

# USER'S GUIDE

## Software Signature Tool (SST)

For **TELIUM™** Terminals



# CONTENTS

<b>1.</b>	<b>Introduction.....</b>	<b>3</b>
1.1	Purpose .....	3
1.2	Reference documents .....	3
1.3	Terminology and abbreviations .....	3
<b>2.</b>	<b>Environment.....</b>	<b>4</b>
<b>3.</b>	<b>Installation process.....</b>	<b>5</b>
<b>4.</b>	<b>General information on tool .....</b>	<b>6</b>
4.1	Mockup version .....	6
4.2	Launching the tool .....	6
4.3	Main functions .....	7
<b>5.</b>	<b>Generating a downloading file .....</b>	<b>8</b>
5.1	Environment .....	8
5.2	Signing a scheme.....	8
5.3	Selecting the default used certificate .....	10
5.4	Selecting the default signed scheme directory .....	11
5.5	Deleting a signed scheme.....	11
5.6	Creating the parameter file.....	11
5.7	Signing an application .....	12
<b>6.</b>	<b>Tool management.....</b>	<b>14</b>
6.1	Changing your own password.....	14
6.2	Event log .....	15
6.3	Modifying card PIN CODE .....	16
6.4	Selecting and testing card reader .....	17
6.5	Changing the tool language .....	17
6.6	Defining a new translation language .....	17
<b>7.</b>	<b>Using SST in command mode.....</b>	<b>18</b>
7.1	Command mode requirements.....	18
7.2	Example of configuration file .....	19
7.3	Running STT in command mode .....	20
<b>8.</b>	<b>Tool de-installation .....</b>	<b>21</b>
<b>9.</b>	<b>Parameter file description .....</b>	<b>22</b>
<b>10.</b>	<b>Appendices .....</b>	<b>24</b>
10.1	List of shortcut keys .....	24
10.2	Problems and solutions.....	24

# 1. INTRODUCTION

## 1.1 PURPOSE

This document describes the manner in which to install and use the Software Signature Tool (SST). This tool allows the VAR to compute the software signature and to generate files to be downloaded in the terminals with *TELIUM*™ technology.

In the continuation of this document, the following designations:

« terminals with *TELIUM*™ technology »  
will be replaced indifferently by:  
the word « terminal ».

## 1.2 REFERENCE DOCUMENTS

- **SDK30 USER'S GUIDE**, reference: OPE 1300

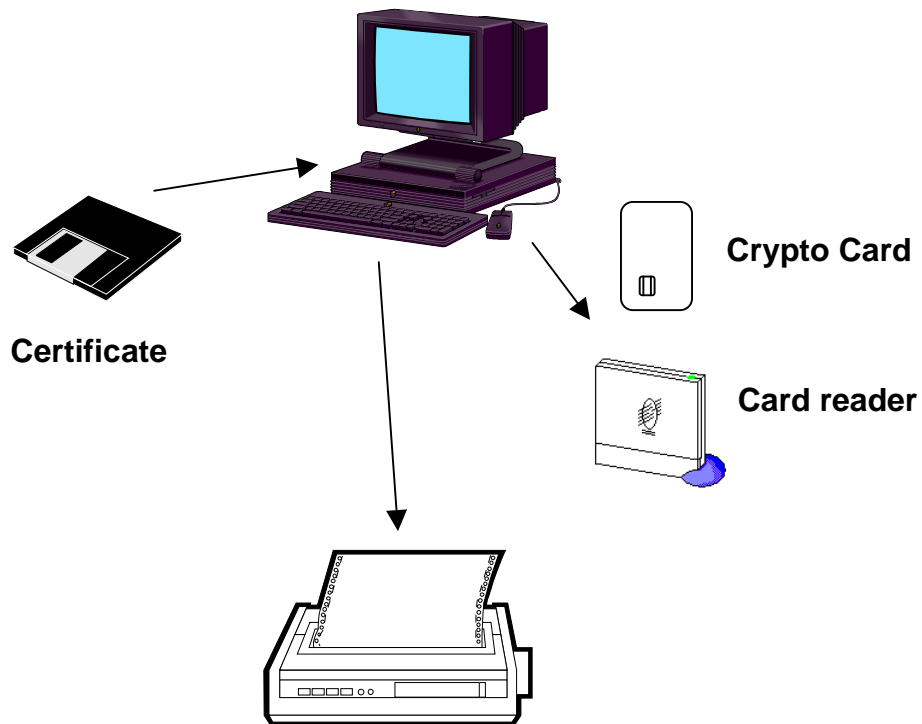
## 1.3 TERMINOLOGY AND ABBREVIATIONS

<b>Application software</b>	:	software module to be downloaded in the main processor of the TELIUM terminals.
<b>Certification authority</b>	:	Entity personalizing cryptographic cards including VAR ciphering key. This entity is also named "Trusted Third Party" for the definition of certification keys..
<b>Crypto card</b>	:	Individual card used by the VAR containing cryptographic algorithms allowing signature generation.
<b>Certificate</b>	:	Individual message including VAR's ciphering key used to sign application software.  This message is signed by a certification key.
<b>Certification key</b>	:	Key provided by the certification authority used to certificate the VAR's ciphering key.
<b>Ciphering key</b>	:	Key provided by the certification authority for the VAR.  This key is used by the VAR to sign its schemes or/and its applications.
<b>PC</b>	:	Computer
<b>Scheme</b>	:	Software module to be downloaded in the cryptographic microprocessor of the TELIUM terminals.
<b>Signature</b>	:	Ciphered message used to authenticate the software issuer.
<b>SST30</b>	:	Software Signature Tool for Telium Terminal.
<b>VAR</b>	:	Value Added Reseller : Entity who develops software for Telium terminals.

## 2. ENVIRONMENT

The Software Signature Tool is an application running under Windows® platform.

Software and hardware equipment are the following:



- A PC with a CD-ROM drive, a serial or an USB port.
- Microsoft ® Windows NT4, 2000 , XP or Vista.
- A printer to print the reports (optional)
- SST software and Data Base
- A USB card reader.
- A crypto card and an individual certificate to sign terminal software.

### 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 SST application, make sure that all applications are closed.

Process installation is the following:

- Insert the CD-ROM containing the SST software,
- if your PC doesn't run the setup automatically, from the task bar, start button, choose run, then browse CD drive and take "setup.exe" with open button,
- follow instructions on the screen. You can install this software in a directory other than the one proposed by default.
- Connect the card reader on a serial port or on an USB of the PC as shown on the card reader box. For serial reader only, connect the reader power cable to the keyboard port. WARNING, THE READER POWER CABLE MUST NOT BE DISCONNECTED FROM THE KEYBOARD PORT WHEN THE COMPUTER IS RUNNING, THIS ACTION MAY DAMAGE YOUR MACHINE! POWER OFF THE PC BEFORE ANY OPERATION ON THAT CONNECTOR!
- Install the matching driver located in the Smart Card Reader Drivers directory and follow instructions of the Readme.txt of this reader.

Once you have completed the setup procedure, you can launch the tool by double-clicking the SST icon.

## 4. GENERAL INFORMATION ON TOOL

### 4.1 MOCKUP VERSION

If the key `Mockup=yes` in the section `[Options]` is present in the `SST30.INI` file, the SST will be started in mock-up mode. In this mode you don't need to have a crypto card and a card reader to generate a downloadable component. In this case the label Mockup version is displayed on the SST login window.

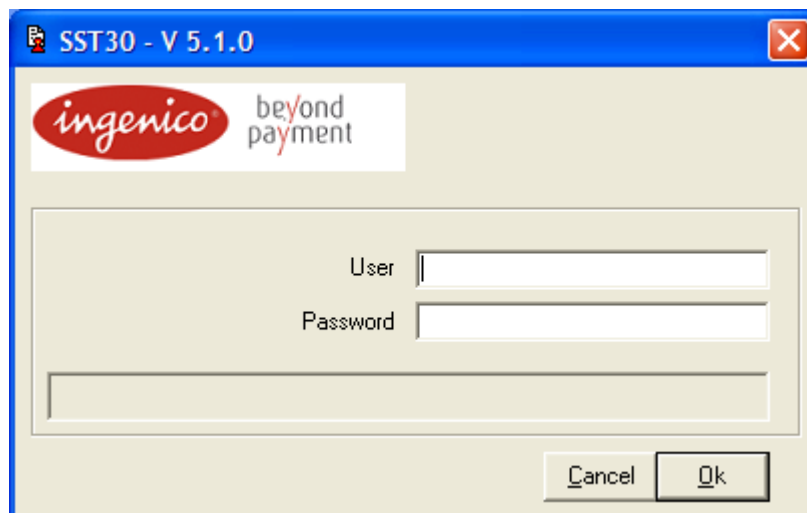
**Note:** This “mockup” component can be downloaded only in a terminal with mockup system.

### 4.2 LAUNCHING THE TOOL

To launch the tool, you can double-click on the icon of SST which is on the desktop. You can also use the “start menu”.

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

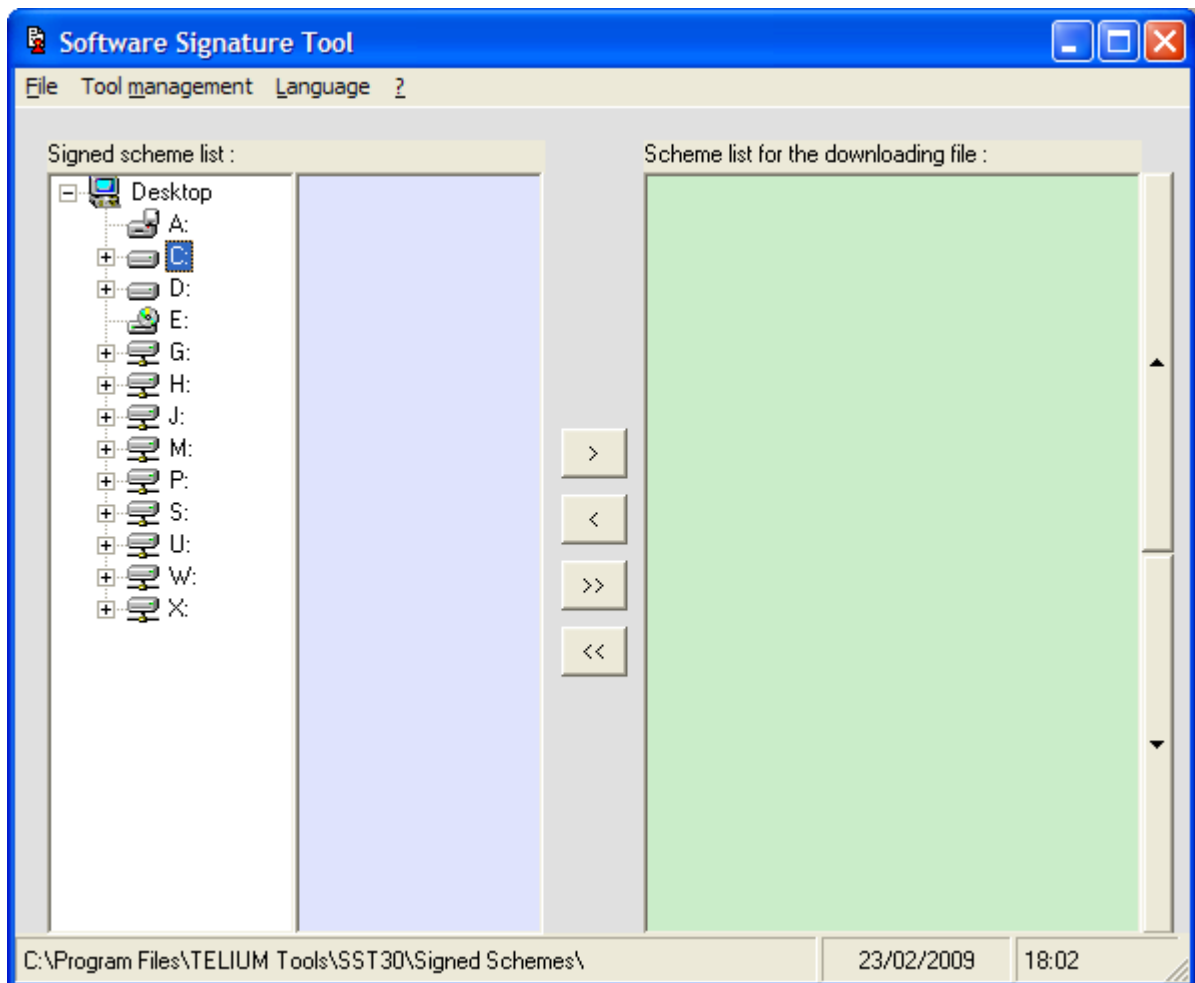
Through this procedure, only an authorized person can access to the tool.



After confirmation, the main screen is displayed.

## 4.3 MAIN FUNCTIONS

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



- sign a scheme,
- delete a signed scheme,
- open / create a parameter file,
- sign an application and create the downloadable files,
- administrate the tool (Password, Card Reader configuration, Events diary, ...)
- change tool language

After launching the SST software, select and test your card reader to the PC from Card Reader configuration menu.

## 5. GENERATING A DOWNLOADING FILE

### 5.1 ENVIRONMENT

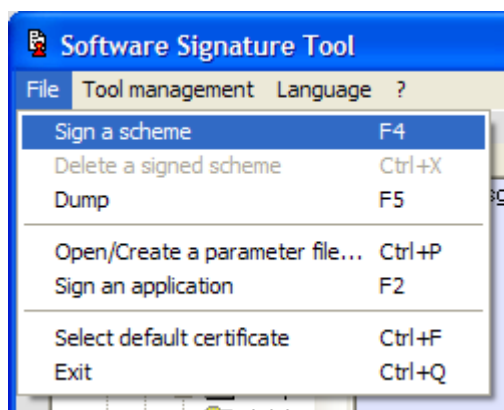
To generate a downloading file, the SST software needs:

1. A crypto card with a couple (Cipherring key / Decipherring key)
2. A certificate with the decipherring key
3. Binary files of the scheme, signed or not signed (optional)
4. Binary files of the application file.

### 5.2 SIGNING A SCHEME

This function is necessary 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**".

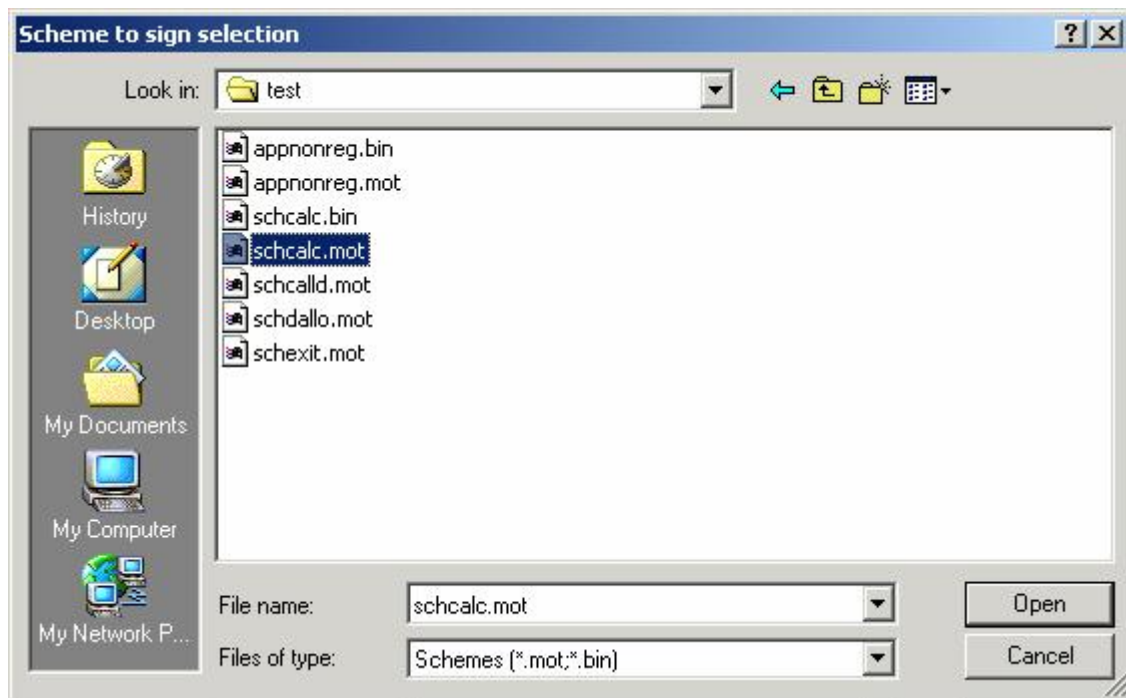


- From the shortcut key **F4**.

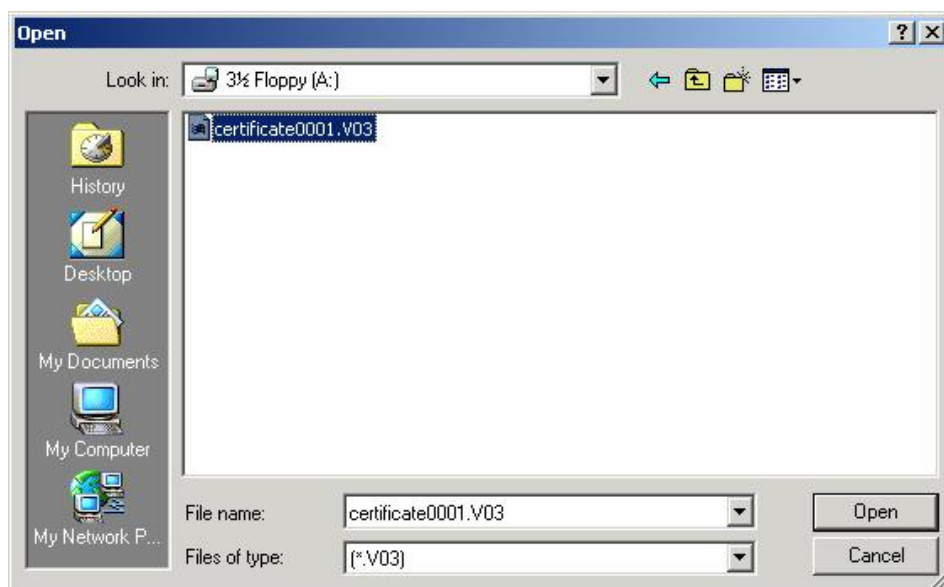
Then follow the instructions given by SST:

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





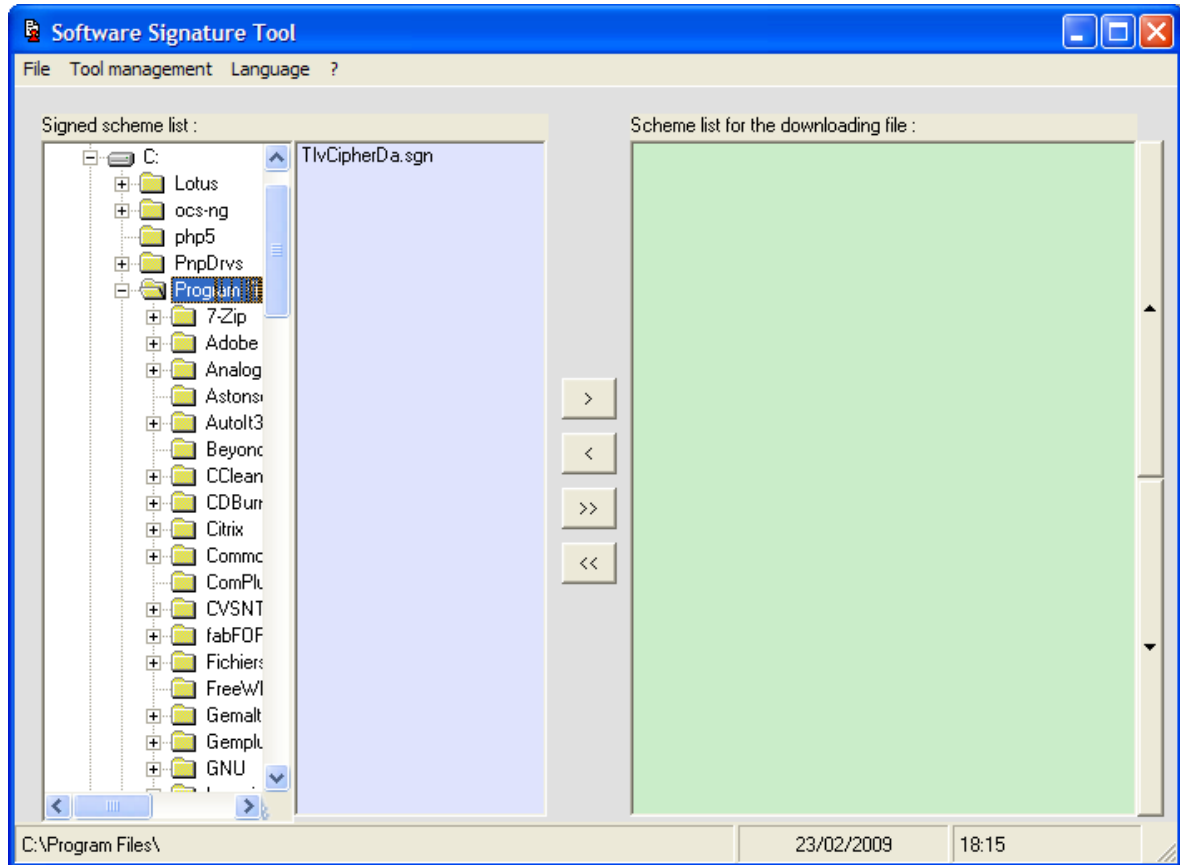
- Insert a crypto card (with the module facing down) in the card reader and select the directory and then the certificate file (file name "certif-xxxxxxx-yyy-zz.V03") in the dialogue box to sign scheme software:



- Enter the card Pin Code:

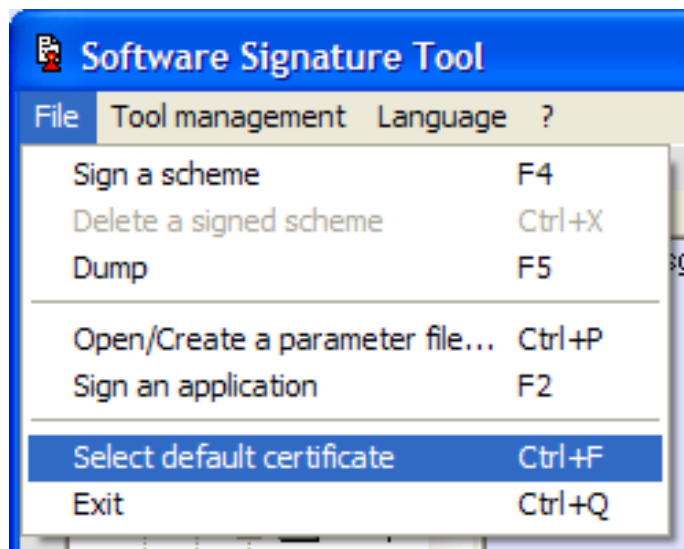


After that, the signed scheme is added to the list in the directory selected (by default in the "Signed Schemes" directory of the SST application):



## 5.3 SELECTING THE DEFAULT USED CERTIFICATE

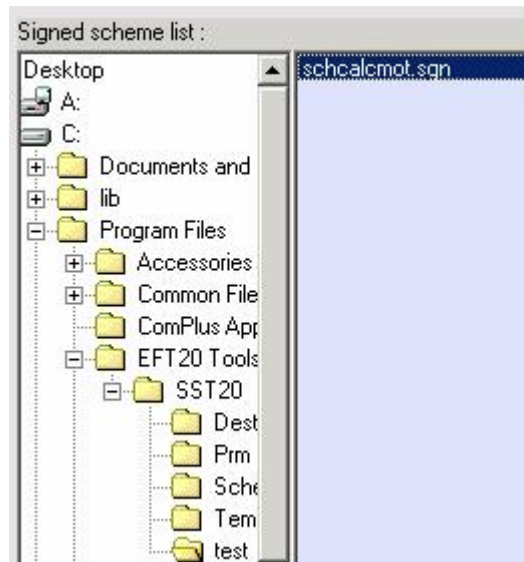
It is possible to define the used certificate once and for all from the menu **File | Select default certificate** or from the shortcut key **CTRL + F**.



## 5.4 SELECTING THE DEFAULT SIGNED SCHEME DIRECTORY

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

For example, in this case "test" directory:



## 5.5 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**.

## 5.6 CREATING THE PARAMETER FILE

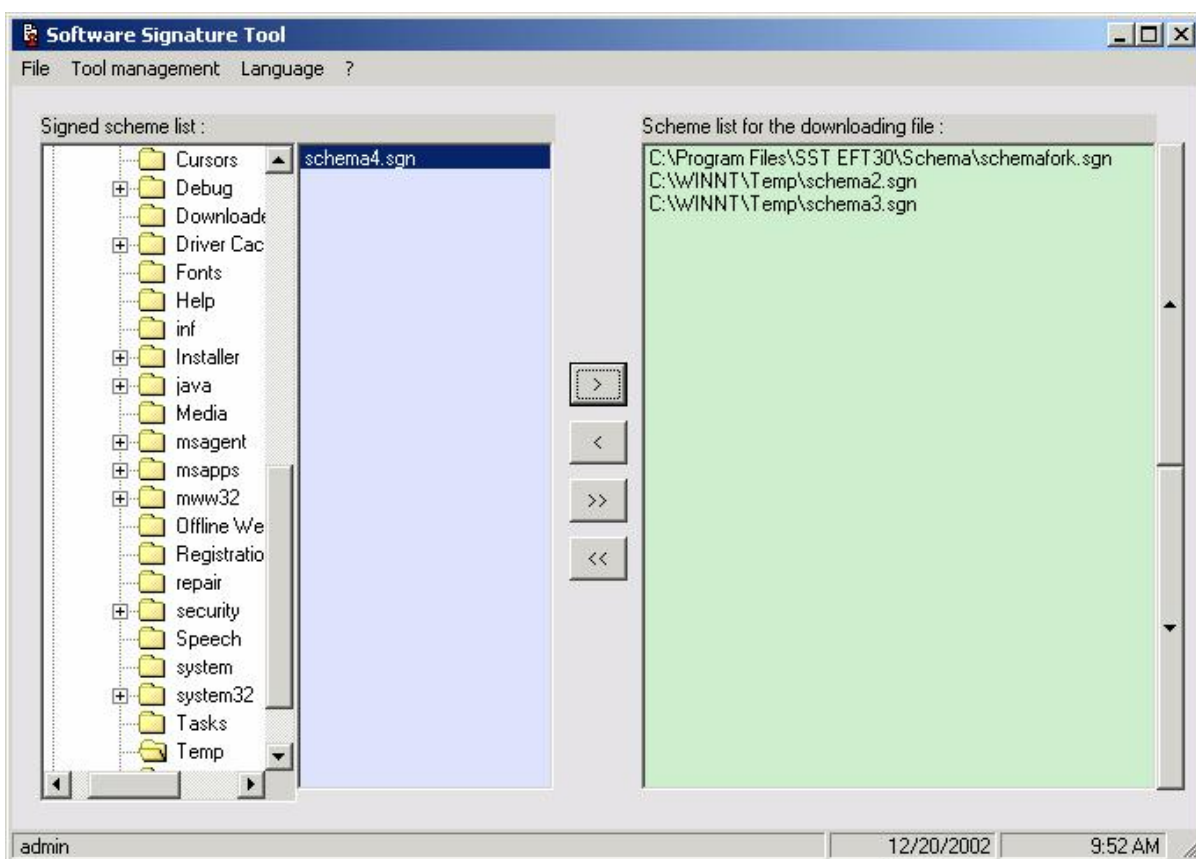
In order to define the application characteristics, you must define a parameter file used during the creating of the final files (see next chapter). Creation of this parameter file will be proposed during the process "Create the downloadable files", but it is possible to create or modify this file before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

## 5.7 SIGNING AN APPLICATION





Use this function to sign an application (with or without scheme) or a DLL (library) and to generate files to download in the terminal.

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 5.3) to select others signed schemes and repeat the previous step.

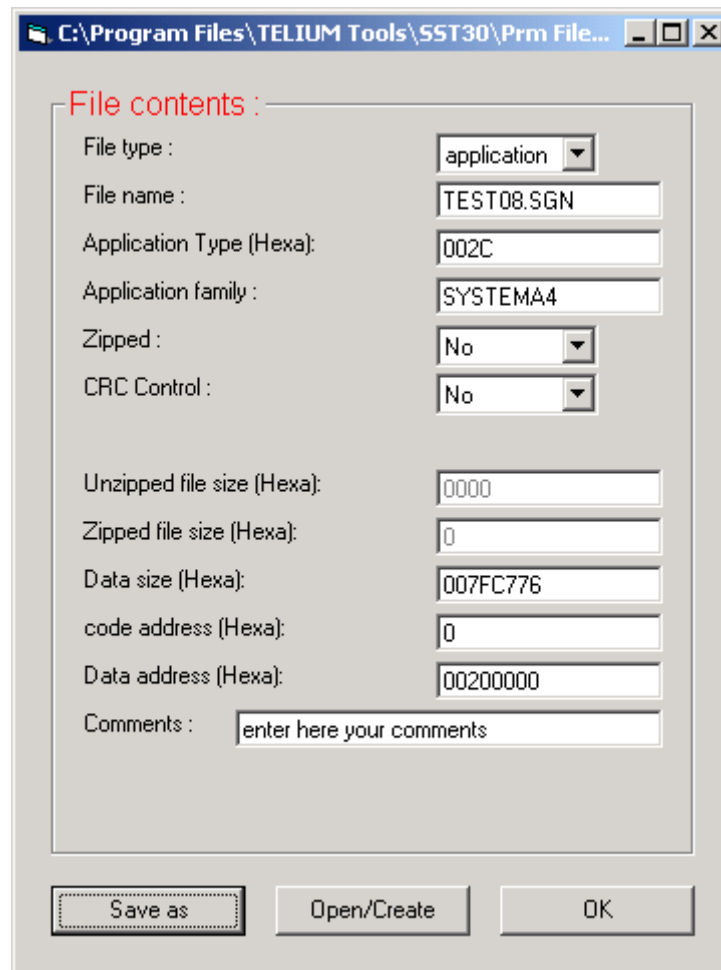
**Step 3.** Define order of the scheme in the downloading list with the "UpDown" buttons  or  .

**Step 4.** Use the menu **"File | Sign an application"** or use the shortcut key **F2**.

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

- Insert a crypto card (with the module facing down) in the card reader and select the directory and then the certificate file (filename "certif-xxxxxxx-yyzz.V03") in the dialogue box to sign application software,
- Select the application file (Motorola format or binary file),
- Enter the crypto card Pin Code,
- Select or create the parameter file (see example below),
- Enter the catalogue file extension (2 characters) depending on target type of terminal (example: 30 for TELIUM stationary terminal).

Example of a parameter file:



For parameter definition, See [Parameter file description](#).

After having enter different parameter value, click:

- "Save as" button to save parameters in a parameter file
- "Open/Create" button to open an existing file or create a new parameter file
- "OK" button to close this window and may be save the new values.

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

- one descriptor file with .ADF, .PDF or .LDF extension,
- one binary file signed with .SGN extension,
- one file with .Mxx extension where "xx" are the two characters identifying the target.

In addition you can print a report or save it in a text file.

#### Report Example:


Generation date and time:  
20/09/02 10:34:12  
Application name:  
A:\Application.mot  
Used schemes list:  
Scheme 1: scheme1.sgn  
Scheme 2: scheme2.sgn  
Scheme 3: scheme3.sgn

## 6. TOOL MANAGEMENT

The SST has only one user, the tool administrator.

### 6.1 CHANGING YOUR OWN PASSWORD

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



The screenshot shows a standard Windows-style dialog box titled "Change your Password". It features a blue title bar with a close button (X) on the right. The main area is light gray and contains three text input fields stacked vertically, each preceded by a label: "Old Password", "New Password", and "Confirm New Password". At the bottom right of the dialog, there are two buttons: "Cancel" and "OK".

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.

## 6.2 EVENT LOG

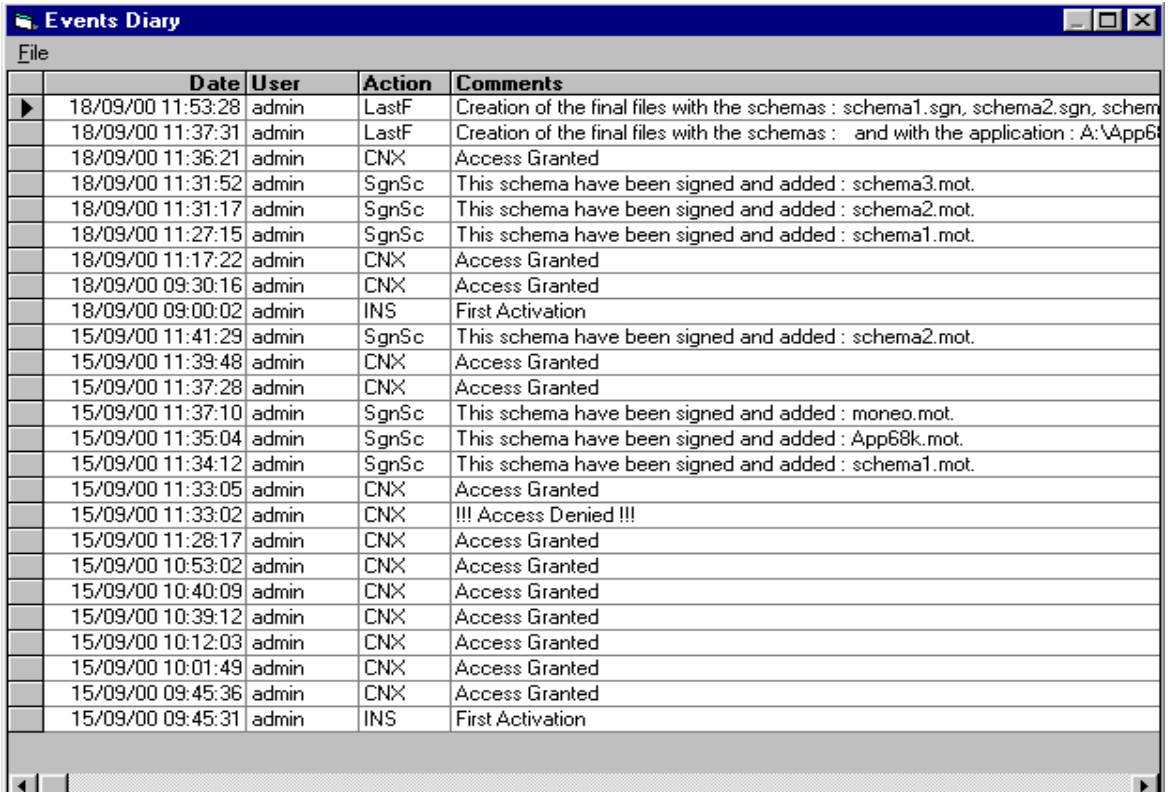
This function is accessible from the main menu **“Tool management | Event log”**.

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 "Events Diary" 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 25 rows of event logs, including actions like "LastF", "CNX", "SgnSc", and "INS" performed by the "admin" user. The comments provide details about schema creation, signing, and access grants.

Date	User	Action	Comments
18/09/00 11:53:28	admin	LastF	Creation of the final files with the schemas : schema1.sgn, schema2.sgn, schem
18/09/00 11:37:31	admin	LastF	Creation of the final files with the schemas : and with the application : A:\App6
18/09/00 11:36:21	admin	CNX	Access Granted
18/09/00 11:31:52	admin	SgnSc	This schema have been signed and added : schema3.mot.
18/09/00 11:31:17	admin	SgnSc	This schema have been signed and added : schema2.mot.
18/09/00 11:27:15	admin	SgnSc	This schema have been signed and added : schema1.mot.
18/09/00 11:17:22	admin	CNX	Access Granted
18/09/00 09:30:16	admin	CNX	Access Granted
18/09/00 09:00:02	admin	INS	First Activation
15/09/00 11:41:29	admin	SgnSc	This schema have been signed and added : schema2.mot.
15/09/00 11:39:48	admin	CNX	Access Granted
15/09/00 11:37:28	admin	CNX	Access Granted
15/09/00 11:37:10	admin	SgnSc	This schema have been signed and added : moneo.mot.
15/09/00 11:35:04	admin	SgnSc	This schema have been signed and added : App68k.mot.
15/09/00 11:34:12	admin	SgnSc	This schema have been signed and added : schema1.mot.
15/09/00 11:33:05	admin	CNX	Access Granted
15/09/00 11:33:02	admin	CNX	!!! Access Denied !!!
15/09/00 11:28:17	admin	CNX	Access Granted
15/09/00 10:53:02	admin	CNX	Access Granted
15/09/00 10:40:09	admin	CNX	Access Granted
15/09/00 10:39:12	admin	CNX	Access Granted
15/09/00 10:12:03	admin	CNX	Access Granted
15/09/00 10:01:49	admin	CNX	Access Granted
15/09/00 09:45:36	admin	CNX	Access Granted
15/09/00 09:45:31	admin	INS	First Activation

## 6.3 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.

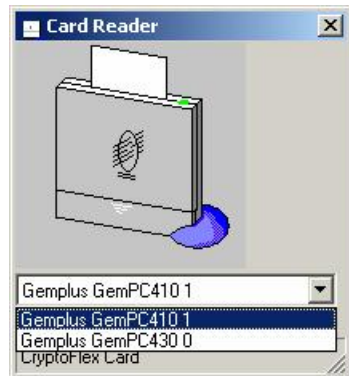
The new PIN CODE must be confirmed to be validated.



## 6.4 SELECTING AND TESTING CARD READER

The card reader for the crypto cards must be connected on a serial port or an USB port of your PC.

To select the card reader from the menu, you can use the function "**Tool management | card reader configuration**".



Furthermore, you can use this window to test your card reader. If your card reader is running it detects the card presence. Once the crypto card introduced, a double click on the image of the card reader displays the card serial number.



## 6.5 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 "**L**anguage" 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.

## 6.6 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 SST 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 SST IN COMMAND MODE

SST can be invoked in command mode. It avoids using SST in interactive mode to generate a new application based on Crypto products requiring a signature. This documents is dedicated to developers that want to quickly generate signed applications on EFT.

### 7.1 COMMAND MODE REQUIREMENTS

When used in command mode, SST needs the following information in order to sign an application :

- Card reader name
- 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 (.V03 file)
- Directory and application binary filename (.mot or .bin file)
- Destination directory of generated files (.sgn and .adf files)
- Temporary directory dedicated to the SST
- 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.

[SST] Section		
Key name	Description	Value
ReaderName	Used Card Reader Name depending on serial or USB Connection	"Gemplus GemPC410 0" (for Serial connection) Or "Gemplus GemPC430 0" Or "Gemplus USB Smart Card Reader 0" (USB for USB connection)
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	
[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	

[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 TELIUM stationary

## 7.2 EXAMPLE OF CONFIGURATION FILE

[SST]

```
ReaderName=Gemplus USB Smart Card Reader 0
CertificateSchemaDir=C:\Program Files\TELIUM Tools\SST30
CertificateAppliDir=C:\Program Files\ TELIUM Tools\SST30
SignedSchemaDir=C:\Program Files\ TELIUM Tools\SST30\Signed Schemes
ParametersDir=C:\Crypto\Manager\Test1
DestinationDir= C:\Program Files\ TELIUM Tools\SST30\Destination
ApplicationDir=C:\Crypto\Manager\Test1
TempDir= C:\Program Files\ TELIUM Tools\SST30\Temp
```

[Schemas]

```
NbSchemas=3
Schema1= C:\Program Files\ TELIUM Tools\SST30\Signed Schemes\Sch1.sgn
Schema2= C:\Program Files\ TELIUM Tools\SST30\Telium Schemes\Sch2.mot
Schema3= C:\Program Files\ TELIUM Tools\SST30\Telium Schemes\Sch3.mot
CertificateFile=Certificate0004.V03
```

[Application]

```
ParameterFile=Appli.txt
CertificateFile=Certificate0004.V03
ApplicationFile=Appli.bin
CatalogFileExtension=30
```

### **Notes**

If one of the 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 SST returns ).

## 7.3 RUNNING SST IN COMMAND MODE

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

- Action number to be done (1 or 2 )
- Directory and filename of the configuration file to use SST in command mode
- PIN code of card to be used ("00000000" to use the SST in Mock-up mode)

**Syntax :** SST30 <action number>,<path>+<configuration filename>,<pincode>  
From SST directory only !

**Example :** "C:\Program Files\Telium Tools\SST30\SST30.exe" 1, C:\Program Files\Telium Tools\SST30\cmdmode.prm,12345678

(do not forget double quote: " ")

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

SST can be invoked from an application, from a DOS window or from WINDOWS (in any cases, path where SST30.EXE is located is to be specified).

SST can be directly called from WINDOWS by clicking on a SST link. In such case, create a link file and modify SST30.EXE properties. In the field Target, specifies the parameters to pass to the SST

Example :

If target is C:\Program Files\Telium Tools\SST30\SST30.exe write :

"C:\Program Files\Telium Tools\SST30\SST30.exe" 1, C:\Program Files\Telium Tools\SST30\cmdmode.prm,12345678

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

Action	Number	[SST]	[Schemes]	[Application]
Sign one scheme or several schemes	1	X	X	
Sign an application without schemes	2	X		X
Sign an application with signed and/or unsigned schemes	2	X	X	X

A section is created in configuration file when SST returns an error. It can be later analysed by the calling application.

[Error]

Code=

- 0 : No error
- 1 : Destination file already existing
- 2 : Card absent
- 3 : Certificate file absent
- 4 : Scheme file absent
- 5 : Incorrect couple of certificate file and card
- 6 : repudiated scheme by another scheme
- 7 : Problem with card reader
- 8 : Parameter file absent
- 9 : DLL error
- 10 : PIN code error
- 11 : Invalid Motorola file Format
- 12 : Application file absent
- 13 : Destination directory absent

- 14 : Temporary directory absent
- 15 : Directory containing signed schemes files absent
- 16 : Scheme Signature not allowed in Mock-up mode.

## 8. TOOL DE-INSTALLATION

1. From the task bar click on "**Start**" button and choose "**Programs -> Telium Tools -> SST30 -> Uninstall SST30**".

Or

1. From the task bar click on "**Start**" button and choose "**Settings -> Control Panel -> Add / Remove programs**".

2. Choose SST30 application, and click on **Add / Remove** button.

3. Remove all components.

## 9. PARAMETER FILE DESCRIPTION

This file ensures to create the descriptor file associated to the signed file. See below the descriptor file extensions.

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

field name	size (byte)	Format	Value	Comments
File Type	1	HEX	0 = parametrer descriptor 1 = application descriptor 2 = librairy descriptor 3 = driver descriptor	indicator to identify what kind of signed file it is
File name	15 Max	ALPHAUP		Component file name, including its extension (.SGN)
Application type	4	HEX		Hexadecimal Code indicating the type of application (system, manager, banking, loyalty,...) <b>This number must be supply by your terminal provider.</b>
Application Family	16 Max	ALPHAUP		name identifying in which family is linked this file
Zipped	1	HEX	0= no,1= yes	compression indicator
CRC checked	1	HEX	0= no,1= yes	CRC control indicator
CRC	4	HEX		Checksum applied on the non compressed file, without signature or certificate <b>Computed by SST and put in the descriptor file</b>
Unzipped file size	8 Max	HEX		Uncompressed file size without signature or certificate <b>Computed by SST and put in the descriptor file</b>
Zipped file size	8 Max	HEX		compressed file size without signature or certificate <b>Computed by SST and put in</b>

				the descriptor file
Data size	8 Max	HEX		maximum size used by application data
code address	8 Max	HEX		If library : loading adresse for code, else : 0 for ARM code 1 for THUMB code
data address	8 Max	HEX		If library : loading adresse for data, else : 00200000H by default
Comments	30 Max	ASCII		Component description

Example of parameter file:

1,TEST\_12.SGN,002C,TEST,0,1,3EC5,03D578E,0,02547C,0,00200000,Test Component

The following list shows the specifics extensions for each kind of descriptor file:

Extension	Type of file
.ADF	Application Description File
.PDF	Parameter Description File
.LDF	Library Description File
.DDF	Driver Description File (reserved SAGEM Monetel)

# 10. APPENDICES

## 10.1 LIST OF SHORTCUT KEYS

Each SST 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
Sign a scheme	F4
Sign an application	F2
Dump	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 PROBLEMS AND SOLUTIONS

Some errors are listed, their description is given below in order to correct potential problem.

Error message	What to do ?
<i>No Card Reader plugged in</i>	Following the used card reader, see <i>Pre-Requisites</i> or <i>Troubleshooting</i> section in the <i>Readme.txt</i> file located in the <i>Smart Card Reader Drivers</i> directory.
<i>Unknown Card</i>	Check if the crypto card is correctly inserted (with the module facing down) into the card reader.
<i>Error 53. File not found: Wincard.dll</i>	Under Windows ® NT4, The Smart Card Base Components are not installed. See the <i>Readme.txt</i> file located in Smart Card Manager sub-directory.



This Document is Copyright © 2008 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 agree 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.

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

Your contact