STARMAG 4.1

Smart Card Management and Application Generator
Smart Card Development Tool

Online Help Printout
Edition 08.2005

Giesecke & Devrient

ID No. 30017123

Giesecke & Devrient GmbH
Prinzregentenstr. 159
Postfach 80 07 29
D-81607 München

Contents

About STARMAG

Characteristics

STARMAG (Smart Card Management and Application Generator) is a universal design and personalization tool for smart card applications based on the STARCOS operating system.

The tool allows applications to be created and downloaded onto smart cards.

Features

Features of STARMAG include:

- Application development
- Validation of smart card applications
- Initialization and personalization of smart cards
- EEPROM image creation for smart card completion
- Memory space calculation

About the Document

Target Group

This manual addresses developers and specialists of smart card applications based on the STARCOS operating system.

Required Knowledge

In order to user STARMAG, you should be familiar with:

– STARCOS 3.0 and 3.1 operating system
– File structures of smart card operating systems

This document assumes that you have a basic understanding of Microsoft Windows terminology and actions. Should you feel that this is not the case, it is suggested that you refer to your Windows manuals first.

More information on the relevant standards may be found in the appendix (see 'B Reference Literature' on page 33).

Notation

In order to facilitate access to required information and to provide quick orientation, the following graphical aids and notations have been used:

This convention	Indicates
Sample	Menu, command or dialog name of the user interface
Sample	Command name

Notes comprise hints and recommendations useful when working with STARMAG.

Please read warnings carefully - they are specified to prevent severe malfunctions and loss of data!

The header page of each chapter features an overview of the topics covered in the chapter. All technical terms and abbreviations used are explained in a glossary at the end of the manual.

Getting Help

All help files and user documentation are stored in the installation folder of STARMAG. Sample applications are provided in the */Examples*Sc30 and */Examples*Sc31 folders.

The guided tour section of the online help provides step-by-step procedures for creating an example card application for card holder authentication using a password.

For the latest product information and release notes, refer to the readme file.

1 Understanding STARMAG

This chapter describes the basic principles of STARMAG and provides background information related to the program.

It is recommended that you are familiar with the material in this chapter before you start operating the program.

Contents

1.1 Basics

What is STARMAG?

STARMAG is a universal design and personalization tool for smart card applications based on the STARCOS operating system. The tool allows smart card applications to be created and downloaded onto smart cards.

Using the menus and dialogs of the program, you can create a new card application or load an existing one and insert the required file system structures. A STARMAG card application usually consists of a card document containing card settings, an MF root, DF container and various EFs (e.g., EF_RULE, EF_PWD, EF_PWDD and EF_PFPC). For each element of the file structure, the required settings must be specified in the corresponding tab of the program.

Before downloading the application to card or file, the card application can be checked for validity and the download settings can be defined. In addition, HTML reports can be created, which can be printed or saved to file. The HTML report provides a summary of all relevant file system information.

STARMAG is a multiple document program, meaning that one or more card documents can be displayed at the same time. Each card document represents the application of a STARCOS card.

1.2 Main Window

Main Window

After launching the program and selecting a STARMAG card, the STARMAG window is organized as follows:

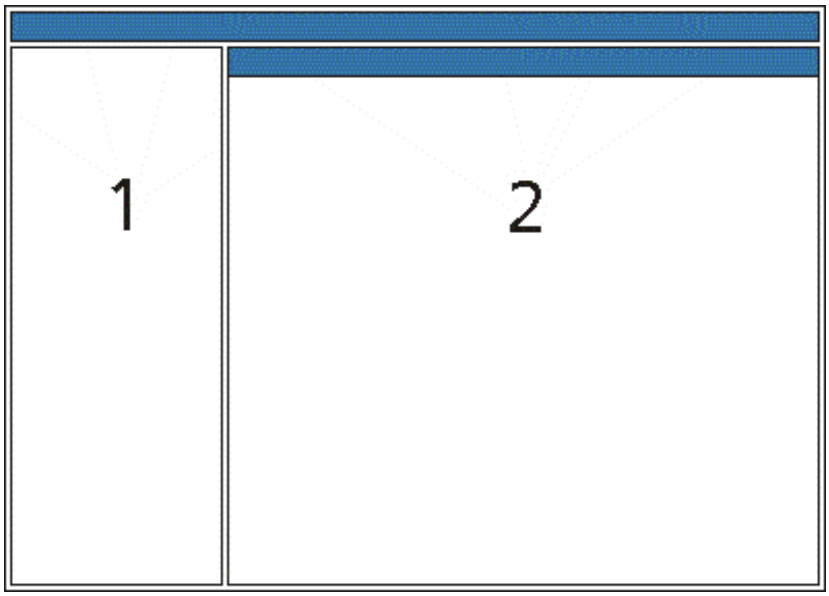

Fig. 1 Window scheme of STARMAG

The STARMAG main window comprises the elements:

– (1) Tree pane
– (2) Content pane

Tree Pane

The tree pane shows the file structure of the STARMAG card application. The card application comprises the following file tree elements:

– Card document
  Shows the name of the card document; e.g., STARCOS 3.0 / STARCOS 3.1 card. When a card document is selected, the card is shown in the content pane.
– Card Settings
  Shows the card settings used for the card application. The settings for EEPROM image and downloading can be specified in the *EEPROM Image* and *Options* tabs, respectively.
– MF
  Shows the MF identified by the file ID '3F 00'. The MF represents the root of the card application. When the MF is selected, the required parameters can be specified in the *FCP*, *Settings*, *ARR File* and *ARR DO* tabs. In addition, the specified parameters can be viewed in the *Report* tab and text comments can be entered in the *Notes* tab.
– DFs and EFs
  Shows the DF and EFs (e.g., EF_RULE, EF_PWD, EF_PWDD, EF_PFPC, etc.) used in the card application. Depending on whether a DF or EF

is selected, the required parameters can be entered in the *FCP*, *Settings*, *Contents*, *ARR File* and *ARR DO* tabs. In addition, the specified parameters can be viewed in the *Report* tab and text comments can be entered in the *Notes* tab.

Content Pane

The tabs displayed in the content pane depend on which tree element is selected in the tree pane.

When the *Card Settings* element is selected in the tree pane, the following tabs are displayed:

– *EEPROM Image*
Refers to the initialization file needed for EEPROM image creation under the *Card* | *Create EEPROM Image* menu. The EEPROM image is internally used by G&D for card production.

– *Options*
Displays the options for downloading and EEPROM image creation.

– *Report*
Displays the parameters selected in the *EEPROM Image* and *Options* tabs.

– *Notes*
Allows additional text to be included for documenting the card settings.

Depending on which file system element (e.g., MF, DF or EF) is selected in the tree pane, the following tabs may be displayed:

– *FCP*
Displays the file name (e.g., MF, DF or EF) and the non-security related File Control Parameters (FCP).

– *Settings*
Specifies EEPROM image creation settings for the MF and DF; i.e., whether deletion of the application is allowed. Also specifies download settings for the MF; i.e., whether the MF is to be activated.

– *Content*
Specifies file-related content information for the various EFs; for example, records can be added and deleted.

– *ARR file*
Specifies Access Rule References (ARR) for the various EFs.

– *ARR DO*
Specifies Access Rules Reference Data Object (ARR DO) for the MF and DF.

– *Report*
Summarizes all information about the selected tree element.

– *Notes*
Allows additional text to be included for documenting the selected tree element.

1.3 About the Guided Tour

Overview of Tour

The tour demonstrates how to create a card application for card holder authentication using a password. After verifying the password, the contents of the EF can be read.

The tour provides step-by-step procedures for:

- Creating a new card application
- Checking the card application
- Defining download settings
- Downloading the card application
- Creating an HTML report

You begin the tour by performing the first procedure (see '2.1 Creating a New Card Application' on page 12).

File Structure of the Card Application

The example card application contains the following file structure:

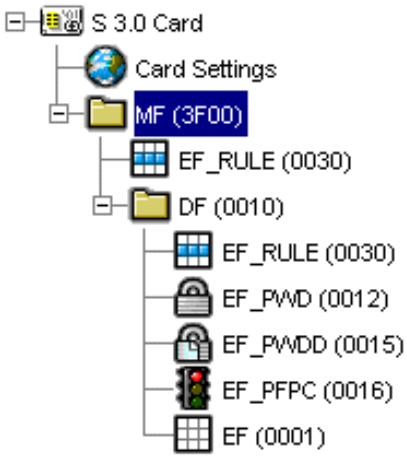

Fig. 2 File structure of the example application in the guided tour

The file structure of the example application contains the following elements:

- *MF*
  Specifies the MF root of the card application and contains an ARR to *EF_RULE*:
  - *EF_RULE*
    Contains an access rule record referenced by the MF, allowing the card to be reset to the delivery state.
- *DF*
  Serves as a container for the EFs of the card application:
  - *EF_RULE*
    Contains two access rule records referenced by *EF (0001)* and *EF_PWDD* at the DF level:

Access rule record 1 allows *EF (0001)* to be read/searched and updated after password verification.
Access rule record 2 allows verification of the password referenced in *PWDD*.

– *EF_PWD*
Specifies the length and value of the password, and whether the password is to be automatically encrypted.

– *EF_PWDD*
Specifies the password description comprising the password reference to *EF_PWD*, storage format, ARR to the second access rule record of *EF_RULE* and Security Environment (SE) template.

– *EF_PFPC*
Specifies the PIN Fault Presentation Counter (PFPC) with an initial value of 3.

– *EF (0001)*
Specifies 'Hello World' as EF content and contains an ARR to the first access rule record of *EF_RULE*, allowing *EF (0001)* to be read/searched and updated after password verification.

2 Guided Tour

You begin the tour by carrying out the first procedure. The tour provides step-by-step instructions for performing each procedure. After completing each procedure, instructions are provided on how to proceed.

This chapter does not contain instructions on how to test the STARMAG card application. For this purpose, the STARTEST tool must be used. STARTEST is included in STARCOS Toolkit.

Contents

2.1 Creating a New Card Application

About this Procedure

This procedure describes how to create a new card application for card holder authentication using a password.

When a new card application is created, an MF is added below the *Card Settings* element in the tree structure.

In the *Settings* tab of the MF, *Activate MF* is activated in order to activate the access rules of the application via the *ACTIVATE* command. All other settings in the *FCP* tab, *ARR File* tab and *ARR DO* tab are not relevant for downloading, since the MF already exists on the card.

The subsequent procedures of the tour describe how to add an EF_RULE access rule file and DF to the MF level.

How to Proceed

File | *New Card*

To create a new card application:

1. Select *File* | *New Card*.
   ↳ The *New Card* window is displayed.
2. Select *STARCOS 3.0 / 3.1* to select a STARCOS card and click *OK*.
   ↳ A new STARCOS 3.0 / 3.1 card document is shown in the tree pane and the MF is highlighted below the *Card Settings* element. The *FCP* tab is activated by default.
3. Accept the default settings in the *FCP* tab and select the *Settings* tab.
   ↳ *Activate MF* is activated by default. During download of the application, the access rules of the application will be activated via the *ACTIVATE FILE* command.
4. Continue with the next procedure (see ’2.2 Adding an Access Rule File (EF_RULE) to the MF Level’ on page 13).

2.2 Adding an Access Rule File (EF_RULE) to the MF Level

About this Procedure

This procedure describes how to add an EF_RULE file to the MF level of the file structure.

The EF_RULE file contains one access rule record referenced by the MF. The record specifies the access mode 'DELETE FILE (self)' and security condition 'Always'.

If the MF contains an ARR to EF_RULE with access mode 'DELETE FILE (self)' and security condition 'Always', the *DELETE MF* command can be performed, causing the card to be reset to the delivery state.

How to Proceed

Edit | *New* | *EF RULE*

To add an EF_RULE file to the MF level of the card application:

1. In the tree pane, select the MF and then and select *Edit* | *New* | *EF RULE*.
   ↳ An EF_RULE file is added to the MF level.
2. Select *EF_RULE*.
   ↳ The *FCP* tab is activated by default.
3. Accept the default settings in the *FCP* tab, select the *Content* tab and click *New* to add a new access rule record.
   ↳ Access rule record 1 is displayed in the activated *Record* tab.
4. Click *Edit*.
   ↳ The *Rule 0* tab is displayed.
5. Click *New AM* to set the access mode.
   ↳ The window is extended for entering access mode settings.
6. Under *Select the way to describe the Access Mode*, accept *Standard Commands* as default setting and under *Set access mode for standard and administration commands*, activate *Bit 7 DELETE FILE (self)*.
7. Click *New SC* to specify the security condition type.
   ↳ The *Security Condition Type* view is displayed.
8. Accept *Always* as default setting and click *OK*.
   ↳ The first rule record displays the byte code '`80 01 40 90 00`'.

   TLV '80 01 40' indicates access mode 'DELETE FILE (self)' and TLV '90 00' indicates security condition 'Always'.
9. In the tree pane, click the MF and select the *ARR File* tab.
   ↳ Accept the default ARR: SE# 'All', Interface 'All', EF File ID 'Default '0030'', and Record# '1'.

10. Continue with the next procedure (see ’2.3 Adding a DF’ on page 15).

2.3 Adding a DF

About this Procedure

This procedure describes how to add a DF to the MF level of the file structure.

The subsequent sections of the tour describe how to add an EF_RULE access rule file and additional EFs (e.g., EF_PWD, EF_PWDD, EF_PFPC and EF) to the DF level of the card application.

How to Proceed

Edit | *New* | *DF*

To add a DF to the MF level of the card application:

1. In the tree pane, select the MF and then select *Edit* | *New* | *DF*.
   ↳ A DF is added to the MF level.
2. Select *DF (0000)*.
   ↳ The *FCP* tab is activated by default.
3. Under *File ID* of *Tag '83'*, enter '0010' as the value for the file ID and accept the other default settings of the *FCP* tab.
   ↳ After exiting this tab, the file ID will display *DF (0010)* instead of *DF (0000)*.
4. Continue with the next procedure (see '2.4 Adding an Access Rule File (EF_RULE) to the DF Level' on page 16).

2.4 Adding an Access Rule File (EF_RULE) to the DF Level

About this Procedure

This procedure describes how to add an EF_RULE file to the DF level of the file structure.

The EF_RULE file contains two access rule records:

– Access rule record 1 referenced by *EF (0001)*
Contains an access mode TLV (Tag '80') and a security condition TLV (Tag 'A4'). This rule allows the records of *EF (0001)* to be read/ searched and updated after password verification.

– Access rule record 2 referenced by *EF_PWDD*
Contains an access mode TLV (Tag '80') and a security condition TLV (Tag '90'). This rule allows password verification.

Adding EF_RULE

Edit | *New* | *EF RULE*

To add an EF_RULE file to the DF level of your the application:

1. In the tree pane, select the DF and then select *Edit* | *New* | *EF_RULE*.
   ↳ An EF_RULE file is added to the DF level.
2. Select *EF_RULE* of the DF level.
   ↳ The *FCP* tab is activated by default.
3. Accept the default settings of the *FCP* tab.
4. Continue with "Adding the First Access Rule Record".

Adding the First Access Rule Record

To add the first access rule record to the EF_RULE file of the DF level:

1. Select the *Contents* tab and click *New* to add the first access rule record.
   ↳ Access rule record 1 is displayed.
2. Click *Edit*.
   ↳ The *Rule 0* tab is displayed.
3. Click *New AM* to set the access mode of the first access rule record.
   ↳ The window is extended for entering access mode settings.
4. Under *Select the way to describe the Access Mode*, accept *Standard Commands* as default setting and under *Set access mode for standard and administration commands*, activate *Bit 1* and *Bit 2* to allow the *READ/SEARCH* and *UPDATE RECORD* commands to be used for *EF (0001)*.
5. Click *New SC* to specify the security condition type of the first access rule record.
   ↳ The *Security Condition Type* view is displayed.
6. Activate *Password* for the example application.

↳ The *SC of Type PWD* view is displayed.

7. Under *Password List* box, click on the *PWD 1* entry.
   ↳ The *Password Reference* view is displayed.
8. Under *Usability*, select *local* and under *Password ID*, select 1 as the password ID to be used and click *OK*.
   ↳ Access rule record 1 displays the byte code '80 01 03 A4 07 95 01 08 83 02 80 01'.

   TLV '80 01 03' indicates access mode 'UPDATE' and 'READ/SEARCH RECORD' and TLV 'A4 07 95 01 08 83 02 80 01' indicates security condition 'Password', including the usage qualifier for card holder authentication TLV '95 01 08' and the password reference TLV '83 02 80 01'.
9. Continue with "Adding the Second Access Rule Record".

Adding the Second Access Rule Record

To add the second access rule record to the EF_RULE file of the DF level:

1. Click *New* to add the second access rule record.
   ↳ Access rule record 2 is displayed below record 1.
2. Click *Edit*.
   ↳ The *Rule 0* tab is displayed.
3. Click *New AM* to set the access mode of the second rule record.
   ↳ The window is extended for entering access mode settings.
4. Under *Select the way to describe the Access Mode*, accept *Standard Commands* as default setting and under *Set access mode for standard and administration commands*, activate *Bit 1* to allow the *VERIFY* command to be used for password verification.
5. Click *New SC* to specify the security condition type of the second access rule record.
   ↳ The *Security Condition Type* view is displayed.
6. Accept *Always* as default setting and click *OK*.
   ↳ Access Rule record 2 displays the byte code '80 01 01 90 00'.

   TLV '80 01 01' indicates access mode 'VERIFY' and TLV '90 00' indicates security condition 'Always'.
7. Continue with the next procedure (see '2.5 Adding a Password File (EF_PWD)' on page 18).

2.5 Adding a Password File (EF_PWD)

About this Procedure

This procedure describes how to add an EF_PWD file to the DF level of the file structure. The EF_PWD file contains one password record.

For the password record, the following must be specified

– Password length
– Password value according to Format 2 PIN Block
– DES encryption

To create a reference value, the 8-byte Format 2 PIN Block is formed according to ISO PIN1 as described in the STARCOS reference manual.

How to Proceed

Edit | *New* | *EF PWD*

To add an EF_PWD file to the DF level of the card application:

1. In the tree pane, select the DF and then select *Edit* | *New* | *EF PWD*.
   ↳ An EF_PWD file is added to the DF level.
2. Select *EF_PWD*.
   ↳ The *FCP* tabbed panel is activated by default.
3. Under *Short File ID* of *Tag '88'* enter '*02*' as the value for the short ID and accept all other default settings of the *FCP* tab.
4. Select the *Content* tab and click *New*.
   ↳ Password record 1 is displayed in the activated *Record* tab.
5. Under *Password/PIN Length*, overwrite the existing value and enter 6 as the value for the password length.
6. Under *Reference Value*, enter '*26 12 34 56 FF FF FF FF*' as the reference value in Format 2 PIN Block for the password '12 34 56'.

   Byte '26' of the reference value indicates the format and length of the password. Filler bytes are indicated with 'FF'.
7. Activate *Automatically Encrypt Password/PIN* to encrypt the password reference value with itself using DES.
8. Continue with the next procedure (see '2.6 Adding a Password Description File (EF_PWDD)' on page 19).

2.6 Adding a Password Description File (EF_PWDD)

About this Procedure

This procedure describes how to add an EF_PWDD file to the DF level of the file structure.

The EF_PWDD file contains one record containing the following additional password information:

- Password reference
- Password storage format
- ARR
- Security Environment data objects with SE reference and transmission format

How to Proceed

Edit | *New* | *PWDD*

To add an EF_PWDD file to the DF level of the card application:

1. In the tree pane, select the DF and then select *Edit* | *New* | *EF PWDD*.
   ↳ An EF_PWDD file is added to the *DF* level.
2. Select *EF_PWDD*.
   ↳ The *FCP* tab is activated by default.
3. Under *Short File ID* of *Tag '88'*, enter '*03*' as the value for the short ID and accept all other defaults of the *FCP* tab.
4. Select the *Content* tab and click *New*.
   ↳ PWDD record 1 is displayed in the activated *Record* tab.
5. Click *Edit*.
   ↳ The *General* tab is displayed.
6. Under *Pwd ID* of *Password Reference (Tag '93')*, select *1* as the value for the password ID and accept the other default settings: Rec. #: '1', Access 'local' and Reference 'Local EF_PWD'.
7. From *Storage Format* of *Tag '89'*, select *'1160' PIN, 6 chars min, DES enc. format 2 PIN block*.
8. Under *Access Rule References (Tag 'A1')*, activate *Use* and then click *New*.
9. Under the *Record#* column, select 2 and accept the other defaults SE# 'All', Interface 'All', EF File ID 'Default '0030' and click *OK*.
10. Click *New SE Template* to specify the security environment data object.
    ↳ The *SE#*1 tab is displayed.
11. Under *SE Reference (Tag '80')*, activate *All SE*.
12. From *Transmission Format* of *Tag '89'*, select *'12' PIN, format 2 PIN block* and click *OK*.

↳ Record 1 displays the byte code ’93 02 01 01 89 02 11 60 A1 03 8B 01 02 7B 06 80 01 00 89 01 12’, indicating parameters selected.

13. Continue with the next procedure (see ’2.7 Adding a PIN Fault Presentation Counter File (EF_PFPC)’ on page 21).

2.7 Adding a PIN Fault Presentation Counter File (EF_PFPC)

About this Procedure

This procedure describes how to add an EF_PFPC file to the DF level of the file structure. The EF_PFPC file contains one PFPC record.

For the PFPC record, the initial value must be set to 3. If this value is exceeded, the password is blocked.

How to Proceed

Edit | *New* | *PFPC*

To add an EF_PFPC file to the DF level of the card application:

1. In the tree pane, select the DF and then select *Edit* | *New* | *EF_ PFPC*.
   ↳ An EF_PFPC file is added to the DF level.
2. Select *EF_PFPC*.
   ↳ The *FCP* tab is activated by default.
3. Under *Short File ID* of *Tag '88'*, enter '04' as the value for the short ID and accept all other default settings of the *FCP* tab.
4. Select the *Content* tab and click *New*.
   ↳ PFPC record 1 is displayed in the activated *Record* tab.
5. Under *Initial value*, accept 3 as the number of retries allowed.
   ↳ If this value is exceeded, the password is blocked.
6. Continue with the next procedure (see '2.8 Adding EF (0001)' on page 22).

2.8 Adding EF (0001)

About this Procedure

This procedure describes how to add an EF to the DF level of the file structure.

For the EF, the following must be specified:

– Data content must be entered
– The first access rule record of the EF_RULE file must be referenced, allowing the content of *EF (0001)* to be read/searched and updated after password verification.

How to Proceed

Edit | *New* | *EF*

To add an EF to the DF level of the card application:

1. In the tree pane, select the DF and then select *Edit* | *New* | *EF*.
   ↳ An EF is added to the DF level.
2. Select *EF (0000)*.
   ↳ The *FCP* tab is activated by default.
3. Under *File ID* of *Tag '83'*, enter '0001' as the value for the file ID, under *Short File ID* of *Tag '88'*, enter '05' as the value for the short ID and accept all other default settings of the *FCP* tab.
   ↳ *EF (0001)* is displayed in the tree pane instead of *EF(0000)*.
4. Select the *Content* tab and click *New*.
   ↳ Record 1 is displayed in the activated *Record* tab.
5. In the record grid, enter '*48 65 6C 6C 6F 20 57 6F 72 6C 64*' as hexadecimal value for 'Hello World'.
6. Select the *ARR File* tab, select *New* and accept the ARR defaults: SE# 'All', Interface 'All', EF File ID 'Default '0030', and Record# '1'.
7. Continue with the next procedure (see '2.9 Checking the Card Application' on page 23).

2.9 Checking the Card Application

About this Procedure

To avoid corrupted applications, the *Check Card* functionality can be used to validate the card application. Validation is automatically performed before downloading the card application.

Validation for the entire card or for selected files can also be explicitly initiated via the *Card* | *Check Card* menu.

If an error or warning occurs, the reason is reported in the message pane.

How to Proceed

Card | *Check Card*

Card | *Selected File*

To check either the entire card or a selected file:

1. Select either *Card* | *Check Card* or *Card* | *Selected File*.

   ↳ Error and warning messages are displayed in the message window. Warnings are indicated with an yellow exclamation point, whereas errors are indicated with a red exclamation point.

2. Continue with the next procedure (see ’2.10 Defining Download Settings’ on page 24).

2.10 Defining Download Settings

About this Procedure

Before downloading the card application to card or file, the required download settings must be defined.

This section describes the procedures for:

– Defining settings for downloading to card
– Defining settings for downloading to file

Defining Settings for Downloading to Card

Extras | *Options*

To define the settings for downloading to card:

1. Select *Extras* | *Options*.
   ↳ The *Options* window is displayed.
2. Deactivate *Run checks before download* if checks are not to be run before downloading to card.
3. Under *Card terminal type*, accept *COM1* or select another communications port to which the card terminal is connected.
4. Under *Slot number*, accept 1 as default value or enter the number of the slot if using a terminal with multiple slots.
5. Under *Access mode*, select either:
   5.a *Exclusive*
   ↳ STARMAG blocks the terminal for exclusive use.
   5.b *Shared*
   ↳ STARMAG shares the terminal with other programs (e.g., STARTEST). To use shared access mode, the terminal must support this function.
   5.c *Terminal Server Shared*
   ↳ STARMAG shares the terminal with other programs via the G&D PC/CTI terminal server. The terminal server is installed along with STARMAG.
6. If terminal commands are to be used, activate *Use terminal command* and select either:
   6.a *Automatic PPS configuration - OFF*
   ↳ Deactivates automatic protocol parameter selection of the terminal.
   6.b *Automatic PPS configuration - ON*
   ↳ Activates automatic protocol parameter selection of the terminal. The card terminal automatically switches to the T=1 protocol if smart card supports T=1 and sets the conversion factor to the smallest value supported by both the card terminal and the smart card.
   6.c *Manual PPS configuration*

↳ Activates manual Protocol Parameter Selection (PPS) of the terminal. The card terminal transmits a PPS command sequence. Under *PPS command*, enter the byte sequence.

7. Click *OK* to accept the changes in the *Options* window.
8. In the tree pane, select *Card Settings* and select the *Options* tab.
9. If the program is not to be interrupted whenever breaks or error occur, deactivate *Break on error* or *Show warnings*.
10. If the existing application is to be deleted using the *DELETE MF* command, set *Delete MF* to *Enabled* or *Prompt*.

    ↳ The *DELETE MF* command is executed before downloading. If the MF contains an ARR to *EF_RULE* with access mode 'DELETE FILE (self)' and security condition 'Always', the *DELETE MF* command deletes the existing application, causing the card to be reset to the delivery state.

11. To select the buffer size, perform either:

    11.a Activate *Auto detect*.

    ↳ Default setting. The maximum I/O buffer size is used which is specified by the terminal.

    11.b Deactivate *Auto detect* and under *I/O buffer size* manually enter the size.

    ↳ The maximum command length L_c is set. If, for example, the I/O buffer size comprises 112 bytes and if a transparent EF comprises 224 bytes, two successive *UPDATE BINARY* commands are used.

12. Continue with the next procedure (see '2.11 Downloading the Card Application' on page 27).

Defining Settings for Downloading to File

Card Settings | *Options tab*

To define the settings for downloading to file:

1. In the tree pane, select *Card Settings* and select the *Options* tab.

   ↳ The *Options* window is displayed.

2. Under *File format*, select either:

   2.a *Standard Line Break*

   ↳ Default setting. The CLA, INS, P1, P2 and L_c bytes are written in one line and the data is written in separate lines, 16 bytes per line.

   The following additional information is written to each command: File name, FID and command description; e.g.:

```
EF (0000) UPDATE BINARY Block #1:
00 D6 00 00 20
AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA
AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA
```

2.b *Standard*

↳ Writes commands to a *.txt file, where one command is written per line.

Each line begins with the prefix 'Command:' followed by the associated bytes; e.g.:

```
Command: 80 E0 00 00 17 01 02 03 04 05 06 07 08 00
...

Command: 00 D6 00 00 10 AA AA AA AA AA AA AA AA AA
...
```

3. Continue with the next procedure (see ’2.11 Downloading the Card Application’ on page 27).

2.11 Downloading the Card Application

About this Procedure

This section describes the procedures for:

– Downloading to card
Writes the command APDUs for creating the card application onto a STARCOS card inserted in the terminal

– Downloading to file
Writes the command APDUs into an ASCII file under the specified *.txt name

Downloading to Card

Card | *Download to Card*

To download the card application:

1. Define the required download settings in the *Options* window of the *Extras* | *Options* menu and *Card Settings* | *Options tab*.
2. Select *Card* | *Download to Card*.

If the card inserted in the terminal differs from the requested card, the program asks if the download is to be aborted.

If *DELETE MF* is set to either *Enabled* or *Prompt* under *Card Settings*, the *DELETE MF* command is executed as first command when downloading the application to card. The command is only successfully executed if the existing application allows the card to be reset to the delivery state.

↳ The complete application of the currently focussed document is downloaded onto the smart card. When downloading is complete, corresponding status information is displayed in the message pane.

3. Continue with the next procedure (see ’2.12 Creating an HTML Report’ on page 28).

Downloading to File

Card | *Download to File*

To download the application to file:

1. Define the required download settings in the *Options* window of the *Extras* | *Options* menu and *Card Settings* | *Options tab*.
2. Select *Card* | *Download to File*.
3. Enter a name for the download file (e.g., initialization.txt) and click *Save*.

↳ The complete application of the currently focussed document is downloaded into an ASCII file. When downloading is complete, corresponding status information is displayed in the message pane.

4. Continue with the next procedure (see ’2.12 Creating an HTML Report’ on page 28).

2.12 Creating an HTML Report

About this Procedure

This section describes the procedures for:

– Saving the HTML report
  Saves the report to the specified *.html file
– Printing the HTML report
  Prints the HTML report to the selected printer

The HTML report contains a detailed summary of all relevant card information. Either all information or selected information can be included in the report.

Saving the HTML Report

File | *HTML Report*

To save the HTML report:

1. Select *File* | *HTML Report*.
   ↳ The *HTML Report* window is displayed.
2. Depending on whether the entire card application or only a selection is to be included in the saved report, activate either:
   2.a *Export all* (default)
   ↳ Saves the entire card application, including all structures.
   2.b *Export selection:*
   ↳ Saves the items selected in the preview pane on the left side of the window. To select specific elements in the tree structure, click on the desired tree elements and simultaneously press the Ctrl key.
3. Click *OK* and enter the name of the report to be generated.
   ↳ The HTML report is saved to the specified *.html name under the selected folder.

Printing the HTML Report

File | *Print*

To print the HTML report:

1. Select *File* | *Print*.
   ↳ The *Print* window is displayed.
2. Depending on whether the entire card application or only a selection is to be included in the printed report, activate either:
   2.a *Export all* (default)
   ↳ Prints the entire card application, including all structures.
   2.b *Export selection*

↳ Prints the items selected in the preview pane. To select specific elements in the tree structure, click on the desired tree elements and simultaneously press the Ctrl key.

3. Click *Print*.
   ↳ The HTML report is printed.

Appendix

The appendix contains additional information provided for a better understanding of STARMAG, whereas the glossary and the index facilitate using the document.

Contents

A Validation Checks Performed via Check Card

Check Card Functionality

To avoid corrupted applications, the *Check Card* functionality can be used to validate the card application. Validation is automatically performed before downloading the card application or creating an EEPROM image.

Card checks can be explicitly run via the *Card* | *Check Card* menu. In the *Options* window of the *Extras* menu, *Run checks before download* can be activated or deactivated as desired.

Scope of Checks Performed

The validation procedure checks if the following conditions are satisfied:

- The AND template must contain at least two security conditions.
- At least one DF AID must exist and a maximum of 255 DF AIDs are allowed.
- At least one EF_RULE must exist per MF or DF level.
- The DF AID must be unique on the entire card.
- Either one ARR may be set for all security environments (SEs) or various ARRs may be set for different SEs.
- The OR template must contain at least two security conditions.
- The following FIDs are reserved: '3F 00', '00 10', '00 12', '00 13', '00 15', '00 16', ‘00 18’, ‘00 19’, '00 30', ’00 31’, ‘00 34’, ‘00 35’, ‘00 36’, ‘40 00’
- The data object of ARR DO must exist.
- The referenced record of the EF_RULE (file ID and record) must exist.
- Security conditions ’Always’ must appear alone or in an OR template.
- Security conditions ’Never’ must appear alone.
- Security conditions ’SPECs’ must appear alone or in an AND template.
- A unique file ID or short file ID must exist within a DF level.

B Reference Literature

ISO

ISO/IEC 7816-3
Information technology -- Identification cards -- Integrated circuit(s) cards with contacts -- Part 3: Electronic signals and transmission protocols
ISO/IEC, 1997

ISO/IEC 7816-4
Information technology -- Identification cards -- Integrated circuit(s) cards with contacts -- Part 4: Interindustry commands for interchange
ISO/IEC, 1995

Other

STARCOS 3.1 Reference Manual
Smart Card Operating System
G&D, ID No. 33016325, 06/2005

C Glossary

AID
: Application ID
An AID identifies an application in a smart card. It is defined in the ISO/IEC 7816-5 standard. A part of the AID can be registered nationally or internationally, in which case it is reserved for the registered application and is unique in the entire world. An AID consists of two data elements, the RID (registered identifier) and the PIX (proprietary identifier).

ARR
: Access Rule Reference

ARR-DO
: Access Rule Reference - Data Object

ASCII
: American Standard Code for Information Interchange
Data exchange format in which 256 characters can be represented; every character is represented by an integer from 0 to 127.

CInt-Studio
: CInt-Studio is a development environment for ANSI C/C++ programming. The programs developed using CInt-Studio are executed by an interpreter. For IFDSIM, it is used to create test scripts.

DES
: Data Encryption Standard
A standard cryptographic algorithm specified as DEA in ISO 873-1. An algorithm for symmetric cryptography. Now used as 'triple DES' in EMV operations (e.g., ARQC generation) where data is encrypted using the first half of a double length key, is decrypted using the second half, then re-encrypted using the first half again.

DF
: Dedicated File
A hierarchical structure element similar to a directory of a file-orientated smart card operating system. DFs contain access conditions and arbitrary EFs (Elementary Files) or other DFs. Depending on the program requirements, DFs may be selected via the FID (File ID), DF Name or AID (Application ID).

EEPROM
: Electrical Erasable Programmable Read-Only Memory

EF
: Elementary File
EFs represent the actual data storage in the file tree of a smart card. EFs contain one of the following internal file structures: Transparent, Linear Fixed, Linear Variable or Cyclic.

FCP
: File Control Parameter

FID
: File ID
A unique file identifier (2 bytes) as the characteristic of a file (each MF, DF and EF have a FID). Provides individual selection of every application. Each file in the card is addressed by either an FID or an AID (Application Identifier).The first byte identifies the type of file in ac-

cordance with the standards ISO/IEC 7816-4, 3GPP 51.011 and EN 726-3: '3F00' = MF, '7F' = first-level DF, '5F' = second-level DF, '2F' = EF under the MF, '6F' = EF under a first-level DF, '4F' = EF under second-level DF

HTML
: HyperText Markup Language
A set of tags and rules used to create hypertext documents that can be viewed with a browser.

MF
: Master File
Root directory implicitly selected by the operating system after resetting the smart card. The MF is a unique file containing access conditions and, optionally, DFs (Dedicated Files) and EFs (Elementary Files). The MF is always assigned the FID (File ID) '3F00'.

PC/CTI
: PC / Card Terminal Interface
G&D driver library for the development of smart card applications.

PFPC
: PIN Fault Presentation Counter

PPS
: Protocol Parameter Select
Refers to the Protocol Type Selection (PTS) in accordance with ISO/IEC 7816-3.

SE
: Security Environment
Security environment for referring to data objects.

smart card
: Strictly speaking, the expression 'Smart Card' is an alternative name for a microprocessor card, in that it refers to a chip card that is 'smart'. Memory cards thus do not properly fall into the category of Smart Cards. However, the expression 'Smart Card' is generally used in English-speaking countries to refer to all types of chip cards.

STARCOS
: Smart Card Chip Card Operating System
Forms the basis of multifunctional smart card applications. STARCOS enables the implementation of various applications (e.g., electronic purse, access control to data networks, and digital signatures).Smart card operating systems control the data transfer, the storage areas, and process information; they manage the resources and supply all necessary functions for the operation and administration of a random number of applications.

T=1 protocol
: Block-orientated communication protocol.

Index

V