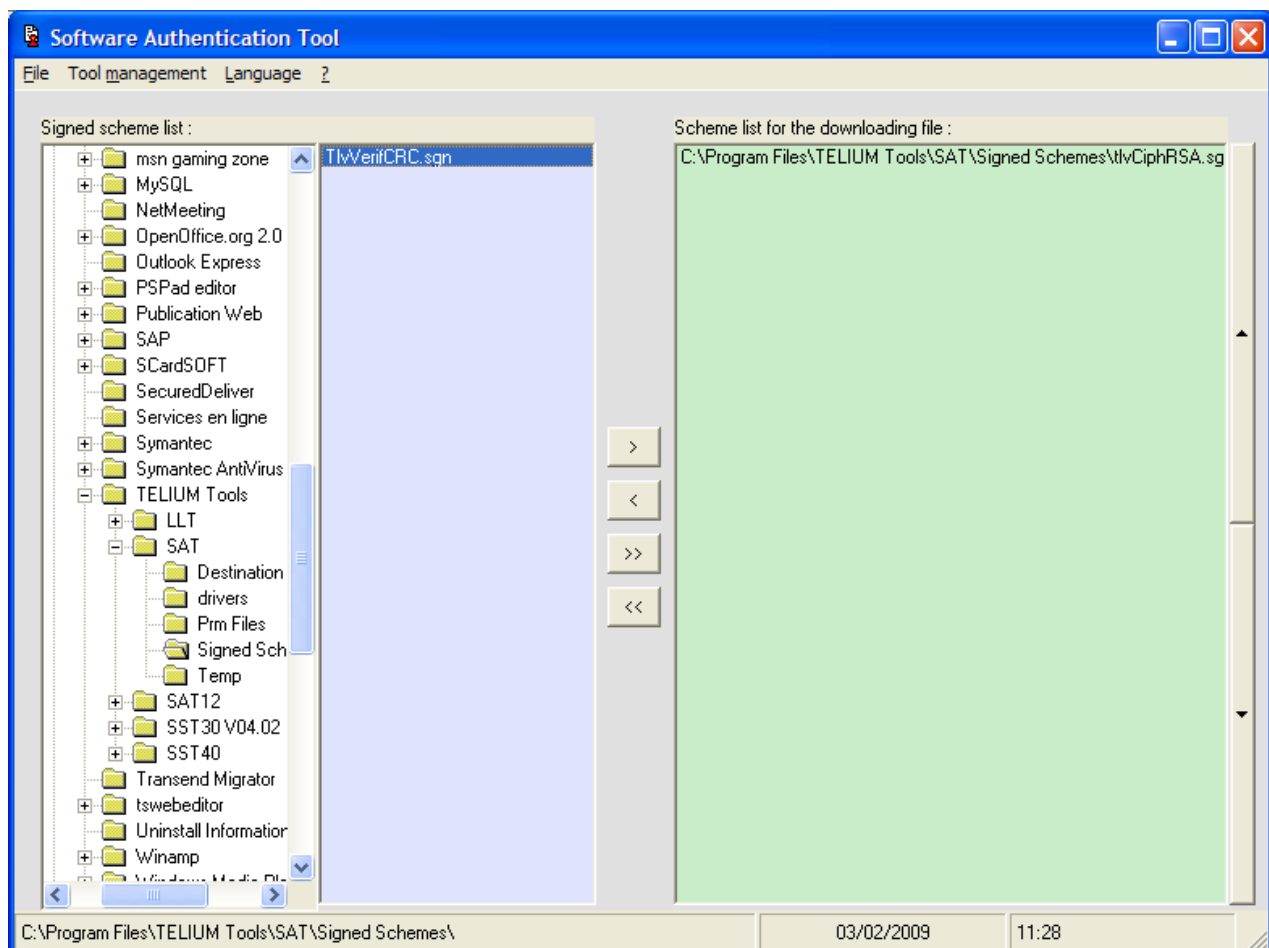
5.5. Signing and authenticating an application

Use this function to locally sign an application (with or without scheme), a DLL (library) or a parameter file and to get a remote authentication of this application. The generated files can be downloaded in the terminal.





Use the menu **"File | Sign and authenticate an application"** or use the shortcut key **F5**.

The process is the following:

Step 1. Select the default directory and scheme files to constitute the scheme list to download:
(Optional: only if the application downloads schemes to cryptographic microprocessor. If not see Step 4 directly).



To add a signed scheme from the left list to the right list, you have to use the four buttons between the two lists.

-  or double click on the scheme file name in the signed scheme list to add one in the downloading list,
-  or double click on the scheme file name in the downloading list to remove one from the downloading list,
-  or  to add or remove all the scheme files from the downloading list.

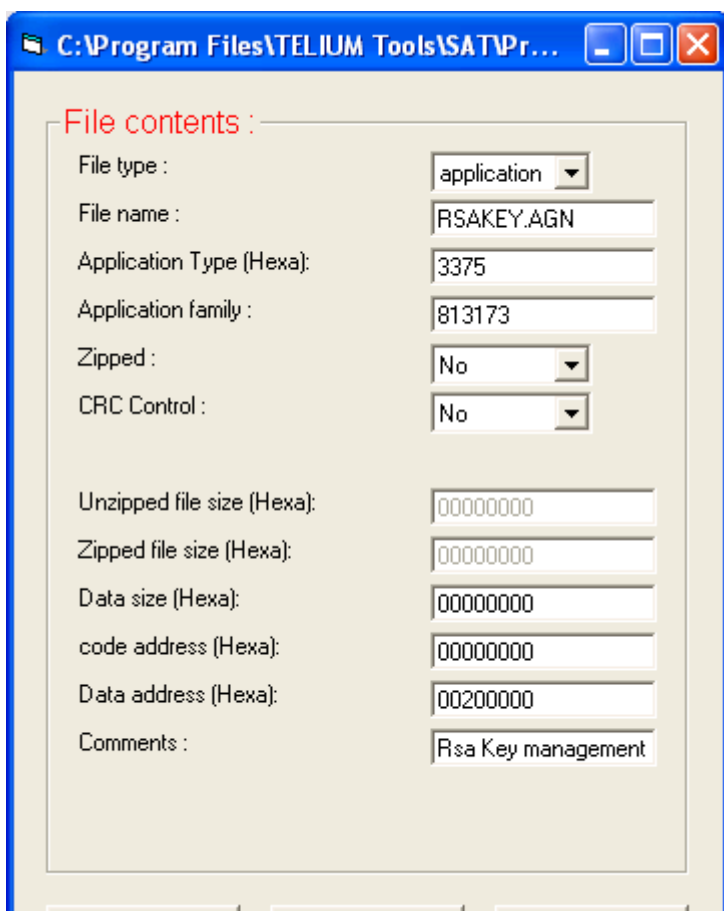
Step 2. You can change default directory (See Chapter 5.4) to select others signed schemes and repeat the previous step.

Step 3. Define order of the scheme in the downloading list with the "UpDown" buttons  or .

Step 4. Use the menu "File | Sign an application" or use the shortcut key F5.

To sign application file and create catalogue file, you must follow the instructions given by the SAT:

- Select the application file (Motorola format or binary file),
- Select or create the parameter file (see example below),



File contents :

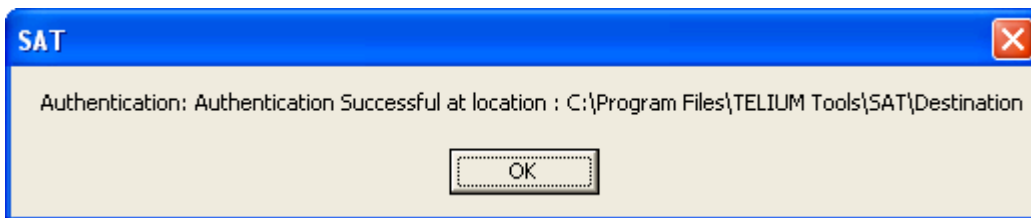
File type :	application
File name :	RSAKEY.AGN
Application Type (Hexa):	3375
Application family :	813173
Zipped :	No
CRC Control :	No
Unzipped file size (Hexa):	00000000
Zipped file size (Hexa):	00000000
Data size (Hexa):	00000000
code address (Hexa):	00000000
Data address (Hexa):	00200000
Comments :	Rsa Key management

For parameter definition, See chapter 9.

- Insert a signature card (with the module facing down) in the card reader and select the directory and then the certificate file (filename "certif-xxxxxxx-yyyy-zz.C13") in the dialogue box to sign application software,
- Enter the signature card Pin Code,



Authentication running



Authentication result

- Enter the catalogue file extension (2 characters) depending on target type of terminal (example: 40 for ICT220 terminal).

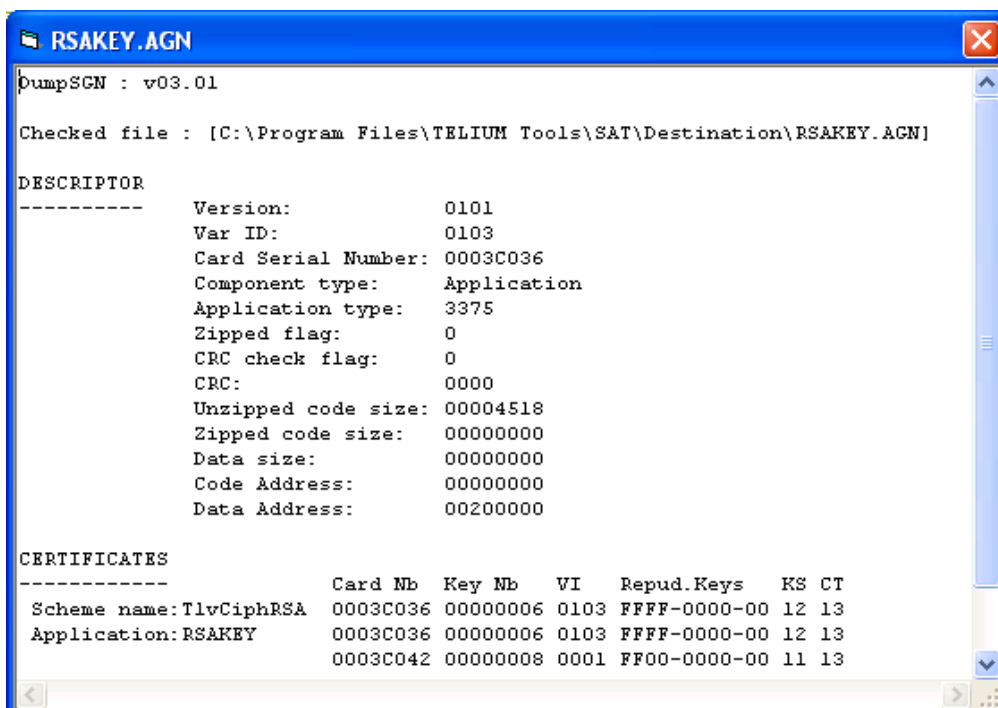
At the end of the process, two files are created (which will be used by the downloading tool) in the "Destination" directory of the SAT application:

- one binary file signed with .xGN extension, where "x" is :
 - 'A' for 'application' file type,
 - 'P' for 'parameter' file type,
 - 'L' for 'library' file type.
- one file with .Mxx extension where "xx" are the two characters identifying the target.

5.6. Checking a signed application

This function is useful to check a signed application.

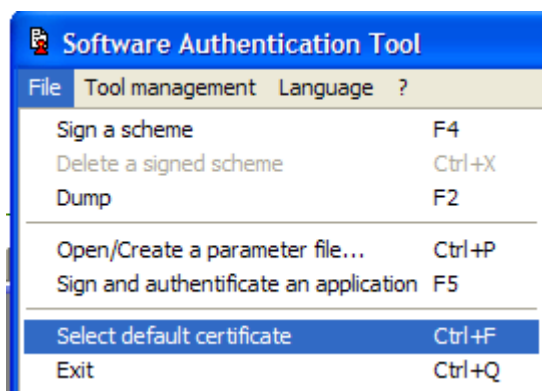
- From the main menu “**File | Dump**” select the result file (*.xGN) or from the shortcut key **F2**.



Are displayed : - the application descriptor,
list of schemes loaded with the application (with their certificates),
application certificates.

5.7. Selecting the default used certificate

It is possible to define the used certificate once and for all from the menu “**File | Select default certificate**” or from the shortcut key **CTRL+F**.

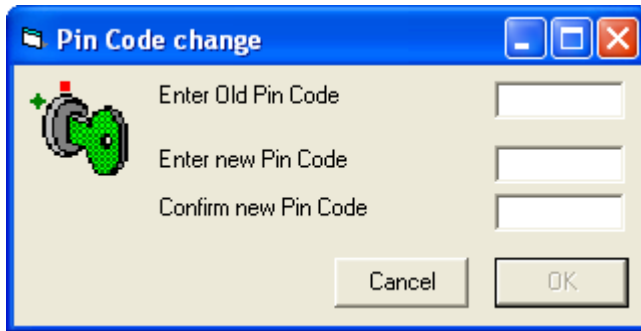


6. Tool management

The SAT has only one user, the tool administrator.

6.1. Modifying card PIN CODE

To modify the card PIN CODE from the menu, you have to use the function “Tool management | Modify card Pin Code”.



You have to enter the old PIN CODE before entering the new one.

The new PIN CODE must be confirmed to be validated.

6.2. Changing your own password

To modify your own password from the menu, you have to use the function “Tool management | Password modification”.



You have to enter your old password before entering the new one.

The new password must be confirmed to be validated.

It is advised that the user change the default password for security reasons.

6.3. Event log

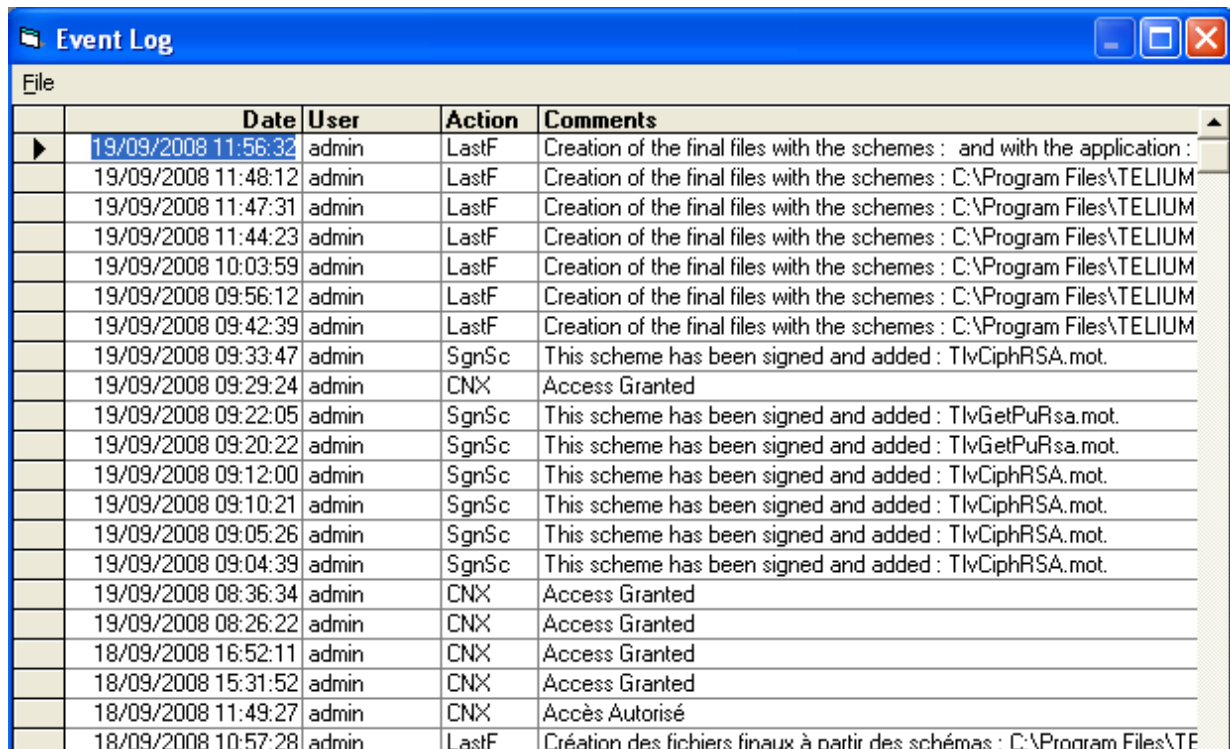
This function is accessible from the main menu "Tool management | Event log".

It contains the various actions performed by the user.

You can sort by date, user action or comments by clicking one of the column headers.

Data of the events diary can be:

- Printed: Menu "File | Print"
- Exported in a text file: Menu "File | Export"



The screenshot shows a window titled "Event Log" with a menu bar containing "File". Below the menu bar is a table with the following columns: Date, User, Action, and Comments. The table contains 20 rows of event data, starting from 19/09/2008 11:56:32 and ending at 18/09/2008 10:57:28. The actions include LastF, SgnSc, CNX, and LastF. The comments describe the creation of final files, signing of schemes, and access grants.

Date	User	Action	Comments
19/09/2008 11:56:32	admin	LastF	Creation of the final files with the schemes : and with the application :
19/09/2008 11:48:12	admin	LastF	Creation of the final files with the schemes : C:\Program Files\TELIUM
19/09/2008 11:47:31	admin	LastF	Creation of the final files with the schemes : C:\Program Files\TELIUM
19/09/2008 11:44:23	admin	LastF	Creation of the final files with the schemes : C:\Program Files\TELIUM
19/09/2008 10:03:59	admin	LastF	Creation of the final files with the schemes : C:\Program Files\TELIUM
19/09/2008 09:56:12	admin	LastF	Creation of the final files with the schemes : C:\Program Files\TELIUM
19/09/2008 09:42:39	admin	LastF	Creation of the final files with the schemes : C:\Program Files\TELIUM
19/09/2008 09:33:47	admin	SgnSc	This scheme has been signed and added : TlvCiphRSA.mot.
19/09/2008 09:29:24	admin	CNX	Access Granted
19/09/2008 09:22:05	admin	SgnSc	This scheme has been signed and added : TlvGetPuRsa.mot.
19/09/2008 09:20:22	admin	SgnSc	This scheme has been signed and added : TlvGetPuRsa.mot.
19/09/2008 09:12:00	admin	SgnSc	This scheme has been signed and added : TlvCiphRSA.mot.
19/09/2008 09:10:21	admin	SgnSc	This scheme has been signed and added : TlvCiphRSA.mot.
19/09/2008 09:05:26	admin	SgnSc	This scheme has been signed and added : TlvCiphRSA.mot.
19/09/2008 09:04:39	admin	SgnSc	This scheme has been signed and added : TlvCiphRSA.mot.
19/09/2008 08:36:34	admin	CNX	Access Granted
19/09/2008 08:26:22	admin	CNX	Access Granted
18/09/2008 16:52:11	admin	CNX	Access Granted
18/09/2008 15:31:52	admin	CNX	Access Granted
18/09/2008 11:49:27	admin	CNX	Accès Autorisé
18/09/2008 10:57:28	admin	LastF	Création des fichiers finaux à partir des schémas : C:\Program Files\TE

6.4. Changing the tool language

At first tool start up, Tool screens and messages are displayed in English.

The language may be modified via the Menu "Language" or function keys CTRL + E (English) or CTRL + L (local language).

At next tool start up, tool screens will be displayed in the last selected language.

6.5. Defining a new translation language

A language file (file with extension ".lng" in the tool installation directory) is used to translate the different screens, menus, or messages in the tool.

By default this file contains 2 languages (French and English) available in SAT tool.

Nevertheless, any language can be used. To use the local language, replace the French translation in this file by the local translation.

7. Using SAT in command mode

SAT can be invoked in command mode. It avoids using SAT in interactive mode to generate a new application based on Crypto products requiring a signature. This document is dedicated to developers that want to quickly generate signed and authenticate applications on ICT220 terminals.

7.1. Command mode requirements

When used in command mode, SAT needs the following informations in order to sign and authenticate an application :

- PIN code of chip card
- Directory and filename of application parameter file (.txt file)
- Directory and filenames of signed schemes (.sgn file) (if needed)
- Directory and filename of the certificate (.C13 file)
- Directory and application binary filename (.mot or .bin file)
- Destination directory of generated files (.sgn)
- Temporary directory dedicated to the SAT
- Catalog File Extension (2 characters)

All these information are put together in a configuration file. This file is an ASCII file. This format is like an INI file.

7.1.1. [SAT] Section

Key name	Description	Value
CertificateSchemaDir	Directory where the certificate to sign schemes is located	
CertificateAppliDir	Directory where the certificate to sign application is located	
SignedSchemaDir	Directory where the signed schemes will be located after signature processing	
ApplicationDir	Directory where the application is located	
ParametersDir	Directory where the parameter file used to sign an application is located	
DestinationDir	Directory where the signed application will be located after signature processing	
TempDir	Directory where temporary files are created	

7.1.2. [Schemas] section

Key name	Description	Value
NbSchemas	Specified the schemes number embedded in application	
SchemaX	Motorola or binary scheme file name	X specify the order of the scheme in the application. File with .mot or .bin extension
CertificateFile	Certificate file name used to sign schemes	

7.1.3. [Application] section

Key name	Description	Value
ParameterFile	parameter file name used to sign an application	
ApplicationFile	Motorola or binary application file name	File with .mot or .bin extension
CertificateFile	Certificate file name used to sign schemes	
CatalogFileExtension	2 characters to identify the product where the application will be downloaded	30 for EFT30 stationary

7.2. Example of configuration file

Configuration file name: "C:\SAT-Working\mode4SAT.ini"

Configuration file content:

```
[SAT]
SignedSchemaDir=C:\Program Files\TELIUM Tools\SAT\Signed Schemes
TempDir=C:\temp
CertificateSchemaDir=C:\Program Files\TELIUM Tools\SAT\Certificats
CertificateAppliDir=C:\Program Files\TELIUM Tools\SAT\Certificats
ParametersDir=C:\Program Files\TELIUM Tools\SAT\Prm Files
ApplicationDir=H:\SAT-Working
DestinationDir=C:\Program Files\TELIUM Tools\SAT\Destination

[schemas]
NbSchemas=2
Schema1= H:\SAT-Working\TlvCiphRSA.bin
Schema2= C:\Program Files\TELIUM Tools\SAT\Signed Schemes\TlvGetPuRsa.sgn
CertificateFile=certif-000105BA-0033-010B.C13

[application]
ApplicationFile=RSaKey.bin
CertificateFile=certif-000105BA-0033-010B.C13
ParameterFile=SAT40.txt
CatalogFileExtension=40
```

Command line:

```
"C:\Program Files\TELIUM Tools\SAT\SAT.exe" 4,H:\SAT-Working\mode4SAT.ini,12341234
```

Notes

If one of directories does not exist, it is created.

If a destination file already exists, it is not overlapped and an error is returned.

Directory paths must not be '\' ended.

Signed and unsigned schemes are put in the same section [Schemas]. Put them in the order they will be loaded by application. Scheme extension (.sgn or .mot / .bin) will indicate if a scheme is already signed or to be signed.

Caution

Temporary and destination directory must be different (because all files in this temporary directory are deleted once SAT returns).

7.3. Running SAT in command mode

When running SAT, 3 parameters must be passed (comma separated) via the DOS command line :

- Action number to be done (1, 4)
- Directory and filename of the configuration file to use SAT in command mode
- PIN code of card to be used ("00000000" to use the SAT in Mock-up mode)

Syntax: SAT <action number>,<path>+<configuration filename>,<pincode>

Example : "C:\Program Files\TELIUM Tools\SAT\SAT.exe" 1, C:\temp\cmdmode.prm,12345678
(do not forget double quote: " ")

Sections from configuration file are not all useful depending on the request.

SAT can be invoked from an application, from a DOS window or from WINDOWS (in any cases, path where SAT.EXE is located is to be specified).

SAT can be directly called from WINDOWS by clicking on a SAT link. In such case, create a link file and modify SAT.EXE properties. In the field Target, specifies the parameters to pass to the SAT

Example : If target is C:\Program Files\TELIUM Tools\SAT\SAT.exe write :

"C:\Program Files\EFT30 Tools\SAT\SAT.exe" 1, C:\temp\cmdmode.prm,12345678

The following table shows which configuration file sections must be filled depending on action to do:

Action	Number	[SAT]	[Schemes]	[Application]
Sign one scheme or several schemes	1	X	X	
Sign and authenticate an application with signed and/or unsigned schemes	4	X	X	X

A section 'Error' is created in configuration file when SAT returns. This section gives a code error and a message error. It can be later analysed by the calling application.

Example:

[Error]
Code=0
msg=files correctly signed.

8. Tool un-installation

1. From the task bar click on "Start" button and choose "Programs -> TELIUM Tools -> SAT -> Uninstall SAT".
Or
1. From the task bar click on "Start" button and choose:
"Settings -> Control Panel -> Add / Remove programs".
2. Choose SAT application, and click on Add / Remove button.
3. Remove all components.

9. Parameter file description

File format is as following :

Parameter File is an ASCII file, each field being separated by a coma ','.

HEX: ASCII hexadecimal character: ("A" – "F", "a" – "f", or "0" – "9") big-Endian format (which is easier for key-in).

ALPHAUP: alphanumerique upper case character ("A" – "Z", or "0" – "9") + "-" + "_" + "."

field name	size (byte)	Format	Value	Comments
File Type	1	HEX	0 = parameter 1 = application 2 = library 3 = driver	indicator to identify what kind of signed file it is
File name	15 Max	ALPHAUP		Component file name, including its extension (.xGN) according to 'File Type'
Application type	4	HEX		Hexadecimal Code indicating the type of application (system, manager, banking, loyalty,...) This number must be supply by your terminal provider.
Application Family	16 Max	ALPHAUP		name identifying in which family is linked this file
Zipped	1	HEX	0= no,1= yes	compression indicator
CRC control	1	HEX	0= no,1= yes	CRC control indicator
CRC	4	HEX		Checksum applied on the non compressed file, without signature or certificate Computed by SAT and put in the descriptor file
Unzipped file size	8	HEX		Uncompressed file size without signature or certificate Computed by SAT and put in the descriptor file
Zipped file size	8	HEX		compressed file size without signature or certificate Computed by SAT and put in the descriptor file
Data size	8	HEX		maximum size used by application data
code address	8	HEX		If library : loading adresse for code, else 00000000H by default
data address	8	HEX		If library : loading address for data, else : 00200000H by default
Comments	30 Max	ASCII		Component description

Example of parameter file:

1,RSAKEY.AGN,3375,813173,0,0,1234,003F3C48,0000475C,00020000,00000000,00200000,Rsa Key management

10. Appendices

10.1. List of shortcut keys

Each SAT function is accessible via the menu and is also accessible via a keyboard function key or a combination of these keys.

This tool can be used without a mouse, each menu function is also accessible by striking on ALT + menu letter . Once the menu is open, access to sub menus is done with keyboard by striking on SHIFT + letter of sub menu.

Main functions are accessible with shortcut keys as well:

Function	Shortcut keys
Display User's Guide	F1
Dump	F2
Sign a scheme	F4
Sign an application	F5
Select default certificate	CTRL + F
Delete a signed scheme	CTRL + X
Open/Create a parameter file	CTRL + P
Change a language	English CTRL + E, Local language CTRL + L
Quit	CTRL + Q

10.2. Installing signature tool terminal driver

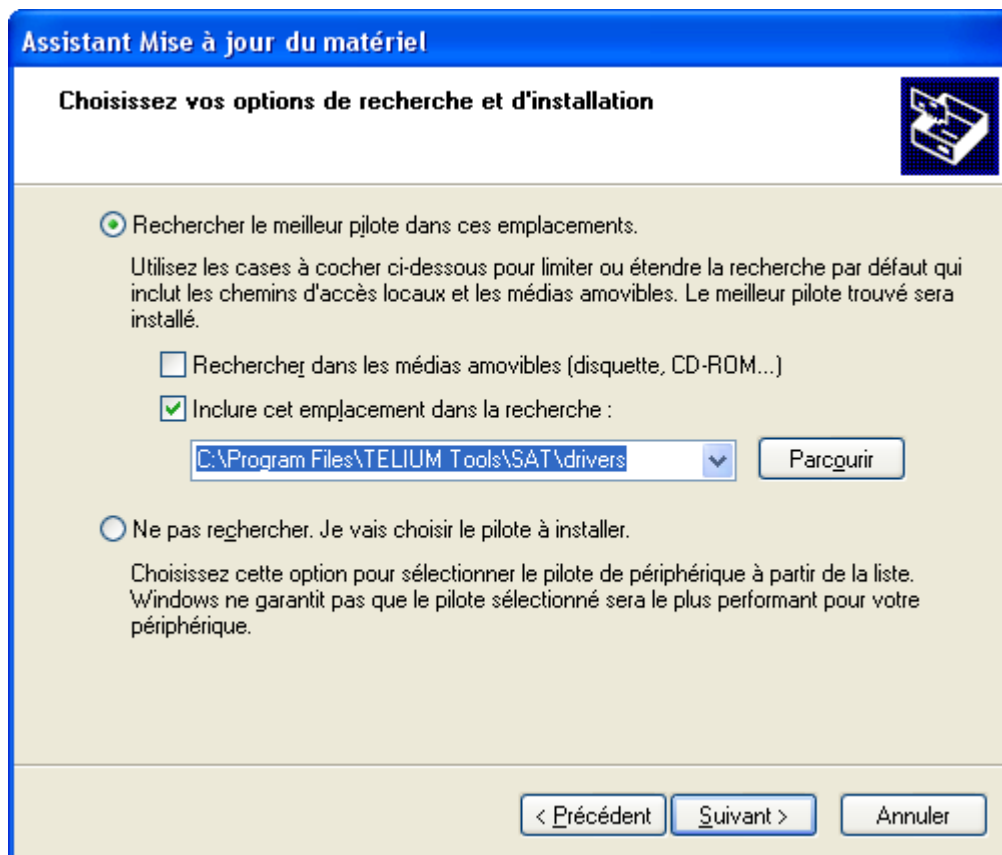
10.2.1. Windows XP Professional

- Connect USB cable between terminal (USB Slave) and PC (USB Host).

When you plug the terminal with USB cable, Windows ® XP suggests to install a new driver in order to manage USB terminal connection.



Click "Next"



Click **Browse** to select the « drivers » sub-directory located in the SAT directory. Then click **Next**.



Then **"Finish"**. Now, the USB driver is installed and ready to be used. The USB connection is seen as a serial port. You must configure this new port (See Installing the null modem driver).

Select the serial port used from **Tool management | Comm Port selection ...** of SAT menu.
Select the port to use from device list

10.2.2. Windows 2000 Professional

- Connect USB cable between terminal (USB Slave) and PC (USB Host).

When you plug the terminal with USB cable, Windows 2000 detects the new device.



Then suggest installing a new driver in order to manage USB terminal connection.



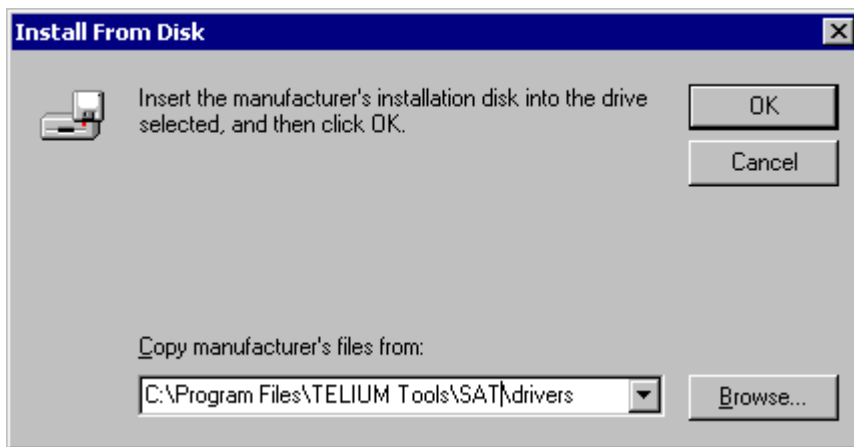
Click **"Next"**



Click **"Next"** to select USB driver for connected Terminal.

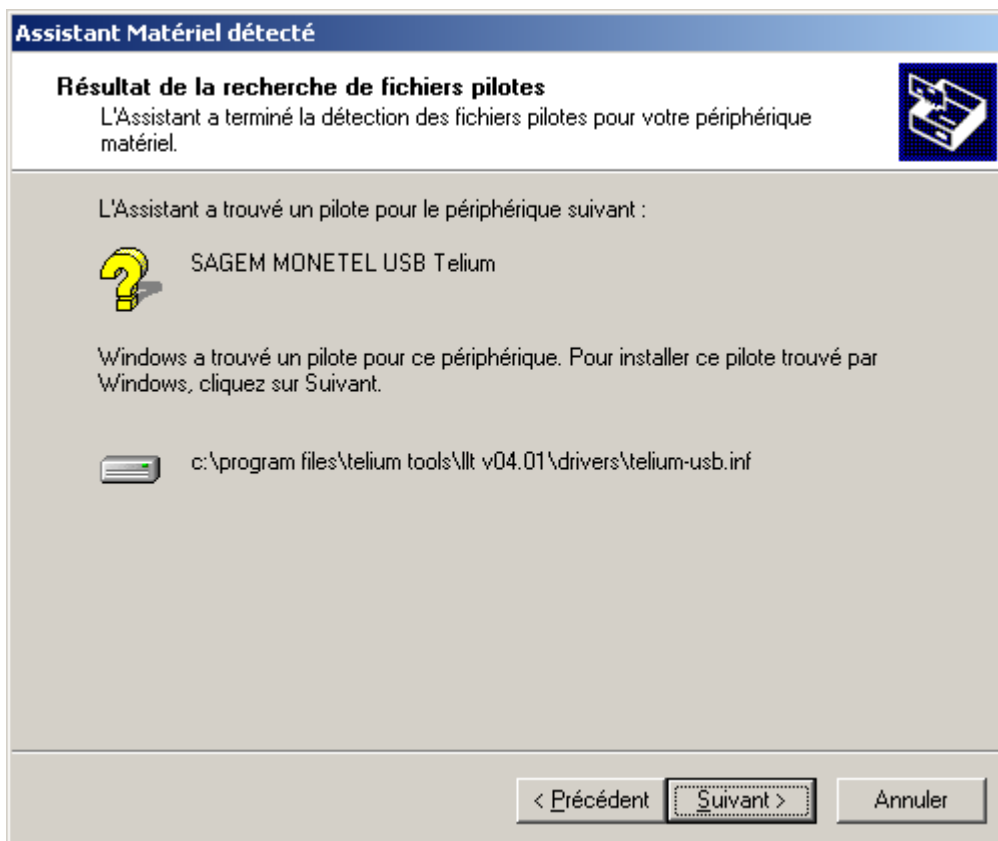


Click **"Next"** and give the directory of SAT application.



and confirm by **OK**.

If the driver has been found, the following screen is displayed:



Click "Next"



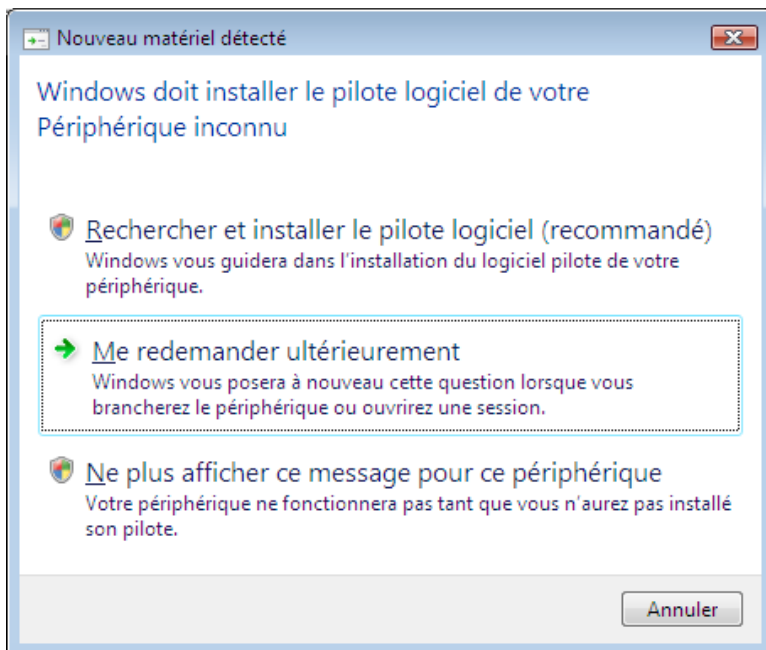
Then **"Finish"**. Now, the USB driver is installed and ready to be used. The USB connection is seen as a serial port.

Select the serial port used from **Tool management | Comm Port selection ...** of SAT menu.
Select the port to use from device list

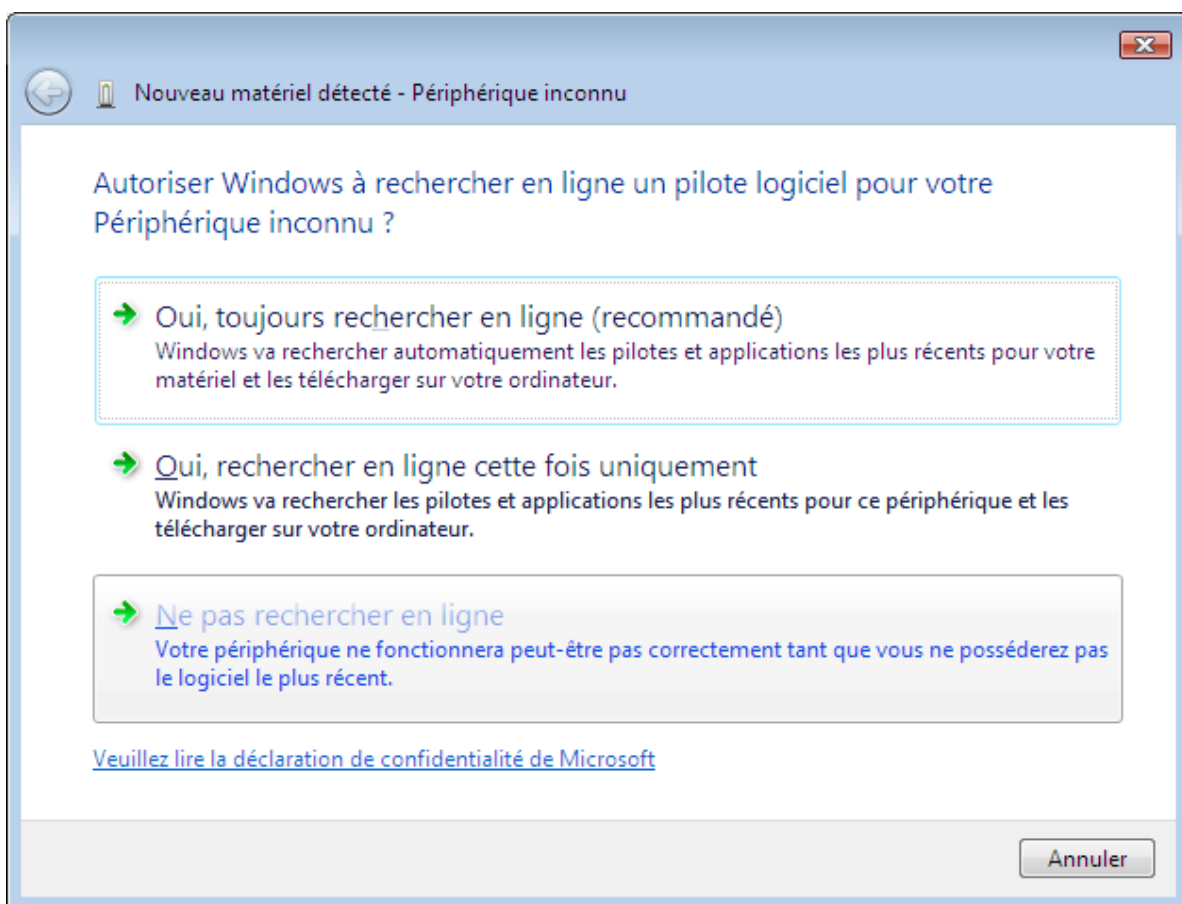
10.2.3. Windows Vista Professional

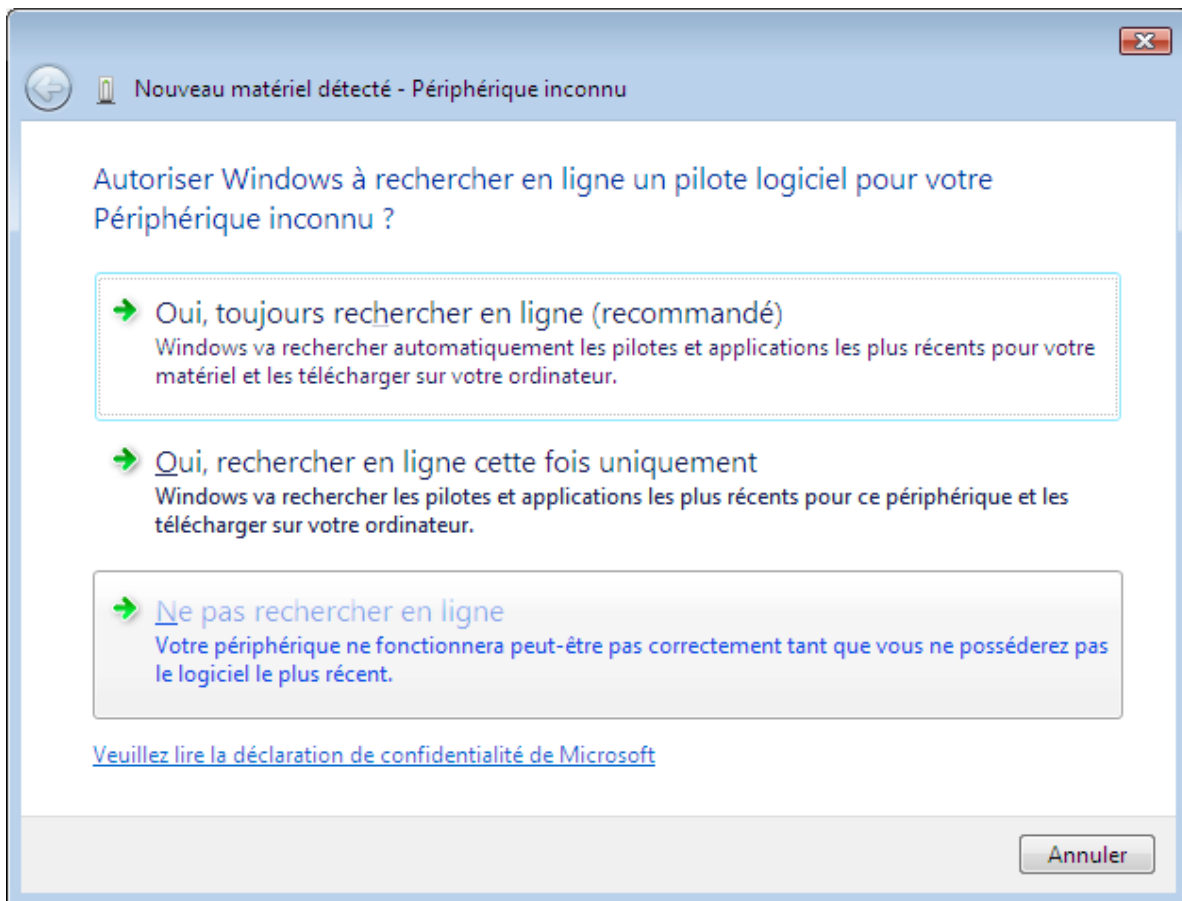
- Connect USB cable between terminal (USB Slave) and PC (USB Host).

When you plug the terminal with USB cable, Windows ® Vista suggests to install a new driver in order to manage USB terminal connection.

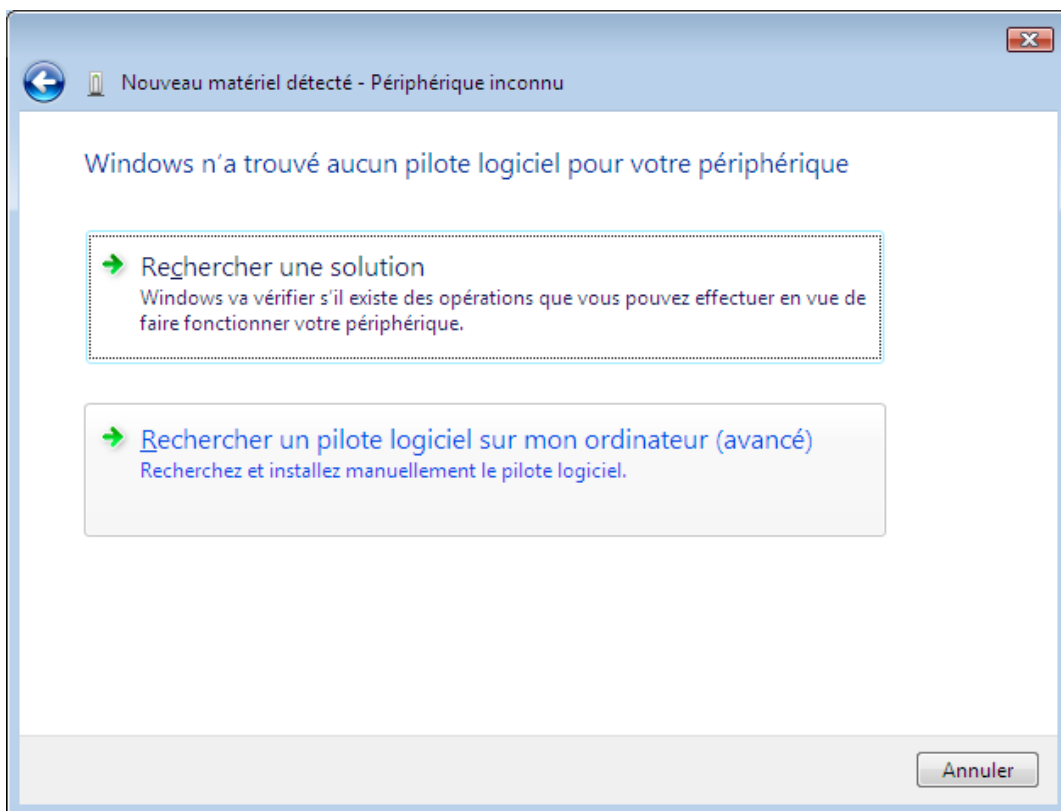


Click **Find and install software driver (recommended)**

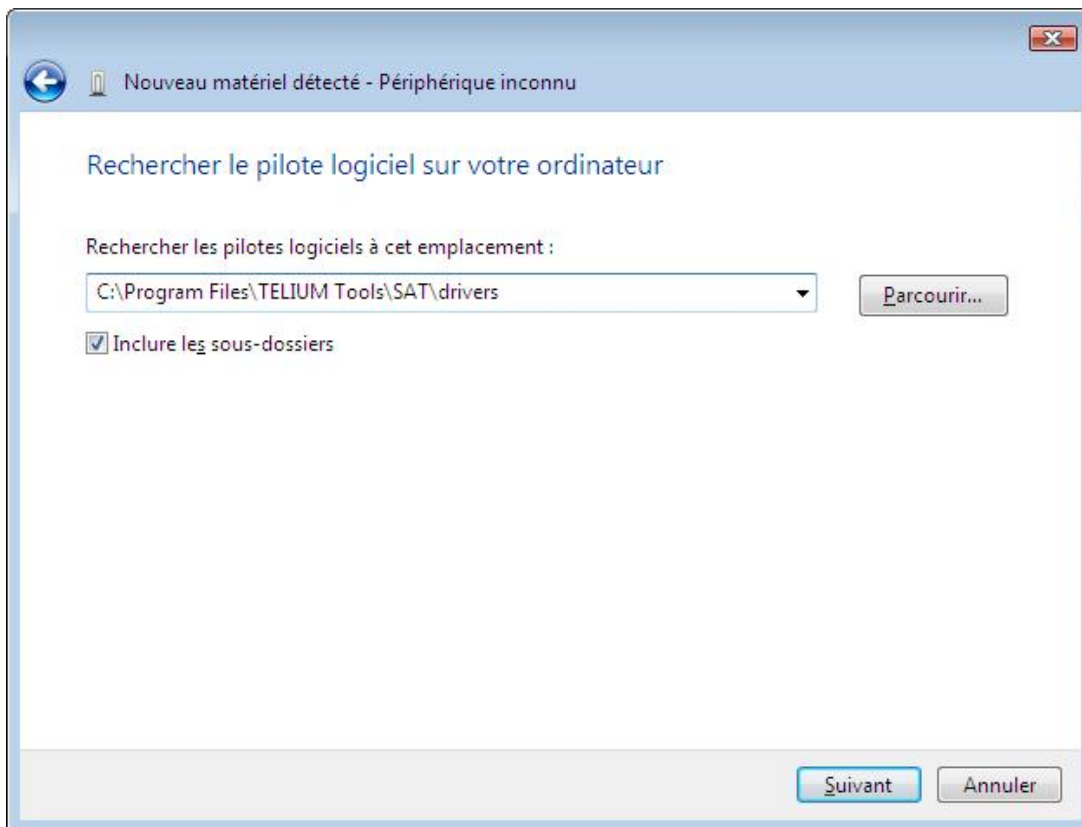




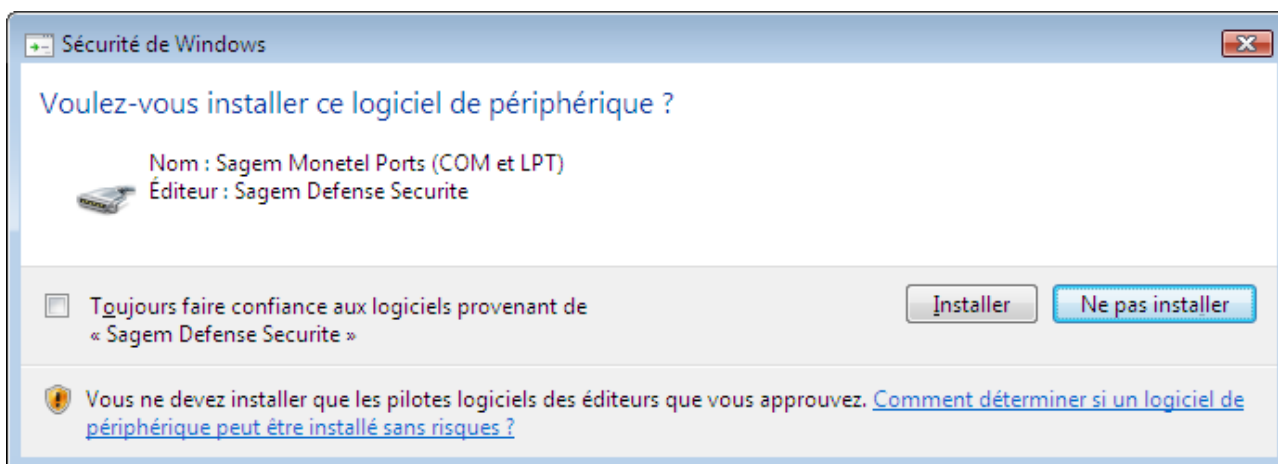
Click “Don’t search in line”



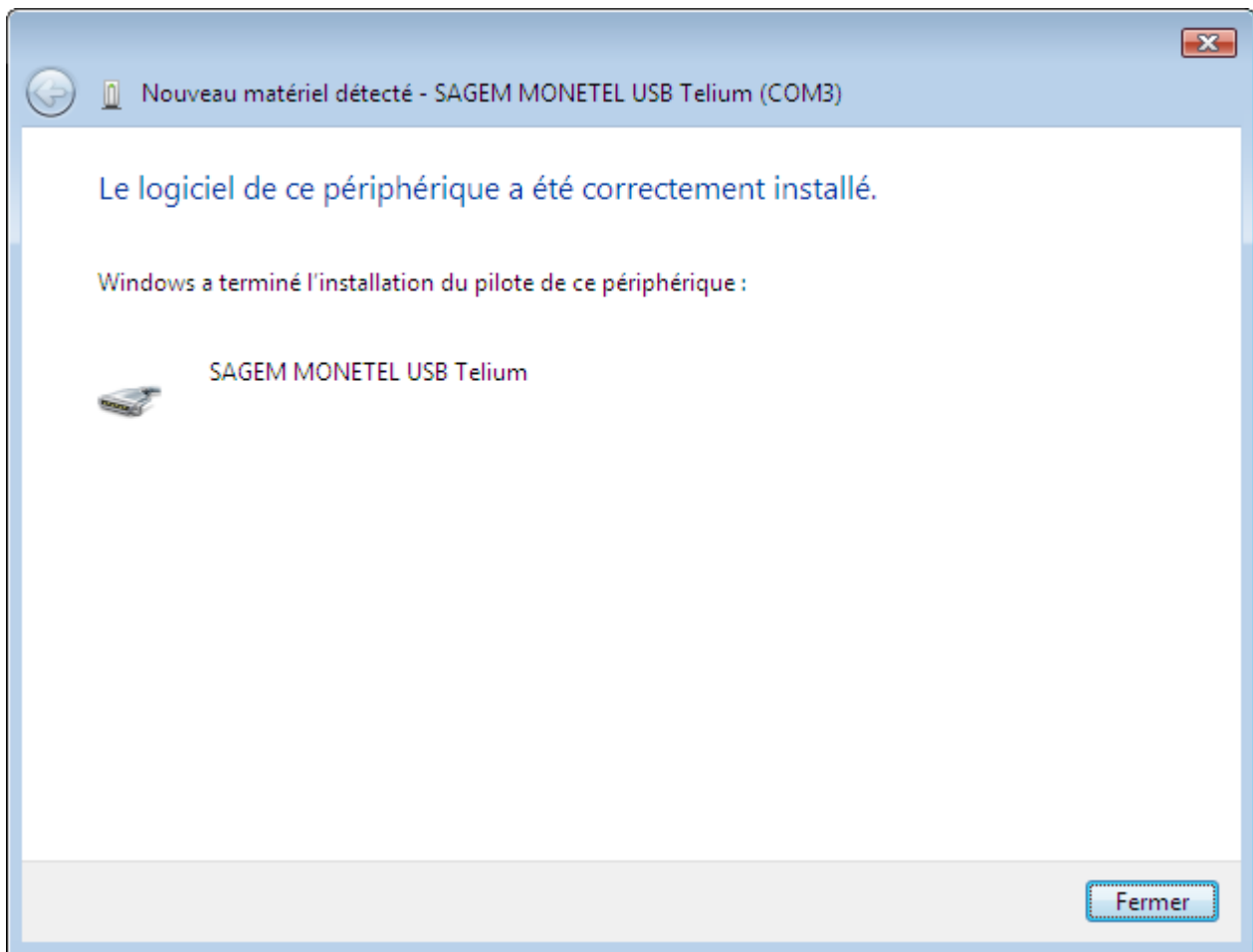
Click “Find software driver on my computer”



Click “Browse” to select the « drivers » sub-directory located in the SAT directory.
Then click “Next”.



Click « **Install** »



Then **"Finish"**. Now, the USB driver is installed and ready to be used. The USB connection is seen as a serial port.

Select the serial port used from **Tool management | Comm Port selection ...** of SAT menu. Select the port to use from device list and click **OK**.

10.2.4. Windows Seven Professional

Power on the terminal.

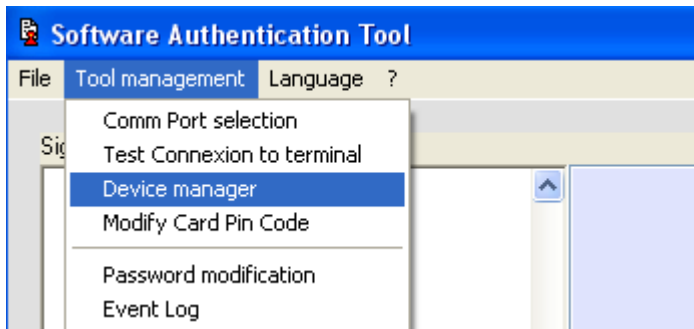
Connect USB cable between terminal (USB Slave) and PC (USB Host).

When you plug the terminal with USB cable, Windows® Seven displays the following message.

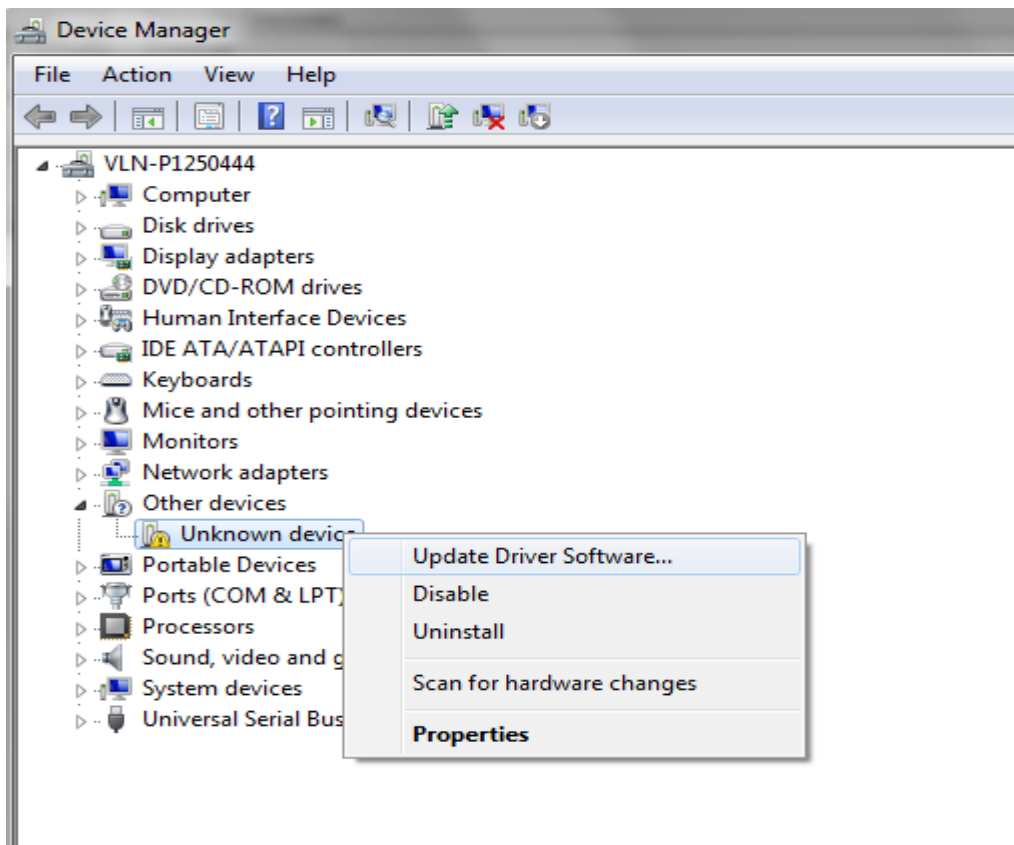


To install a new driver in order to manage USB terminal connection, select via the SAT menu: **'Tool management | Device manager ...'**.

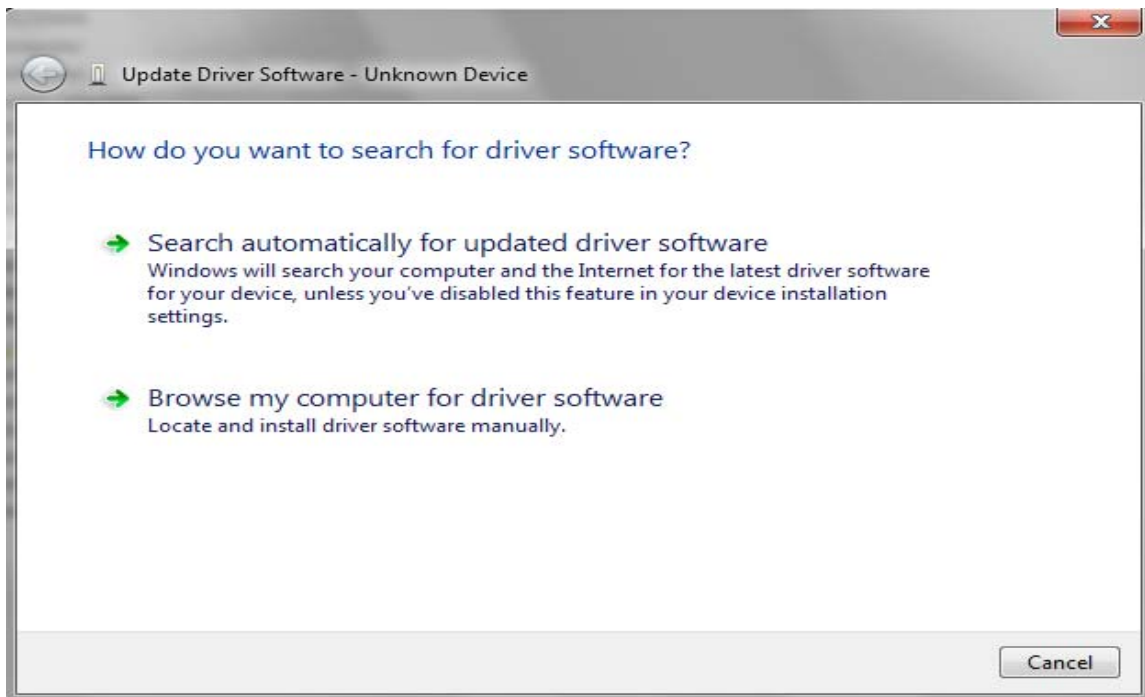
Warning : if the device manager panel is not displayed, close and restart the SAT application.



Select the 'Unknown device' and (with a right click) 'Update Driver Software'



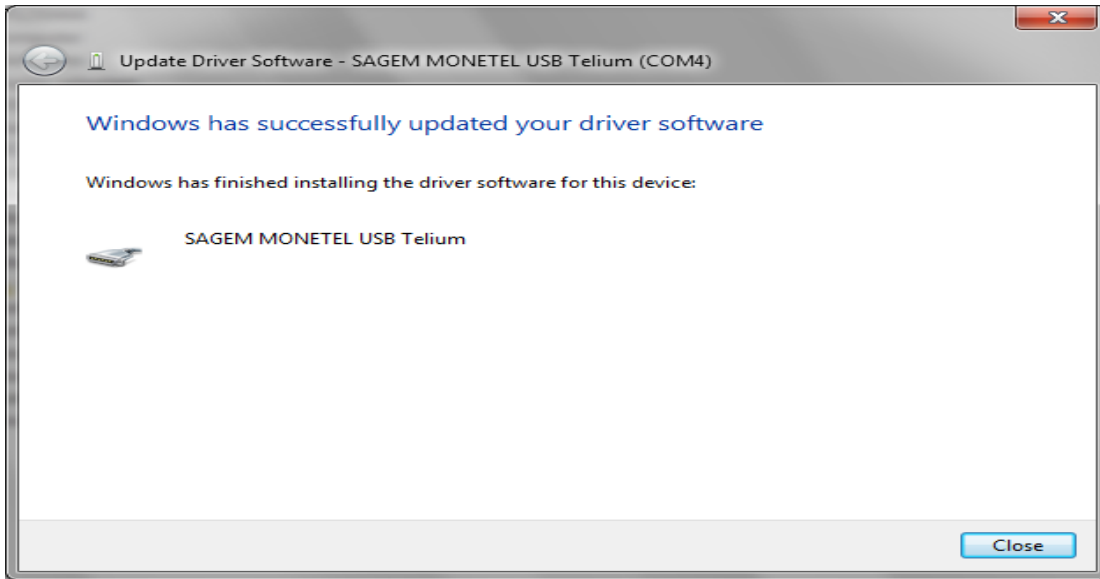
After locate and install driver software manually ('Browse my computer for driver software'):



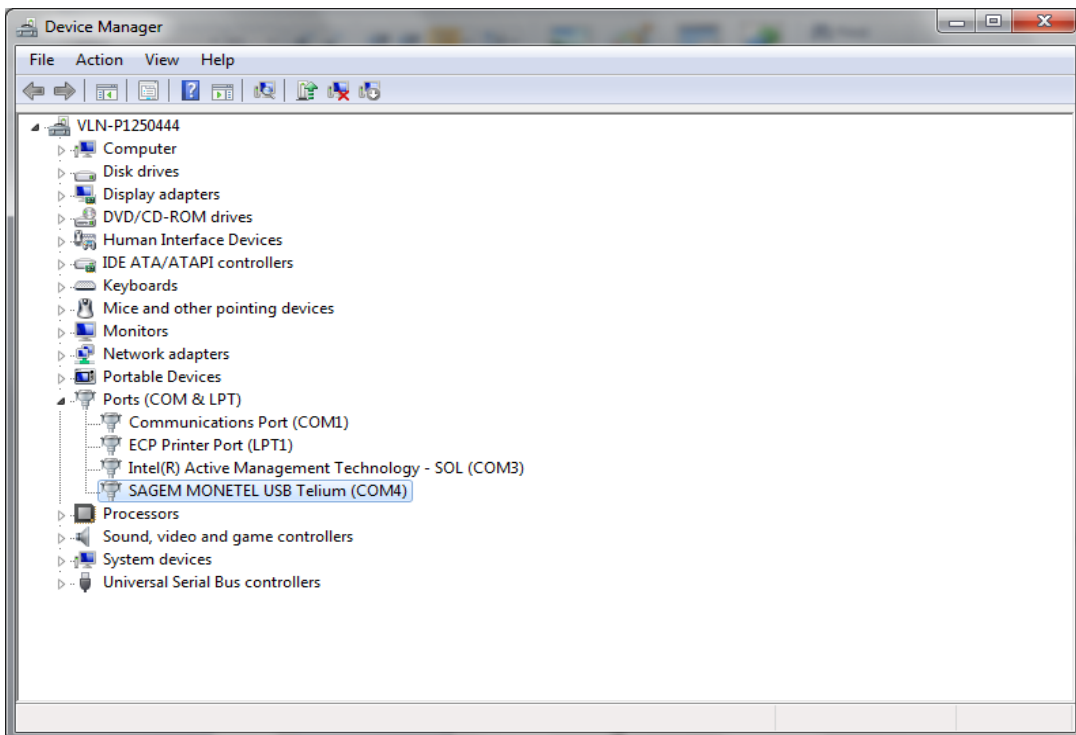
Click 'Browse' to select the subfolder 'drivers' under SAT installation folder and click 'Next'.



Check USB driver is correctly installed and click 'Close'.



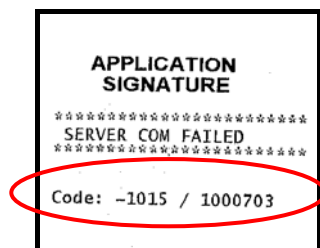
Now, the new device is displayed.



10.3. Network connection Troubleshooting

This chapter helps you to solve network connection problems.

The next chapter summarizes main communication errors you can encounter during an authentication process when a 'Server com failed' ticket is printed:



Error Code	Error message
- 1602	IP configuration Error.
-1015 / 1000703	Ethernet cable disconnected.
- 1002	GPRS error (APN error, SIM card error, insufficient GSM signal)

- 1602 :

Your IP configuration is not effective. In Ethernet mode, print a ticket like described in chapter 3.2.1 . If your ticket seems correct, check if your firewall is configured to connect host 86.206.130.148 on port 25000.

- 1015 / 1000703 :

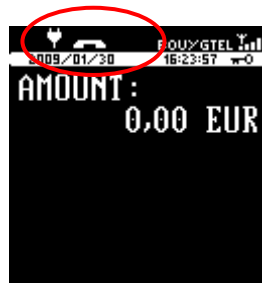
Your Ethernet cable doesn't seem to be connected. Check your Ethernet connexion.

Caution, If you attempt to use a GPRS connection whereas your manager is configured in Ethernet mode, you will have the same error code. So check that GPRS connection is selected (See chapter 3.2.2.2). The next picture illustrates the expected screen before authenticating an application in Ethernet mode.



-1002:

An error occurred because of a GPRS problem. Check if you receive a GPRS signal on the top-right of the manager menu and if the name of your provider is printed on the screen.



Then check your APN, login, password and gateway like described in chapter [3.2.2.2](#). It is advised to fall back on an Ethernet connection if this ticket appears permanent.

This Document is Copyright © 2009 by INGENICO Group. INGENICO retains full copyright ownership, rights and protection in all material contained in this document. The recipient can receive this document on the condition that he will keep the document confidential and will not use its contents in any form or by any means, except as agreed beforehand, without the prior written permission of INGENICO. Moreover, nobody is authorized to place this document at the disposal of any third party without the prior written permission of INGENICO. If such permission is granted, it will be subject to the condition that the recipient ensures that any other recipient of this document, or information contained therein, is held responsible to INGENICO for the confidentiality of that information.

Care has been taken to ensure that the content of this document is as accurate as possible. INGENICO however declines any responsibility for inaccurate, incomplete or outdated information. The contents of this document may change from time to time without prior notice, and do not create, specify, modify or replace any new or prior contractual obligations agreed upon in writing between INGENICO and the user.

INGENICO is not responsible for any use of this device, which would be non consistent with the present document.

All trademarks used in this document remain the property of their rightful owners

Your contact

Ingenico
192 avenue Charles de Gaulle
92200 Neuilly sur Seine - France
Tél.: + 33 1 46 25 82 00 - Fax: + 33 1 47 72 56 95
www.ingenico.com

