



# Card ADMIN

Getting Started

All information herein is either public information or is the property of and owned solely by Gemalto NV. and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto's information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

**Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.**

**Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.**

© Copyright 2011 Gemalto N.V. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto N.V. and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

GEMALTO, B.P. 100, 13881 GEMENOS CEDEX, FRANCE.

Tel: +33 (0)4.42.36.50.00 Fax: +33 (0)4.42.36.50.90

Printed in France.

Document Reference: D1225357A

June 2, 2011

<b>Preface</b>		<b>xi</b>
	How This Book Is Organized . . . . .	xi
	Audience . . . . .	xii
	Prerequisites . . . . .	xii
	For Further Help . . . . .	xii
	If You Find an Error . . . . .	xii
<b>Chapter 1</b>	<b>Installing Card ADMIN</b>	<b>1</b>
	Hardware and Software Requirements . . . . .	1
	Hardware Requirements . . . . .	1
	Software Requirements . . . . .	2
	Installing Card ADMIN . . . . .	3
	Product Licensing . . . . .	4
<b>Chapter 2</b>	<b>Features of Card ADMIN</b>	<b>5</b>
	Modular Structure . . . . .	5
	Latest Card ADMIN Features . . . . .	6
	Using GemXplorer . . . . .	7
	Starting Card ADMIN . . . . .	7
	Menu Bar . . . . .	9
	Configuring Card ADMIN . . . . .	11
	Media Management . . . . .	12
	Types of Media Supported . . . . .	12
	Using a Card Reader with Card ADMIN . . . . .	13
	Installing a Card Reader . . . . .	13
	Troubleshooting a Card Reader . . . . .	13
	Card Image Files . . . . .	14
<b>Chapter 3</b>	<b>Key Features of Card Management</b>	<b>15</b>
	Reading a Card . . . . .	15
	Cards Supported by Card ADMIN . . . . .	15
	Card Boot Selection . . . . .	15
	Card Typing Functionality . . . . .	17
	Managing the ATR . . . . .	22
	Model Editor . . . . .	23
	Managing Card Data . . . . .	26
	Viewing the File Structure of a Card . . . . .	26
	Secret Code Management . . . . .	28
	Viewing the Contents of a Specific File . . . . .	30
	Viewing File Properties . . . . .	31
	Generating a Content Report . . . . .	32
	Generating Content Report for Applications . . . . .	36
	Viewing a Content Report . . . . .	36
	Converting a Content Report to XPI Format . . . . .	37
	Generating a Comparison Report . . . . .	37
	Generating a Comparison Report for Applications . . . . .	39
	Viewing a Comparison Report . . . . .	40

	Printing Reports . . . . .	40
	Checking Standard Compliance . . . . .	40
	Working with Card Image Files . . . . .	41
	Adding Files to a Card Image File . . . . .	41
	Viewing the Structure of a Card Image File . . . . .	41
	Editing Files on a Card Image File . . . . .	41
	Editing Card Image File Properties . . . . .	41
	Viewing the File Contents of a Card Image File . . . . .	42
	Using Variables in Card Image Files . . . . .	43
	Saving Card Image Files to Disk . . . . .	44
	Importing Card Image Files . . . . .	44
	Copying Data Between Cards and Card Image Files . . . . .	44
	File Copying Rules . . . . .	45
	Copying Files . . . . .	45
	Communicating with the Card . . . . .	47
	Sending Commands via the High-level Interface . . . . .	47
	Sending Commands via the Intermediate-level Interface . . . . .	47
	APDU Exchange . . . . .	48
	Using the ATF Trace Mode to Record Commands . . . . .	49
<b>Chapter 4</b>	<b>Working in the SIM Mode</b>	<b>53</b>
	Selecting the SIM applet . . . . .	53
	Browsing GSM File Systems . . . . .	54
	Communicating with the Card . . . . .	55
	GSM Commands . . . . .	55
	Secret Code Management Commands . . . . .	55
	File Selection Command . . . . .	55
	File Management Commands . . . . .	56
	GSM Authentication . . . . .	57
	Put Ki . . . . .	58
<b>Chapter 5</b>	<b>Working in the 3G Application Mode</b>	<b>59</b>
	Selecting the 3G Application . . . . .	59
	Working with USIM applications . . . . .	60
	USIM Sessions on 3G Cards . . . . .	60
	USIM Session Management in GemXplorer . . . . .	61
	Default ADF Activation . . . . .	61
	3G Commands . . . . .	62
	Secret Code Management Commands . . . . .	62
	File Management Commands . . . . .	63
	File Selection Command . . . . .	64
	3G Authentication . . . . .	65
	GBA Authentication in Bootstrapping Mode . . . . .	71
	GBA Authentication in NAF Derivation Mode . . . . .	73
	VGCS/VBS Authentication . . . . .	75
	MSK Update ( LTKM Authentication) . . . . .	78
	MTK Generation (STKM Authentication) . . . . .	81
	MUK/MSK Key Deletion . . . . .	83
	Authentication Related Files . . . . .	84
	Voice Broadcast Service Ciphering Algorithm (VBSCA) . . . . .	84
	Voice Group Call Service Ciphering Algorithm (VGCSCA) . . . . .	84
	GBA Bootstrapping Parameters (GBABP) . . . . .	84
	GBA Network Application Function List (GBANL) . . . . .	84
	Phone Book Management . . . . .	85

Phone Book Files	85
Other Phone Book Related Files	94
File Linking	95
Constructed and Primitive Tags	95
Linking by Record	97
Linking by Index	97
Linking by TLV	99
Phone Book Procedures	100
Initialization	100
Creation and Deletion of Information	100
Hidden Phone Book Entries	100
Phone Book Interpreter	101
How to Create a Phone Book	103
Using the Phone Book Interpreter to Manage Phone Book Entries	103
3G Phone Book Interpreter	105
ISIM Management	108
IMS Authentication and Key Agreement (AKA) Context	108
IMS AKA Authentication in ISIM	109
Generic Bootstrapping Architecture Security Context	111
ISIM Files	111
EAP Management	116
EAP Authentication Using EAP-SIM Method	116
EAP Authentication Using EAP-AKA Method	119
EAP Files	121
<b>Chapter 6 Working in the Card Manager Mode</b>	<b>127</b>
Selecting the Card Manager Applet	128
The Card Settings File	129
Getting Card Manager Properties	131
Card Manager Commands	132
Managing Key Sets	133
Using the Application Manager	135
Introduction	135
Overview of Defining and Running an Application	135
Starting the Application Manager	136
The Application Manager Window	137
<b>Chapter 7 Working in the SCWS Mode</b>	<b>139</b>
Selecting the SCWS Application	139
Working with SCWS application	140
Browsing SCWS File Systems	140
Configuring SCWS	140
SCWS Management in GemXplorer	141
SCWS Commands	142
<b>Chapter 8 Working In the CDMA Application Mode</b>	<b>145</b>
Selecting the CDMA Application	145
CDMA Commands	146
Authentication Management Commands	146
Secret Code Management Commands	146
File and Application Management Commands	147
EF Management Commands	147
OTAPA/OTASP Commands	148

Overview of CDMA Security Mechanisms . . . . .	149
CDMA Authentication Procedure . . . . .	149
Authentication Management Commands . . . . .	150
Authentication . . . . .	150
Base Station Authentication . . . . .	152
Mobile Station Authentication . . . . .	153
Voice Privacy Mask . . . . .	155
Store ESN_ME . . . . .	157
Store MEID . . . . .	157
HRPD Access Authentication . . . . .	159
SimpleIP Authentication . . . . .	160
MobileIP Authentication . . . . .	161
CDMA OTAF Simulator . . . . .	164
OTA Concepts . . . . .	164
Creating a New User with Database Values . . . . .	165
OTA Processing: Retrieving IMSI_T . . . . .	167
 <b>Chapter 9    Wireless Application Protocol (WAP) Content Provisioning</b>	 <b>171</b>
WAP Content Provisioning . . . . .	171
WAP Content Provisioning Creation Wizard . . . . .	173
 <b>Appendix A    Test Card Specifications</b>	 <b>175</b>
 <b>Appendix B    BER-TLV Files</b>	 <b>177</b>
Generic Behavior of BER-TLV Viewer . . . . .	177
Relationship between EFMMML (Multimedia Message List) and EFMMDF (Multimedia Data File) . . . . .	178

## List of Tables

Table 1 - Menu Bar Commands and Sub-menus .....	9
Table 2 - Primitive Tag Values .....	96
Table 3 - Phone Book Linking Capabilities .....	96
Table 4 - Binary Data After Tag A9 in EFPBR .....	98
Table 5 - Binary Data for 1 Record in EFIAP .....	99
Table 6 - Record Pointers in Files Linked by TLV .....	99
Table 7 - Menu Bar Commands and Sub-menus of 3G Phonebook Manager ....	106
Table 8 - Code Values of Sample Card in Card ADMIN Kit .....	175

## List of Figures

Figure 1 - Starting Card ADMIN	7
Figure 2 - GemXplorer Details View	8
Figure 3 - Menu Bar	9
Figure 4 - Examples of Selecting the Mode to Work	16
Figure 5 - The Card Typing Window	18
Figure 6 - The New Card Type Window	19
Figure 7 - ATR Manager	22
Figure 8 - Model Editor	24
Figure 9 - Scanning the Card Contents	26
Figure 10 - The GemXplorer Main Window	26
Figure 11 - Examples of Secret Code Management	28
Figure 12 - Verify Key	30
Figure 13 - Interpreted File View	31
Figure 14 - Binary File View	31
Figure 15 - File Viewer Window for a Transparent File	32
Figure 16 - Generating a Content Report — Gemalto Cards	33
Figure 17 - Generate Content Report — Non-Gemalto Cards	34
Figure 18 - Generate Content Report for Applications	36
Figure 19 - Converting Content Report to XPI Format	37
Figure 20 - Generating a Comparison Report for 2G Card	38
Figure 21 - Generating a Comparison Report for Applications	39
Figure 22 - Check Standard Compliance	40
Figure 23 - An Update Window	42
Figure 24 - The Variables Property Sheet	43
Figure 25 - Importing Card Image File	44
Figure 26 - The Copy Process Window	45
Figure 27 - Examples of Exchange APDU	48
Figure 28 - The Record ATF Window	49
Figure 29 - The Replay ATF Script Window	50
Figure 30 - Examples of Selecting SIM Mode	54
Figure 31 - Put Ki in GSM Context	58
Figure 32 - Examples of Selecting USIM Mode	59
Figure 33 - Put Ki in 3G Context	70
Figure 34 - Phone Book Reference File (PBR)	86
Figure 35 - Abbreviated Dialing Numbers (ADN)	87
Figure 36 - Extension 1 (EXT1)	88
Figure 37 - Index Administration Phone Book (IAP)	88
Figure 38 - Second Name Entry (SNE)	89
Figure 39 - Additional Number (ANR)	90
Figure 40 - Additional Number (AAS)	91
Figure 41 - Grouping File (GRP)	91
Figure 42 - Grouping Information Alpha String File (GAS)	92
Figure 43 - Email Address File (EMAIL)	92
Figure 44 - Capability Configuration Parameters 1 File (CCP1)	93
Figure 45 - Unique Identifier File (UID)	93
Figure 46 - Phone Book Control File (PBC)	94
Figure 47 - Relationship of EFADN Entries to EFIAF Record Pointers	98
Figure 48 - Phone Book Settings	101
Figure 49 - Phone Book Interpreter	102
Figure 50 - Phone Book Reference File (PBR)	103



Figure 51 - 3G Phonebook Interpreter Details View . . . . .	106
Figure 52 - 3G Phonebook Interpreter Menu Bar . . . . .	106
Figure 53 - IP Multimedia Subsystem Private User Identity (IMPI) . . . . .	112
Figure 54 - Home Network Domain Name (Domain) . . . . .	112
Figure 55 - IMS Public User Identity (IMPU) . . . . .	113
Figure 56 - Administrative Data (AD) . . . . .	113
Figure 57 - ISIM Access Rule Reference (ARR) . . . . .	114
Figure 58 - ISIM Service Table (IST) . . . . .	114
Figure 59 - Proxy Call Session Control Function (PCSCF) . . . . .	115
Figure 60 - GBA Bootstrapping Parameters (GBABP) . . . . .	115
Figure 61 - GBA Network Application Function List (GBANL) . . . . .	116
Figure 62 - EFEAP DERIVED KEY . . . . .	122
Figure 63 - EFEAP AUTHENTICATION STATUS . . . . .	122
Figure 64 - EFEAP PERMANENT USER IDENTITY . . . . .	123
Figure 65 - EFPSEUDONYM . . . . .	123
Figure 66 - EFPSEUDONYM . . . . .	124
Figure 67 - EFUPLMNWLAN . . . . .	124
Figure 68 - EFUWSIDL . . . . .	125
Figure 69 - EFWRI . . . . .	125
Figure 70 - Examples of Select Mode — Java Card . . . . .	128
Figure 71 - The File Selection Window. . . . .	130
Figure 72 - The Card Manager Properties Window . . . . .	131
Figure 73 - An Example of Key Management . . . . .	133
Figure 74 - Starting the Application Manager . . . . .	136
Figure 75 - The Application Manager Main Window . . . . .	137
Figure 76 - Selecting SCWS Mode. . . . .	139
Figure 77 - Selecting the CDMA Mode. . . . .	145
Figure 78 - Base Station Authentication. . . . .	152
Figure 79 - MSRT Authentication . . . . .	153
Figure 80 - MSO Authentication . . . . .	154
Figure 81 - MSUC Authentication. . . . .	155
Figure 82 - Key VPM Authentication . . . . .	156
Figure 83 - Store ESN_ME Parameter Window . . . . .	157
Figure 84 - Store_MEID Parameter Window . . . . .	158
Figure 85 - HRPD Parameter Window . . . . .	159
Figure 86 - SimpleIP Parameter Window . . . . .	160
Figure 87 - MobileIP (MN-HA Tab) Authentication Parameter Window . . . . .	161
Figure 88 - MobileIP (MIP-RRQ Hash Tab) Authentication Parameter Window . . .	<b>162</b>
Figure 89 - MobileIP (MN-AAA Tab) Authentication Parameter Window . . . . .	162
Figure 90 - OTASP/OTAPA Features Window. . . . .	166
Figure 91 - OTA Parameters Window . . . . .	167
Figure 92 - Processing Request List . . . . .	168
Figure 93 - Setting Up Secure Mode . . . . .	169
Figure 94 - Secure Mode Parameters Window . . . . .	169
Figure 95 - Configuration Request Parameters . . . . .	170
Figure 96 - DF PKCS#15 Directory in 2G Mode . . . . .	172
Figure 97 - PKCS#15 Directory in 3G Mode . . . . .	172
Figure 98 - Generic Behavior of BER-TLV Viewer . . . . .	177
Figure 99 - Relationship Between EFMMML and EFMMDF . . . . .	178



This document helps you learn about Card ADMIN (comprises Card ADMIN for 2G and 3G) which addresses the card administration needs of an OP, 2G and 3G card. Step by step, you perform first basic then more advanced tasks using Card ADMIN. These tasks include:

- Installing Card ADMIN
- Using GemXplorer to explore and manage the contents of a card
- Working in the Card Manager (Open Platform) mode
- Working in the GSM Application (SIM) mode
- Working in the 3G Application (USIM) mode
- Working in the C-CAT (CDMA Card Application Toolkit) Application (CDMA) mode
- Working in the Smart Card Web Server Application (SCWS) mode

## How This Book Is Organized

Chapters 1 to 3 describe the common features which are available when you are working in the Card Manager, GSM or 3G Application modes. The features and tasks specific to the respective modes can be found in chapter 4 onwards.

The dialog boxes for your card may differ from those depicted in this document. You may refer to the Help button in the respective command window for more information.

## Audience

This document is intended for:

- SIM card administrators. These people typically have an in-depth knowledge of the SIM card from a 3GPP TS 31.102 point of view, and are mainly interested in managing the contents of cards such as checking personalization.
- Technical marketing people. These people frequently need to personalize the content of a SIM card's file system, and to rapidly prototype SIM Toolkit applications.
- People involved in mobile testing.

## Prerequisites

This document assumes that you are familiar with the operating systems and with Java Card, Open Platform (OP), 3GPP Specifications and Global Systems for Mobile Communications (GSM) specifications.

## For Further Help

Further help is provided in the Gemalto Self Support portal at [support.gemalto.com](http://support.gemalto.com).

You can find information on how to contact your Gemalto representative by clicking **Contact Us** at the Gemalto web site, [www.gemalto.com](http://www.gemalto.com).

## If You Find an Error

Gemalto makes every effort to prevent errors in its documentation. However, if you discover any errors or inaccuracies in this document, please inform your Gemalto representative. Please quote the document reference number found at the bottom of the legal notice on the inside front cover.

# Installing Card ADMIN

To install Card ADMIN, insert the Card ADMIN CD-ROM into your computer's CD drive. Double-click the CD icon, and then follow the on-screen instructions.

After the installation, you will be prompted to activate your copy of the product (see "Product Licensing" on page 4).

## Hardware and Software Requirements

### Hardware Requirements

The following hardware is required to install and use Card ADMIN:

- A workstation with:
  - Intel® Pentium® 4 processor, 2.0 GHz or faster.
  - A minimum of 1 GB of RAM (2 GB is recommended).
  - 1150 MB of available disk space, including 400 MB required in the system disk for default ProgramFiles directory.
  - Minimum screen resolution of 1024 x 768 on a 4:3 display, and 1280 x 800 on a 16:9 (widescreen) display.
  - A CD-ROM drive (optional).
  - One free USB port.
- PC/SC-compatible card reader (such as PCTwin).

## Software Requirements

### Operating System

Card ADMIN runs under any of the following:

- Microsoft® Windows XP (with Service Pack 2).
- Microsoft Windows® 2000 (with Service Pack 4).
- Microsoft® Windows Vista.
- Microsoft® Windows 7.

### Other Software

The following software is also required:

- Microsoft XML Parser version 6 (with Service Pack 1).
- Microsoft Internet Explorer 6 or Microsoft Internet Explorer 7.0.
- Adobe® Acrobat® Reader 5.0 or later (to read PDF files).

# Installing Card ADMIN

---

**Important:**

An installation of Card Admin 2.X will automatically uninstall the previous versions of Card Admin (such as, versions 1.7 or 2.0). However, you will have to uninstall the product manually if an older version of Card Admin (version 1.6 and below), GemXplore Admin or GemXplore CASE had been installed previously.

Please be reminded that you will need to renew the licence for an upgrade of Card Admin over an existing installation. Please refer to "Product Licensing" for the renewal procedure.

---

**To install Card ADMIN:**

- 1 Configure your display settings to be at least 1024 by 768 pixels on a 4:3 display, and 1280 x 800 on a 16:9 (widescreen) display.
  - 2 Log in with an account that has Administrator rights on your computer.
  - 3 Ensure that the directory into which you are installing the product is in Read/Write mode.
  - 4 Insert the Card ADMIN CD-ROM. The installation program starts automatically.
  - 5 Launch the setup extractor.
  - 6 Click on "Setup" button to install Card Admin.
  - 7 Follow the on-screen instructions for installation.
  - 8 The setup will install the prerequisite Microsoft XML Parser 6.0 if the program is not found in your computer.
- 

**Note:** Do not relaunch the installation during the file extraction process. Please wait patiently.

---

- 9 The installation automatically installs the 2G, 3G, CDMA, Advanced Multimedia and Phonebook Manager application.
- 10 At the end of the Card Admin installation Gemalto Live Update will be installed.

## Product Licensing

You will be prompted to request a licence of the Card ADMIN the first time you start Card ADMIN.

- **Trial**  
This is a 20-day tryout licence effective from the day of the installation.
- **Temporary**  
This is a time bound licence with expiry date which allows you to use the product up to a specified time.

If you are working with a trial licence or an expired licence, the License Key Manager window will display the expiry date and status of the licence when Card Admin is launched.

---

**Note:** When the license you are using has expired, you will not be able to use Card Admin.

---

### To request a licence:

- Check with your Gemalto representative person regarding any issues with the licensing of Card Admin.

To continue using Card Admin, you may need to request for a new licence or to renew the licence after upgrade.

- 1 Launch Card Admin.
- 2 Click on **Help** and then **License Management**.
- 3 In the License Key Manager dialog, click on **Export Profile**.
- 4 Fill in the form.

---

**Note:** The Product Profile field should be filled with the location where you want to save your licence request file.

---

- 5 Click on **Save and Send**, it will open the default e-mail which enable the client to send the licence request file to `tools_licensing@gemalto.com`, then click **Send**.
- 6 Your licence file will be sent to you by email. Download this licence email and save it on your machine.
- 7 Return to License Key Manager dialog, and click **Import License**. A file browser will appear, choose the Licence file that has been sent to you.
- 8 Now your Card Admin has been licensed.



# Features of Card ADMIN

This section introduces the structure of the Card ADMIN software and also highlights some of the latest features.

## Modular Structure

The Card ADMIN product offers telecom operators and handset manufacturers structured and easy-to-use products to meet their needs in the card administration of 2G, 3G, CDMA cards. Applet development, simulation and deployment are possible via the Developer Suite and Simulation Suite products.

**Card ADMIN for 2G** is the basic feature which telecom operators and handset manufacturers need in order to browse, edit, authenticate and download applications to any 2G (SIM) card.

**Card ADMIN for 3G** addresses the 3G card administration needs such as browsing and editing the contents of 3G cards. Additionally, this provides an interpretation of the 3G phone book.

**Card ADMIN for CDMA** addresses the CDMA card administration needs such as browsing and editing the contents of Gemalto's CDMA cards.

**SCWS feature** addresses the Smart Card Web Server administration needs such as browsing and contents management.

## Latest Card ADMIN Features

The Card ADMIN smart card administration module called GemXplorer supports all the latest evolutions in Gemalto and Java Card based smart card technology including:

- Support for Gemalto's latest product family cards.  
These cards provide full support for the Java Card 2.1.1, OP 2.0.1, 3GPP TS 31.102, 3GPP TS 31.103, 3GPP TS 31.111, ETSI 102.221 specifications, allowing them to be deployed in a wide range of business, financial, multimedia and mobile telephony environments.
- Support for 3GPP/GSM standards compliance check. A feature which enables a card's content to be compared with that of the standards.
- Support for IP Multimedia Services Identity Module (ISIM) application according to 3GPP TS 31.103 standard.
- Support for PPS=97h communication between a card and reader.
- Support for Extensible Authentication Protocol methods in 3G mode.
- Support for License Key Manager for product licensing control.
- Support for Security Channel Protocol '02' according to GlobalPlatform Card Specification 2.1.1.
- Support for Smart Card Web Server (SCWS). A web server which resides on the card that allows service providers to extend their multimedia services via the hypertext transfer protocol (HTTP).
- Support for multi-profile management. A feature which enables the association of a card to multiple card types.
- Support for grouping the associated custom card types together.
- Support for PC/SC readers selection in Card ADMIN's configuration.
- Support for 3G IP authentication — High Rate Packet Data (HRPD), SimpleIP and MobileIP.
- Support for 3G Phonebook Interpreter in GUI environment.
- Support for service and content protection for Mobile TV broadcasting service with OMA BCAST Smart Card Profile (SCP).
- Enhancement to EF<sub>TOKEN</sub> INFO and Certificate Directory File (CDF) under the PKCS#15 directory.
- Support for Gemalto Smart Dongle as a PCSC device to browse UICC file system and applets.
- Support for protocol switching from ISO to IC-USB.
- CSIM C.S0065-A V1.0 Support: Interpretation of files, Authentication (AKA, CAVE, Packet Data: SIP, MIP, HRPD), STORE\_ESN\_ME, Updating RUIMID, and Standard compliance check.
- Browsing LTE files under DF HNB and DF MMSS.
- Support for Microsoft® Windows 7 (32bit / 64bit).

## Using GemXplorer

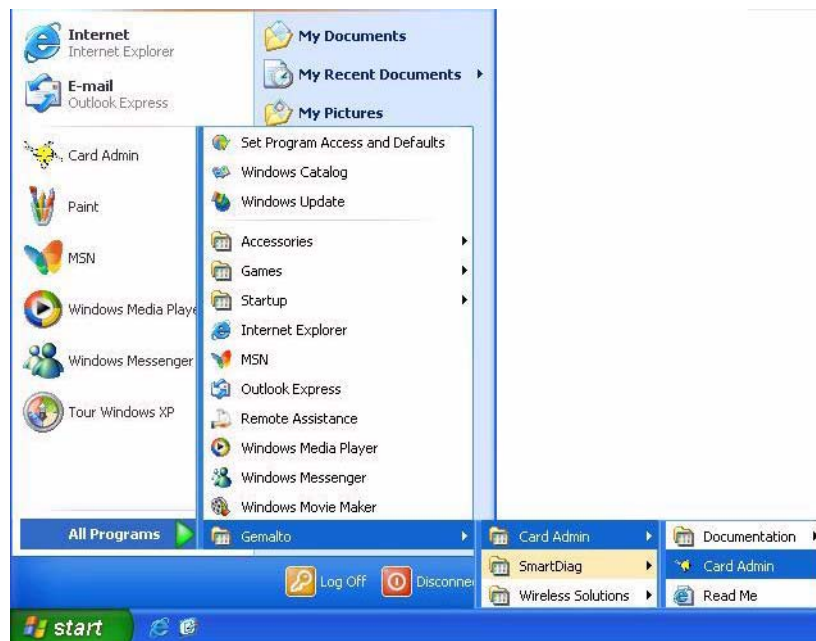
GemXplorer is Card ADMIN's smart card administration module. It provides a graphical interface for you to do the following:

- Browse a card's file system using GemXplorer's tree-like display.
- View a card's file system from the large icons, small icons or list view.
- Display the contents of data files in either an easy-to-read interpreted view or a binary representation.
- Issue commands to applications from easy-to-use command windows. Commands are selected from context-sensitive menus that only display commands valid for the selected application type.
- Display the various types of business application installed on the card, including system-internal applications and custom OP and SIM Toolkit applications.
- Record and replay actions and results using the trace scripting tool.

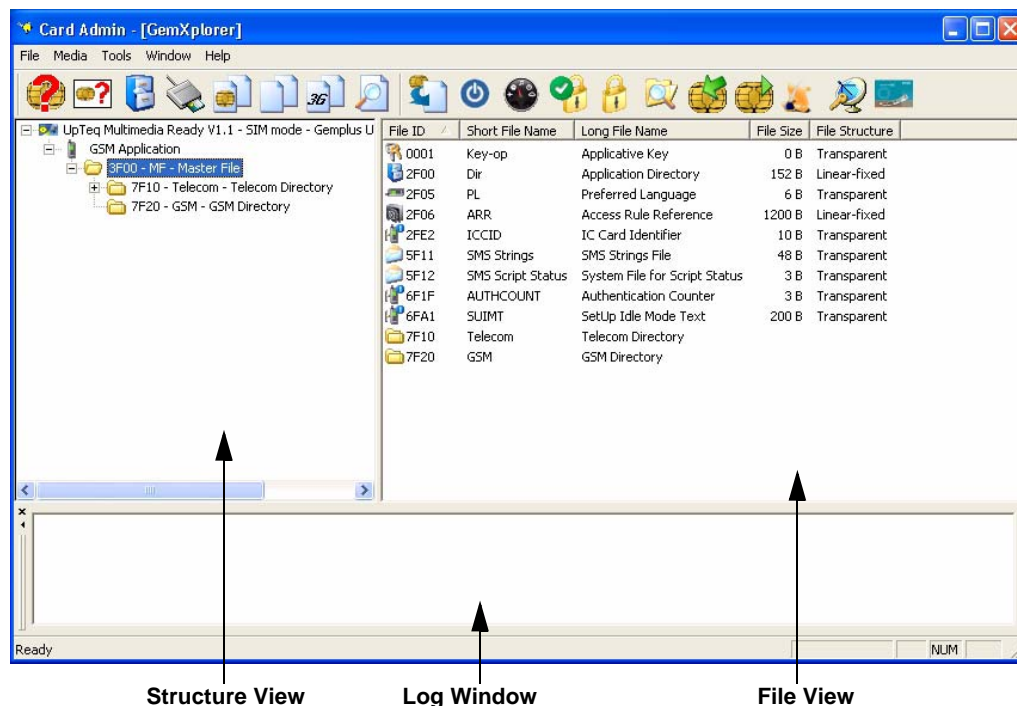
## Starting Card ADMIN

Start Card ADMIN by choosing **Start > Programs > Gemalto > CardAdmin> CardAdmin**.

**Figure 1 - Starting Card ADMIN**



The layout of the standard Card ADMIN interface is shown in the following figure.

**Figure 2 - GemXplorer Details View**

**Note:** You must insert a card in the card reader or select a card image file before anything is displayed in GemXplorer.

If the card is unknown, select a type for the card. See “Card Typing Functionality” on page 17 for details.

The default view is the **Details** view. You can also choose to view the GemXplorer interface in the large icons, small icons or list view. To change the view, select **Window** on the menu bar and click the preferred view.

## Menu Bar

The GemXplorer menu bar contains sub-menus which you use to carry out the various tasks.

**Note:** Tool icons are available as shortcuts keys for some sub-menus to make access easy.

**Figure 3 - Menu Bar**



A summary of the sub-menus is shown in the following “Table 1”.

**Table 1 - Menu Bar Commands and Sub-menus**

Main Menu	Sub-menus	Description
File	Exit	Quit Card ADMIN
Media	Media Management...	Define the type of media — real cards or card image files — for use
	External Tools > Calculator	Launch the calculator
	External Tools > Text Editor	Launch the notepad
	Imports...	Import a “.gxp” card image file used in GemXplore CASE 2.x and convert it to “.gxc”
	Application Download > 2G	Launch the 2G Application Manager tool
	Application Download > 3G	Launch the 3G Application Manager tool
Tools	Card Profile Management > Check Standard Compliance	Launch the check standard compliance viewer
	Card Profile Management > Convert Content Report to XPI	Generate the content report in XPI format.
	Card Profile Management > Generate Comparison Report for 2G...	Generate the comparison report which compares two content reports
	Card Profile Management > Generate Comparison Report for 3G...	Generate the comparison report which compares two content reports
	Card Profile Management > Generate Comparison Report for Application...	Generate the comparison report which compares the properties of two applications

**Table 1 - Menu Bar Commands and Sub-menus (continued)**

Main Menu	Sub-menus	Description
Tools (continued)	Card Profile Management > View Comparison Report...	Display the comparison report
	Card Profile Management > View Content Report...	Display the content report
	Card Settings Management	Manage the card settings file data
	Card Type Management > AID Manager...	Manage how application identifiers (AIDs) or ranges of AIDs are recognized in GemXplorer
	Card Type Management > ATR Manager...	How ATRs are associated with card types for card recognition purposes
	Card Type Management > Card Typing...	Manage the card type list
	Options	Options to configure Card ADMIN
	OTAF Simulator	Launch the OTAF simulation tool if the card is in the CDMA mode.
Window	Phonebook Manager	Launch the Phonebook Manager.
	Status Bar	Show/Hide the status bar
	Log Window	Show/Hide the log window
	Large Icons	Display files in a large graphical representation
	Small Icons	Display files in a small graphical representation
	List	Display files by their IDs
	Details	Display files by details — file ID, short file name, long file name, file size, file structure
Help	Help Card Admin	Display the Card ADMIN online help
	Tutorials	A guide to the features of Card ADMIN
	License Agreement	Display information about the licence.
	About Card Admin	Display information about Card ADMIN

## Configuring Card ADMIN

The **Options** window allows you to configure the Card ADMIN program. The values of the options are stored in the “.ini” or “.card” files.

To access this window, click **Tools** on the menu bar and select **Options**. The **Options** window with seven tabs: **Workspace**, **Telecom Configuration**, **2G Scan Configuration**, **2G PIN Configuration**, **3G Scan Configuration**, **3G PIN Configuration**, **Out Grammar** and **Reader Selection** are displayed.

### Workspace

This tab allows you to set and modify default paths to store user defined data. You can also add or remove the external tools such as the Text Editor and Calculator from Tools in the menu bar.

Additionally, you can set for “Insert Item in Mapping” and “Delete Item in Mapping File” to be automatically selected in the **Create** and **Delete** windows respectively. When this feature is selected in the Create window, the file you are creating is added to the card mapping file so that the next time the card is inserted, the file is automatically scanned and listed in GemXplorer. And vice-versa in the Delete window.

### Telecom Configuration

This tab allows you to add, update or remove the PLMN (Public Land Mobile Network) codes such as the mobile country code, mobile network code and the name of the operator. Additionally, you can add, update or remove the list of service names in the SST (SIM Service Table). The updates done here will also be updated in other file viewers such as EFMSI (which includes the PLMN code) and EFSST (which contains the list of services).

### 2G Scan Configuration

This tab enables you to define the range of DFs and EFs which will be used in scanning non-Gemalto cards.

You can also choose to enable or disable the check for default GSM model files whenever a SIM application is selected. If this is enabled, Card ADMIN will check if all the files specified in the default GSM card model are physically present on the card that is being read. After the check, only the files present on the card will be displayed. If this is disabled, Card ADMIN will simply display all the files specified in the default model.

Additionally, you can choose to enable or disable the option for GemXplorer to be automatically refreshed after a card warm reset. That is, after a card warm reset, the Java Card applications are re-scanned and displayed in GemXplorer.

### 2G PIN Configuration

This tab allows you to configure the secret codes (PIN) values and store them in the “.card” file so that the values are automatically presented when you select the **Verify All PINs** function. The secret codes which can be configured include CHVs and ADMs. For the predefined CHV codes, you can enter the code value in the Hex or ASCII mode.

**Custom Command** is used to configure non-Gemalto, proprietary APDUs in order to verify CHV and ADM. See the online help for details.

### 3G Scan Configuration

This tab allows you to define the range of DFs and EFs which will be used in scanning non-Gemalto cards. You can also choose to enable or disable the check for default 3G model files whenever a USIM application is selected.

### 3G PIN Configuration

This tab allows you to configure the secret codes (LPIN, GPIN, UPIN, ADM) values and store them in the ".card" file so that the values are automatically presented when you select the **Verify All PINs** function. The secret codes which can be configured, include Local PIN (LPIN), Global PIN (GPIN), Universal PIN (UPIN) and ADMs. For the predefined LPIN, GPIN, UPIN codes, you can enter the code value in the Hex or ASCII mode. For ADMs, you can enter the code name and the value of the corresponding command.

### Out Grammar

The Gemalto production file (\*.out) is a text file that stores a card's diversified data such as PIN codes and key values, based on the card's ICCID (IC Card Identifier). The data in the \*.out file, for example the Kic and Kid values, are retrieved and used during the setting up of a secure session with the Card Manager. Additionally, the secret codes values stored in the \*.out file are retrieved and displayed for your convenience when you are prompted for secret code verification. An \*.out file is associated with a card type.

The grammar file (\*.ogr) is used to manage the \*.out file. This window allows you to create or modify different grammar files for different card types. Alternatively, a grammar file can be re-used for several card types.

### Reader Selection

This tab displays the PC/SC smart card readers that have been used by Card ADMIN and identifies the status of the readers that are connected to your PC. While running Card ADMIN, you can choose to select the readers you require, start using readers that are connected to the PC or remove the readers which you wish to remove from the reader list.

---

**Note:** During a Card ADMIN session, you can only delete readers from the reader list if they are not connected.

---

## Media Management

Before you can begin working with GemXplorer, you must define the media you want to work with.

### Types of Media Supported

GemXplorer uses the concept of card media. A card "medium" can be a real card or a card image file.

#### Real Cards

A real card should be used to check and validate the content of a card and test functionalities of the card such as network authentication and application downloading. To work with real cards, you must have a PC/SC compatible card reader connected to the local workstation.

GemXplorer detects when a card is inserted into a card reader. After you select the mode you want to work in, the contents of the card are displayed in GemXplorer. Conversely, when the card is removed from the card reader, the card and its contents are removed from GemXplorer's display.



## Card Image Files

A card image file is a representation of the contents of a card stored as a file on a workstation's hard disk. A card image file differs fundamentally from a real card in that you cannot communicate with the applications stored on it. For example, you cannot exchange APDU commands with applications on a card image file. A card image file also does not contain any of the security mechanisms of a real card. Card image files are used to transfer data from one medium to another, to exchange card file system profiles or to back up and restore the contents of a real card. This is currently available for Gemalto 2G cards only.

## Using a Card Reader with Card ADMIN

You must install and configure both PC/SC software and at least one card reader of a type supported by Card ADMIN before you can work with real cards in GemXplorer. The Card ADMIN Setup program automatically detects any compatible card reader connected to the local workstation and installs the appropriate PC/SC driver software.

## Installing a Card Reader

If you did not install your card reader during the Card ADMIN installation or if you want to install an additional card reader after having installed the software, you will need to follow this manual installation procedure.

Most modern card readers are plug-and-play compatible. New versions of Windows supports plug-and-play. As such, Windows detects the presence of the card reader during the next system startup and prompts you for an appropriate driver.

### To install a new card reader:

- 1 Power-off your PC and plug in a card reader to the USB port.
- 2 Restart your PC. Your card reader will be detected automatically and you may be prompted to supply the driver. You can either use the operating system's built-in driver or one supplied on the Card ADMIN installation CD.
- 3 Select **Start > Settings > Control Panel** to open the control panel.
- 4 Double-click the **Add/Remove Hardware** icon. In the list of **Devices**, select **USB Smart Card Reader > Next > Finish**.

## Troubleshooting a Card Reader

In order to solve card reader problems in your Card ADMIN environment, you can use the SmartDiag v2.0 utility. This utility is available on Gemalto's website at <http://support.gemalto.com>.

The aim of SmartDiag v2.0 is to verify that smart card readers and the cards they contain are available to other programs. It identifies the PC/SC readers that are connected to your PC. If the reader is connected properly, you can insert a card to check if the card is working properly.

This tool reports any software or hardware problems and gives troubleshooting information. If the displayed information still does not solve the problem, you can generate a diagnostic report. This report will be required if you ask technical support for help.

---

**Note:** SmartDiag v2.0 tests only the smart cards' basic functionality. It does not test the suitability of your smart card for use with a specific application.

---

### To diagnose a card reader problem:

Select **Programs > Gemalto > SmartDiag v2.0**.

There are three possible outcomes:

-  **Passed**
-  **Failed**
-  **Warning**

If the result is **Warning**, click **Advanced View** to obtain all the details. The Advanced View provides a real-time status and description of smart card related resources. This can be particularly useful to reveal obscure and low-level problems, or to identify the version of various software and hardware smart card components.

If the outcome is **Failed**, read the accompanying message carefully. It explains the most probable source of the problem and how to get your smart card and reader working. In addition, you can generate a diagnostic report by clicking **Get Assistance**. This action generates a diagnostic report that your technical support representative will need in order to help you.

If the Diagnostic Wizard reports **Passed**, but you have difficulty using your smart card(s), refer to the documentation of the software using this smart card.

**To generate a diagnostic report:**

The diagnostic report copies all the information in the Advanced View into a readable text file.

- 1 In the **Advanced View**, click **Generate** from the **Report** menu or,
- 2 If the Diagnostic Wizard reports a failure, click **Get Assistance**.

## Card Image Files

---

**Note:** This feature is currently available for Gemalto 2G cards only.

---

**To create a new card image file:**

- 1 Select **Media > Media Management...** on the menu bar.
- 2 In the **File** tab, click the **Add** button and select **New...** to select the location and name of your card image file.
- 3 Under **File name**, type the name of the card image file. For example, "GXXV3.gxc".
- 4 Select a card type from the list and click **Open**.

A card image file entry is added to the media list and is displayed in the **Card** tab.

When a GemXplore Xpresso V3 card images are first created, the card image file appears in the list of media in GemXplorer's Structure view containing a default business application. Refer to "Working with Card Image Files" on page 41 for more information about adding business or custom applications to your card image.

**To open an existing card image file:**

- 1 Select **Media > Media Management...** on the menu bar.
- 2 In the **File** tab, click **Add > Open...**
- 3 Browse and select an existing card image file (\*.gxc).
- 4 Click **Open**.

The media type is added to the media list and is displayed in the **Card** tab.

# Key Features of Card Management

This chapter describes the card management features which are available whether you are working in the Card Manager, GSM Application or 3G Application mode. The features and tasks which are specific to the respective modes can be found in “Chapter 4 - Working in the SIM Mode” and “Chapter 5 - Working in the 3G Application Mode”.

## Reading a Card

### Cards Supported by Card ADMIN

Card ADMIN supports the following cards:

- LinqUs card range
- Qipso card range
- UpTeq card range
- Gemalto legacy cards
- Any non-Gemalto cards

There are two categories of cards:

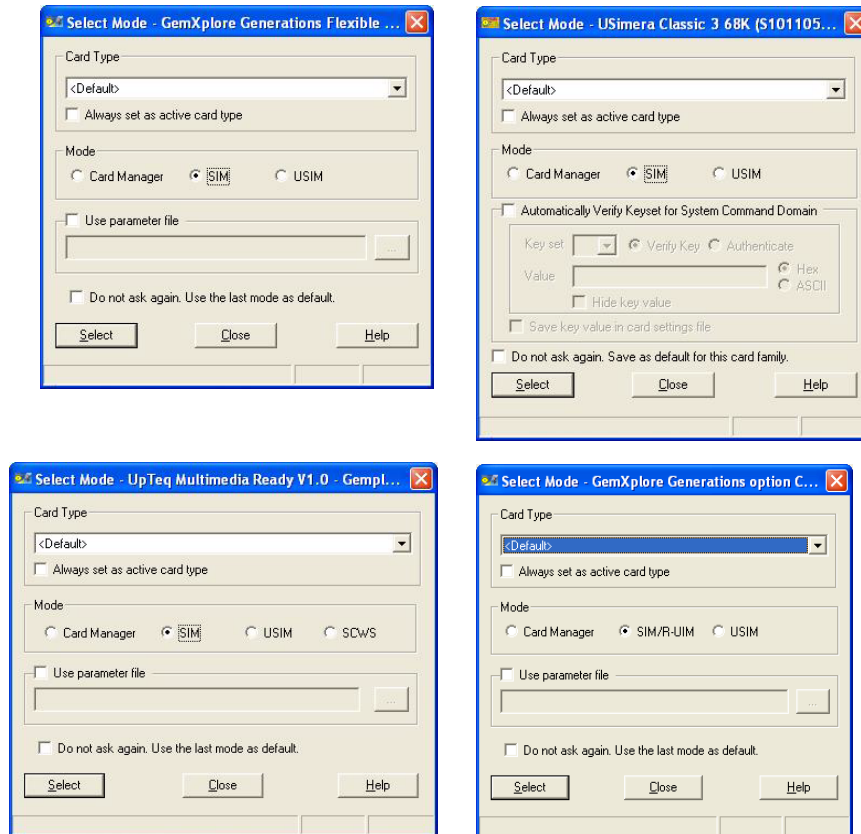
- 1 Gemalto cards are recognized automatically.
- 2 Non-Gemalto SIM or USIM cards that can be supported using the card typing functionality.

### Card Boot Selection

When a Gemalto card is inserted in a card reader, Card ADMIN will detect it and a **Select Mode** window will be displayed depending on the card inserted.

You can now choose the mode you want to work in — Card Manager, SIM, SIM/RUIM, USIM or SCWS.

Select **Card Manager** to access the applets installed and functions available in the Card Manager or select **SIM** to access the GSM functions and file system available for use. Select **SIM/R-UIM** to access the CDMA and GSM functions and file system available for use. Select **USIM** or **SCWS** to access the 3G or SCWS functions and file system available for use respectively.

**Figure 4 - Examples of Selecting the Mode to Work**

The **Card Type** list displays the types of cards associated with the ATR of the card in the reader and highlights the card type in the reader. You can change the current card type associated to the card in the reader by changing the selection from the list. The active card type is displayed as the first in the list.

To modify the active card type and set it to the card type you have selected, check the **Always set as active card type** box and Card ADMIN will then associate the card to the new card type the next time the card is inserted. You can associate more card types to an ATR via the ATR Manager.

For some cards, there is an option to use a previously saved parameter (\*.out) file by selecting the **Use parameter file** box and browse to select the file. The \*.out file is a Gemalto production text file that stores a card's diversified data such as PIN codes and key values. When this option is selected, the data stored in the \*.out file is retrieved and used during the setting up of a secure session with the Card Manager and during secret code verification.

The **Automatically Verify Keyset for System Command Domain** option may be available depending on the cards you are working with. You may deselect it so that the key set verification for system command domain will not be automatically made.

To save the mode that you have just selected, select **Do not ask again. Save as default for this card family**. The next time you use a card from the same card family type, the Select Mode window will not appear to prompt you for a selection again.

You can change to work in a different mode at any time via **Select Mode** in the contextual menu.

You can check a card's default card type by accessing the Card Information window through the contextual menu of the top-level icon of the card media in the GemXplorer's Structure view.

---

**Note:** The SIM mode is automatically selected for cards that are not Open Platform (OP) compatible.

---

## Card Typing Functionality

GemXplorer uses a number of built-in card detection routines to identify the type of card and its manufacturer whenever a card is inserted in a card reader.

For the usage of card typing, please refer to the following.

### Handling Unrecognized or Non-Gemalto Cards

When GemXplorer fails to identify a card, you can choose to select an existing card type or create a new card type based on the card's known characteristics and subsequently use it to identify other cards of the same type.

### Criteria for Automatic Recognition

GemXplorer provides direct support for a wide range of smart card types. You can create card image files of these types in GemXplorer. Real cards of these types are automatically recognized by GemXplorer and displayed in the GemXplorer window.

GemXplorer also includes a number of sophisticated detection algorithms designed to identify other smart card types, including non-Gemalto card types. These detection algorithms use the following criteria to identify card types:

- The card's answer-to-reset (ATR) setting. GemXplorer maintains a list of known custom ATR-to-card values.
- For Visa Open Platform (OP)-compatible cards, the AIDs of the Card Manager applet and other system-internal applets.
- For Gemalto-manufactured cards, Gemalto-specific ICC information, typically stored in the Elementary File EFICC or in the card's ROM.
- Other data stored in particular EF files or the card's ROM.
- Proprietary APDU commands, which GemXplorer may issue to query the card. These commands do not cause any changes in the card's life state or session status, nor are any files created or deleted. For example, GemXplore Xpresso v3 cards support an extended version of the OP-standard **Get Status** command, so these cards could be detected by sending a **Get Status** command to the card and interpreting the response.

### Manually Identifying a Card

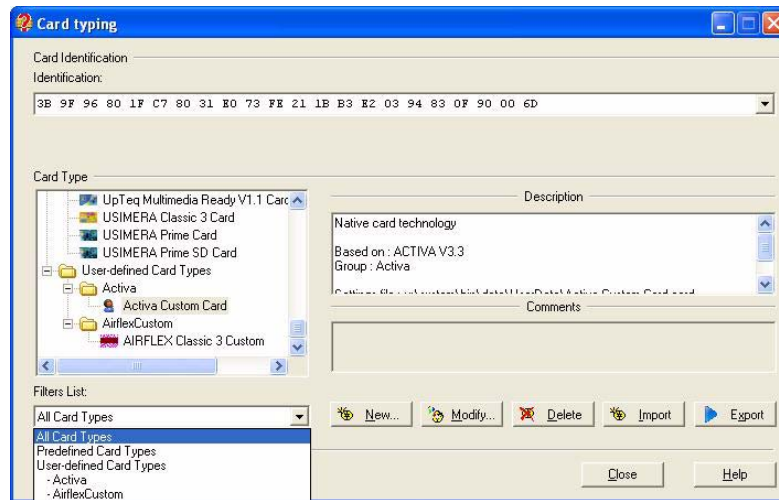
When a real card is inserted in a card reader while Card ADMIN is running, GemXplorer immediately attempts to identify the card and add it to the list of media in both the Media Manager and the GemXplorer windows.

If for any reason GemXplorer fails to recognize a card, it is shown as "Unknown". If it is a Gemalto card, you may manually identify the card based on an existing Gemalto card type. Refer to "Typing a Card Based on an Existing Card Type" on page 18 for details. If the unknown card is a non-Gemalto card, you may have to define a new card type for it. Refer to "Defining a New Card Type" on page 19 for details.

### Typing a Card Based on an Existing Card Type

If the card was unrecognized at insertion, the **Card Typing** window will automatically be displayed.

**Figure 5 - The Card Typing Window**



A card type is a card definition that is associated with real cards based on an ATR “mask”. In the **Card Type** list, Card ADMIN displays card types which may be:

- Predefined card types. These are known as Gemalto card types (for example, GemXplore Xpresso V3 Card). These card types are typically used if you have inserted a Gemalto card that was not recognized for some reason, for example, due to a custom ATR value.
- User-defined types, if you have already created your own card types.

The card’s ATR is displayed in the Identification field. You can either use the ATR as it is or create an ATR “mask” (that is, an ATR with “wildcard” X characters).

If you use the ATR as it is returned by the card, only cards with exactly the same ATR will be associated with the card type that you are defining.

If you create an ATR “mask”, all cards matching the “mask” will be associated with the card type that you are defining. This enables you to associate a wider range of cards with the same card type.

#### To type a card or change the type of a card:

- 1 If the inserted card’s ATR is recognized, it is displayed in the **Identification** list. If you want to change the ATR, select the ATR from the Identification list or click to edit the values. In the **Identification** list, some nibbles can be replaced by the value ‘X’ so as to define a “mask”. Hence, all cards with ATRs matching the “mask” will be recognized as cards belonging to the new card type.

For example, an ATR is set to 3B 3F 95 00 80 65 AF 03 1X 21 XX XX.

Cards with ATRs 3B 3F 95 00 80 65 AF 03 18 21 92 73 and 3B 3F 95 00 80 65 AF 03 18 21 5E C7 which match the mask are recognized.

- 2 In the **Card Type** box, select the card type name.

If the card type is not listed, proceed to define a new card type as described in “Defining a New Card Type” on page 19.

- 3 Click **Apply**.

---

**Note:** Only customized card types can be modified or deleted.

---

If you have created an ATR “mask” and you want to undo the associations, go to **Tools > ATR Manager** to modify or delete the ATR or ATR “mask”.

If you select an OP compliant card type, you must ensure that the card settings used by Card ADMIN correspond to your particular card.

## Defining a New Card Type

If you are not sure of a card's type, or the card type is not listed on the Card Typing window (for example, it is a non-Gemalto card), you can create a new card type.

New cards can be of two basic types:

- A native card is a GSM SIM card containing a proprietary operating system.
- A multi-application Java card is a Java-based card that complies with one or more industry standard OP specifications.

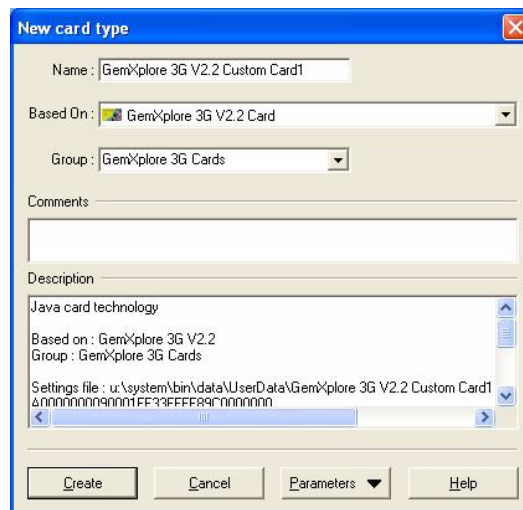
**Tip:** If an ATR/mask is available in the identification box before a new card type is created, the association between the new card type and the ATR is done automatically once a new card type is created.

**To create a new card type:**

- 1 In the **Card Typing** window, click **New**.

The **New Card Type** window is displayed:

**Figure 6 - The New Card Type Window**



- 2 Enter the name of the new card type in the **Name** field. This name will appear in the **Card Type** list on the Card Typing window and in the GemXplorer window.
- 3 From the **Based On** drop-down list, select a card type for your new card type to be based on. The card settings of the selected card type will be applied to your new card type.
- 4 To associate the new card type to a custom group, select the group from the **Group** list. To create a new group, type the group name in the **Group** list. You can leave it blank if you do not wish to assign the card type to a group.



- 5 If there are any useful comments to add regarding the new card type creation, type in the **Comments** field.

---

**Note:**

If you do not explicitly associate a command file, a mapping file, a setting file or applications with the card type, Card ADMIN will associate the default files or applications with the newly defined card type.

For Native type, only the mapping file and command file are associated with a new Native card type. There is no association of the card settings file or applications to a Native card type.

- 
- 6 To select the commands file to associate with the card type, click **Parameters > Commands file**. Browse to select the command file (in .AMF format). This is an APDU macro file that contains the APDU commands associated to a card type.

To select a mapping file to associate with the card type, click **Parameters > Default Model > Select**. Browse to select the .mapping file. The mapping file stores the file structure (DFs and MFs) of the card.

To select the applications file to associate with the card type, click **Parameters > Applications**.

To select the settings file to associate with the card type, click **Parameters > Card Settings**. The card settings file stores keys that Card ADMIN uses in order to set up a secure channel with the Card Manager.

- 7 Click **Create**.

Now that you have created a new card type corresponding to your card, your card will be automatically recognized each time it is inserted in the reader.

## Modifying a Custom Card Type

**To modify the characteristics of a custom card type:**

- 1 In the **Card Type** list, select the custom card type to modify.

---

**Note:** You cannot modify the characteristics of any of the predefined card types supplied with Card ADMIN.

---

- 2 Click **Modify**.
- 3 Change any of the custom card type's characteristics, as described in "Defining a New Card Type" on page 19.
- 4 Click **Apply** to save the changed characteristics.



## Deleting a Custom Card Type

To delete a custom card type:

- 1 Select the card type from the **Card Type** list.
- 2 Click **Delete**.
- 3 Click **Yes** to confirm your action.

---

**Note:** Predefined card types such as Gemalto's cannot be deleted.

---

## Importing a Custom Card Type

To import a previously saved custom card type:

- 1 In the **Card Typing** window, click the **Import** button and select the \*.zip file (containing previously saved information and parameters) of the particular card type you want to import.
- 2 Click **Open**.

After a successful import, the card type is displayed in the **Card Type** list.

## Exporting a Custom Card Type

To export a custom card type:

- 1 In the **Card Typing** window, select a card type from the **Card Type** list.
- 2 Click the **Export** button.

## Managing the ATR

Customized ATRs (Answer To Reset) and card type associations are displayed in the **ATR Manager** window. If you have previously created an ATR “mask” during card typing and you want to undo the associations, you can use the **ATR Manager** to modify or delete the ATR or ATR “mask”.

**Tip:**

- Click on any column title to sort the data by the ascending or descending order.
- Select the type of filter from **Display Filter** list box to show only the group of items you wish to see in the **Card Identification** list. Subsequently, a combo box is available to complete the filter selection.

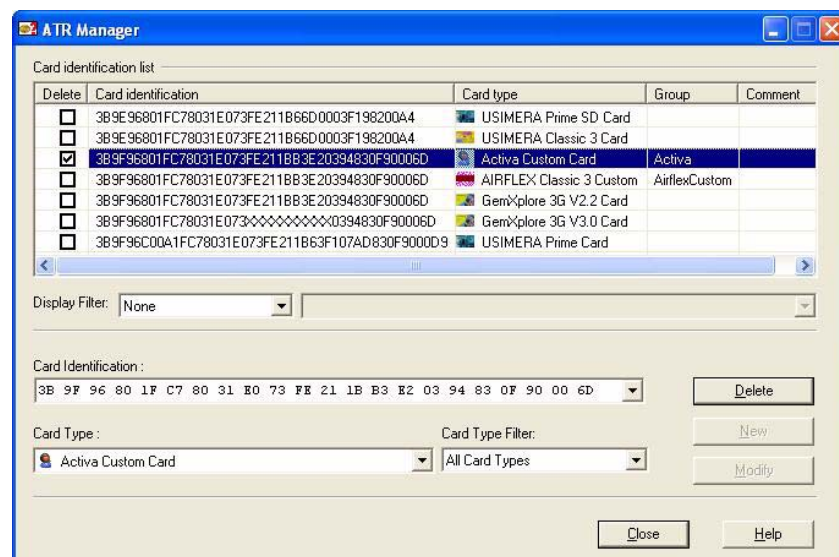
### Creating a new ATR to Card Type Association

To create a new ATR to card type association:

- 1 In the GemXplorer menu bar, click **Tools > Card Type Management > ATR Manager**.

The ATR Manager window is displayed.

**Figure 7 - ATR Manager**



- 2 In the **Card Identification** box, select the ATR from the list box or type the new card's ATR or mask. The list box contains the ATRs of the cards that are currently in use with Card ADMIN.
- 3 In the **Card Type** list box, select a card type from the drop-down list box and click **New**.

**Note:** The **New** button is enabled only when the new ATR to card type association is valid and provided that the association does not exist in the list.

## Deleting an ATR to Card Type Association

To delete an existing ATR to card type association:

- 1 In the GemXplorer menu bar, click **Tools > Card Mangement > ATR Manager**.
- 2 Check the **Delete** box next to the Card Identification you wish to delete and click **Delete**.

## Modifying an ATR to Card Type Association

To modify an existing ATR to card type association:

- 1 In the GemXplorer menu bar, click **Tools > Card Mangement > ATR Manager**.
- 2 In the **Card Identification** box, select the association you wish to modify.
- 3 Modify the **Card Identification** or **Card Type** in their respective boxes and click **Modify**.

---

**Note:** The **Modify** button is enabled only when the new ATR to card type association is valid and provided that the association does not exist in the list.

---

## Model Editor

Each file type has a file mapping (also known as file model). Based on the file mapping, Card ADMIN electively displays the file structure of the card. Hence, only DFs and EFs listed in the file model are displayed after the initial card scan.

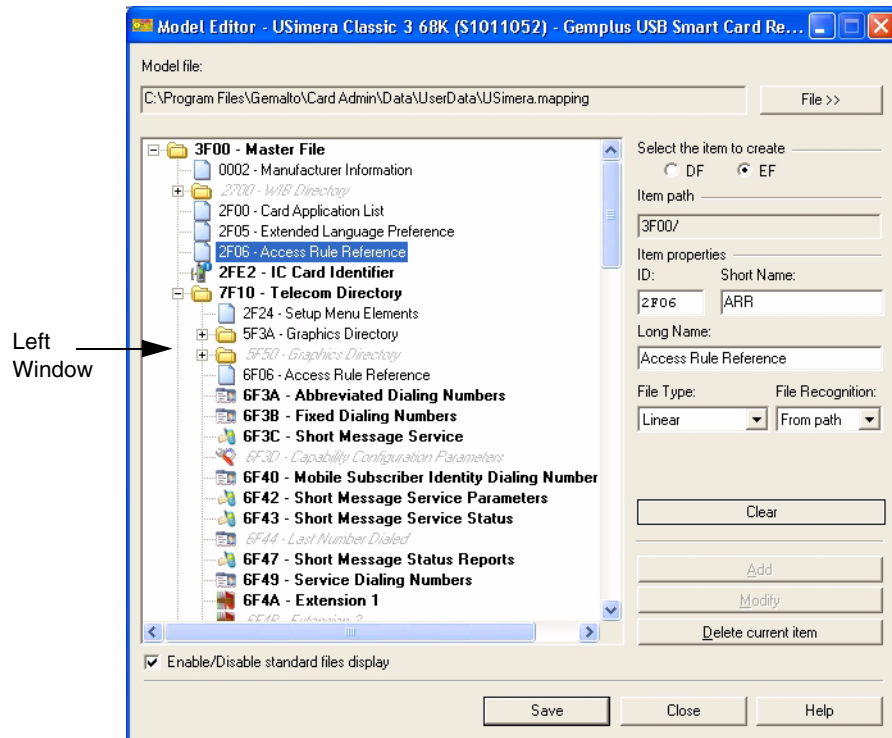
When a card type is defined, a default model is associated with it. Initially, the model only contains the file structure of a default GSM application (for example, mandatory telecom EFs). Unless you explicitly ask for an entire or deep scan of the card, Card ADMIN only displays the DFs and EFs in the model and all other files that are not in the model are hidden, whether they are standardized, customized or user defined.

The Model Editor allows you to update the file mapping such as to add, modify or delete a DF or several EFs under a particular DF. Card ADMIN will scan the card according to the model and will only display the files you want, without deep scans of the card to search for customized files.

To use the model editor:

- 1 On GemXplorer Structure view, right-click on a card to select **Model Editor...** .  
The Model Editor window is displayed. If the **Enable/Disable standard files display** box is checked, the typical file structure as defined in the standards is displayed in the left window.

Figure 8 - Model Editor



- 2 Click **File >>** to select the model file you wish to update. The contents of the model file are displayed on the left window.
- 3 To add a DF, EF or :

---

**Note:** DFs or EFs that are added to the model via the Model Editor are not physically created in the card. They are DFs or EFs which already exist in the card. By adding them to the model will enable Card ADMIN to display them at the next scan of the card (whether you request for the scan or when a card is inserted into the card reader). To create a new file, refer to “File Management Commands” on page 56.

---

- a) Select **DF**, **EF** or under **Select the item to create**.
- b) Type the file **ID**, **Short Name** and **Long Name**. Select the **EF type** (if you are creating an EF) and **File Recognition** from their respective drop-down lists.
- c) Click **Add**.

**To modify the file properties in a model file:**

---

**Note:** DFs or EFs that are modified in the model via the Model Editor are not physically modified in the card.

---

- a) Select the file from the left window.
- b) Update the **ID**, **Short Name**, **Long Name**, **EF type** (if EF has been selected) accordingly in their respective boxes.
- c) Click **Modify**.

**To delete an item from the model file:**

---

**Note:** DFs or EFs that are deleted from the model via the Model Editor are not physically deleted in the card.

---

- a) Click to select the item from the left window.
- b) Click **Delete current item**.

- 4 Click **Save**.

## Managing Card Data

### Viewing the File Structure of a Card

To view the file structure of a card:

- 1 Insert a card into a card reader.
- 2 Select the mode you want to work in, either **Card Manager**, **SIM USIM** or **SCWS**.

The parameter file refers to the Gemalto production text file (\*.out) that stores a card's diversified data such as PIN codes and key values. The data stored is retrieved and used during the setting up of a secure session with the Card Manager and during secret code verification.

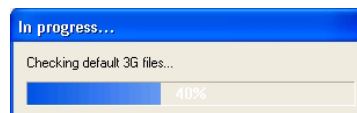
---

**Note:** For 2G cards, the SIM mode is automatically selected.

---

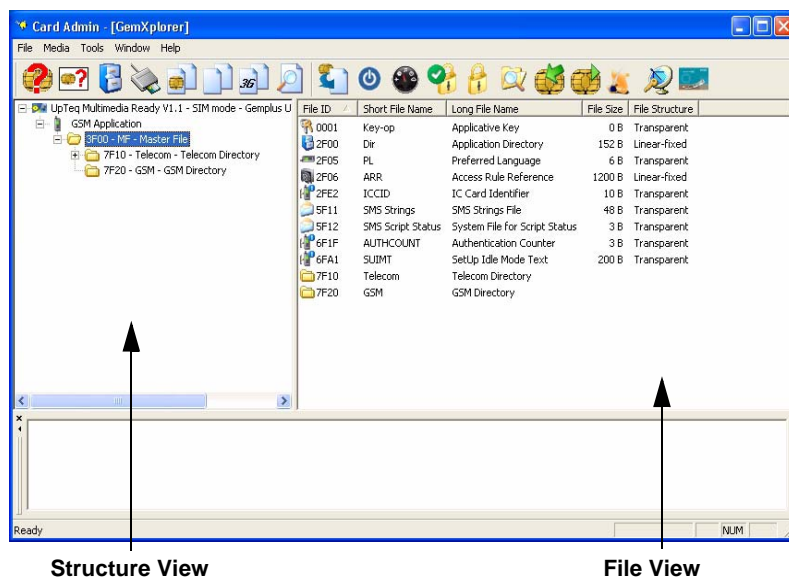
GemXplorer automatically detects that a card has been inserted into the card reader and begins scanning the contents of the card.

**Figure 9 - Scanning the Card Contents**



- 3 In GemXplorer, select the icon representing the card in the Structure view. Click the plus signs (+) to display the applications stored on the card and the directories within applications that have file systems. Click a file directory in the Structure view to display a list of files in the directory.

**Figure 10 - The GemXplorer Main Window**



The GemXplorer main window is divided into two panes.

On the left, the Structure view displays all the media that have been defined, together with the applications and file structure stored on each real card and where appropriate, the file system of an application. Objects in the Structure view are displayed at different levels and are according to the mode you are working in.

On the right, the File view displays a list of the files in the file directory currently selected in the Structure view. For example, if the "7F10 TELECOM" directory is selected, all files in the directory are listed in the File view.

A different icon is used to represent each different type of file displayed (for example, EF directory files, transparent or linear files). For a description of the files, see the appropriate card operating system specification and the online help available for each file.

---

**Note:** The default view is the details view. You can also choose to view the GemXplorer interface in the large icons, small icons or list view. To change the view, select **Window** on the menu bar and click the preferred view.

---

---

**Tip:** You can sort the files in the right pane by alphabetical, ascending or descending order. To do this, click on the respective column.

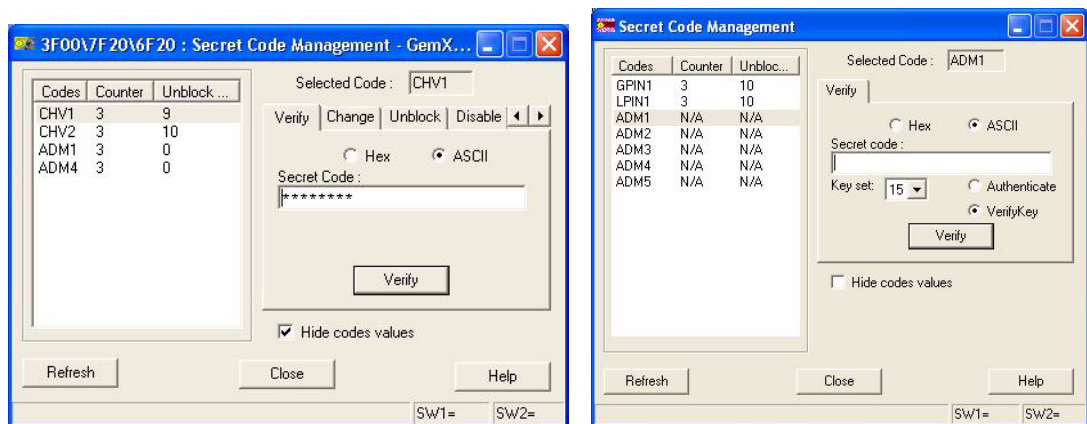
---

## Secret Code Management

Files are generally protected by security mechanisms. These require that one or more secret codes must be provided before carrying out certain operations (for example, reading the contents of a file, modifying a file, or deleting a file). The secret code required for a given command is specified when the file is created. The conditions for accessing a file are available in the file's properties. Refer to "Viewing File Properties" on page 31.

For example, GemXplorer prompts you to enter the Card Holder Verification (CHV) or ADMinistrative (ADM) secret code required to perform the command on a GSM file depending on the cards used, as shown in "Figure 11".

**Figure 11 - Examples of Secret Code Management**



On 3G cards, there are two types of secret codes:

- Local secret codes are locally used by specific USIM applications. These codes are stored in LPIN objects. The rights required for LPIN codes are only valid for the current USIM application session.

**Note:** Depending on the cards you are working with, the LPIN code may only be displayed in the Secret Code Management dialog box if you have opened a session for the corresponding USIM application.

- Global secret codes may be used by any application. These codes are stored in GPIN, ADM1 to ADM10 objects.

### To verify a secret code:

- Select a code in the list on the **Secret Code Management** window and select to verify the code in **Hex** or **ASCII** in the respective buttons.
- For some cards, there is a **Hide codes values** box available. Check the box if you want to mask the code values as "\*". If you want the code values to show, leave this box unchecked.

**Note:** If you have checked the **Hide codes values** box, enter the value carefully as an incorrect value will decrement the ratification counter of the secret code.

- Enter the code's value in the **Secret Codes** box. For some cards, there is a **Key set** option available to allow you to choose the version to be used for the ADM codes before entering the code value.

**Note:** The code value is automatically filled when it is set in the \*.card file using option panel (CHVx) or in the **Card Setting File Management** window (which is the key set value for ADMx).



**4 Click Verify.**

For some cards, there is an **Authenticate** or **VerifyKey** option to be performed on the security level of the key set used for the ADM codes.

**Note:****For Gemalto cards:**

- If you have previously configured and stored the secret code value in Options > 2G PIN Configuration, the secret code values will appear in this window.
- For some cards, only CHVx can be stored in the Options > 2G PIN Configuration. Key set values for ADM are stored via the Card Settings File Management window.

**For non-Gemalto 2G cards:** if you have previously configured and stored the secret code values in **Options > 2G PIN Configuration**, the secret code values will appear in this window.

**For non-Gemalto 3G cards:** if you have previously configured and stored the secret code values in **Options > 3G PIN Configuration**, the secret code values will appear in this window.

The result and the corresponding status words are displayed in the status bar at the bottom of the windows. If you enter an incorrect value, **Counter** (the ratification counter) is decremented. If **Counter** reaches 0, the code is blocked. In this case, the secret code is no longer usable and the corresponding unblocking code must be presented (via the **Unblock** property sheet) before the secret code can be re-used.

The correct presentation of a secret code gives you the access rights necessary to apply the corresponding command or commands to the file.

Alternatively, the secret codes that are stored in the card configuration file can be verified at once.

---

**Note:** This feature may not be available on some cards.

---

**To verify all PINs:**

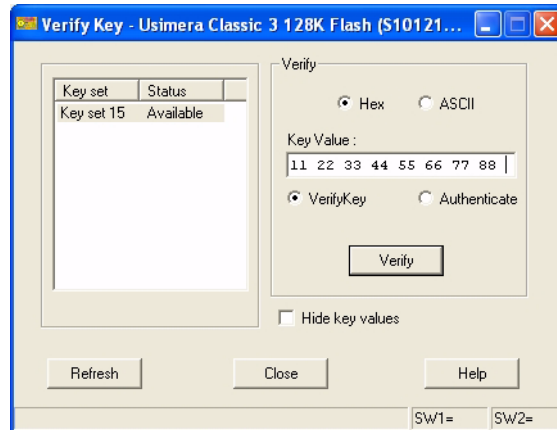
- 1 For Java cards, check that the card is in the SIM mode. (To select mode, see “Card Boot Selection” on page 15.) The SIM mode is automatically selected for Native cards.
- 2 In GemXplorer Structure view, right-click on the GSM application and select **Verify All PINs**. The Verify All PINs window is displayed.
- 3 If you do not want a certain PIN to be verified, uncheck the box next to that PIN.
- 4 Click **Verify**.

Representation of the color of the dot:

- Green means that the check is successful.
- Red means that the check has failed.
- Yellow means that the secret codes with ratification counters set to 1 are not checked.

**To verify a key set:**

For some cards, it is possible to verify a specific key set that has not yet been verified first at the card level by right-clicking the contextual menu in the GemXplorer's Structure view and select **Verify Key** command. This is useful only if **System Command Domain** is not granted during the session.

**Figure 12 - Verify Key**

## Viewing the Contents of a Specific File

To read the contents of a file, double-click the file in GemXplorer's File view.

Depending on the access conditions that were set for the file when it was created, you may be prompted to enter a secret code in order to read it. Refer to "Examples of Secret Code Management" on page 28 for more information about secret codes. Most card files can be displayed either using an interpreted or binary view. The purpose of each file is described in GemXplorer's contextual help, displayed by clicking the **Help** button in the **Interpreted** view. For the coding of each file, refer to the 3GPP TS 31.102 standard for details.

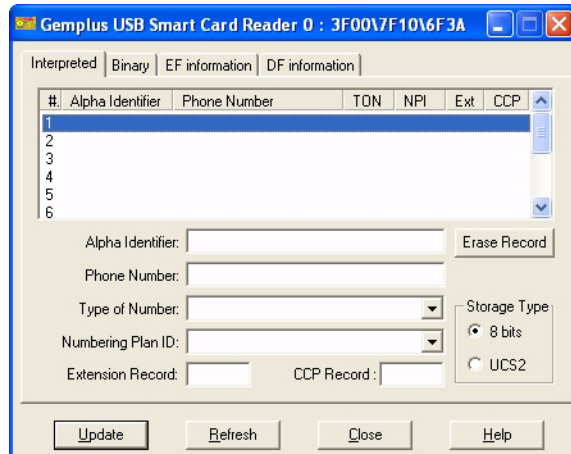
---

### Note:

- 1 You can generate a content report containing the details of the file contents in the card. See "Generating a Content Report" on page 32 for details.
  - 2 Files that are defined in the 3GPP standards have both interpreted and binary views. User-specified or proprietary files have at least the binary view while some such as Gemalto proprietary files may also have the interpreted view.
- 

## Using the Interpreted View

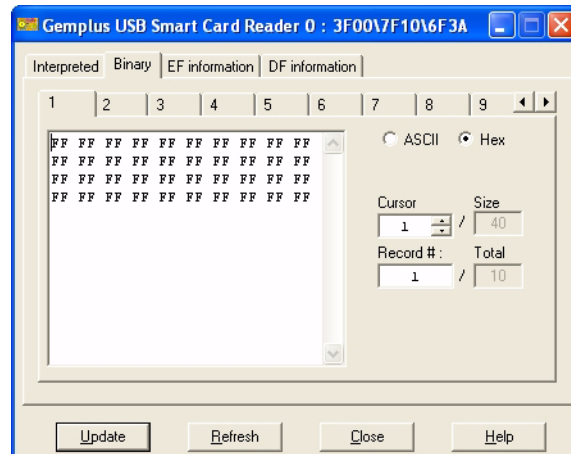
The interpreted view allows you to read and edit files' contents directly without having an in-depth knowledge of their coding. Any changes made in the interpreted representation are immediately applied to the underlying binary representation. However, the changes are not physically applied until you click **Update**.

**Figure 13 - Interpreted File View**

Because there are numerous different file types on a typical card, most file types are associated with a particular file viewer window. Refer to the online help for information on how to interpret and if necessary modify the information on the file viewer windows.

### Using the Binary View

The **Binary** property sheet displays the data as it is actually stored in the file. Any changes made here are immediately applied in the Interpreted view (that is, the binary data is “interpreted” so that it is clearly understandable).

**Figure 14 - Binary File View**

Refer to the online help for more information.

## Viewing File Properties

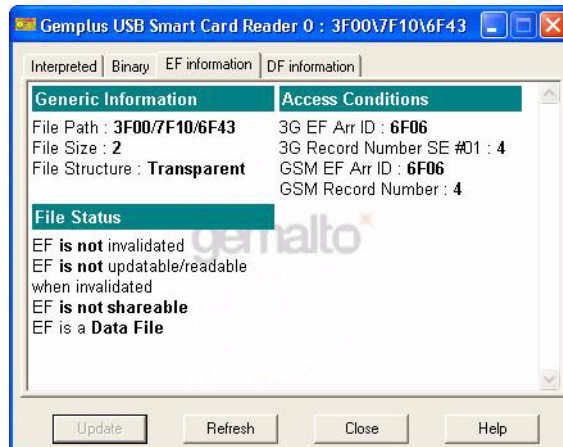
The characteristics and security restrictions of each card file are held in the status and properties specific to that file.

Property information is useful in manipulating the card's contents. The file's parent DF or MF properties display the amount of free space remaining in the parent directory, which is useful when creating a file. The current file's properties hold, for example, the file's access conditions.

**To display a file's properties:**

Right-click on the file in GemXplorer's File view and select **Properties**. The window that is displayed depends on the file type. For example:

**Figure 15 - File Viewer Window for a Transparent File**



In general, the **EF Information** property sheet displays the properties of the current file, while the **DF Information** property sheet displays the properties of the file's parent DF or MF directory.

### Current File Status (EF Information)

**Generic Information** describes the file information (such as path, id, size) and the structure of the data that it contains.

**Access Conditions** describes how the file is protected. This also indicates the file commands that are restricted and the access rights/authentication required to use them.

**File Status** indicates whether the file is invalidated and if so the type of operation that can be performed on it.

### Parent File Status (DF/MF Information)

**Generic Information** indicates the memory allocation of the MF or parent DF, the number of EFs and DFs, secret code information and the electrical characteristics of the card.

**Access Conditions** describes how the directory is protected. This also indicates the file commands that are restricted and the access rights/authentication required to use them.

**CHV1 Information/CHV2 Information** provides the current status of the CHV1 (user PIN) and CHV2 codes.

## Generating a Content Report

This feature allows for a content report that includes the following information to be generated from any card:

- IDs of all the EFs, DFs and s present on the card (including secret codes EFs)
- Attributes of each EF, DF and (including secret codes EFs)
- Body content of each EF

The content report generation can be based on the default mapping files or on real card files and can include the file content if required. Additionally, the content report can be saved or printed.

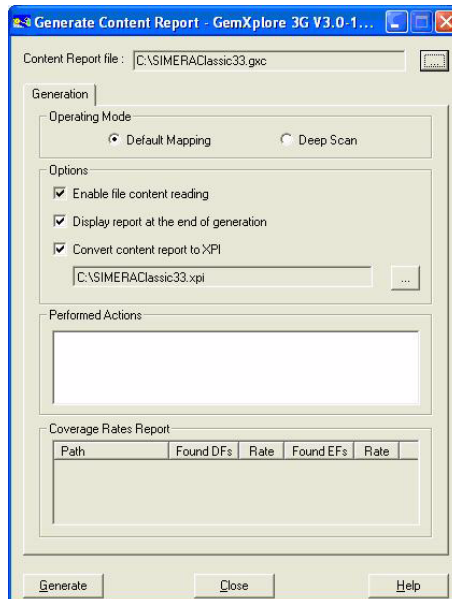
### For Gemalto Cards

To generate a content report:

- 1 In GemXplorer Structure view, right-click on a card, select **Generate Content Report...**

The Generate Content Report window is displayed.

**Figure 16 - Generating a Content Report — Gemalto Cards**



- 2 In the **Content Report file** box, browse to select the report output file name.
- 3 In the **Generation** tab, select **Default Mapping** for a content report which will be generated from files found in the default card mapping or, **Deep Scan** for all the files physically present on the card.
- 4 If you want all file contents to be added to the report, check the **Enable file content reading** box.

---

**Note:** If this is enabled, you will be prompted to enter all required secret codes during report generation in order to read all file contents.

---

- 5 If you want to view the report after it has been generated, check the **Display report at the end of generation** box.
- 6 If you want to generate the report in the XPI format after it has been generated, check the **Convert content report to XPI** box.
- 7 Click **Generate**.

A content report which is saved in the .GXC format is displayed in the Internet Explorer browser.

---

**Note:** To stop a content report generation at anytime, click **Abort**.

---

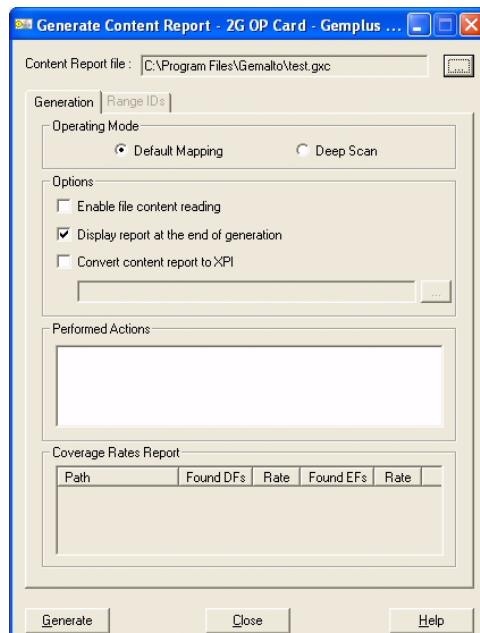
## For Non-Gemalto (2G and 3G standard) Cards

To generate a content report:

- 1 In GemXplorer Structure view, right-click on a card, select **Generate Content Report...**

The Generate Content Report window is displayed.

**Figure 17 - Generate Content Report — Non-Gemalto Cards**



- 2 In the **Content Report file** box, browse to select the report output file name.
- 3 In the **Generation** tab, select **Default Mapping** for a content report which will be generated from files found in the default card mapping or, **Deep Scan** for all the files physically present on the card.

---

**Note:** If **Deep Scan** is selected, you must specify the range of file IDs to be scanned, in the **Range IDs** tab. See “Range IDs” on page 35 for information.

---

- 4 If you want all file contents to be added to the report, check the **Enable file content reading** box.

---

**Note:** If this is enabled, you will be prompted to enter all required secret codes during report generation in order to read all file contents.

---

- 5 If you want to view the report after it has been generated, check the **Display report at the end of generation** box.
- 6 Click **Generate**.

A content report which is saved in the .GXC format is displayed in the Internet Explorer browser.

---

**Note:** To stop a content report generation at anytime, click **Abort**.

---

### Coverage Rates Report

The scan coverage rate report enables you to know the number of files defined in the scan ranges versus the number of files which are physically present on the card. Hence, to increase the coverage rate, you need to extend the scan range. However, as the file location may be different for a non-Gemalto card, some files in the card may not be located easily.

After a successful content report generation, the number of files found is displayed in the **Coverage Rates Report** box.

**Path** refers to the location path of the DF/EF.

**Found DFs**, for example, "2/4" means that two DFs have been found out of the actual four DFs which supposedly exist.

---

**Note:** The coverage rate cannot be displayed for 3G standard cards. Hence, only the files found under each DF or are displayed.

---

### Range IDs

In the **Range IDs** tab, you can define the range of DFs or EFs which will be used in scanning non-Gemalto (2G and 3G standard) cards. Here, you can add, modify or remove a range of DFs and EFs.

Low ID refers to the start (first file ID) of the range and High ID refers to the end (last file ID) of the range you want to specify for the scan.

## Generating Content Report for Applications

**Note:** This feature is only available when the card is in the Card Manager mode.

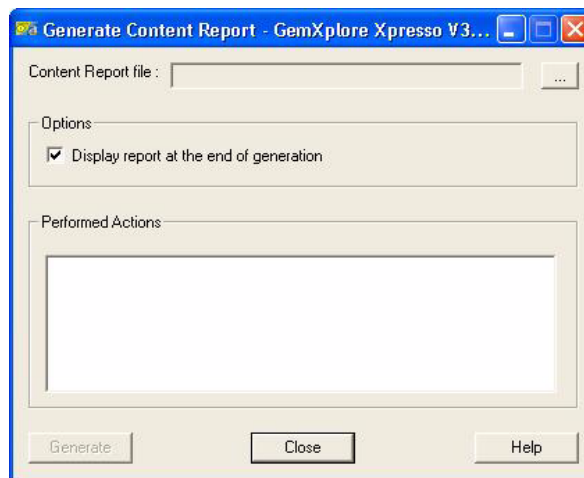
This feature allows for a content report that contains the existing applet instances to be generated from any card.

The content report generation can be based on the default mapping files or on real card files and can include the file content if required. Additionally, the content report can be saved or printed.

**To generate a content report for applications:**

- 1 In GemXplorer Structure view, right-click on a card, select **Generate Content Report...** .  
The Generate Content Report window is displayed.

**Figure 18 - Generate Content Report for Applications**



- 2 In the **Content Report file** box, browse to select the report output file name.
- 3 If you want to view the report after it has been generated, check the **Display report at the end of generation** box.
- 4 Click **Generate**.  
A content report which is saved in the .GXC format is displayed in the Internet Explorer browser.

**Note:**

- To stop a content report generation at anytime, click **Abort**.
- You may save the displayed report as an HTML file and view the results in the Internet Explorer browser without launching Card ADMIN.

## Viewing a Content Report

If you did not select **Display report at the end of generation** but want to review the report after it has been generated:

- 1 In GemXplorer menu bar, click **Tools > Card Profile Management > View Content Report...** .
- 2 Select the file > **Open**.



## Converting a Content Report to XPI Format

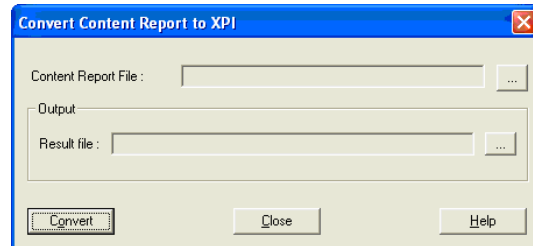
This feature enables you to convert the content report generated from the card to an XPI format. The content report generation is based on the default mapping files or on real card files and may include the file content if required.

**To convert a content report:**

- 1 In GemXplorer menu bar, click **Tools > Card Profile Management > Convert Content Report to XPI**.

The **Convert Content Report to XPI** window is displayed.

**Figure 19 - Converting Content Report to XPI Format**



- 2 In the **Content Report file**, browse and select the content report files to be converted.
- 3 In the **Result** file box, browse to select the report output file location.
- 4 Click **Convert**. An XPI file is saved in the selected location.

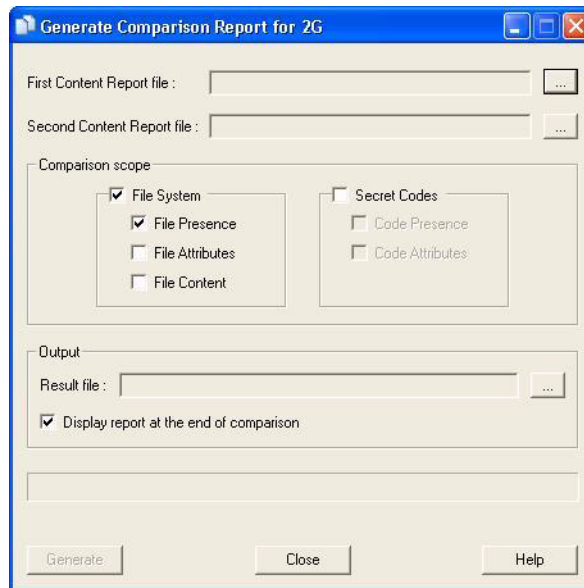
## Generating a Comparison Report

This feature enables you to compare two content reports and generate a new report called the comparison report. Comparison is only available on reports of the same type, for example, a SIM card with another SIM, or a USIM card with another USIM.

**To generate a comparison report:**

- 1 In GemXplorer menu bar, click **Tools > Card Profile Management > Generate Comparison Report for 2G...** or **Generate Comparison Report for 3G...**.

The **Generate Comparison Report** window is displayed.

**Figure 20 - Generating a Comparison Report for 2G Card**

- 2 Browse and select the content report files to be compared, from the **First Content Report file** and **Second Content Report file** boxes
- 3 For 3G card comparison report, the s in the selected files are displayed under **comparison scope**. Select the s you want to have compared.
- 4 In the **Comparison scope** box, check the boxes of the items you will like to have compared, such as, File System, File Presence, File Attributes and File Content.  
For File Attributes, the following values are compared: access level, file type, record size, record number, EF invalidated, EF readable when invalidated and EF trigger applet when file is updated.
- 5 In the **Secret Codes** box, check the boxes of the items you will like to have compared, such as Code Presence and Code Attributes.  
For Code Attributes, the following values are compared: code is enabled, code is activated, disable/enable/change is authorized, the number of remaining attempts/unblocking attempts and ADM rights granted.
- 6 In the **Result file** box, browse to select the report output file name.
- 7 If you want to view the report after it has been generated, check the **Display report at the end of comparison** box.
- 8 Click **Generate**.

A comparison report is displayed in the Internet Explorer browser.

---

**Note:** You may save the displayed report as an HTML file and view the results in the Internet Explorer browser without launching Card ADMIN.

---

## Generating a Comparison Report for Applications

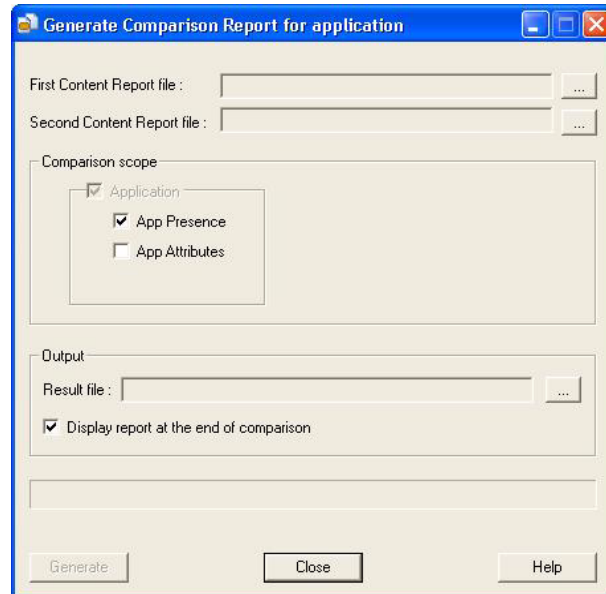
This feature enables you to compare two application content reports and generate a new report called the comparison report. Comparison is only available for reports of the same type, for example, a SIM card with another SIM.

**To generate a comparison report for Applications:**

- 1 In GemXplorer menu bar, click **Tools > Card Profile Management > Generate Comparison Report for Applications...**

The **Generate Comparison Report for Applications** window is displayed.

**Figure 21 - Generating a Comparison Report for Applications**



- 2 Browse and select the content report files to be compared, from the **First Content Report file** and **Second Content Report file** boxes.
- 3 In the **Comparison scope** box, check the boxes of the items you will like to have compared, such as, Application Presence and Application Attributes.  
For Application Presence, the AID of applets or packages are compared applet privileges.  
For Application Attributes, the following values are compared: applet life cycle and applet privileges and package life cycles.
- 4 In the **Result file** box, browse to select the report output file name.
- 5 If you want to view the report after it has been generated, check the **Display report at the end of comparison** box.
- 6 Click **Generate**.

A comparison report is displayed in the Internet Explorer browser.

In cases where there are differences between the two content reports, a summary will be highlighted in the comparison report.

You may save a copy of the report via the Internet Explorer.

## Viewing a Comparison Report

If you did not select **Display report at the end of generation** but want to review the content report for files or applications after it has been generated:

- 1 In GemXplorer menu bar, click **Tools > Card Profile Management > View Comparison Report...**
- 2 Select the file > **Open**.

## Printing Reports

To print reports:

- 1 Open the report file in the Internet Explorer browser.
- 2 Select **File** and click **Print**.

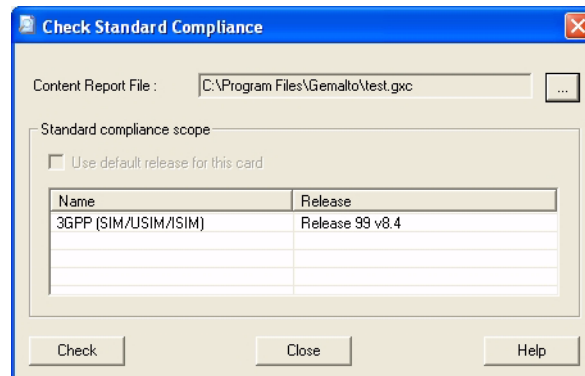
## Checking Standard Compliance

This feature allows you to compare a card's content with that of 3GPP/GSM standards.

To check standard compliance:

- 1 In GemXplorer menu bar, click **Tools > Card Profile Management > Check Standard Compliance...**. The Check Standard Compliance window is displayed.

**Figure 22 - Check Standard Compliance**



- 2 In the **Content Report File** box, click the ... button to select a ".gxc" file.
- 3 Select **User Standard Associated** if you want to compare the card content with its associated standard.
- 4 If you want to compare the card content with another standard, select the **Standard** from the drop-down list.
- 5 Click **Check**.
- 6 The **Standard Compliance Report** is generated and displayed.

## Working with Card Image Files

A card image file is a representation of the contents of a card stored as a file on a workstation's hard disk. It is used to transfer data from one medium to another or to back up and restore the contents of a real card. Refer to "Card Image Files" on page 13 for more information.

---

**Note:** This feature is currently available for Gemalto 2G cards only.

---

### Adding Files to a Card Image File

Two methods can be used to add files to a card image:

- Select the containing directory (for example, 3F00) in GemXplorer's Structure view, right-click in the file view and select **Create** from the contextual menu.
- Dragging-and-dropping files from a card or another card image.

---

**Note:** On this type of media, the file structures corresponding to the latest available version of the GemXplore operating system are used by default. For any given file identifier, however, the contents of the file may vary from one operating system version to another. To create files for an earlier operating system version (for example, GemX8/16), use the **Properties** command to set specific fields (for example, to set remote access conditions used only on GemX8/16 cards).

---

### Viewing the Structure of a Card Image File

To view the structure of a card image file:

Open or create a card image file using **Media > Media Management**.

The name assigned to the media when it was created is displayed and the file structure of the card image file is shown in a similar way as for a real card. See "Viewing the File Structure of a Card" on page 26 for details.

### Editing Files on a Card Image File

It is possible to edit both the contents and properties of files on card image files.

---

**Note:** When card files are held as card image files, you can change a file's properties after it has been created.

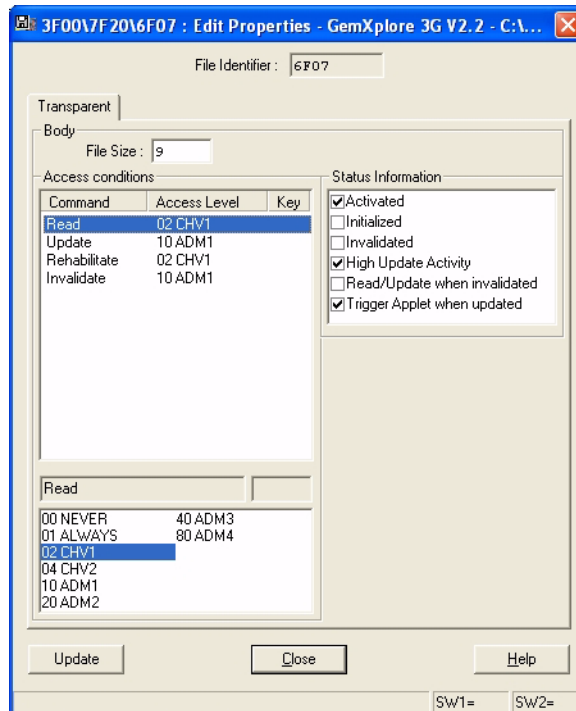
When copying a file from one card to another, this allows you to reset the access conditions, number of records or file size, and file validity settings required for the target card.

---

### Editing Card Image File Properties

To edit the properties of a file on a card image:

- 1 Select the file to be edited in the GemXplorer window.
- 2 Right-click on the file and select **Edit Properties** from the contextual menu. The window displayed depends on the file type:

**Figure 23 - An Update Window**

In the **Update** window, you can edit the properties of an existing card image file. You cannot do this on a card file as the properties are set definitively when it is first created. The settings entered here are unrestricted in terms of card management and organization (for example, memory management, file identifiers, and so on).

**Note:** Changing the size of a record in a transparent or cyclic EF causes all the records in that file to be padded with FFh.

## Viewing the File Contents of a Card Image File

To view the file contents of the card image file in the HTML format:

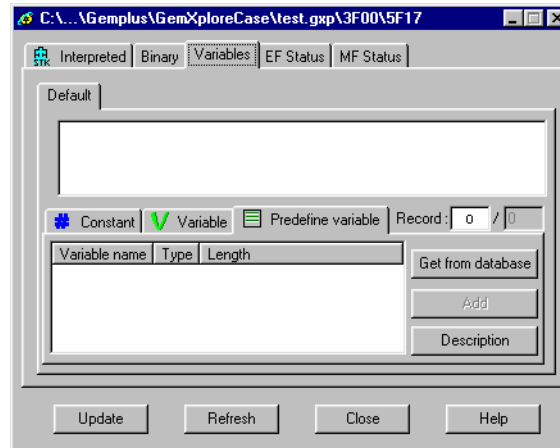
- 1 Open a card image file using **Media > Media Management**.
- 2 In the GemXplorer Structure view, select the card image file, right-click and select **View HTML...**

A content report of the card image file is displayed in your Internet Explorer web browser.

It is possible to compare the contents of two card image files or to compare the content of a card image file with a real card content. The procedure is similar to that of a real card. See "Generating a Comparison Report" on page 37 for details.

## Using Variables in Card Image Files

The **Variables** tab, displayed when viewing a file's properties, is only available on card images.



**Figure 24 - The Variables Property Sheet**

In GemXplorer, variables are typically used when generating scripts for OTA (Over The Air) administration. See the *GemXplorer CASE OTA User Guide* for information about generating OTA scripts using variables in GemXplorer.

Although initially intended for OTA purposes, variables can also be used to generate more flexible card profiling scripts for personalizing test cards. Such scripts provide a quick and easy means of reproducing the same file structure on several cards using specific values for each card.

The **Variables** property sheet is used to break down the content of the current file (for transparent EFs) or record (for linear fixed or cyclic EFs) into variables and constants so that it can be generated in that form (rather than as a series of fixed values) in any scripts generated from the card image file structure. See “*Generating GemXplorer Macro Language Scripts*” on page 33 for further details on generating scripts in GemXplorer.

### Example

The content of the records in dialing number files such as EF<sub>ADN</sub> or EF<sub>FDN</sub> can be represented using the following variables and constants:

**Name:** 0B

**TON/NPI Number:** FF FF

The constants are defined locally (that is, in the PC “.gxp” file) in the **Constant** property sheet.

The variables and the corresponding values are either defined locally in the Variable property sheet or taken from a card data table created in GemXplorer CASE’s Database Manager module. The link with the card data table is provided in the **Predefined Variable** property sheet.

In Linear Fixed and Cyclic EFs, you can create a default definition which assigns the same variable/constant structure to all the records, or you can create specific variable/constant structures for each record.

## Saving Card Image Files to Disk

The contents of the card image file are automatically saved after each modification and when the card image file is closed.

**To save the contents of a card image to a different file:**

- 1 Right-click on the top-level card image file icon in GemXplorer's Structure view window and select **Save as** from the contextual menu.
- 2 Browse to the directory in which to save the card image file and enter the file name. A .GXC extension is added to the file name you enter.

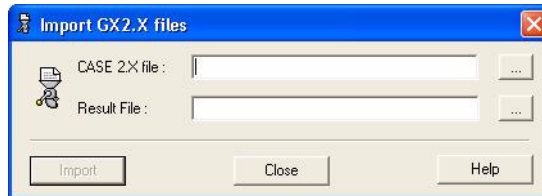
## Importing Card Image Files

You can import card image files created with earlier versions of Card ADMIN (called GemXplore CASE).

**To import a GemXplore CASE v2.x card image file:**

- 1 Select **Tools > Import** from the GemXplorer menu bar. The Import GemXplorer 2.0 Files window is displayed:

**Figure 25 - Importing Card Image File**



- 2 Select a GemXplorer CASE 2.x card image file (.GXP) to convert.
- 3 Enter the name of the card image file (.GXC) to create.
- 4 Click **Import**, and the imported card image file is converted to .GXC format.

## Copying Data Between Cards and Card Image Files

You cannot copy files directly from one card to another; you must use a card image as an intermediate transport media to accomplish this.

---

**Note:**

- 1 When card files are held as card image files, you can change a file's properties after it has been created.
  - 2 When copying a file from one card to another, you can reset the file's properties, such as access conditions, number of records or file size, and file validity settings, as required for the target card.
  - 3 The copying of files should be performed only between matching corresponding card and card image types.
-



## File Copying Rules

### You can copy files:

- From a real card to a card image
- From a card image to a card
- From one card image to another card image
- Within a PC card image

### You cannot copy files:

- From one directory to another within a real card
- Directly from one real card to another. You must use a card image file as the intermediate target

---

**Caution:** If the file to be copied already exists in the same location in the target file structure, the copied file will replace the target file.

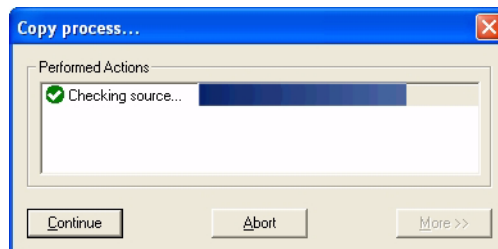
---

## Copying Files

### To copy files:

- 1 Select the file or files to be copied in the GemXplorer window. Multiple selections are allowed if the files are on the same level. Selecting a DF copies all the files located under it.
- 2 Drag and drop the selection onto the target directory. The **Copy Process** window appears as shown in “Figure 26” on page 45.

**Figure 26 - The Copy Process Window**



The copy process is performed in three steps:

- The source check
- The target check
- The file copying process

### The Source Check

This involves the following checks:

- File presence

On a card source, if the copied file is displayed in the tree structure but not physically present on the card (that is, the card was not scanned before copying), the copy process is aborted.

- Readability

If the following conditions occur:

- the file is invalidated and the “readable and updatable when invalidated” flag is set to “no”, or
- the Read access condition has not been verified or is set to NEVER,

a warning is displayed indicating that the file contents cannot be read. If you choose to continue, only the file structure is created but no content is copied.

### The Target Check

The following target checks are performed:

- Access Condition Checks

The following conditions will generate errors or warnings:

- Update or Create command access condition not met in the target DF.
- Create and/or Extend command access conditions set to NEVER in the target DF.
- For GemXplore Xpresso cards, the applet security category for the target DF must be met.
- DF Status Check
- A check is performed to see if the target DF is invalidated, in which case Create and Extend commands are not allowed.

- Source and Target Consistency Checks

The following source and target inconsistencies will generate errors or warnings:

- The copied file exists on the target but has a different file type.
- Different record sizes between the source and the target.

- Operating System Version Compatibility Check

The following operating system incompatibilities will generate errors or warnings:

- Source file is a script file and the target card is a GemXplore Xpresso or GemX8/16 card.
- Source file uses ADM 0 (10 00) as an access condition and the target card is a GemX8/16 card.
- Maximum number of DF levels exceeded on the target card.

- Cyclic File Checks

The following cyclic file conditions will generate errors or warnings:

- Decrease mode selected on the source cyclic file and the target card is a GemX8/16 or GemXplore Xpresso v1 card.
- Decrease mode selected on the source cyclic file and the target cyclic file already exists on a GemXplore 98 or GemXplore Xpresso card but with Update mode selected.

- **Memory Space Check**

A check is performed to make sure that there is sufficient memory in the target directory.

### **The File Copying Process**

For each step (that is, source check, target check and copy process), the **Copy Process** box displays a status indication, where:

- A green tick (✓) indicates that the check succeeded.
- A yellow tick (⚠) is a warning. A warning does not abort the copy process but may affect the result obtained. For example, if you try to copy a file protected by a CHV1 code, without the corresponding access rights, the copy process generates a warning indicating that it does not have the right to read the file's data. It will however allow you to copy just the structure without the data.
- 3 A red cross (✗) indicates that an error occurred. An error ends the copy process.

## **Communicating with the Card**

In GemXplorer you can send APDU commands to any of the applications on the card.

There are three methods for sending APDU commands in GemXplorer, each providing a different level of detail in the parameter settings and in the analysis of the card's response:

- A "high-level" interface is provided via the command windows available from GemXplorer's contextual menus. See "Sending Commands via the High-level Interface" that follows.
- An "intermediate-level" interface is provided via the GemXplorer file view. See "Sending Commands via the Intermediate-level Interface" on page 47.
- A "low-level" interface is provided via the **APDU Exchange** feature. See "APDU Exchange" on page 48.

---

**Note:** All the commands sent using these different interfaces can be recorded in APDU Trace Format (.ATF) script files and replayed with GemXplorer's ATF trace tool. See "Using the ATF Trace Mode to Record Commands" on page 49.

---

### **Sending Commands via the High-level Interface**

Commands are available on the contextual menus displayed by right-clicking an application in GemXplorer's Structure view. The contextual menus only display commands applicable to the business applications and services associated with the application.

For a detailed description of each command window, refer to the contextual help displayed by clicking the **Help** button in the respective command window.

### **Sending Commands via the Intermediate-level Interface**

Elementary commands such as **Update Record**, **Read Record**, **Seek** and **Increase** can be sent to elementary files on the card. In GemXplorer file view, right-click on a file and click **Elementary Command...**

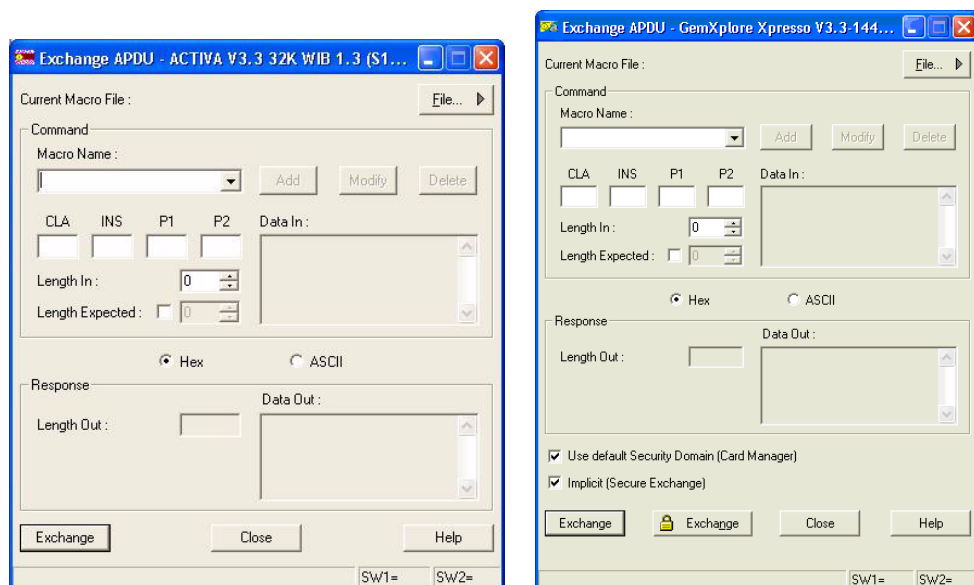
## APDU Exchange

The APDU exchange feature allows you to send any APDU command supported by an application and view the application's response. This APDU exchange tool is generic, meaning that it can be used to format any APDU command for any type of application. Compared to the high-level command interface, it provides additional flexibility in terms of parameter settings and leaves totally open the range of commands that can be sent in GemXplorer. Commands sent in an APDU exchange can also be stored as macros and re-used or modified later.

### To issue an APDU command:

- 1 For multi-application cards, ensure the target application is the selected application. Normally the core business application is usually selected by default. For example, on a GSM card, the GSM applet is normally selected by default.
- 2 Right-click on the top-level icon in GemXplorer's Structure view and choose **Exchange APDU** from the contextual menu. The **Exchange APDU** window is displayed:

**Figure 27 - Examples of Exchange APDU**



- 3 To record the parameters in an APDU macro file (\*.AMF), click **File**. You can subsequently load the parameters from this file to avoid having to re-enter the command's parameters. Select **New** to create a new macro file or select **Open** to open an existing file. By default, the previously used macro file is opened automatically.
- 4 For some cards, there is an option to choose **Use default Security Domain (Card Manager)** or the **Implicit (Secure Exchange)** from the Security domain settings file to initiate a secure channel session.
- 5 Enter the APDU command's parameters and click **Exchange**. The response and any returned data are displayed in the **Response** part of the window, and the **SW1=** and **SW2=** fields show the APDU response codes.
- 6 Enter a name for your macro in the **Macro Name** box and click **Add** to add the macro to the current APDU Macro file.

Click the **Help** button for detailed information about using the Exchange APDU window.

## Using the ATF Trace Mode to Record Commands

GemXplorer allows you to record a sequence of commands sent to the card so that they can be replayed automatically later.

This tool can be used for a number of purposes (for example, an ATF file may be used to quickly personalize test cards, or to see the details of command exchanges between GemXplorer and the card).

You can replay a task sequence in one of two modes: “single step” mode or “continuous” mode. Single step mode replays each command individually, waiting for you to prompt it to replay the next step. Continuous mode replays the recorded task sequence from beginning to end.




You can mix these two modes, for example, starting the trace in continuous mode and switching to single step mode if an error code is returned. You can then finish the trace sequence in continuous mode, or continue step-by-step.

### To create an ATF trace file:

- 1 Right-click on a top-level icon in GemXplorer’s Structure view and select **Trace**, then **Start record ATF** from the contextual menu.
- 2 Enter the name of the new trace sequence and click **Save**. The **Record ATF** window is displayed to indicate that recording has started:

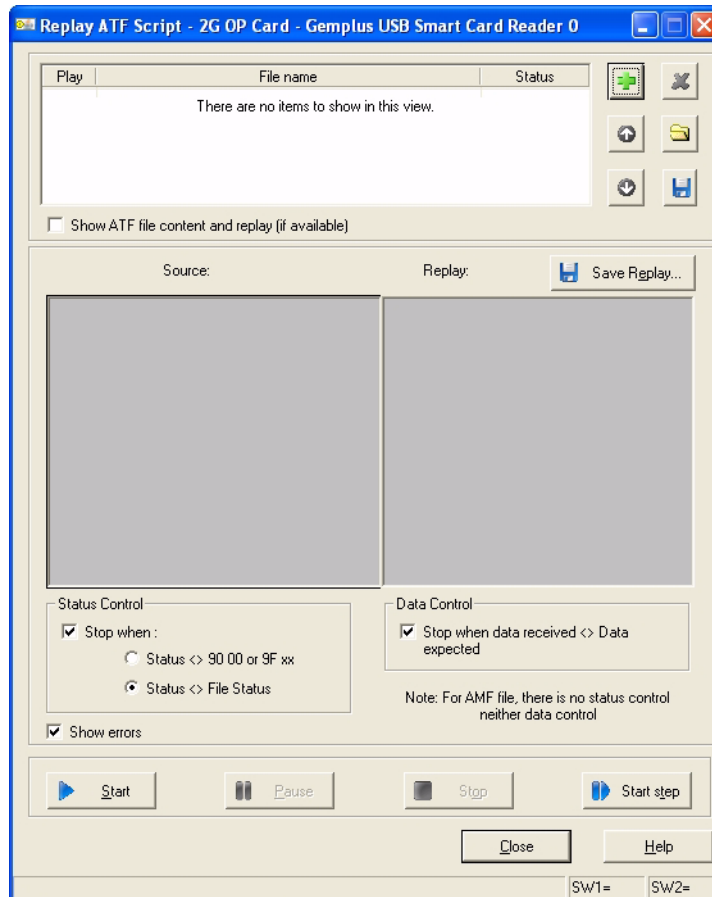
**Figure 28 - The Record ATF Window**









- 3 Perform the sequence of commands to be recorded in GemXplorer. At any time, you can:
  - Click the **Pause** button  on the Record ATF window to temporarily suspend recording. The **Record** button  flashes until the **Pause** button is pressed again to restart recording.
  - Either click the **Stop** button  on the Record ATF window to stop recording and close the trace file, or right-click in the Structure view and select **Trace**, then **Stop record ATF**.

### To replay an ATF trace file:

- 1 Right-click on a top-level icon in GemXplorer’s Structure view and select **Trace**, then **Replay ATF** from the contextual menu. The **Replay ATF Script** window is displayed.

**Figure 29 - The Replay ATF Script Window**

- 2 Click  to add an ATF file or multiple trace files (\*.atf or \*.amf) to the play list. Alternatively, click  to open a previously saved list of ATF files (\*.gal).
  - To remove ATF file(s) from the play list:  
Click on the file in the play list and click .
  - To move an ATF file up the play list:  
Click on the file in the play list and click .
  - To move an ATF file down the play list:  
Click on the file in the play list and click .
  - To save a list of ATF files:  
First add the ATF files to the play list and then click  to save them in one (\*.gal) file.
- 3 Select the **Show ATF file content and replay (if available)** option if needed.
- 4 Select any required **Status Control** settings. You can use these settings to highlight and analyze the status words returned by the card, as described below:
  - **Stop when Status <> 90 00 or 9F xx:**  
Select this option to highlight (that is, display in red) any status words which are different than 90 00 or 9F xx (successful command execution). In continuous mode, the execution of the script is stopped immediately after the command for which an incorrect status was returned.

- **Stop when Status <> File Status:**

Select this option to highlight (that is, display in red) any status words that are different from those recorded in the trace file. In continuous mode, the execution of the script is stopped immediately after the command for which an “incorrect” status was returned.

**5** Make the required **Data Control** settings.

You can use the data control settings to highlight and analyze the data returned by the card.

- **Stop when Data received <> Data expected:**

Select this option to highlight (that is, display in red) any data which are different than the data expected. In continuous mode, the execution of the script is stopped immediately after the command for which “incorrect” data was returned.

**6** Choose whether to **Show errors**.

When this option is selected, any error messages that occur while replaying the script are displayed in the right-hand column of the window.

**7** Start the trace replay.

- **Start**

Replays the trace in continuous mode.

- **Start Step**

Replays the first step of the trace.

- **Pause**

Pauses replaying of the trace.

- **Stop**

Stops the replay of the trace.





# Working in the SIM Mode

This chapter describes GemXplorer's GSM-specific features.

## Selecting the SIM applet

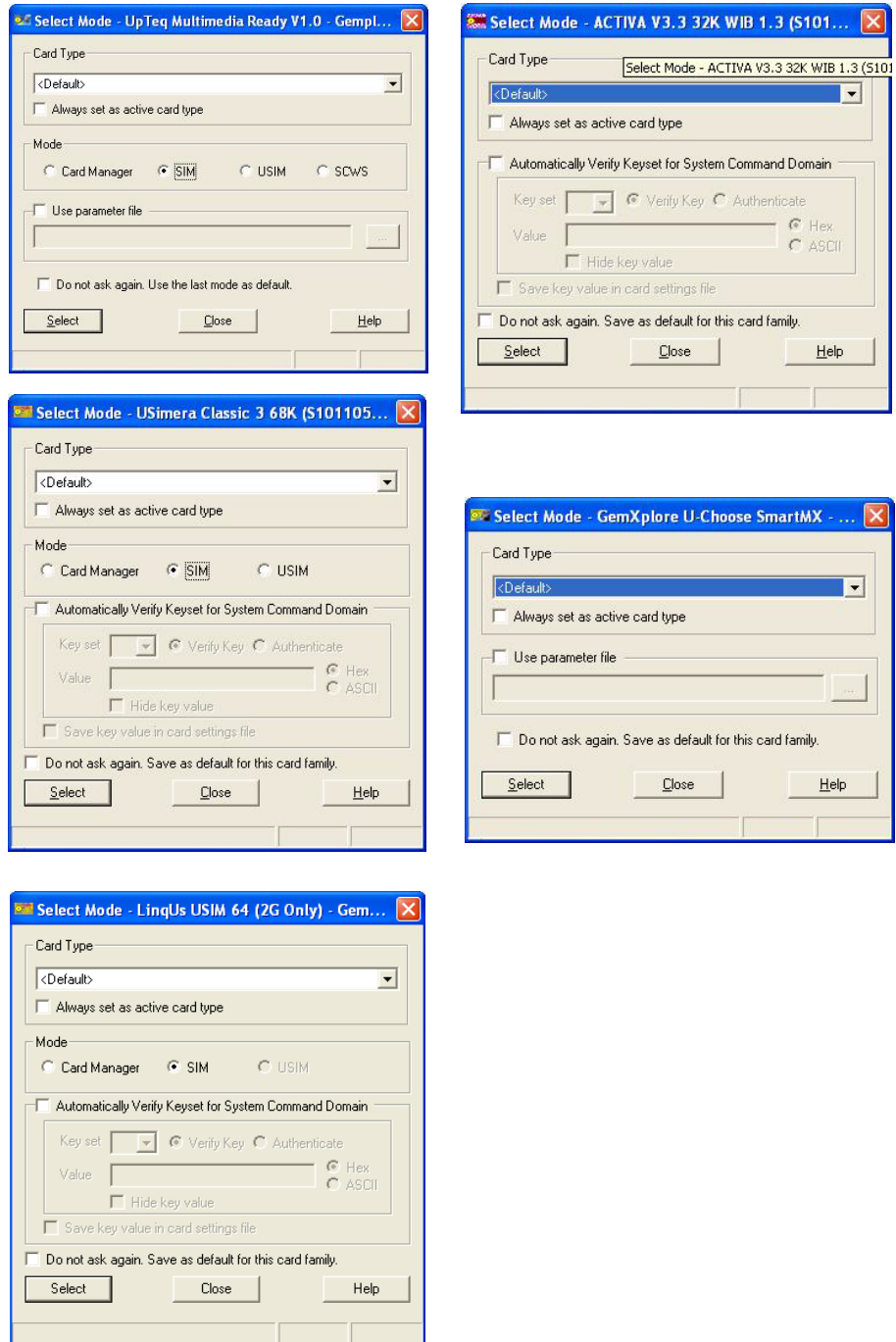
The GSM Application is always present on a card which supports GSM standard. It is responsible for managing the GSM card's file system present on the card.

---

**Note:** The SIM (GSM) mode is automatically selected for non-OP/VOP GSM cards such as GX98/U-Choose. For OP/VOP cards, you need to explicitly select the SIM mode as shown in "Figure 70 - Examples of Select Mode — Java Card" on page 128.

---

- 1 The **Card Type** list displays the types of cards associated with the ATR of the card in the reader and highlights the card type in the reader. You can change the current card type associated to the card in the reader by changing the selection from the list. The active card type is displayed as the first in the list.
- 2 To modify the active card type and set it to the card type you have selected, check the **Always set as active card type** box and Card ADMIN will then associate the card to the new card type the next time the card is inserted. You can associate more card types to an ATR via the ATR Manager.
- 1 For some cards, there is an option to use a previously saved parameter (\*.out) file by selecting the **Use parameter file** box and browse to select the file.
- 2 The **Automatically Verify Keypset for System Command Domain** option may be available depending on the cards you are working with. You may deselect it so that the key set verification for system command domain will not be automatically made.
- 3 To save the mode that you have just selected, select **Do not ask again. Save as default for this card family**. The next time you use a card from the same card family type, the Select Mode window will not appear to prompt you for a selection again.
- 4 You can check a card's default card type by accessing the Card Information window through the contextual menu of the top-level icon of the card media in the GemXplorer's Structure view.

**Figure 30 - Examples of Selecting SIM Mode**

## Browsing GSM File Systems

Refer to “Managing Card Data” on page 26 for information such as viewing the contents of a card, secret code management, viewing the contents of a file and viewing the properties of a file.

## Communicating with the Card

There are three methods for sending APDU commands in GemXplorer — a “high-level” interface is provided via the command windows available from GemXplorer’s contextual menus, an “intermediate-level” interface via the GemXplorer file view and a “low-level” interface is provided via the APDU Exchange feature. Refer to “Sending Commands via the High-level Interface” on page 47, “Sending Commands via the Intermediate-level Interface” on page 47 and “APDU Exchange” on page 48 for more information.

## GSM Commands

The GSM commands are categorized as follows:

- Secret code management commands
- File selection commands
- File Management commands

### Secret Code Management Commands

The secret code management commands enable you:

- **Verify** a secret code
- **Replace** an existing PIN or ADM secret code value by a new one.
- **Unblock** a PIN or ADM secret code that has been blocked by a given number of consecutive wrong PIN/ADM code verifications.
- **Disable** a PIN or ADM secret code. When you disable a secret code, any commands using it as an access rule will be accessible with no restriction.
- **Re-enable** a PIN or ADM secret code value which has been disabled by the **Disable** command. If you re-enable a secret code, all the commands using it as an access rule will again be restricted.

To access the Secret Code Management commands, right-click a file or directory in the GemXplorer window and select **Verify Code** from the contextual menu.

For more information about the use of the secret code management commands, click the **Help** button in the command window.

### File Selection Command

The **Select** command is used to select a file in the card’s file structure. Before handling the application data stored in an elementary file (EF), you must as a general rule first select its parent file and then the elementary file itself.

Only one directory file (DF), or one DF and an EF can be selected at a time. Selecting a new file automatically deselects the previous file.

To issue a **Select** command, right-click on the directory or file to be selected in the GemXplorer window and choose **Select** from the contextual menu.

In Card ADMIN, a MF, DF or EF can be selected by clicking the corresponding file icon located in the Structure view or the File view.

For more information about the use of the Select command, click the **Help** button in the command window.

## File Management Commands

This group of commands enables you to manage the directories and files under the GSM Application.

<b>Create</b>	Use this command to create a new file under the current directory or the root of the file system. Not all 3G cards support file creation in SIM mode. For example, only Gemalto 3G v 3.0 and GemXplore Generations Flexible cards allow files to be created in both SIM and USIM modes.
<b>Delete</b>	<p>Use this command to delete a DF, even if it is not empty, or an EF, even if it has been extended. It is possible to delete any EF and any DF (except the MF) at any time, even if this one is not the last created EF or DF, except if this file is selected by another context. A Delete DF command automatically deletes all the sub-entities within the DF. The access condition to be fulfilled is always located in the parent file of the file to be deleted. In the GemXplore Xpresso V3, the memory is recovered.</p> <p>Note: s cannot be deleted except for USimera Prime cards.</p>
<b>Invalidate</b>	Use this command to invalidate the file currently selected. Invalidating a file restricts the commands that can be applied to it.
<b>Rehabilitate</b>	Use this command to rehabilitate a file after it has been invalidated (that is, restore the use of the commands previously restricted by the <b>Invalidate</b> command). Rehabilitating a DF does not reinstate invalidated EFs inside the DF.
<b>Terminate</b>	For GemXplore Generations Flexible cards only. Use this command to change the state of the DF/EF to terminated. This action is irreversible and will make a DF/EF unusable.
<b>Terminate Card Usage</b>	For GemXplore Generations Flexible cards only. Use this command to change the state of the card to terminated. This action is irreversible and will make a card unusable.
<b>Resize</b>	Use this command to increase or reduce the size of transparent EFs or the number of records of linear fixed EFs.

For more information about the use of the commands, click the **Help** button in the command window.

## GSM Authentication

The GSM authentication is a procedure by which the SIM card is authenticated by the network. This process basically involves two steps: first, the SIM calculates a result (SRES) from a random number (challenge) sent by the network, then the network retrieves SRES from the SIM and compares it with its own result based on the same Random, where both entities use the A3 algorithm. As part of the procedure, a session key (Kc) is also created.

Card ADMIN enables you to simulate the entire authentication process as performed on the card or in the application and on the network via the easy-to-use Network Authentication Application (NAA) wizard or manually via the **Authenticate Verify** command.

### To perform a GSM network authentication using the NAA wizard:

- 1 In the GemXplorer Structure view, right-click on GSM application and select **Network Authentication Application....** The Network Authentication Application window is displayed.
- 2 Select the **assistant** mode for a step-by-step guide that will take you through EFIMSI, EFKEYOP and the Authenticate Verify command, to register the IMSI value, Key Op (Ki) value and to execute the authentication process.  
Alternatively, select the **simple subscription** mode for a one-step process to register the IMSI and Key Op values and execute the authentication process. Refer to **Help** for more information.

---

**Note:** The algorithm available via NAA is always set to XOR and is not updateable.

---

### To perform a GSM network authentication via manual input:

- 1 In the Card ADMIN Structure view, Select **DFGSM (7F 20)** and right-click **Authenticate Verify...**
- 2 In the **Verify** tab and in the **Algorithm** box, select an algorithm from the drop-down list.
- 3 Select a key in the **Key Number** box.

---

**Note:**

The key files and keys that can be used may differ depending on the smart card's operating system version. Check with your Gemalto Technical Consultant for details.

If the internal authentication key is associated with the COMP128 algorithm, the Internal Authentication command can only be run under DFGSM (7F 20h) or its child DFs.

---

- 4 If you have already saved the key value in a binary file, click **Load** to retrieve it from the disk. Otherwise, enter the secret key value in the **Key** box. To store the value in a binary file for later use, click **Save**.
- 5 Click **Random** to generate a RAND that is sent when you click Authenticate.
- 6 To have the card or application actually compute SRES and Kc, click **Authenticate**. The result of the card's calculation of these values is displayed in the Result box. If these values match the result calculated by the terminal (in this case GemXplorer), the authentication is successful.

## Put Ki

**Note:** This command is only available on Aactiva, Simera and USimera cards.

In GemXplorer, you can load new key – Ki to the card via the contextual menu. This command allows Key Ki to authenticate the card's identity to the network and it is stored in key set 16 (10h).

The following are the algorithms that are supported by the card network authentication:

- COMP128-1
- COMP128-2
- COMP128-3
- Milenage

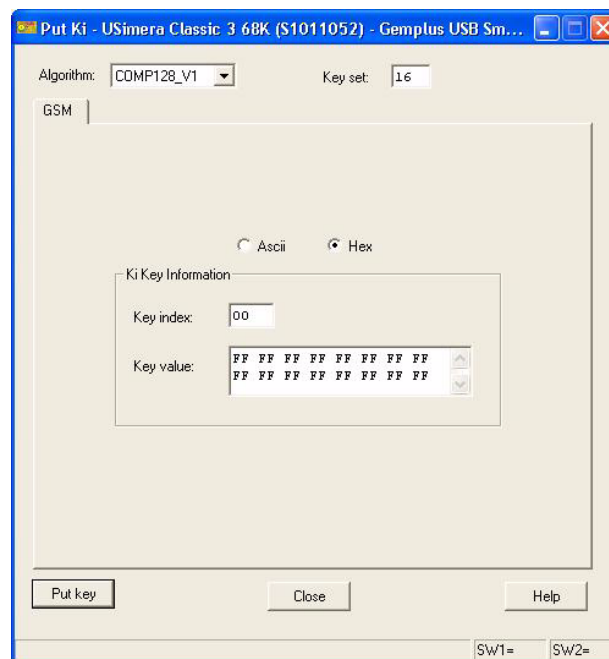
**Note:** The algorithm, Milenage, is only available on USimera cards.

**To edit the key file in GSM tab:**

**Note:** In the GemXplorer Structure view, right-click on the directory under GSM application and select **Authentication > Put Ki** from the contextual menu.

The **Put Ki** window is displayed.

**Figure 31 - Put Ki in GSM Context**



- 1 In the **Algorithm** box, select the encryption algorithm.
- 2 Enter a **Key set** value.  
This is selectable only when a USimera card is used, otherwise Key set 16 will be used.
- 3 Click to select the display mode: Hexadecimal or ASCII.
- 4 Enter the value of the key in the **Key value** field.
- 5 To have the GSM application actually updates the key set, click **Put key**. The result of the update will be displayed in the status bar at the bottom of the window.

# Working in the 3G Application Mode

This chapter describes GemXplorer's 3G-specific features.

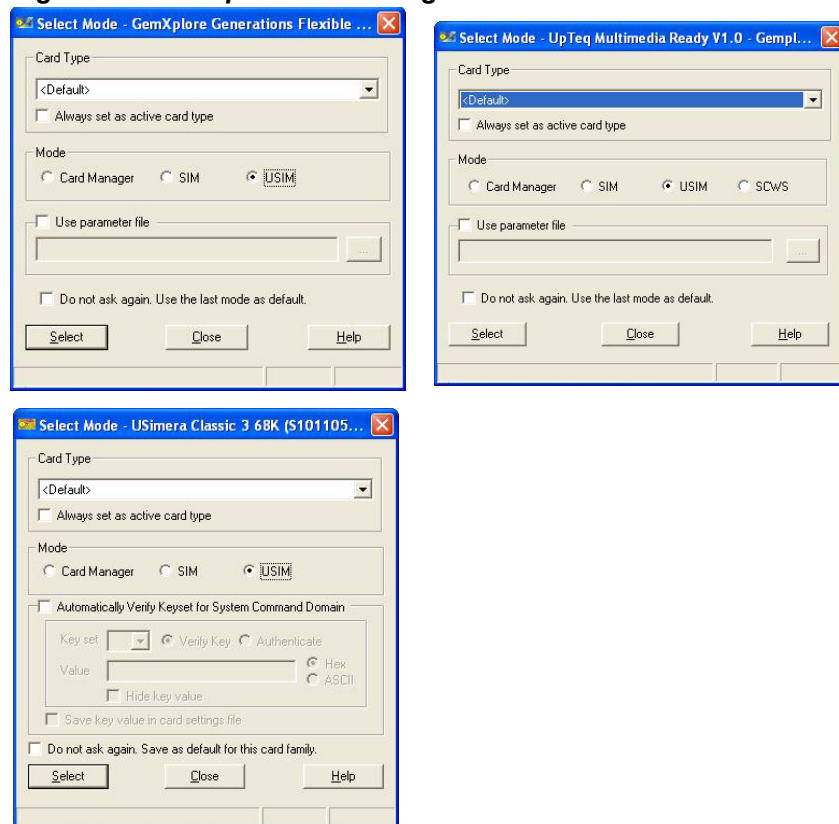
## Selecting the 3G Application

To work in the 3G mode:

- 1 Insert a 3G card in the smart card reader.

The **Select Mode** window is automatically displayed.

**Figure 32 - Examples of Selecting USIM Mode**



- 2 The **Card Type** list displays the types of cards associated with the ATR of the card in the reader and highlights the card type in the reader. You can change the current

card type associated to the card in the reader by changing the selection from the list. The active card type is displayed as the first in the list.

- 3 To modify the active card type and set it to the card type you have selected, check the **Always set as active card type** box and Card ADMIN will then associate the card to the new card type the next time the card is inserted. You can associate more card types to an ATR via the ATR Manager.
- 4 Select **USIM** to access the 3G file system and functionality.  
To save the mode that you have just selected, select **Do not ask again. Save as default for this card family**. The next time you use a card from the same card family type, the **Select Mode** window will not appear to prompt you for a selection again.
- 5 For some cards, there is an option to use a previously saved parameter (\*.out) file by selecting the **Use parameter file** box and browse to select the file.
- 6 The **Automatically Verify Keyset for System Command Domain** option may be available depending on the cards you are working with. You may deselect it so that the key set verification for system command domain will not be automatically made.
- 7 You can check a card's default card type by accessing the Card Information window through the contextual menu of the top-level icon of the card media in the GemXplorer's Structure view.

## Working with USIM applications

You can view a file's status and properties, and you can read the contents of a file. Access to files depends on:

- Whether the appropriate application has been selected, for files located in a USIM application,
- Whether or not the appropriate access rights have been acquired.

## USIM Sessions on 3G Cards

On a Universal Integrated Circuit Card (UICC), the operational 3G features associated with a given subscription are managed by a USIM application and the associated file system. There can be more than one USIM application on a card.

You must select the USIM application to activate a session with it before you can send commands and access the file system (for example, to read or update the content of a particular file on the USIM). On 3G cards, the USIMs available for selection are listed in the EFDIR file under the MF.

USIM session management may involve:

- Activating a USIM session. This is done via a **Select by AID** command.
- Terminating the USIM session. This may be done explicitly via a **Select by AID** command with the appropriate settings or implicitly by selecting another USIM application.
- Resetting the USIM application. The main effect of the session reset is that it cancels any access rights acquired during the previous session.



## USIM Session Management in GemXplorer

In GemXplorer, you can manage USIM sessions via the contextual menu, USIM List and the Select command dialog boxes.

### To manage USIM sessions via the contextual menu:

In the GemXplorer Structure view, right-click the ADF of the UICC application and select **Activation** or **Termination** accordingly.

### To manage USIM sessions via the USIM list:

- 1 In the GemXplorer Structure view, right-click the MF of the UICC application and then **Application List...**
- 2 To open a USIM session, choose the USIM in the list and click **Activation**.
- 3 You can then close the USIM session either explicitly by choosing it in the list and clicking **Termination**, or implicitly by selecting another application.

### To manage USIM sessions via the Select command

- 1 In the GemXplorer Structure view, right-click the MF or DF or ADF of the UICC application and then **Select**.
- 2 Select the **By Aid** option.
- 3 You can then activate, reset and terminate USIM sessions by:
  - a) Choosing a Selection Mode. When you choose **Only**, you can select any USIM on the UICC. In this case you must enter the USIM's full AID. When you choose **Last**, you select the last USIM selected on the UICC. In this case you need only enter the first byte(s) of the USIM's AID.
  - b) Selecting an Application Mode. Choose **Activation** to open a USIM session and **Termination** to close a USIM session.

---

**Note:** The AIDs of the USIM applications installed on the UICC are stored in the EFDIR file (2F 00h) under the MF.

---

## Default ADF Activation

In the USIM mode, the first ADF found in EFDIR is automatically activated. If you have more than one ADF in a card, you select an ADF and set it to be automatically activated, that is, set it as the '**Default Activated**'.

To do this, right-click on your selected ADF and click **Activation and Set As Default Activated...**

## 3G Commands

The 3G commands are categorized as follows:

- Secret code management commands
- File selection command
- File management commands

### Secret Code Management Commands

To access the Secret Code Management commands, right-click a directory in GemXplorer window or a file in the File view and select **Secret codes...** from the contextual menu. For more information about the use of these commands, click the **Help** button in the command window.

#### Verify PIN/CHV

This command is used to check that the cardholder or administrator knows the appropriate PIN or ADM code. When the secret code is verified, the rights attached to it are granted. If the code is incorrect, the ratification counter is decreased. When the ratification counter reaches zero, the secret code is blocked and any rights associated with it are lost.

#### Change PIN/CHV

This command is used to replace an existing PIN or ADM secret code with a new code. If the old secret code specified in the command parameters is correct, it is replaced by the new one. An incorrect specification of the secret code decrements the ratification counter. If the counter reaches 0, the secret code is blocked and any rights associated with it are lost.

#### Disable PIN/CHV

This command is used to disable a PIN or secret code after a correct code presentation. Additionally in 3G, this command allows the use of the Universal PIN to replace the disabled PIN/code, if it is activated and enabled. After the successful execution of this command and if no replacement has been done, all processes and file accesses that were conditional on entering the PIN/Secret code correctly can then be accessed freely with no restriction, and without the requirement to enter the PIN/Secret code. Otherwise, the Universal PIN has to be verified first.

#### Enable PIN/CHV

This command is used to enable a PIN or secret code which has been disabled by the Disable PIN/CHV command. On enabling a code value, all the commands using the PIN/secret code as an access condition will again be restricted.

#### Unblock PIN/CHV

This command unblocks a PIN/ADM secret code which has been blocked by a given number (N) of consecutive wrong PIN/ADM code presentations. It does this by resetting the code's ratification counter to its maximum value (N).

## File Management Commands

This group of commands enables you to manage the directories and files under the 3G Application. To access the File Management commands, right-click a directory in GemXplorer window or a file in the File view to locate the respective commands. For more information about the use of these commands, click the **Help** button in the command window.

### Create File

This command is used to create files such as the standard files ADF, DF, EF (transparent, linear, cyclic, BER-TLV or virtual) and proprietary key files (keys for Key-OP, GBA, VBS, VGCS, MUK and MSK).

---

**Note:**

- File creation of ADF is not supported in GemXplore Generations cards.
  - File creation of BER-TLV is only available for cards newer than GemXplore Generations v 1.1 card.
  - File creation of virtual is only available for USimera cards.
- 

### Extend

This command is used to extend the size of the specified elementary file (except cyclic files). The file to be extended must be a child of the current DF but not necessarily the currently selected file. To extend a file requires knowledge of a secret code that satisfies the access conditions set during file creation.

---

**Note:** This command applies to all Gemalto cards up to 3G v 2.2. It is replaced by the **Resize** command for all new cards.

---

### Delete

This command is used to delete any DFs or EFs in the file structure, including DFs/ADFs which still contain other files and EFs with extensions. However, it cannot be used to delete the MF.

---

**Note:** File deletion of ADF is currently only supported in USimera Prime cards.

---

### Lock

When this command is used in a 3G mode, it sets all the access conditions in the file to "Never".

### Deactivate/Invalidate File

This command initiates a reversible deactivation of an EF. Deactivating or invalidating a file restricts the commands that can be applied to it. When a file is deactivated or invalidated, only the Select and Activate File commands can operate on the file.

### Activate/Rehabilitate File

This command combines the file selection and reactivate mechanisms in one single command to activate a deactivated file.

**Terminate**

For GemXplore Generations Flexible cards only. Use this command to change the state of the DF/EF/ADF to terminated. This action is irreversible and will make a DF/EF/ADF unusable.

**Terminate Card Usage**

For GemXplore Generations Flexible cards only. Use this command to change the state of the card to terminated. This action is irreversible and will make a card unusable.

**Resize**

Use this command to increase or reduce the size of transparent EFs or the number of records of linear fixed EFs.

**File Selection Command****Select**

This command is used to select a MF, ADF, EF or DF.

## 3G Authentication

**Note:** The procedure described below is applicable to the 3Gv3.0 and GemXplore Generations cards. There may be some differences in other types of 3G card. Please check with a Gemalto Technical Consultant for more information.

For USimera cards, the **Put Ki** command is used to update the key value instead of EFKEYOP in the 3G network authentication.

The purpose of this procedure is for the network to authenticate the user and establish a new key between the USIM and the mobile equipment. In Card ADMIN, you can test that the USIM application is able to authenticate itself to the 3G network and vice-versa. The full authentication mechanism involves the following steps:

- the terminal or network (in this case GemXplorer) sends a random number (challenge) and authentication data to the USIM application.
- the USIM application makes a number of verifications on the received data before calculating a result (RES) from the random number.
- the terminal or network then retrieves RES from the USIM application and compares it with its own result.

The card also returns the following data with RES:

- CK: the ciphering key used to encrypt the transmission over the radio channel, calculated from the random number and the key specified in the Authenticate command parameters.
- IK: an application-specific key value, also calculated from the random number and the key specified in the Authenticate command parameters.
- KC: the key used for enciphering in a GSM access network but only if service 27 "GSM access" is available in the USIM application's UST file.

The authentication result can be divided into three cases:

- Authentication accept case: the USIM checks that XMAC = MAC and that the sequence number is correct, returns the RES, CK and IK parameters to the mobile equipment.
- MAC failure case: the USIM identifies the calculated XMAC value is different from the MAC and returns an error.
- SQN failure case: the USIM verifies that the SQN is not in the correct range, returns an authentication failure message, AUTS for re-synchronization.

In a 3G session, the algorithms supported are: 3G Dummy XOR and 3G Milenage.

**To perform a 3G network authentication using the 3G Dummy XOR algorithm for 3Gv3.0 or GemXplore Generations Flexible cards:**

- 1 In the GemXplorer Structure view, select the USIM and right-click **Activation**. Then right-click **Secret Codes > Verify GPIN1**.
- 2 In the GemXplorer File view, double-click **EFKEYOP**.
- 3 In the **Interpreted** tab, select **3G Dummy XOR** from the drop-down list in the **Algorithm** box.
- 4 For GemXplore Generations Flexible cards, in the **3G** tab, enter the **Key Value**.

*For example:*

**Key value (in hexa):** 46 5B 5C E8 B1 99 B4 9F AA 5F 0A 2E E2 38 A6 BC

- 5 In the GemXplorer Structure view, select the USIM and right-click **Authenticate...**
- 6 Select **3G Context** and then **Dummy** from the drop-down list in the **Algorithm** box.
- 7 Enter the network's **Key value**, **Random value**, **AMF** and **SQN**.

*For example:*

**Key value (in hexa):** 46 5B 5C E8 B1 99 B4 9F AA 5F 0A 2E E2 38 A6 BC

**Random value (in hexa):** 23 55 3C BE 96 37 A8 9D 21 8A E6 4D AE 47 BF35

**AMF (in hexa):** B9 B9

**SQN (in hexa):** 55 F3 2F B4 35 77

- 8 Click **Authenticate**.

The results such as RES, CK, IK or KC are returned if service 27 of the EFUST is activated.

**To perform a 3G network authentication using the 3G Milenage algorithm for 3Gv3.0:**

---

**Note:** To perform a successful authentication using the values in the example below, first update record 1 of EFSQN with "FF 9B B4 00 00 00" and record 25 with "00 00 00 00 00 00".

---

- 1 In the GemXplorer Structure view, select the USIM and right-click **Activation**. Then right-click **Secret Codes > Verify GPIN1**.
- 2 In the GemXplorer File view, double-click **EFKEYOP**.
- 3 In the **Interpreted** tab, select **Milenage** from the drop-down list in the **Algorithm identifier** box.
- 4 Select the **Key** tab, enter the **Key value** and **Key mask**.

*For example:*

**Key value (in hexa):** 46 5B 5C E8 B1 99 B4 9F AA 5F 0A 2E E2 38 A6 BC

**Key mask (in hexa):** 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

- 5 Select the **OP/OPc** tab and in the **OP/OPc indicator** box, enter 00 00 for OPc or 55 00 for OP.

*For example:*

**OPc (in hexa):** 00 00

- 6 Enter the **OP/OPc value** and **OP/OPc mask** and click **Update**.

*For example:*

**OPc value (in hexa):** CD 63 CB 71 95 4A 9F 4E 48 A5 99 4E 37 A0 2B AF

**OPc mask (in hexa):** 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

- 7 In the GemXplorer Structure view, select the USIM and right-click **Authenticate...**
- 8 Select **3G Context** and then **Milenage** from the drop-down list in the **Algorithm** box.

Select GSM Context when a USIM application is required to perform GSM authentication.

- 9 Enter the network's **Key value**, **OPC value**, **Random value**, **AMF** and **SQN**.

*For example:*

**Key value (in hexa):** 46 5B 5C E8 B1 99 B4 9F AA 5F 0A 2E E2 38 A6 BC

**OPC value (in hexa):** CD 63 CB 71 95 4A 9F 4E 48 A5 99 4E 37 A0 2B AF

**Random value (in hexa):** 23 55 3C BE 96 37 A8 9D 21 8A E6 4D AE 47 BF35

**AMF (in hexa):** B9 B9

**SQN (in hexa):** 55 F3 2F B4 35 77

- 10 Click **Authenticate**.

The results such as RES, CK, IK or KC are returned if service 27 of the EFUST is activated.

When an "incorrect AUTN" error occurs, check that the values of AMF and SQN are correctly entered.

When a synchronization error occurs, check that the input SQN is correctly entered with values higher than record 25 in EFsqn. Refer to 3GPP TS 33.102 for details.

### To perform a 3G network authentication using the 3G Milenage algorithm for GemXplore Generations Flexible card:

**Note:** To perform a successful authentication using the values in the example below, first update record 1 of EFSQN with "FF 9B B4 00 00 00" and record 25 with "00 00 00 00 00 00".

- 1 In the GemXplorer Structure view, select the USIM and right-click Activation. Then right-click Secret Codes > Verify GPIN1.
- 2 In the GemXplorer File view, double-click EFKEYOP.
- 3 In the Interpreted tab, select **Milenage** from the drop-down list in the Algorithm identifier box.
- 4 Select the **3G** tab, enter the **Key** value.

**For example:**

**Key value (in hexa):** 46 5B 5C E8 B1 99 B4 9F AA 5F 0A 2E E2 38 A6 BC

- 5 Click to select **OP** or **OPc**.
- 6 Enter the **OP/OPc** value and click **Update**.

**For example:**

**OPc value (in hexa):** CD 63 CB 71 95 4A 9F 4E 48 A5 99 4E 37 A0 2B AF

- 7 Select the **Constants** tab, enter the C1 to C5 and R1 to R5 parameters used by the 3G Milenage algorithm.

**For example:**

**C1 (in hexa):** 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

**C2 (in hexa):** 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01

**C3 (in hexa):** 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02

**C4 (in hexa):** 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04

**C5 (in hexa):** 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08

**(In decimal) R1:** 64, **R2:** 0, **R3:** 32, **R4:** 64, **R5:** 96

You may take the same C1 and R1 values as given in the following **Parameters**.

**Note:** C1 to C5 and R1 to R5 are parameters used by the 3G Milenage algorithm. Their values are specific to each operator/card and cannot be chosen arbitrarily. Hence, you must enter the correct values defined for the card you are using.

- 8 In the GemXplorer Structure view, select the USIM and right-click **Authenticate...**
- 9 Select **3G Context** and then **Milenage** from the drop-down list in the **Algorithm** box.
- 10 Click **Parameters >>** to enter the C1 to C5 and R1 to R5 values. Then click **Save** and **<< Parameters**.  
You may take the same C1 and R1 values as given in **Constants** tab.
- 11 Enter the network's Key value, OPC value, Random value, AMF and SQN.

**For example:**

**Key value (in hexa):** 46 5B 5C E8 B1 99 B4 9F AA 5F 0A 2E E2 38 A6 BC

**OPC value (in hexa):** CD 63 CB 71 95 4A 9F 4E 48 A5 99 4E 37 A0 2B AF

**Random value (in hexa):** 23 55 3C BE 96 37 A8 9D 21 8A E6 4D AE 47 BF35

**AMF (in hexa):** B9 B9

**SQN (in hexa):** 55 F3 2F B4 35 77



**12 Click Authenticate.**

The results such as RES, CK, IK or KC are returned if service 27 of the EFUS is activated.

The authentication result can be divided into three cases:

- Authentication accept case: the USIM checks that XMAC = MAC and that the sequence number is correct, returns the RES, CK, IK, and KC parameters to the ME.
- MAC failure case: the USIM identifies the calculated XMAC value is different from the MAC and returns an error.
- SQN failure case: the USIM verifies that the SQN is not in the correct range, returns an authentication failure message, AUTS for re-synchronization.

**To perform a 3G network authentication using the Network Authentication Application wizard:**

- 1 In the GemXplorer Structure view, right-click an ADF to activate it. Right-click on the selected ADF and select **Network Authentication Application...**. The Network Authentication Application window is displayed.
- 2 Select the **assistant** mode for a step-by-step guide that will take you through EFIMSI, EFKEYOP and Authenticate command, to register the IMSI value, Key Op (Ki) value and to execute the authentication process.
- 3 Alternatively, select the **simple subscription** mode for a one-step process to register the IMSI and Key Op values and execute the authentication process.

Refer to **Help** for more information.

---

**Note:** The algorithm available via NAA is Dummy XOR or Milenage and is not updateable.

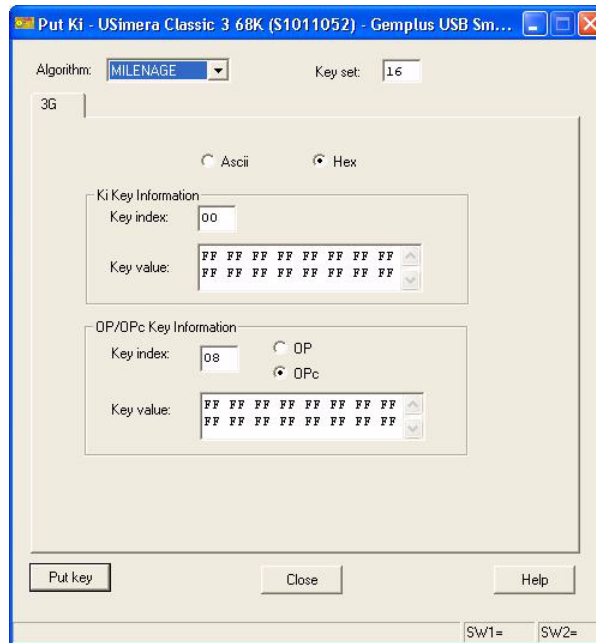
---

**Note:** The following is only available on USimera cards.

**To update the key value in the USimera Card:**

- 1 In the GemXplorer Structure view, right-click on the directory under USIM application and select **Authentication > Put Ki** from the contextual menu.  
The **Put Ki** window is displayed.

**Figure 33 - Put Ki in 3G Context**



- 2 In the **Algorithm** box, select the encryption algorithm.
- 3 Click to select the display mode: Hexadecimal or ASCII.
- 4 In the **Ki Key Information** field, enter the **Key index** and **Key value** values.
- 5 Enter the value of the key in the **Key value** field.
- 6 Click to indicate the presence of the **OP** or **OPc** value.
- 7 In the **OP/OPc Key Information** field, enter the **Key index** and **Key value** values.
- 8 Click **Put key** to update the key sets to the card.

## GBA Authentication in Bootstrapping Mode

---

### Note:

- The procedure described below is only available for 3G cards supporting GBA authentication.
  - This is also used for the ISIM application authentication.
- 

The GBA authentication in Bootstrapping Mode is used during the procedure for mutual authenticating of the USIM/ISIM application and the Bootstrapping Server Function (BSF) and for deriving the bootstrapped key material (GBA\_U) from the AKA run.

In Card ADMIN, you only test that the USIM/ISIM application is able to authenticate itself in the Bootstrapping context. The full authentication mechanism would involve the following steps:

- the terminal/network (in this case GemXplorer) sends a random number (challenge) and authentication token to the USIM/ISIM
- the USIM/ISIM makes a number of operations on the received data such as computing the anonymity key, and retrieving the sequence number SQN before calculating a result (RES) from the random number
- the terminal/network (GemXplorer) then retrieves RES from the USIM/ISIM and compares it with its own result.

The card also returns the following data with RES  $GBA\_U = CK || IK$  (CK concatenated with IK):

- CK: the ciphering key used to encrypt the transmission over the radio channel, calculated from the random number and the key specified in the Authenticate command parameters.
- IK: an application-specific key value, also calculated from the random number and the key specified in the Authenticate command parameters.

The authentication result can be divided into three cases:

- Authentication accept case: the USIM checks that  $XMAC = MAC$  and that the sequence number is correct, returns the RES and GBA\_U parameters to the mobile equipment.
- MAC failure case: the USIM identifies the calculated XMAC value is different from the MAC and returns an error.
- SQN failure case: the USIM verifies that the SQN is not in the correct range, returns an authentication failure message, AUTS for re-synchronization.

In a GBA authentication, the algorithms supported are: Dummy XOR and Milenage.

**To perform a GBA Bootstrapping authentication using the 3G Milenage algorithm for GemXplore Generations cards:**

**Note:** To perform a successful authentication using the values in the example below, first update record 1 of EFSQN with “FF 9B B4 00 00 00” and record 25 with “00 00 00 00 00 00”.

- 1 In the GemXplorer Structure view, select the USIM and right-click **Activation**. Then right-click **Secret Codes > Verify GPIN1**.
- 2 In the GemXplorer File view, double-click **EFKEY GBA**.
- 3 In the **Interpreted** tab, select **Milenage** from the drop-down list in the **Algorithm identifier** box.
- 4 Select the 3G tab and enter the **Key value**.

*For example:*

**Key value (in hexa):** 46 5B 5C E8 B1 99 B4 9F AA 5F 0A 2E E2 38 A6 BC

- 5 Click to select the **OP** or **OPc** in the **OP/OPc Information** box.

- 6 Enter the **OP/OPc value** and click **Update**.

*For example:*

**OPc value (in hexa):** CD 63 CB 71 95 4A 9F 4E 48 A5 99 4E 37 A0 2B AF

Select the **Constants** tab, enter the C1 to C5 and R1 to R5 parameters used by the 3G Milenage algorithm.

- 7 In the GemXplorer Structure view, select the USIM and right-click **Authenticate...**
- 8 Select **GBA Bootstrapping** context and click to select **Global Key** or **Application Key**. Select **GSM** context when a USIM application is required to perform GSM authentication.
- 9 Select **Milenage** from the drop-down list in the **Algorithm** box.
- 10 Click **Parameters >>** to enter the C1 to C5 and R1 to R5 values. Then click **Save** and **<< Parameters**.

*For example:*

**C1 (in hexa):** 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

**C2 (in hexa):** 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01

**C3 (in hexa):** 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02

**C4 (in hexa):** 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04

**C5 (in hexa):** 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08

**(In decimal) R1: 64, R2: 0, R3: 32, R4: 64, R5: 96**

**Note:** C1 to C5 and R1 to R5 are parameters used by the Milenage algorithm. Their values are specific to each operator/card and cannot be chosen arbitrarily. Hence, you must enter the correct values defined for the card you are using.

- 11 Enter the network's **Key value**, **OPC value**, **Random value**, **AMF** and **SQN**.

*For example:*

**Key value (in hexa):** 46 5B 5C E8 B1 99 B4 9F AA 5F 0A 2E E2 38 A6 BC

**OPC value (in hexa):** CD 63 CB 71 95 4A 9F 4E 48 A5 99 4E 37 A0 2B AF

**Random value (in hexa):** 23 55 3C BE 96 37 A8 9D 21 8A E6 4D AE 47 BF35

**AMF (in hexa):** B9 B9

**SQN (in hexa):** 55 F3 2F B4 35 77

- 12 Click **Authenticate**.

The results such as AK, MAC, RES or GBA\_U are returned if service 68 of the EFUST is activated for USIM application, or if service 2 of service EFIST is activated for ISIM application.

When an “incorrect AUTN” error occurs, check that the values of AMF and SQN are correctly entered.

When a synchronization error occurs, check that the input SQN is correctly entered with values higher than record 25 in EFSQN. Refer to 3GPP TS 33.102 for details.

---

**Note:** If you are performing an authentication in the GBA NAF derivation context, do not close the authentication viewer.

---

## GBA Authentication in NAF Derivation Mode

---

**Note:**

- The procedure described below is only available for 3G cards supporting GBA authentication.
- The GBA\_U and Random values are derived from the previous GBA Bootstrapping authentication and they are the parameters required in this context. It is mandatory to perform the GBA Bootstrapping authentication successfully at least once before making a GBA NAF Derivation authentication.
- This is also used for the ISIM application authentication.

---

The purpose of this procedure is to derive the Network Application Function (NAF) specific keys (Ks\_int\_NAF and Ks\_ext\_NAF) from the GBA\_U generated in the GBA Bootstrapping mode.

In Card ADMIN, you only test that the USIM/ISIM application is able to authenticate itself in the NAF Derivation context. The full authentication mechanism would involve the following steps:

- the terminal/network (in this case GemXplorer) sends the IMPI (IMS Private User ID), GBA\_U and Random values from the previous GBA Bootstrapping authentication and NAF\_ID to USIM/ISIM

---

**Note:** In the case of an ISIM application, the IMPI value is taken from EFIMPI under the ADF<sub>ISIM</sub>.

---

- the USIM/ISIM makes a number of verifications on the received data before deriving the Ks\_int\_NAF and Ks\_ext\_NAF from GBA\_U
- the terminal/network then retrieves Ks\_ext\_NAF from the USIM/ISIM

The authentication result can be divided into two cases:

- Authentication accept case: the USIM/ISIM stores the Ks\_int\_NAF and associated B-TID together with NAF\_ID in its memory and updates the EFGBANL.
- GBA Bootstrapping failure case: the key material is not present and returns an error.

**To perform a GBA Authentication in NAF Derivation Mode using the 3G Milenage algorithm for GemXplore Generations cards:**

The following example assumes that you have performed a successful authentication in the GBA Bootstrapping context and did not close the authentication viewer.

- 1 In the authentication viewer, select **GBA NAF Derivation** context and click to select **Global Key** or **Application Key**.
- 2 Check to verify that the GBA\_U and Random value fields are filled with the values from the successful authentication in the GBA Bootstrapping context. These values are found in the **GBA Bootstrapping** tab.
- 3 Enter the **IMS Private User Identity**.

**For example:**

**IMS Private User Identity:** *Myid@mynet.com*

---

**Note:** For ISIM application, this value is retrieved from EFIMPI.

---

- 4 In the GemXplorer File view, double-click **EFGBANL** (6F D7h). In the **Interpreted** tab, initialize a record with a 15-byte length NAF\_ID.

In the authentication viewer, enter the same **NAF\_ID** and **Length** values as you have entered in **EFGBANL**.

**For example:**

**NAF\_ID (in hexa):** *99 99 99 99 99 99 99 99 99 99 99 99 99 99 99*

**Length:** *15*

- 5 Click **Authenticate**.  
The results Ks\_ext\_NAF, Ks\_int\_NAF and their respective lengths are returned.

## VGCS/VBS Authentication

---

**Note:** The following procedure is only available for 3G cards supporting the authentication in the VGCS/VBS context only if the respective services are available:

- VGCS: services 57 and 64
  - VBS: services 58 and 65
- 

This procedure defines the Voice Group Call Service/ or the Voice Broadcast Group key to be used for group calls.

In Card ADMIN, you only test that the USIM application is able to authenticate itself in the VGCS/VBS mode. The full authentication mechanism would involve the following steps:

- USIM searches the Group\_Id that corresponds to an identifier stored in VGCS Group Identifier of EFvGCS or in VBS Group Identifier of EFvBS.
- USIM retrieves the V\_Ki corresponding to the given Group\_Id and VK\_Id.
- USIM uses V\_Ki and VSTK RAND as input parameters to derive the Short Term Key (VSTK).
- the terminal/network then retrieves VSTK from the USIM application

The card returns the Short Term Key (VSTK) associated to the Voice Group Service (VGCS)/Voice Broadcast Service (VBS) group identifier which is referenced in EFvGCS and EFvBS respectively.

The authentication result can be divided into three cases:

- Authentication accept case: the USIM checks that the VGCS/VBS group is activated and uses the selected key value (VK\_1 or VK\_2) to compute the returned VSTK.
- Key algorithm failure case: the USIM verifies that the algorithm of the key is incorrect and returns an error.

In a VGCS/VBS authentication, the algorithms supported are: Dummy XOR and Milenage.

### To perform a VGCS/VBS authentication using the 3G Milenage algorithm for GemXplore Generations cards:

**Note:** To perform a successful authentication using the values in the example below, first double-click EFKEY VGCS or EFKEY VBS to activate or create a Group ID and activate it (for example, a Group ID of 10).

- 1 In the GemXplorer Structure view, select the USIM and right-click **Activation**. Then right-click **Secret Codes > Verify GPIN1**.
- 2 In the GemXplorer File view, double-click **EFKEY VBS** or **EFKEY VGCS**.  
Note: The keys cannot be read, but you may update the information in the keys when you are doing a test.
- 3 In the **Interpreted** tab, select the group identifier (Gp ID) to be used and **Milenage** from the drop-down list in the **Algorithm identifier** box (for example, a Group ID of 10).
- 4 Click to select VK\_Id 1.
- 5 Select the 3G tab and enter the **Key value**.

**For example:**

**Key value (in hexa):** 46 5B 5C E8 B1 99 B4 9F AA 5F 0A 2E E2 38 A6 BC

- 6 Click to select the **OP** or **OPc** in the **OP/OPc Information** box.
- 7 Enter the **OP/OPc value** and click **Update**.

**For example:**

**OPc value (in hexa):** CD 63 CB 71 95 4A 9F 4E 48 A5 99 4E 37 A0 2B AF

- 8 Select the **Constants** tab, enter the C1 to C5 and R1 to R5 parameters used by the 3G Milenage algorithm.

**For example:**

**C1 (in hexa):** 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

**C2 (in hexa):** 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01

**C3 (in hexa):** 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02

**C4 (in hexa):** 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04

**C5 (in hexa):** 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08

**(In decimal) R1:** 64, **R2:** 0, **R3:** 32, **R4:** 64, **R5:** 96

- 9 Click to select VK\_Id 2 and input the same information as for VK\_Id 1 (refer to steps 3 — 8 stated above).

**Note:** The current version of GemXplore Generations Flexible cards accept an update of a group of keys only if both VK\_Id are updated.

- 10 In the GemXplorer Structure view, select the USIM and right-click **Authenticate...**
- 11 Select **VGCS/VBS** context and click to select **Global Key** or **Application Key**.
- 12 Select **Milenage** from the drop-down list in the **Algorithm** box.



- 13 Enter the network's **Key Value**, **OPc Value**, **Random value**, **Group identifier**, and select the **VGCS/VBS**, **VK\_Id** options.

*For example:*

*Key value (in hexa): 46 5B 5C E8 B1 99 B4 9F AA 5F 0A 2E E2 38 A6 BC*

*OPc value (in hexa): CD 63 CB 71 95 4A 9F 4E 48 A5 99 4E 37 A0 2B AF*

*Random value (in hexa): 23 55 3C BE 96 37 A8 9D 21 8A E6 4D AE 47 BF35*

*Group identifier: 10*

*VGCS/VBS: VGCS*

*VK\_Id: 1*

- 14 Click **Authenticate**.

The result V\_STK associated to the Voice Group Broadcast Group (VGCS) or Voice Broadcast Service (VBS) will be returned if the respective service of the EFUS is activated.

## MSK Update ( LTKM Authentication)

---

### Note:

- The procedure described below is only available for UpTeq cards supporting MSK Update (LTKM) Authentication only.
  - The GBA\_U and Ks\_int\_NAF values are derived from the previous GBA Bootstrapping authentication and they are the parameters required in this context. It is mandatory to perform the GBA Bootstrapping authentication successfully at least once before making a LTKM authentication.
- 

The purpose of this procedure is to derive the MBMS User Key (MUK) from the GBA\_U and Ks\_int\_NAF generated in the GBA Bootstrapping mode, and the smartcard key (SCK) residing in the card.

In Card ADMIN, you only test that the USIM application is able to authenticate itself in the LTKM mode to generate MUK. The full authentication mechanism would involve the following steps:

- USIM detects the presence of an MSK update message in the received MIKEY message. You may configure the settings for MIKEY message as in “Configuring MIKEY Message” on page 78.
- USIM searches the Ks\_int\_NAF that corresponds to the GBA\_U generated in the GBA Bootstrapping procedure.
- USIM uses Ks\_int\_NAF and SCK as input parameters to derive the MUK.
- the terminal/network then retrieves MUK from the USIM application and establishes the mobile TV connection.

The card returns the MUK ID and checks if a new NAF derivation procedure is performed with the received MUK ID and that it corresponds to the one generated in the previous bootstrapping procedure.

The authentication result can be divided into two cases:

- Authentication accept case: the USIM returns 98 65h.
- Authentication failure case: the USIM verifies that the MUK ID is incorrect and returns an error.

### Configuring MIKEY Message

The MIKEY Interpreter allows you to configure the parameters to set up a secure multimedia session using the multimedia internet keying (MIKEY) protocol for real-time applications that are used between the service provider and the card. MIKEY is a key management protocol which is used to set up encryption keys using SRTP as defined in RFC 3830.

To access this function, in the GemXplorer Structure view under ADFUSIM, right-click **Authenticate** and select the MSK Update (LTKM) context. Click **Generate** to access the MIKEY Interpreter. The MIKEY Interpreter window contains the ten tabs that are configurable in USIM:

- HDR
 

This is the header of the MIKEY protocol, also known as the common header payload (HDR), which is necessary as the first payload for each message. Each HDR consists of a MIKEY crypto session bundle (CSB ID) related data and general description of the message.

- EXT\_MBMS

In cases where a card receives a MIKEY message containing a MTK and the presence of General Extension payload is detected with no presence of EXT\_BCAST, the MIKEY message is assumed to be an MBMS MTK message. The LTKM is then processed from the card.

- EXT\_BCAST

An MIKEY message is considered as a BCAST LTKM if the MIKEY message includes contains a General Extension payload of Type 5. The EXT\_BCAST is defined in the LTKM to protect the streaming contents over the interactive channel.

- TS

Timestamp Payload (TS) allows you to track and synchronize the time set for a specific incoming payload against the subscription period to prevent replay attacks between the terminals over the network.

- RAND

A 16-byte pseudo(random) number which is generated per CSB and is also used during the MTK Generation mode to generate MBMS Traffic Key (MTK).

- IDi

Security parameter of a payload in key management which corresponds to the value in Ks\_int\_NAF.

- IDr

Security parameter of a payload in key management which corresponds to the value in GBA Bootstrapping Transaction Identifier (B-TID) and IMS Private User ID (IMPI) value.

- SP

Contains a set of policies that apply to a specific security protocol in this payload.

- KEMAC

The key data transport payload (KEMAC) contains a set of encrypted sub-payloads to authenticate a user. This is to protect the distribution rights of the contents providers. Each of the payload may contain one or more key data payloads such as TGK. The entire KEMAC is encrypted with the encryption key and the MAC is created using the authentication key.

- Ver

Contains the calculated verification message from the pre-shared key and the public-key transport methods transmitted by the content provider.

For a detailed description of each setting, refer to the contextual help displayed by clicking the **Help** button in the respective tab.

**To perform a LTKM authentication for UpTeq cards:**

---

**Note:** To perform a successful LTKM authentication, a bootstrapping procedure must first be generated.

---

- 1** In the GemXplorer Structure view, select the USIM and right-click **Authenticate**.
- 2** Select **MSK Update** context and click to select **Global Key** or **Application Key**. Click to select **Global Key** or **Application Key** for verification. Depending on the type of key selected, this key value will either be filled with the values taken from the key file stored in the application or the global key file located under the MF.
- 3** In the **MIKEY** field, you can either enter the MIKEY value or retrieve it from the MIKEY Interpreter via **Generate**.
- 4** Click **Authenticate**.

98 65h is returned if service 69 of the EFUS is activated for USIM application.

When an incorrect authentication error occurs, check that the values of MUK ID and MIKEY are correctly entered.

## MTK Generation (STKM Authentication)

---

### Note:

- The procedure described below is only available for UpTeq cards supporting MTK Generation (LTKM) Authentication only.
  - The MSK ID and MTK values from the received MIKEY message are the parameters required in this context. It is mandatory to retrieve the MSK before performing a STKM authentication.
- 

The purpose of this procedure is to perform a MBMS Service key (MSK) validation and derivation using the MSK Key Domain ID and the MSK ID from the MIKEY message to derive a temporary key to connect to the Mobile TV service on a pay-per-view basis.

In Card ADMIN, you only test that the USIM application is able to authenticate itself in the STKM mode to generate MBMS Traffic Key (MTK). The full authentication mechanism would involve the following steps:

- USIM detects the presence of an MUK ID in the received MIKEY message. You may configure the settings for MIKEY message as in “Configuring MIKEY Message” on page 78.
- USIM uses MUK values as input parameters to derive a temporary key.
- USIM checks the presence of an MBMS Traffic Key (MTK) and a Salt key in the received MIKEY message.
- USIM performs an MBMS Generation and Validation Function if MBMS Traffic Key (MTK) and a Salt key are present.

The card returns the MUK ID and checks if a new NAF derivation procedure is performed with the received MUK ID and that it corresponds to the one generated in the previous bootstrapping procedure.

The authentication result can be divided into two cases:

- Authentication accept case: the USIM returns 90 00h.
- Authentication failure case: the USIM verifies that the MSK is incorrect and returns an error, 98 62h.

### Configuring MIKEY Message

The MIKEY Interpreter allows you to configure the parameters to set up a secure multimedia session using the multimedia internet keying (MIKEY) protocol for real-time applications that are used between the service provider and the card. MIKEY is a key management protocol which is used to set up encryption keys using SRTP as defined in RFC 3830.

To access this function, in the GemXplorer Structure view under ADFUSIM, right-click **Authenticate** and select the MTK Generation (STKM) context. Click **Generate** to access the MIKEY Interpreter. The MIKEY Interpreter window contains the nine tabs that are configurable in USIM:

- HDR

This is the header of the MIKEY protocol, also known as the common header payload (HDR), which is necessary as the first payload for each message. Each HDR consists of a MIKEY crypto session bundle (CSB ID) related data and general description of the message.

- EXT\_MBMS

In cases where a card receives a MIKEY message containing a MTK and the presence of General Extension payload is detected with no presence of EXT\_BCAST, the MIKEY message is assumed to be an MBMS MTK message. The STKM is then processed from the card.

- EXT\_BCAST

An MIKEY message is considered as a BCAST STKM if the MIKEY message includes the EXT MBMS payload (indicating MTK delivery) and the EXT BCAST payload. The EXT\_BCAST is defined in the STKM to protect the streaming contents over the interactive channel.

- TS

Timestamp Payload (TS) allows you to track and synchronize the time set for a specific incoming payload against the subscription period to prevent replay attacks between the terminals over the network.

- RAND

A 16-byte pseudo(random) number which is generated per CSB and is also used during the MTK Generation mode to generate MBMS Traffic Key (MTK).

- IDi

Security parameter of a payload in key management which corresponds to the value in Ks\_int\_NAF.

- IDr

Security parameter of a payload in key management which corresponds to the value in GBA Bootstrapping Transaction Identifier (B-TID) and IMS Private User ID (IMPI) value.

- SP

Contains a set of policies that apply to a specific security protocol in this payload.

- KEMAC

The key data transport payload (KEMAC) contains a set of encrypted sub-payloads to authenticate a user. This is to protect the distribution rights of the contents providers. Each of the payload may contain one or more key data payloads such as TGK. The entire KEMAC is encrypted with the encryption key and the MAC is created using the authentication key.

For a detailed description of each setting, refer to the contextual help displayed by clicking the **Help** button in the respective tab.

### To perform a STKM authentication for UpTeq cards:

---

**Note:** To perform a successful STKM authentication, a bootstrapping procedure must first be generated.

---

- 1 In the GemXplorer Structure view, select the USIM and right-click **Authenticate**.
- 2 Select **MTK Generation** context and click to select **Global Key** or **Application Key**. Click to select **Global Key** or **Application Key** for verification. Depending on the type of key selected, this key value will either be filled with the values taken from the key file stored in the application or the global key file located under the MF.
- 3 In the **MIKEY** field, you can either enter the MIKEY value or retrieve it from the MIKEY Interpreter via **Generate**.

4 Click **Authenticate**.

90 00h is returned if service 69 of the EFUS is activated for USIM application.

If the USIM detects that the given MTK ID is invalid, a SEQp freshness failure occurs and the USIM aborts the function. 98 65h is returned indicating a key freshness failure.

If the integrity validation of the MIKEY message is unsuccessful, the USIM aborts the function and returns 98 62h indicating an authentication error with incorrect MAC.

## MUK/MSK Key Deletion

Values stored in the specific records of EFMSK or EFMUK can be cleared using the **MUK/MSK Key Deletion** command.

**To clear a record in EFMSK:**

- 1 In the GemXplorer Structure view, select the USIM and right-click **Authenticate**.
- 2 Select **MUK/MSK Key Deletion** context and click **MSK Deletion** check box to enable record deletion for EFMSK.
- 3 Enter the **Key Domain ID** and the **Key Group** to be cleared.
- 4 Click **Authenticate**.

**To clear a record in EFMUK:**

- 1 In the GemXplorer Structure view, select the USIM and right-click **Authenticate**.
- 2 Select **MUK/MSK Key Deletion** context and click **MUK Deletion** check box to enable record deletion for EFMUK.
- 3 Select to enter the value either in hexadecimal or in ASCII, and enter the **IMS User Identity** and the **NAF ID** to be cleared.
- 4 Click **Authenticate**.

## Authentication Related Files

### Voice Broadcast Service Ciphering Algorithm (VBSCA)

EFVBSCA (6F D5h) is a transparent file and contains the ciphering algorithm identifiers for each of the Master Group Key (V\_Ki) of every VBS group that the user subscribed to. Each Master Group Key consists of two keys: 1st V\_Ki and 2nd V\_Ki.

Please refer to 3GPP TS 31.102 for more details.

### Voice Group Call Service Ciphering Algorithm (VGCSCA)

EFVGCSCA (6F D4h) is a transparent file and contains the ciphering algorithm identifiers for each of the Master Group Key (V\_Ki) of every VGCS group that the user subscribed to. Each Master Group Key consists of two keys: 1st V\_Ki and 2nd V\_Ki.

Please refer to 3GPP TS 31.102 for more details.

### GBA Bootstrapping Parameters (GBABP)

EFGBABP (6F D6h) is a transparent file and contains the parameters for AKA random challenge (RAND) and GBA Bootstrapping Transaction Identifier (B-TID) which are needed in the GBA procedure.

### GBA Network Application Function List (GBANL)

EFGBANL (6F DAh) is a transparent file and contains the list of NAF\_ID and B-TID associated to the NAF derivation procedure.



## Phone Book Management

A phone book is a set of entries, with each entry being made up of several pieces of information, for example, a name, a telephone number, a group, and an email address. These various pieces of information are not stored in a single file, but instead are spread across several phone book files. It is only when the individual pieces of information contained in the various files are brought together that a complete entry is formed, and only when all the entries are brought together that a phone book is formed.

The method by which the information in these files is brought together depends on the information in the phone book reference file (EFPBR). The structure of the phone book reference file is presented in “Phone Book Reference file (PBR)” on page 86 and “File Linking” on page 95.

There may be more than one phone book on the UICC. The global phone book, which always exists, is contained in the DFPHONEBOOK directory which is under DFTELECOM under the master file. Each USIM application may have a local phone book contained in the DFPHONEBOOK located under its respective Application Directory ADFUSIM. Each application-specific phone book is protected by the application PIN. Information held in different phone books is never merged.

### Phone Book Files

The organization of files in DFPHONEBOOK under ADFUSIM and under DFTELECOM follows the same rules. The files that may contribute information to a phone book entry for a local phone book are:

- Phone Book Reference file (PBR) - 4F 30h
- Abbreviated Dialing Numbers file (ADN) - 4F XXh
- Extension 1 file (EXT1) - 4F XXh
- Index Administration Phone book file (IAP) - 4F XXh
- Second Name Entry file (SNE) - 4F XXh
- Additional Number file (ANR) - 4F XXh
- Additional number Alpha String file (AAS) - 4F XXh
- Grouping file (GRP) - 4F XXh
- Grouping information Alpha String file (GAS) - 4F XXh
- Email address file (EMAIL) - 4F XXh
- Phone Book Control file (PBC) - 4F XXh
- Capability Configuration Parameters 1 file (CCP1) - 4F XXh
- Unique Identifier file (UID) - 4F XXh
- Phone Book Synchronization Counter (PSC) - 4F 22h
- Change Counter (CC) - 4F 23h
- Previous Unique Identifier (PUID) - 4F 24h

---

**Note:** File identifiers in this document that differ from the above values use as reference the example phone book from 3GPP TS 31.102. On the card, the last two digits of the file identifier (marked XXh above) are personalized by the card provider.

The files EFUID, EFPSC, EFCC and EFPUID concerned with synchronization are conditional. If synchronization is supported by the phone book, then EFPSC, EFCC and EFPUID are mandatory.

---

To create a phone book you need to enter information into some or all of these files and you have to establish their linking relationships in EFPBR. See “File Linking” on page 95 for information on this. All of the files if present are located in the DFPHONEBOOK directory, either under DFTELECOM or under individual USIM applications.

**Note:** In order to access phone book files under a USIM application, you must first select the USIM application.

Having modified the contents of a file, click **Update** in the file’s viewer to write the data to the card. A brief overview of each file is given in the following pages. See each file’s contextual help in GemXplorer for more information.

## Phone Book Reference file (PBR)

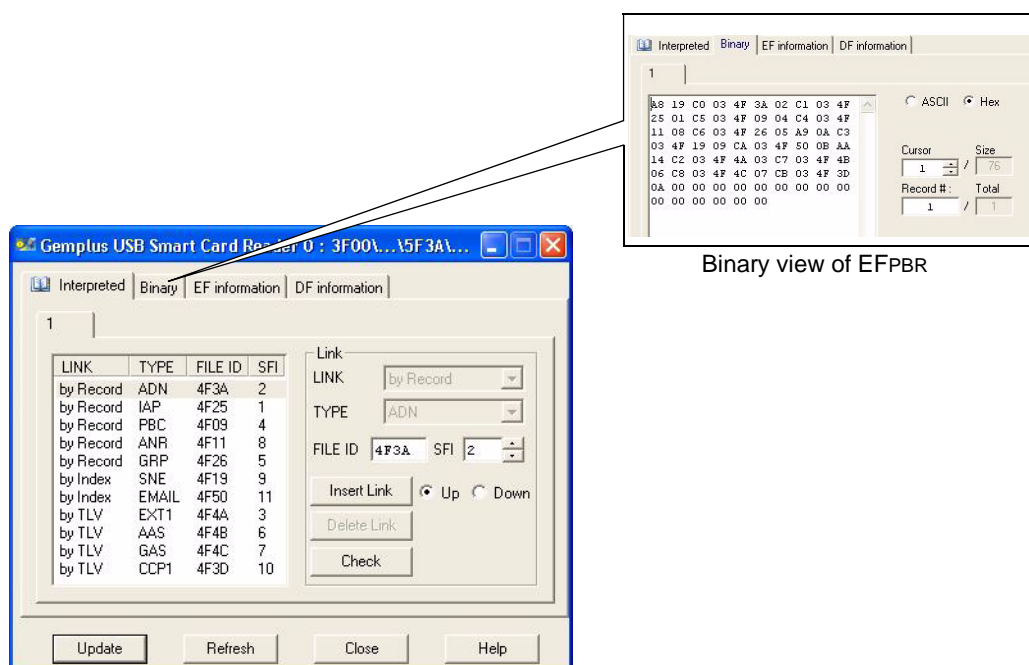
**Note:** You can define your own phone book structure. If your structure is different from the one presented in this *Card ADMIN Getting Started* document, please contact a Gemalto Technical Consultant for assistance and for more information.

EFPBR (4F 30h) defines the structure of the phone book from three aspects:

- **As a container.** It stores the different TLV objects that define the way a record in a phone book file is used to create a complete entry in the phone book.
- **As a switch.** It defines the method of linking an entry in the phone book to its information (for example, its dialing number or email address).
- **As an identifier.** It specifies the file identifiers (FIDs) personalized by the card provider for all files that contribute information to the phone book.

One record in EFPBR can define the structure of up to 254 entries in the phone book. The entry structure is the same for all records in EFPBR. If more than 254 entries are to be stored, a second record is needed.

**Figure 34 - Phone Book Reference File (PBR)**



“Figure 34” shows an example EFPBR, both the interpreted and binary view. In the interpreted view **Link** determines the linking mechanism for the file selected in **Type**. In the binary view we can see the TLV data objects which enable combining the data in different files to make a complete entry in the phone book.

In EFPBR there are two types of TLVs, constructed tag TLVs and primitive tag TLVs. Primitive tag TLVs nest inside constructed ones and use the tags numbered from C0h to CBh (see Table 2, “Primitive Tag Values”, on page 96 for a list of the file types associated to these primitive tags). Constructed tag TLVs determine the type of link, whereas primitive tag TLVs are constituted so that their tag (C0, C1, and so on) determines the file types (EFADN, EFSNE, and so on) and the value field determines the file ID (4F 3A, 4F 19, and so on). These file IDs can vary according to the personalization of the card. If we examine the binary view taken from the example EFPBR in “Figure 34” on page 86:

```

A8 0F C0 03 4F 3A 02 C1 03 4F
25 07 C6 03 4F 26 03 A9 0A C3
03 4F 19 05 CA 03 4F 50 06 AA
05 C3 03 4F 4C 04 FF

```

Tags A8h, A9h and AAh head the three constructed tag TLVs used in EFPBR. They designate which of the three link types are used by the files whose primitive tag is nested within the constructed tag's TLV. The only exception is the first primitive tag TLV after tag A8, which always designates the master EF (EFADN, 4F 3Ah in the above example).

Files are linked in three ways:

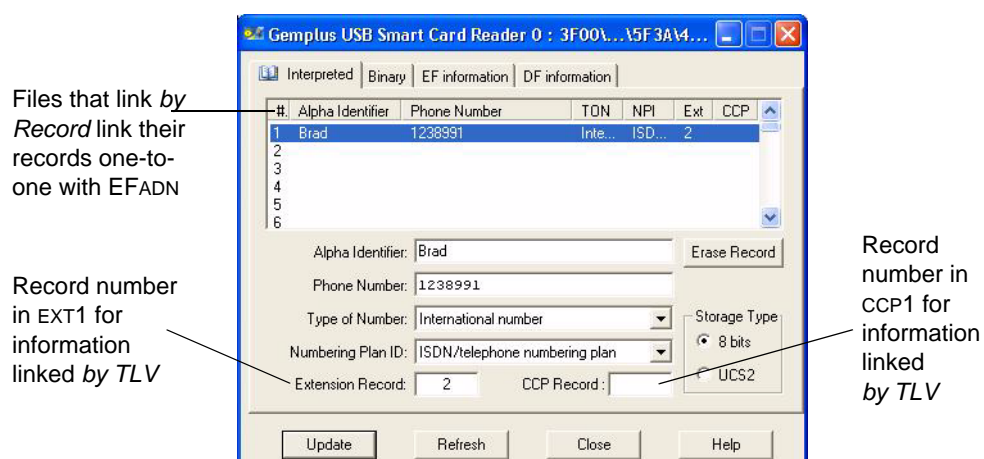
- *by Record* with tag A8h. There is a one-to-one linking between records in the file and records in EFADN.
- *by Index* with tag A9h. A file uses a pointer in EFIAP to reference a particular record in another file.
- *by TLV* with tag AAh. A file uses the structure of EFPBR to reference a particular record in another file.

For information on file linking and these TLV data objects, see “File Linking” on page 95.

### Abbreviated Dialing Numbers file (ADN)

This file contains the name and telephone number of the correspondent, as well as other dialing information. For the purposes of file linking, this file is the master EF. EFEXT1 is linked to EFADN *by TLV*. This file is always present if DFPHONEBOOK exists.

**Figure 35 - Abbreviated Dialing Numbers (ADN)**



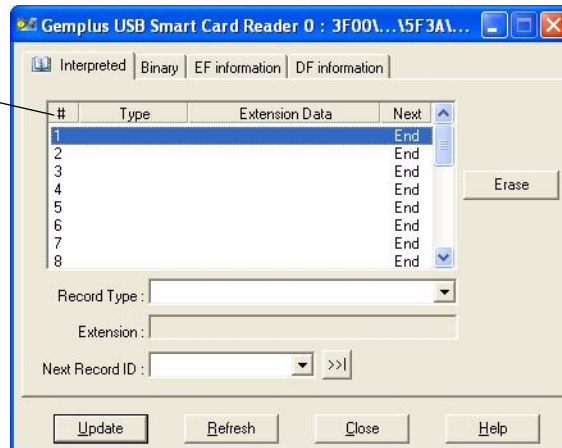
### Extension 1 file (EXT1)

This file contains extension data for the records in EFADN. Extension data is required when the 20 digit capacity of a record in EFADN is exceeded. This file is linked to EFADN by TLV.

This file is always present if DFPHONEBOOK exists.

**Figure 36 - Extension 1 (EXT1)**

The extension 1 record identifier byte in EFADN and EFANR indicates which record number holds extension information



### Index Administration Phone book file (IAP)

EFIAP is linked *by Record* to EFADN and contains pointers to records in the files linked *by Index*. Its presence in the phone book (mandatory if tag **A9** is indicated in EFPBR) means linking *by Index* is possible. For more information see “File Linking” on page 95.

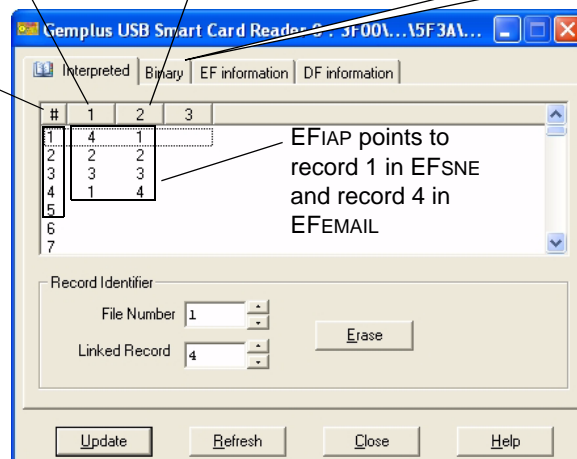
In the binary view of EFPBR (see “Figure 34” on page 86), we can see that the primitive tag TLVs, referenced after the constructed tag A9h, are C3h and CAh respectively. Referring to the list of primitive tag types (see Table 2, “Primitive Tag Values”, on page 96) determines that EFSNE is the first file in EFPBR listed after tag A9h and that EFEMAIL is the second. Thus each record in EFIAP in this example contains two pointers, one for each file. If a third file were present after tag A9h in EFPBR, three pointers would be present.

**Figure 37 - Index Administration Phone Book (IAP)**

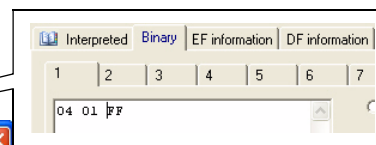
Pointer 1: EFSNE (using the example in “Figure 34”)

Pointer 2: EFEMAIL (using the example in “Figure 34”)

EFIAP records linked one-to-one with EFADN



EFIAP points to record 1 in EFSNE and record 4 in EFEMAIL



Binary view of record 4 of EFIAP

In this example, binary data for record 4 of EFiAP is 01 04. This means EFiAP links the forth entry in EFADN to a second name entry in EFSNE, and that this second name is contained in record 1 of EFSNE. It also means EFiAP links the forth entry in EFADN to an email entry in EFEMAIL, and that the email address is contained in record 4 of EFEMAIL.

## Second Name Entry file (SNE)

This file contains optional second name entries which may be attached to phone book entries.

**Note:** Each phone book entry links to a different record in EFSNE: records cannot be shared, even if the second name is the same for several phone book entries.

The records in this file may be linked one-to-one with records in EFADN (*by Record*), or the records may be linked via pointers in EFiAP (*by Index*).

The number of second name entries may be less than or equal to the number of records in EFADN. Additional numbers for an entry require additional EFSNE files.

For the example shown in “Figure 34”, the file list shows EFSNE is linked *by Index*. This means the data in a record in EFSNE is pointed to by EFiAP. When linking *by Index*, matching the data to the phone book entry always depends on the master EF, so EFiAP is linked record to record with EFADN. Taking the example of “Figure 35” on page 87 where record 1 indicates the alpha identifier “Brad”, we see record 1 in EFiAP has two pointers. The first pointer applies to EFSNE and indicates that record 4 in EFSNE contains the second name for this entry in EFADN. Thus the second name entry must be “Wylie”.

**Figure 38 - Second Name Entry (SNE)**

Files that link by *Record* link their records one-to-one with EFADN

#	Alpha Identifier	Phone Number	TON	NPI	Ext	CCP
1	Brad	1238991	Inte...	ISD...	2	
2						
3						
4						
5						
6						

Alpha Identifier: Brad  
 Phone Number: 1238991  
 Type of Number: International number  
 Numbering Plan ID: ISDN/telephone numbering plan  
 Extension Record: 2  
 CCP Record:   
 Storage Type:   
☒ 8 bits  
☐ UCS2

Following all the examples through in a similar manner would give these names: “John” “Dixon”, “Dominic” “Harris” and “Nigel” “Parker”. See “Figure 49” on page 102 for the global view.

See “File Linking” on page 95 for more information on file linking methods.

**Note:** When linking *by Record*, the fields **ADN file SFI** and **ADN Record ID** are not used because files link record-to-record. When linking *by Index*, the file ID of the master EF and the record number of the entry are mandatory.

## Additional Number file (ANR)

This file contains optional additional numbers which may be attached to phone book entries, for example, a fax number, or a fixed telephone number.

**Note:** Each phone book entry links to a different record in EFANR: records cannot be shared, even if the additional number is the same for several phone book entries.

The records in this file may be linked one-to-one with records in EFADN (*by Record*), or they may be linked via pointers in EFIAP (*by Index*). The linking mechanism is identical to that described in “Second Name Entry file (SNE)” on page 89.

The number of additional number entries may be less than or equal to the number of records in EFADN. Additional numbers for an entry require additional EFANR files.

**Figure 39 - Additional Number (ANR)**

Records here are referenced by a pointer in EFIAP (*by Index*), or they are linked one-to-one with EFADN (*by Record*)

Sets the record number in EFAAS which contains the alpha string name for the additional dialing number

Record number in EXT1 for information linked *by TLV*

Record number in CCP1 for information linked *by TLV*

### Additional Number (ANR)

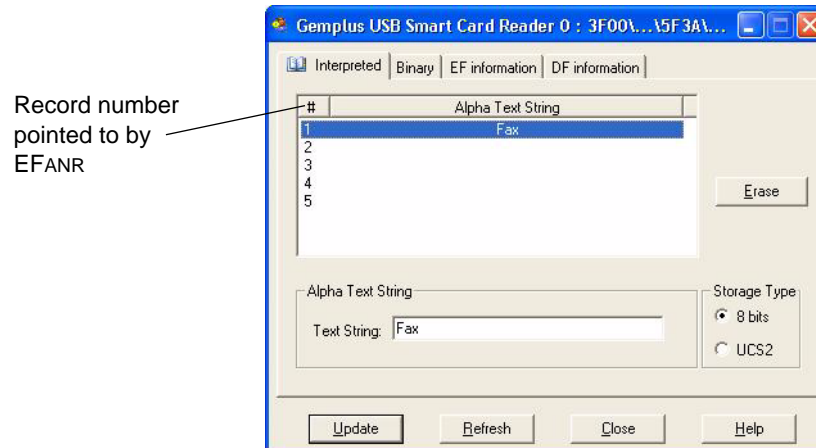
When there is a name associated to the additional number (for example, FAX), the Additional Number identifier byte indicates which record number in EFAAS contains the name. Set the record in the **Add Number ID** spin box.

**Note:** When linking *by Record*, the fields **ADN file SFI** and **ADN Record ID** are not used because files link record-to-record. When linking *by Index*, the file ID of the master EF and the record number of the entry are mandatory.

## Additional number Alpha String file (AAS)

This file contains the names given to the additional number entries referenced in EFANR and is linked to EFANR *by TLV*. See “File Linking” on page 95 for more information on this linking method.

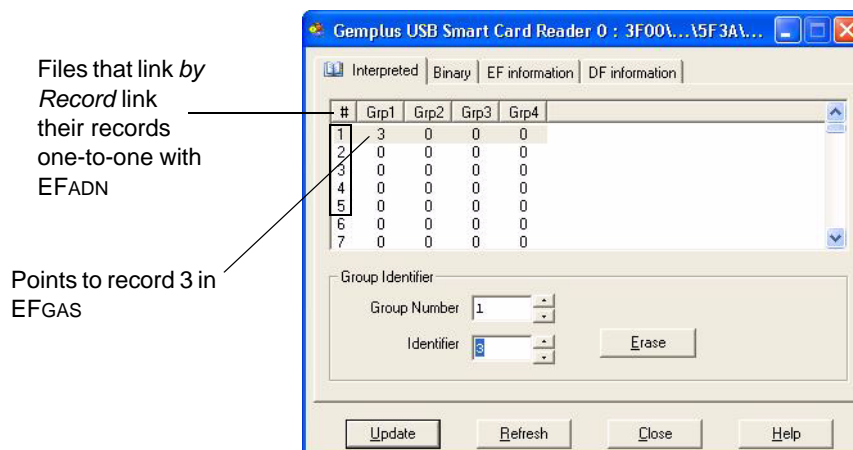


**Figure 40 - Additional Number (AAS)**

### Grouping file (GRP)

This file contains grouping information for each phone book entry. Records in EFGRP contain group identifiers that correspond to group names stored in EFGAS. Each record in EFGAS contains the name of a group to which an entry can belong. An entry can be a member of up to ten groups.

EFGRP is linked to EFADN *by Record*. See “File Linking” on page 95 for more information on this linking method.

**Figure 41 - Grouping File (GRP)**

Referring to “Figure 41”, record 1 in EFGRP points to the alpha text string contained in record 3 of EFGAS. Thus “Brad” is a member of “Friends” (see the example in “Grouping information Alpha String file (GAS)” on page 91).

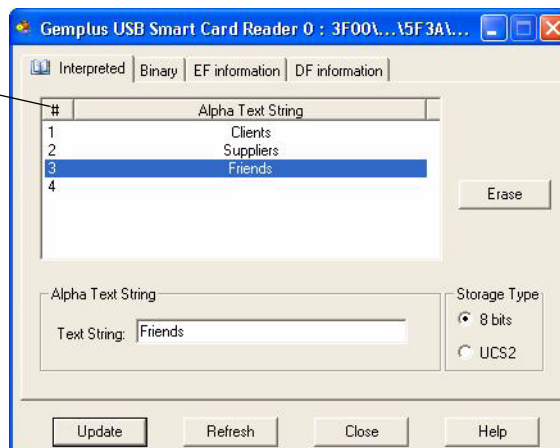
**Note:** In this example, a phone book entry can be a member of five different groups. The number of group columns is decided in the file creation process. If there were more **Grp** columns (**Grp6**, **Grp7**, and so on), entries would be able to belong to more groups. The number of **Grp** columns determines the number of groups to which an entry can belong, up to a maximum of 10.

### Grouping information Alpha String file (GAS)

This file contains the names given to the groups referenced in EFGRP and is linked to EFGRP *by TLV*. See “File Linking” on page 95 for more information on this linking method.

**Figure 42 - Grouping Information Alpha String File (GAS)**

Record number pointed to by EFGRP



Referring to “Figure 35 - Abbreviated Dialing Numbers (ADN)”, “Figure 41 - Grouping File (GRP)” and “Figure 42 - Grouping Information Alpha String File (GAS)”, *Brad* is a member of *Friends*, *John* is a member of *Clients*, *Dominic* is not a member of a group, and *Nigel* is a member of *Clients*. No-one is a member of *Suppliers*. See “Figure 49 - Phone Book Interpreter” on page 102, under **Grp1** for an illustration of this.

### Email address file (EMAIL)

This file contains optional email addresses, which may be attached to phone book entries.

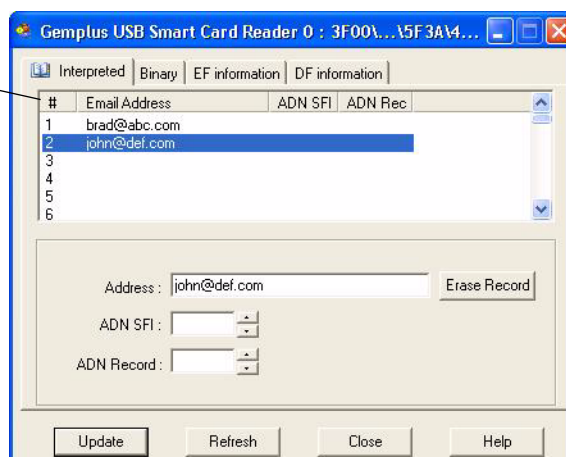
**Note:** Each phone book entry links to a different record in EFEMAIL: records cannot be shared, even if the email address is the same for several phone book entries.

The records in this file may be linked one-to-one with records in EFADN (*by Record*), or the records may be linked to EFADN via pointers in EFIAP (*by Index*). For the example shown in “Figure 34”, the records are linked to EFADN via pointers in EFIAP. The linking mechanism is identical to the one described in “Second Name Entry file (SNE)” on page 89. “Figure 37” shows how the pointers have been set up for this example.

The number of email addresses may be less than or equal to the number of records in EFADN. Additional email addresses for an entry require additional EFEMAIL files.

**Figure 43 - Email Address File (EMAIL)**

Record numbers pointed to by Pointer 2 in EFIAP



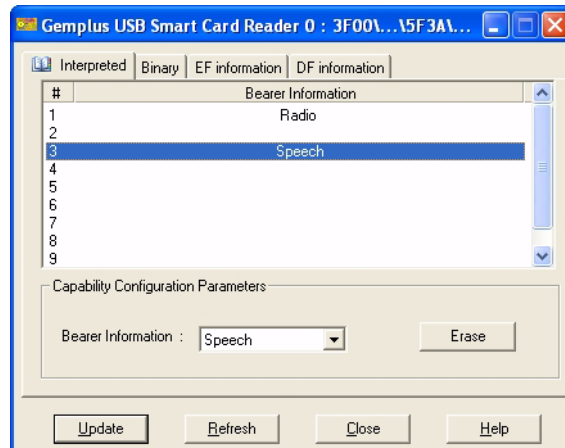


**Note:** When linking *by Record* the fields **ADN file SFI** and **ADN Record ID** are not used because files link record-to-record. When linking *by Index* the file ID of the master EF and the record number of the entry is mandatory.

### Capability Configuration Parameters 1 file (CCP1)

This file contains bearer parameters for calls established using a phone book entry. The bearer is that which indicates the type of communication (Speech or Radio).

**Figure 44 - Capability Configuration Parameters 1 File (CCP1)**

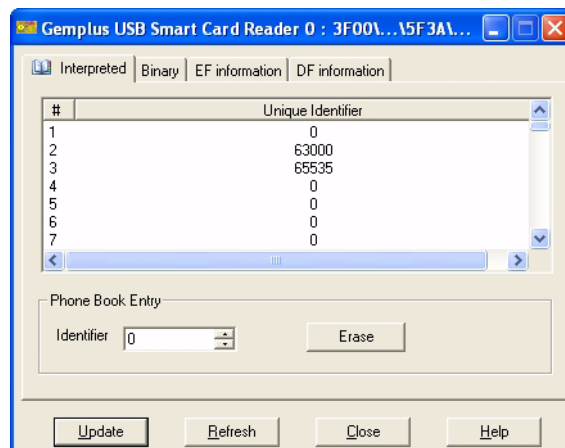


The records in this file are linked to EFADN and EFANR *by TLV*. See “File Linking” on page 95 for more information on this linking method. The CCP1 byte for an entry in EFADN and EFANR points to a record in CCP1 to establish bearer parameters for calls. For more information, refer to the contextual help for EFCCP1.

### Unique Identifier file (UID)

This file contains a unique identifier for an entry to keep track of the entry in the phone book. It is assigned when the entry is created, and remains unchanged unless the phone book ID is regenerated, at which point new values are assigned phone book entries, starting from 1. The UID associated to a deleted entry is not reassigned until the phone book ID is regenerated.

**Figure 45 - Unique Identifier File (UID)**



EFUID is linked to EFADN *by Record*. See “File Linking” on page 95 for more information on this linking method.

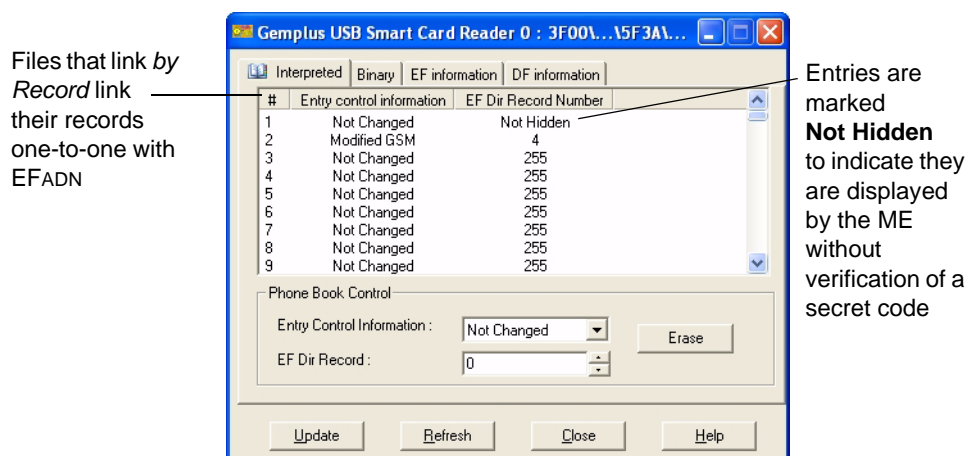
## Phone Book Control file (PBC)

This EF is linked *by Record* to EFADN and contains control information related to each entry in the phone book. In effect, if a 3G card is inserted into GSM mobile equipment and a phone book entry is modified, the change is flagged in this file.

Additionally this file flags whether a secret code must be presented before access to hidden phone book entries is granted to the user. If verification is necessary, the "Hidden Information" byte is set to the record in EFDIR that references the phone book's corresponding USIM or GSM application that contains the secret code for hidden phone book entries. If not, the byte is set to 00h or "Not Hidden". For more information, see the contextual help on EFPBC.

**Note:** If the 3G card supports hidden phone book entries, this file must be present. If the 3G card supports GSM SIM applications, this file must be present.

**Figure 46 - Phone Book Control File (PBC)**



## Other Phone Book Related Files

### Incoming Call Information (ICI)

EFICI (6F 80h) is a cyclic file that contains information describing the last (typically ten) incoming calls received by the mobile. The minimum information provided includes the time, duration and status (answered/ unanswered) of the incoming call.

When calling line identification is supported, and the incoming number matches a number stored in an EFADN, a link is created between the incoming call information and the corresponding phone book entry. This mobile equipment enabled feature permits users to retrieve extra information on the calling party (for example, a name, an additional phone number, and so on).

Incoming call information can be linked to different ADN files and phone books stored under DFTELECOM or the local phone book within a USIM application (an entry pointer in EFICI is used to clearly identify the phone book location: either global, under DFTELECOM, or local, within the USIM application).

### Outgoing Call Information (OCI)

EFOCI (6F 81h) is a cyclic file that contains information describing the last (typically ten) outgoing calls made from the mobile. The minimum information provided includes the time and duration of the outgoing call.

When the outgoing call number matches a number stored in an EFADN, a link is created between the outgoing call information and the corresponding phone book entry. This mobile equipment enabled feature permits users to retrieve extra information on a called party (for example, a name, an additional phone number, and so on).

Outgoing call information can be linked to different ADN files and phone books stored under DFTELECOM or within a USIM application (an entry pointer in EFOCI is used to clearly identify the phone book location: either global, under DFTELECOM, or local, within the USIM application).

### Key for Hidden Phone Book Entries (HIDDENKEY)

EFHIDDENKEY (6F C3h) is a transparent file and contains the hidden key that has to be verified in order for mobile equipment to display the phone book entries that are marked as hidden. The hidden key can consist of 4 to 8 digits.

---

**Note:** The phone book entries marked as hidden are not encrypted by means of the hidden key: they are stored in plain text in the phone book and require a correct entry of the hidden key to be displayed. However, to the card reader no entries are hidden, rather hidden entries are displayed in a different color to “normal” phone book entries.

---

## File Linking

The individual phone book files are linked together to form a complete entry for a person or an entity. The phone book reference file (EFPBR) is the container of all the TLV data objects with their different constructed and primitive tags that establish these linking relationships. See “Phone Book Reference file (PBR)” on page 86 for a binary view of EFPBR and a description of file contents.

## Constructed and Primitive Tags

The structure of EFPBR is entirely made up of Tag Length Value data objects, called constructed TLV DOs and primitive TLV DOs. This document uses the terms constructed tag TLVs (or constructed tag) and primitive tag TLVs (or primitive tag) to refer to these data objects.

Constructed tag TLVs permit clear identification of the type of linking used in EFPBR. The value field of each constructed tag contains, in turn, one or a series of primitive tag TLVs. The primitive tag permits clear identification of the type of data and the value field of each primitive tag indicates the file identifier personalized by the card provider.

Thus the linking relationship for each file to an entry in the phone book is established by the presence or absence of the primitive tag in the value field of the constructed tag.

**There are three types of constructed tags in EFPBR:**

- Constructed tag **A8h** indicates that the primitive tags present in its value field are linked *by record*. The first primitive tag after tag A8 indicates in its value field the file ID of the master EF, or EFADN.
- Constructed tag **A9h** indicates that the primitive tags present in its value field are linked *by Index*.
- Constructed tag **AAh** indicates that the primitive tags present in its value field are linked *by TLV*.

All primitive tags possible in EFPBR are listed in Table 2, "Primitive Tag Values", on page 96.

**Table 2 - Primitive Tag Values**

Primitive Tag	Tag Description
C0	EFADN data object
C1	EFIAP data object
C2	EFEXT1 data object
C3	EFANE data object
C4	EFANR data object
C5	EFPBC data object
C6	EFGRP data object
C7	EFAAS data object
C8	EFAS data object
C9	EFUID data object
CA	EFEMAIL data object
CB	EFCCP1 data object

---

**Note:** If a particular EF does not exist in the phone book structure, its corresponding primitive tag is not present.

---

A summary of file linking by type of link is found in Table 3, "Phone Book Linking Capabilities", on page 96.

**Table 3 - Phone Book Linking Capabilities**

Name	linked by Record	linked by Index	linked by TLV
EFAAS			to EFANR through tag AAh in EFPBR
EFADN	is master EF		
EFANR	to EFADN	to EFADN through EFIAP	
EFEMAIL	to EFADN	to EFADN through EFIAP	
EFEXT1			to EFADN through tag AAh in EFPBR
EFAS			to EFGRP through tag AAh in EFPBR
EFGRP	to EFADN		
EFIAP	to EFADN		
EFPBC	to EFADN		

**Table 3 - Phone Book Linking Capabilities**

Name	linked by Record	linked by Index	linked by TLV
EFSNE	to EFADN	to EFADN through EFiAP	
EFUID	to EFADN		
EFCCP1			to EFADN and EFANR through tag AAh in EFPBR

**Note:** A file that can use either *by Record* or *by Index* linking, can use both in the same phone book. For instance, a phone book entry may have two emails, one entry linked *by Record*, the other linked *by Index*. However, different phone book entries cannot link to the same record in a file.

These linking methods are explained in the sections that follow.

## Linking by Record

A file can be linked *by Record*, which means that the primitive tag of the file in question is listed in EFPBR after tag **A8h**. Linking this way means the file's records are linked one-to-one with the records in the master EF (that is, EFADN). In effect, files linked this way have the same number of records as EFADN and their records are in the same order as in EFADN. The mechanism is constructed as follows:

- 1 During phone book initialization, the mobile equipment reads the TLV data of EFPBR. See "Constructed and Primitive Tags" on page 95 for information on the structure of these TLVs.
- 2 The first primitive tag after constructed tag A8h in EFPBR is C0h, whose value field contains the file identifier for EFADN, establishing EFADN as the master EF.
- 3 After the primitive tag TLV data object for the master EF, there is a series of primitive tag TLVs. Their value fields contain the file IDs of all files whose contents are linked by Record to EFADN.

With a method for knowing the file ID and the record for a phone book entry, the link is complete.

**Note:** Since the master EF is used as the reference file, when a file is linked in this way it contains the same number of records as the master EF, thus consuming more card resources than linking *by Index* or *by TLV*.

## Linking by Index

A file can be linked *by Index*, which means that the primitive tag of the file in question is listed in EFPBR after tag **A9h**. Linking this way means the file is linked to an entry in the master EF (that is, EFADN) by means of EFiAP. The mechanism is constructed as follows:

- 1 During phone book initialization, the mobile equipment reads the TLV data of EFPBR. See "Constructed and Primitive Tags" on page 95 for information on the structure of these TLVs.
- 2 The first primitive tag after constructed tag A8h in EFPBR is C0h, whose value field contains the file identifier for EFADN, establishing EFADN as the master EF.

- 3 Also after constructed tag A8h in EFPBR is primitive tag C1h, whose value field contains the file identifier for EFAP, establishing EFAP as linked *by Record* to EFADN.

**Note:** If EFAP is not present, linking *by Index* is not possible in the phone book and the constructed tag A9h is not present.

If EFAP is present, after the constructed tag A9h in EFPBR, there is a series of primitive tag TLVs. Their value fields contain the file IDs of all files whose contents are linked *by index* to EFADN by means of a record pointer in EFAP.

The order of these primitive tag TLVs determines to which files the record number pointers in EFAP refer.

**Note:** The binary data in each record in EFAP is simply the record number for these files. See “Figure 37” on page 88 and Table 5, “Binary Data for 1 Record in EFAP”, on page 99 for an illustration of this.

Take as an example the following binary data from the example in “Figure 34” on page 86.

A9 0A C3 03 4F 19 05 CA 03 4F 50 06

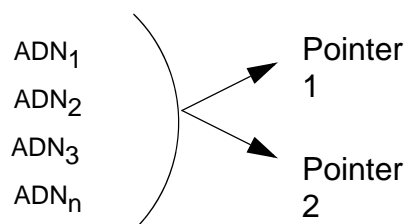
The data is described as follows:

**Table 4 - Binary Data After Tag A9 in EFPBR**

constructed tag TLV	T	A9			constructed tag to link <i>by Index</i>	
	L	0A			length of constructed tag	
	Value	primitive tag TLV	C3	T	primitive tag for EFSNE	Pointer 1
			03	L	length of file ID	
			4F 19	V	file ID for EFSNE	
			05		short file indicator (SFI)	
			CA	T	primitive tag for EFEMAIL	Pointer 2
			03	L	length of file ID and SFI	
			4F 50	V	File ID for primitive tag	
			06		short file indicator (SFI)	

In Table 4, “Binary Data After Tag A9 in EFPBR”, on page 98, the binary data describes that the order of the TLVs after tag A9h determines that pointer 1 is for file ID 4F 19 (EFSNE) and pointer 2 for 4F 50 (EFEMAIL). The order of these pointers is the same for all entries in EFADN.

**Figure 47 - Relationship of EFADN Entries to EFAP Record Pointers**



Now take as an example the following binary data from “Figure 37” on page 88. Since record 4 in EFIAP is linked *by record* to EFADN, the binary data is simply the number of the record in the files pointed to.

01 04

The data is described as follows:

**Table 5 - Binary Data for 1 Record in EFIAP**

01	Record 1 in 4F 19 (EFSNE)
04	Record 4 in 4F 50 (EFEMAIL)

With a method for knowing the file ID and the record for a phone book entry, the link is complete. This linking mechanism saves on card resources, compared to linking *by Record*.

For more information on linking *by Index*, see “Index Administration Phone book file (IAP)” on page 88.

## Linking by TLV

A file can be linked *by TLV*, which means that the primitive tag of the file in question is listed in EFPBR after tag **AAh**. The record containing the data is provided by the file needing the link. Four files use linking *by TLV*:

- Data in EFEXT1 is linked *by TLV* to an entry in EFADN and to an entry in EFANR
- Data in EFAAS is linked *by TLV* to an entry in EFANR
- Data in EFGAS is linked *by TLV* to an entry in EFGRP
- Data in EFCCP1 is linked *by TLV* to an entry in EFADN and EFANR

**Note:** EFGAS and EFGRP are either both present in EFPBR, or both absent. If no files are linked *by TLV*, tag **AAh** is not present in EFPBR.

The mechanism is constructed as follows:

- 1 During phone book initialization, the mobile equipment reads the TLV data of EFPBR. See “Constructed and Primitive Tags” on page 95 for information on the structure of these TLVs.
- 2 The presence of a file's primitive tag after constructed tag **AAh** in EFPBR establishes that the file links *by TLV*. The value fields of these primitive tags establish the IDs of the files as personalized by the card provider.

The three files that use linking *by TLV* have a special byte which flags whether they use the linking mechanism or not.

**Table 6 - Record Pointers in Files Linked by TLV**

EFs using link <i>by TLV</i>	Byte name in EFs using linking <i>by TLV</i>	Byte value in EFs using link <i>by TLV</i> : Unused / Free / Record Number
EFADN linked to EFEXT1	extension 1 record identifier byte	FFh / FFh / XXh
EFADN linked to EFCCP1	capability/configuration 1 identifier byte	FFh / FFh / XXh
EFANR linked to EFAAS	additional number identifier byte	00h / FFh / XXh

**Table 6 - Record Pointers in Files Linked by TLV (continued)**

EFs using link by TLV	Byte name in EFs using linking by TLV	Byte value in EFs using link by TLV: Unused / Free / Record Number
EFANR linked to EFCCP1	capability/configuration 1 identifier byte	FFh / FFh / XXh
EFANR linked to EFEXT1	extension 1 record identifier byte	FFh / FFh / XXh
EFGRP linked to EFGAS	group name identifier byte	00h / 00h / XXh

In effect, the presence of a value other than *Unused* or *Free* (FFh, 00h) indicates there is a link. The value of the identifier byte indicates the record number in the EF that is linked by TLV. With a method for knowing the file ID and the record for a phone book entry, the link is complete. This linking mechanism saves on card resources, compared to linking by *Record*.

## Phone Book Procedures

### Initialization

The mobile equipment (ME) first reads the contents of EFPBR to determine the configuration of the phone book. Thus the ME establishes the structure of the master EF (EFADN), which is always the first file ID to follow tag A8h. If EFIAP is indicated in EFPBR (following tag A8h), the ME reads the contents of EFIAP in order to establish the relationship between the contents in the files indicated using tag A9h and files indicated by tag A8h. The ME may then read the contents of the phone book related files in any order.

### Creation and Deletion of Information

In order to avoid unlinked data introducing fragmentation of the files containing phone book data, the following procedures are followed when a new phone book is created. The data related to EFADN is first stored in the relevant record. As the record number is used as a pointer, the reference pointer is now defined for the entry. When storing additional information for an entry, the reference pointer is created before the actual data is written to the location.

When an entry is deleted, either partly or completely, the data is deleted before the reference pointer is deleted. When an entry is deleted completely, the contents of EFADN are the last to be deleted.

### Hidden Phone Book Entries

If a phone book entry is marked as hidden by means of EFPBC, the ME first prompts the user to enter the Hidden Key. The key presented by the user is compared with the value that is stored in the corresponding EFHIDDENKEY. If the keys match, the ME displays the data stored in this phone book entry. If the keys do not match, the contents of the phone book entry are not displayed by the ME. No entries are hidden to a card viewer, rather hidden entries are highlighted by use of a different color to "normal" phone book entries.



## Phone Book Interpreter

The phone book interpreter provides you with a global view of the whole phone book, that is to say, all the file linking relationships defined in EFPBR are combined here to show all related information on any given entry. The phone book entries are displayed in the same order as in EFADN.

Via the Phone Book Interpreter you can view, modify and delete phone book entries. Modifications made here update the individual files concerned.

You can also select specific files to display on the phone book interpreter instead of all the files located in the EFPBR. This selection can be made in the phone book settings window.

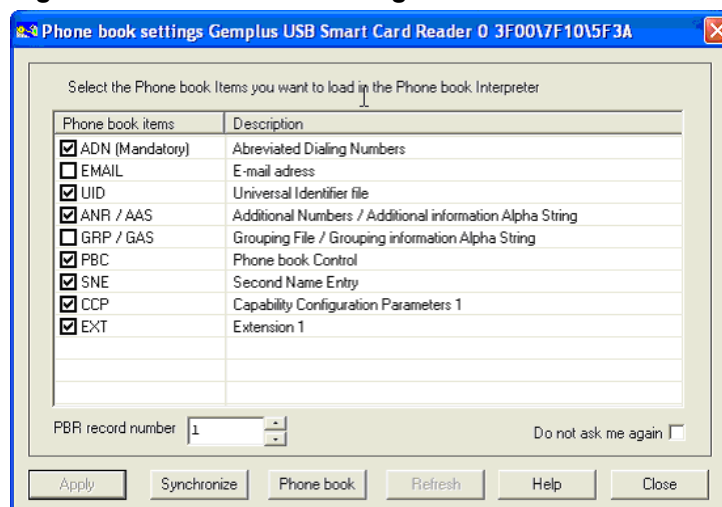
### To set the phone book settings:

- 1 Select the phone book directory file under DFTELECOM or under a USIM application.
- 2 Right-click on the phone book directory file, and choose **Phone Book Settings...**

#### Note:

- a) When the phone book settings window is launched for the first time, it will display all the files available in the EFPBR.
- b) EFADN is always checked.
- c) The **phone book settings** window is blank when the access condition to EFPBR is not met. Enter the required PIN code in the **Secret Code Management** window and click **Refresh**.

**Figure 48 - Phone Book Settings**



- 3 Under **phone book items**, select the files you wish to have displayed only, by checking the boxes beside them.
- 4 In the **PBR record number** box, select the record number of the PBR you wish to read. An error occurs when the number selected is higher than the number of records present in a card's EFPBR.

**Apply** - click this button to save and apply your selection.

**Synchronize** - click this button to synchronize your settings with the selected record content in EFPBR.

**Phone Book** - click this button to launch the phone book interpreter based on settings saved.

**Refresh** - click this button to re-read the data on the card.

**Close** - click this button to cancel all actions and close this window. The phone book interpreter will not be launched.

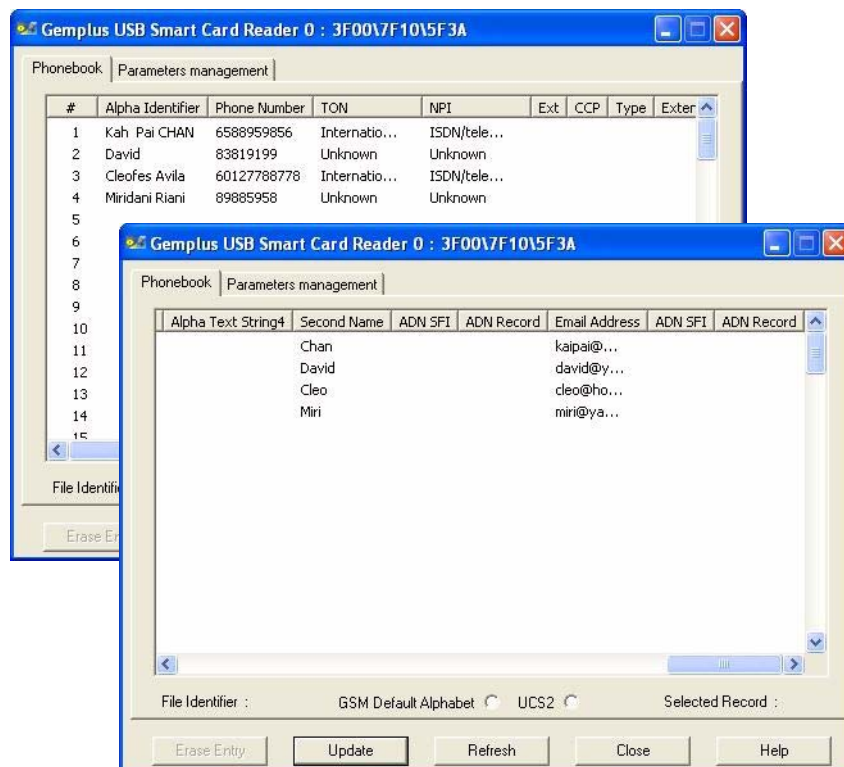
If the “**Do not ask me again**” box is not checked, this phone book settings window will appear again the next time you launch the phone book interpreter. However, if this box is checked, your selection is saved and the phone book settings will not appear the next time you select the phone book interpreter.

If your saved settings are not coherent with the contents and registry of EFPBR, a warning will appear. Select **Phone Book Settings** to re-select your settings or **Phone book** to display only the files that match.

**To open the phone book interpreter:**

- 1 Select the phone book directory file under DFTELECOM or under a USIM application.
- 2 Right-click on the phone book directory file, and choose **Phone Book Interpreter....**

**Figure 49 - Phone Book Interpreter**



The **Phone Book Interpreter** simplifies management of phone book entries.

- **Update.** Write modifications to the card.
- **Close.** A message box offers to save changes before closing the interpreter.
- **Refresh.** Re-read the data on the card. A message box offers to save your changes before they are discarded.
- **Erase Entry.** Delete the entire entry from the phone book.

---

**Note:** Hidden entries are displayed in a different color from “normal” entries.

---

## How to Create a Phone Book

To create a phone book:

- 1 In the phone book directory file (5F 3A) under DFTELECOM or under a USIM application, create phone book files such as ADN, ANR, EMAIL and GRP. Refer to “Phone Book Files” on page 85 for more information.

- 2 In the EFPBR, specify how the files are linked.

For example, to *link by record*, EFGRP to EFADN:

In GemXplorer File view, double-click to open EFPBR (4F 30). Select link by record, type - GRP, file ID - 4F 26 and SFI - 5 > Click **Insert Link > Update**.

For example, to *link by TLV*, EFGAS to EFGRP:

In GemXplorer File view, double-click to open EFPBR (4F 30). Select link by TLV, type - GAS, file ID - 4F 4C and SFI - 7 > Click **Insert Link > Update**.

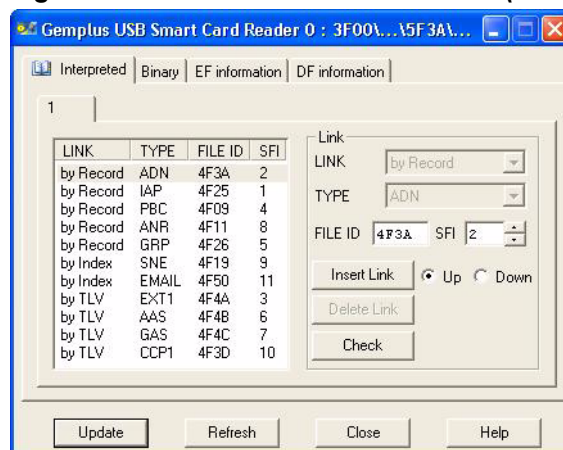
For example, to *link by Index*, EFIAP to EFADN:

In GemXplorer File view, double-click to open EFPBR (4F 30). Select link by record, type - IAP, file ID - 4F 25 and SFI - 1 > Click **Insert Link > Update**. Next, select link by index, type - EMAIL, file ID - 4F 50 and SFI - 11 > Click **Insert Link > Update**.

Refer to “File Linking” on page 95 for more information.

The EFPBR will appear like this:

**Figure 50 - Phone Book Reference File (PBR)**



## Using the Phone Book Interpreter to Manage Phone Book Entries

A phone book must be created before the phone book interpreter can display the phone book entry fields and for these entries to be easily viewed, modified, deleted and linked.

**To manage a phone book using the phone book interpreter:**

- 1 Right-click the phone book directory file, and select **Phone Book settings...**. This allows you to select specific files to display on the phone book interpreter instead of all the files located in the EFPBR. Refer to “Phone Book Interpreter” on page 101 for more information.
- 2 Click **Phone Book** to launch the phone book interpreter.

- 3 In the **Parameters management** tab, under **Column Name**, select the fields to be displayed in the **Phone Book** tab.

---

**Note:**

- a) Deselecting an entry means the Interpreter does not display it and by reducing the amount of information displayed, you can simplify working with the Interpreter.
- b) Selecting the **Display File Link fields** option selects all fields in all phone files referenced in EFPBR that relate to the linking mechanism by TLV (tag AA).

- 
- 4 In the **PBR record number** box, select the record number of the PBR you wish to read.

- 5 In the **Phone Book** tab, select a record, click the respective fields to view, modify and delete information.

For example, to create groups and assign groups to phone book entries:

In GemXplorer File view, double-click to open EFGAS (4F 4C). Create group names, for example, business, work, family and so on.

In the **Phone Book Interpreter**, select a record, in the **Grp1** field, enter the group identifier, for example, '1' for business.

## 3G Phone Book Interpreter

The 3G Phonebook Interpreter extends the existing Phone Book Interpreter functionality primarily on the management of contact information in the graphical user interface (GUI) environment.

The 3G Phonebook Interpreter provides a detailed interpretation of the whole 3G phone book which includes the 3G phone book entries and its associated files. There are options to view, modify and delete the phone book entries and in addition, a detailed graphical view of the entire phone book structure with its associated files.

The features of the 3G Phonebook interpreter include the following:

- Support for importing existing phone book entries from the card and UXP file.
- Support for phone book backup to XML format.
- Support for tree-like structures data representation.

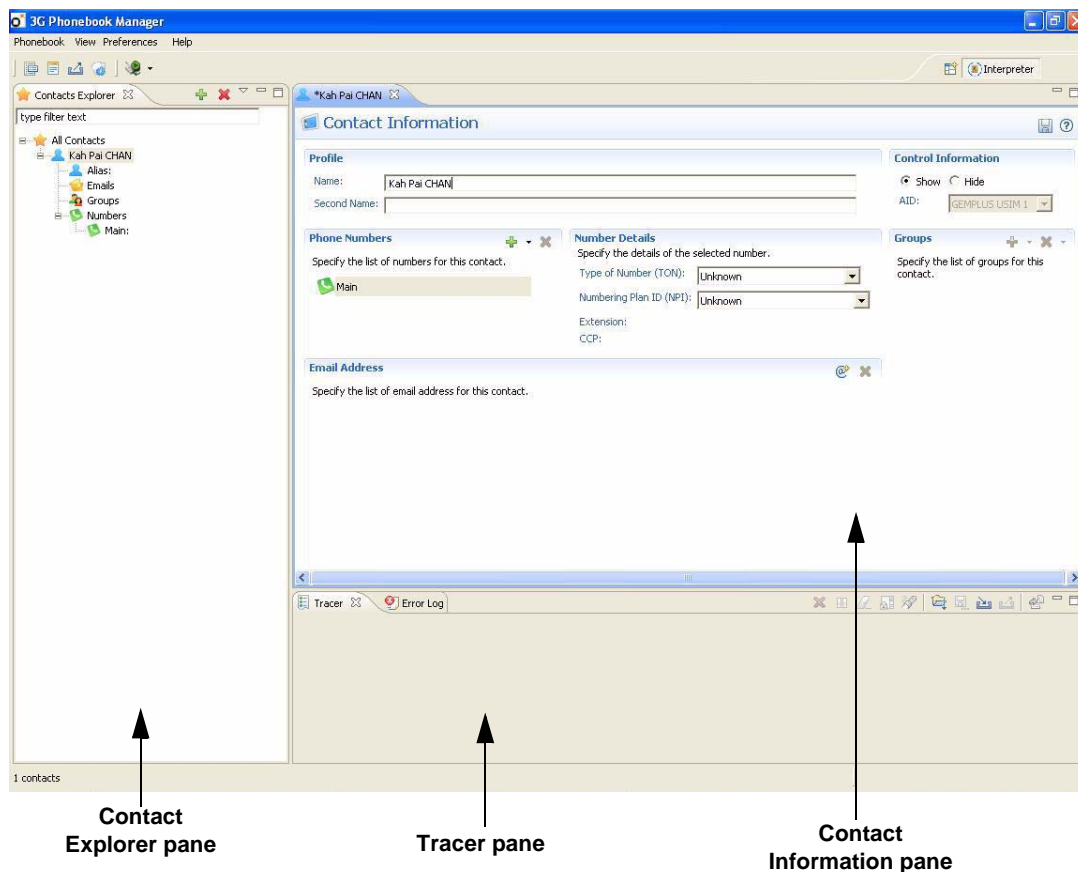
There are two ways to browse the 3G phone book via the 3G Phonebook interpreter — loading a card to the card reader to view the phone book contents and loading an XML file containing the phone book structure. The phone book contents are subsequently displayed in the Contact Explorer and Contact Information panes of the 3G Phonebook interpreter.

### Starting the 3G Phone Book Interpreter

**To start the 3G Phone Book Interpreter:**

- 1 In GemXplorer Structure view, right-click the icon representing the card type, together with the card's name and card reader type and select **3G Phone Book Interpreter** to launch phone book interpreter.
- 2 There are two ways to load phone book information. On the Phonebook menu, select **Load Card** via the card reader or **Load File** via specifying the location of the file.
- 3 A Verify Code window will appear when **Load Card** is selected. You will need to present the PIN in order to read the phone book information. The correct presentation of the PIN gives you the access rights to load the phone book information. With the successful authentication, you can then choose the type of operations that you would like to perform on the **3G Phone Book Interpreter**.

For more information about the use of the **3G Phone Book Interpreter**, click the Help button in the command window.

**Figure 51 - 3G Phonebook Interpreter Details View**

## Menu Bar

The 3G Phonebook Interpreter menu bar contains the sub-menus which allows to perform the various tasks for contact management.

**Note:** Tool icons are available as shortcuts keys for some sub-menus to make access easy.

**Figure 52 - 3G Phonebook Interpreter Menu Bar**

A summary of the sub-menus of 3G Phonebook Manager is shown as follows: .

**Table 7 - Menu Bar Commands and Sub-menus of 3G Phonebook Manager**

Main Menu	Sub-menus	Description
Phonebook	Load Card	Load card from reader
	Load File	Load file from UXP file
	Group Manager	Manage the groups in the phone book
	Number Type Manager	Manage the phone number types in the phone book
	Export Phonebook	Generate a copy of the phone book in a UXP format
	Exit	Quit the 3G Phonebook Manager tool

**Table 7 - Menu Bar Commands and Sub-menus of 3G Phonebook Manager (continued)**

Main Menu	Sub-menus	Description
View	Structure Summary	Display the linked view of the 3G Phonebook structure
Help	Welcome	Display information about 3G Phonebook Manager, links to workspace, tutorial and online help
	Help Contents	Display the 3G Phonebook Manager online help
	Dynamic Help	Display the related topics links in 3G Phonebook Manager
	About 3G Phonebook	Display information about 3G Phonebook Manager

## ISIM Management

---

**Note:** This feature is currently available for GemXplore Generations cards only.

---

3GPP IP Multimedia Subsystem (IMS) enables the provision of mobile multimedia services within the converging networks which in turn offer IP based services for users, independently of the network accessed.

IP Multimedia Services Identity Module (ISIM) is an application running on a UICC smart card in a 3G mobile phone operating in the IMS environment. The ISIM authentication is achieved by using IMPI to authenticate you to secure the IMS framework which is used for enabling IP based services and applications.

The IMS authentication used is based on the mutual authentication in UMTS networks called UMTS AKA.

ISIM supports the following contexts under the USIM mode:

- IMS AKA
- GBA context in bootstrapping mode
- GBA context in NAF derivation mode

### IMS Authentication and Key Agreement (AKA) Context

This authentication mechanism is used to generate the secret keys (CK and IK) and also to authenticate the communication of ISIM to the network and vice versa in an IMS environment.



## IMS AKA Authentication in ISIM

---

**Note:** The procedure described below is available for 3G cards containing an ISIM application.

---

The purpose of this procedure is used to authenticate the communication of ISIM to the network and vice versa in an IMS environment and to generate the secret keys — CK and IK.

In Card ADMIN, you only test that the ISIM application is able to authenticate itself in the IMS AKA context. The full authentication mechanism would involve the following steps:

- the terminal or network (in this case GemXplorer) sends a random number (challenge) and authentication data to the ISIM application
- the ISIM application makes a number of verifications on the received data before calculating a result (RES) from the random number
- the terminal/network then retrieves RES from the ISIM application and compares it with its own result

The card also returns the following data with RES:

- CK: the ciphering key used to encrypt the transmission over the radio channel, calculated from the random number and the key specified in the **Authenticate** command parameters.
- IK: an application-specific key value, also calculated from the random number and the key specified in the **Authenticate** command parameters.

The authentication result can be divided into three cases:

- Authentication accept case: the ISIM checks that XMAC = MAC and that the sequence number is correct, returns the RES, CK and IK parameters to the mobile equipment.
- MAC failure case: the ISIM identifies the calculated XMAC value is different from the MAC and returns an error.
- SQN failure case: the ISIM verifies that the SQN is not in the correct range, returns an authentication failure message, AUTS for re-synchronization.

In an IMS AKA authentication, the algorithms supported are: Dummy XOR and Milenage.

### To perform an IMS AKA authentication using the Milenage algorithm for GemXplore Generations cards:

---

**Note:** To perform a successful authentication using the values in the example below, first update record 1 of EFsqn with “FF 9B B4 00 00 00” and record 25 with “00 00 00 00 00 00”.

---

- 1 In the GemXplorer Structure view, select the USIM and right-click **Activation**. Then right-click **Secret Codes > Verify GPIN1**.
- 2 In the GemXplorer File view, double-click **EFKEYOP**.
- 3 In the **Interpreted** tab, select **Milenage** from the drop-down list in the **Algorithm identifier** box.
- 4 Select the **3G** tab, enter the **Key value** and **Key mask**.

**For example:**

**Key value (in hexa):** 46 5B 5C E8 B1 99 B4 9F AA 5F 0A 2E E2 38 A6 BC

- 5 Click to select the **OP** or **OPc** tab.
- 6 Enter the **OP/OPc value** and click **Update**.  
*For example:*  
**OPc value (in hexa):** CD 63 CB 71 95 4A 9F 4E 48 A5 99 4E 37 A0 2B AF
- 7 Select the **Constants** tab, enter the C1 to C5 and R1 to R5 parameters used by the 3G Milenage algorithm.  
 For example, you may enter the same values for **Parameters** shown below.
- 8 In the GemXplorer Structure view, select the USIM and right-click **Authenticate...**
- 9 Click to select **Global Key** or **Application Key**.
- 10 Select **IMS AKA** context and then **Milenage** from the drop-down list in the **Algorithm** box.
- 11 Click **Parameters >>** to enter the C1 to C5 and R1 to R5 values. Then click **Save** and **<< Parameters**.

*For example:*

**C1 (in hexa):** 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

**C2 (in hexa):** 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01

**C3 (in hexa):** 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02

**C4 (in hexa):** 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04

**C5 (in hexa):** 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08

**(In decimal) R1: 64, R2: 0, R3: 32, R4: 64, R5: 96**

---

**Note:** C1 to C5 and R1 to R5 are parameters used by the Milenage algorithm. Their values are specific to each operator/card and cannot be chosen arbitrarily. Hence, you must enter the correct values defined for the card you are using.

---

- 12 Enter the network's **Key Value**, **OPC value**, **Random value**, **AMF** and **SQN**.

*For example:*

**Key value (in hexa):** 46 5B 5C E8 B1 99 B4 9F AA 5F 0A 2E E2 38 A6 BC

**OPC value (in hexa):** CD 63 CB 71 95 4A 9F 4E 48 A5 99 4E 37 A0 2B AF

**Random value (in hexa):** 23 55 3C BE 96 37 A8 9D 21 8A E6 4D AE 47 BF35

**AMF (in hexa):** B9 B9

**SQN (in hexa):** 55 F3 2F B4 35 77

- 13 Click **Authenticate**.

The results such as RES, CK or IK are returned.

When a "Mac Does Not Match" error occurs, check that the values of the Key and Constants C1 to C5, and R1 to R5 are correctly entered.

When a synchronization error occurs, check that the input SQN is correctly entered with values higher than record 25 in EFsqn. Refer to 3GPP TS 33.103 for details.

When an "incorrect AUTN" error occurs, check that the values of AMF and SQN are correctly entered.

## Generic Bootstrapping Architecture Security Context

The aim of GBA is to provide a means of shared cryptographic relationship between an application server and a mobile to secure an application.

GBA re-uses this relationship and offers an application-independent mechanism based on the AKA infrastructure to provide a common shared secret. This shared secret is then used to authenticate the communication between the client and the server.

In GBA context, authentication is generally achieved using the AKA protocol to mutually authenticate the Bootstrapping Server Function (BSF) and the ISIM, and the session keys applied between ME and the application server, the Network Application Function (NAF).

Within this context, this security function operates under two different modes:

- GBA context in bootstrapping mode
- GBA context in NAF derivation mode

### Bootstrapping Mode

This mode operates during the procedure for mutual authenticating of the ISIM and the Bootstrapping Server Function (BSF) and the derivation of the bootstrapped key material generated from AKA.

See “GBA Authentication in Bootstrapping Mode” on page 71 for more details on ISIM Authentication in GBA Bootstrapping Mode.

### NAF Derivation Mode

This derives the Network Application Function (NAF) specific keys from the bootstrapped key material generated previously from the bootstrapping mode.

See “GBA Authentication in NAF Derivation Mode” on page 73 for more details on ISIM Authentication in GBA NAF Derivation Mode.

## ISIM Files

These files are involved in the management of ISIM and are stored under ADF<sub>ISIM</sub>.

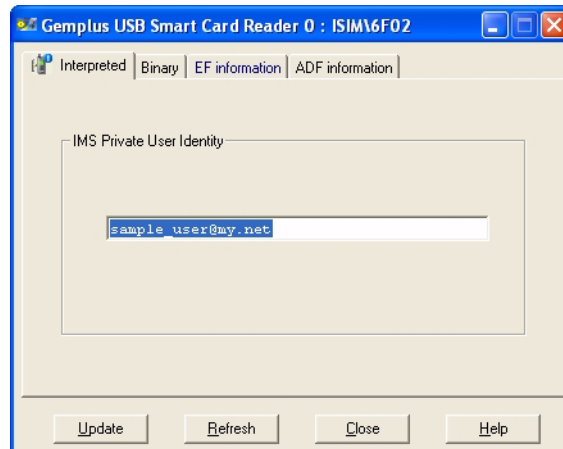
To access the ISIM application, information have to be contributed to some or all of these files to establish the security and authentication process.

- IP Multimedia Subsystem Private User Identity (IMPI) - 6F 02h
- The Home Network Domain Name - 6F 03h
- IMS Public User Identity (IMPU) - 6F 04h
- Administrative Data (AD) - 6F ADh
- ISIM Access Rule Reference (ARR) - 6F 06h
- ISIM Service Table - 6F 07h
- Proxy Call Session Control Function (P-CSCF) - 6F 09h
- GBA Bootstrapping Parameters (GBABP) - 6F D5h
- GBA Network Application Function List (GBANL) - 6F D7h

## IP Multimedia Subsystem Private User Identity

EFIMPI (6F 02h) is a transparent file which contains the private information of the user.

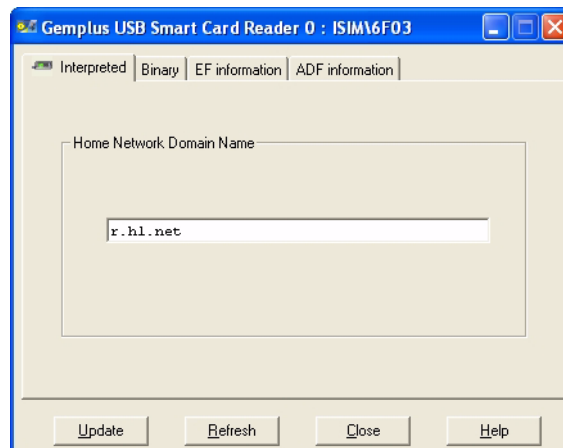
**Figure 53 - IP Multimedia Subsystem Private User Identity (IMPI)**



## Home Network Domain Name

EFDOMAIN (6F 03h) holds the URL of the home operator's network.

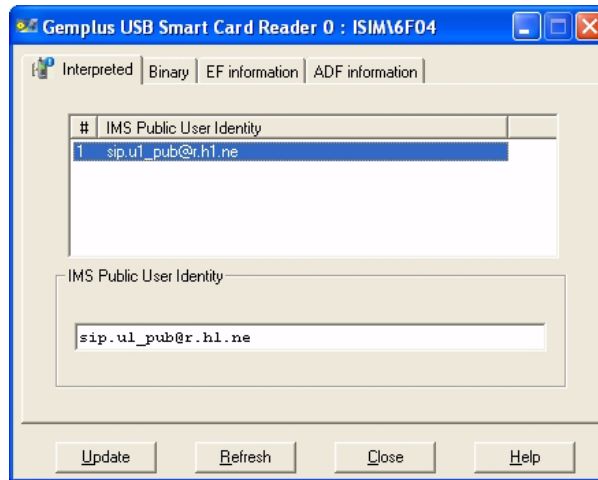
**Figure 54 - Home Network Domain Name (Domain)**



## IMS Public User Identity

EFIMPU (6F 04h) is a linear fixed file which contains the public SIP Identity (SIP URI) of the user.

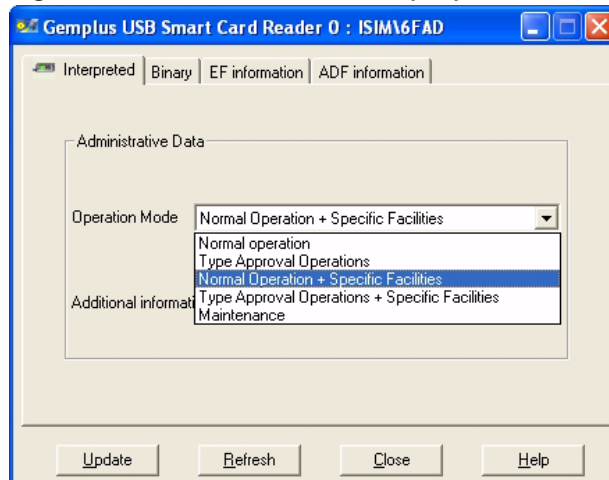
**Figure 55 - IMS Public User Identity (IMPU)**



## Administrative Data

EFAD (6F ADh) is transparent file which contains information on the operation modes used in the ME.

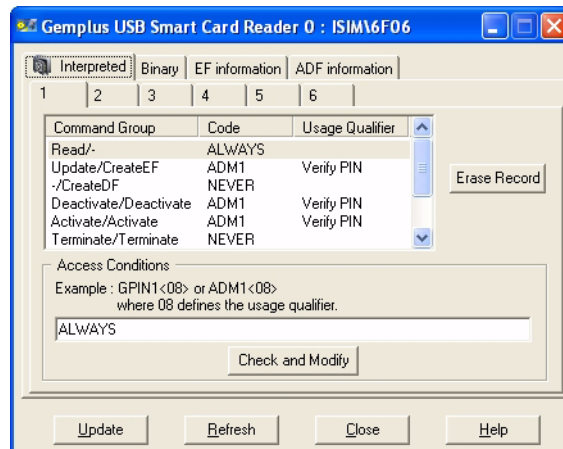
**Figure 56 - Administrative Data (AD)**



## ISIM Access Rule Reference

EFARR (6F 06h) is located under ADFISIM on the UICC.

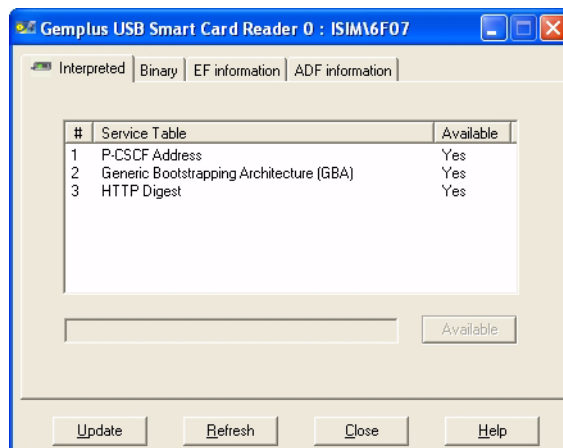
**Figure 57 - ISIM Access Rule Reference (ARR)**



## ISIM Service Table

EFIST (6F 07h) is a transparent file which indicates the list of optional services that are available in ISIM.

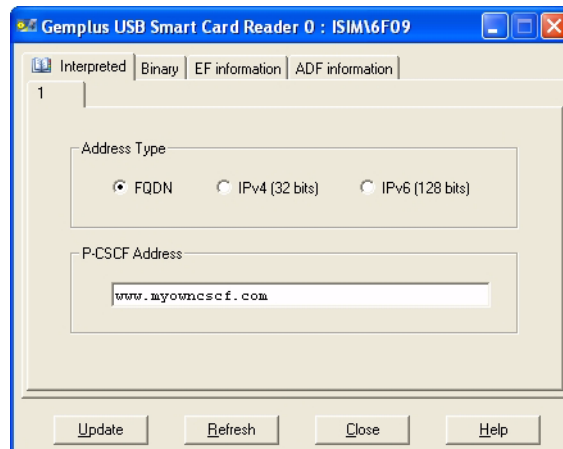
**Figure 58 - ISIM Service Table (IST)**



## Proxy Call Session Control Function

EFPCSCF (6F 09h) contains the SIP proxy which is used as the initial interface (SIP Server) between the mobile and the IMS terminal.

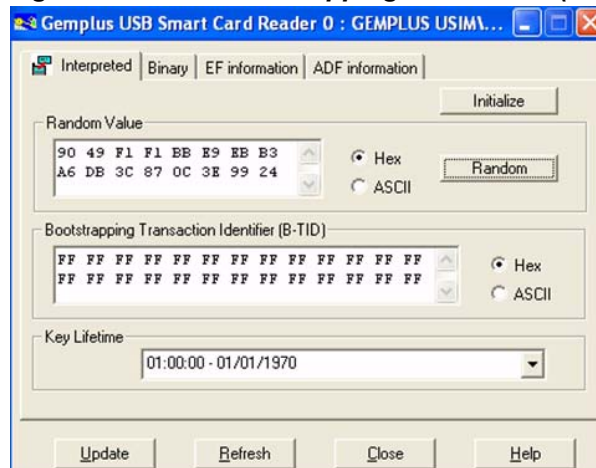
**Figure 59 - Proxy Call Session Control Function (PCSCF)**



## GBA Bootstrapping Parameters

EFGBABP (6F D5h) contains the random challenge (RAND) and GBA Bootstrapping Transaction Identifier (B-TID).

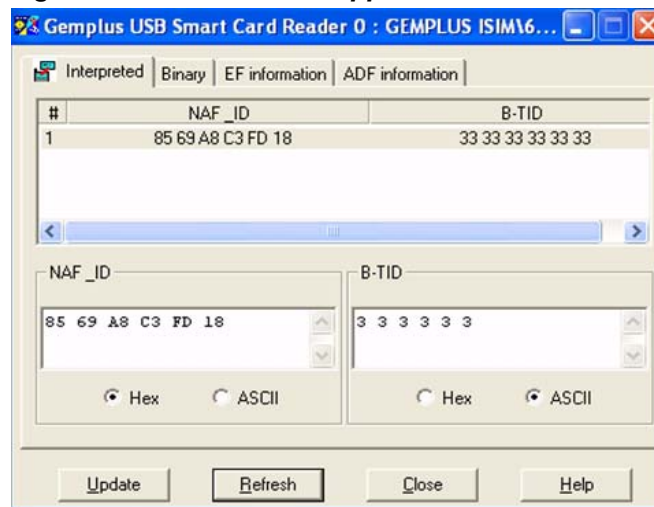
**Figure 60 - GBA Bootstrapping Parameters (GBABP)**



## GBA Network Application Function List

EFGBANL (6F D7h) contains the list of NAF\_ID and B-TID associated to a GBA NAF derivation procedure.

**Figure 61 - GBA Network Application Function List (GBANL)**



## EAP Management

The purpose of using Extensible Authentication Protocol (EAP) is to supplement the existing Point-to-Point Protocol. EAP is a universal authentication framework used for several different authentication methods such as in the wireless (WIFI) networks and point-to-point connections.

There are two authentication methods used in GemXplorer:

- EAP-SIM which is based on Global System for Mobile Communications (GSM) Subscriber Identity Module (SIM).
- EAP-AKA which is based on Authentication and Key Agreement (AKA) mechanism in UMTS Subscriber Identity Module (USIM) and CDMA2000 User Identity Module (R)UIM.

These two methods support authentication credentials that include digital certificates, user-names and passwords, secure tokens, and SIM secrets.

## EAP Authentication Using EAP-SIM Method

### A Full EAP-SIM Authentication

**Note:** The procedure described below is only available for GemXplore Generations Flexible card.

A typical full EAP-SIM authentication basically involves the following steps:

- The network (in this case GemXplorer) sends an EAP request identity (a IMSI or a pseudonym) message to the card to initiate the procedure.
- The card or network makes a number of verifications on the received packet before the application returns the EAP response (SIM/Start) to the card.
- The card sends the EAP response (SIM/Start packet) to the network using the card Nonce MT to calculate the MAC.



- The network sends a SIM/Challenge request with the calculated MAC and the required parameters to the card.
- The card sends the EAP packet received to the application and the application then returns the EAP response (SIM/Challenge packet) to the card.
- The card sends the EAP response (SIM/Challenge packet) to the network, which computes the MAC and compares it with the received MAC.
- If verifications are successful, the network sends the EAP success packet to the card and the card retrieves the key material (master session key and extended master session key) from EFAPKEYS. The card uses the key material for security purposes such as the security for WLAN link layer.

**To perform a full EAP authentication using the EAP-SIM method for GemXplore Generations Flexible cards:**

- 1 In the GemXplorer Structure view, select the USIM and right-click **EAP-SIM Authenticate**.
  - 2 In the GemXplorer File view, double-click **EFKEYOP**.
  - 3 In the **Interpreted** tab, select the encryption algorithm from the drop-down list in the **Algorithm identifier** box.
  - 4 Select the **3G** tab, enter the **Key value**.  
**For example:**  
**Key value (in hexa):** 46 5B 5C E8 B1 99 B4 9F AA 5F 0A 2E E2 38 A6 BC
  - 5 If **Milenage** is chosen as the encryption algorithm:
    - Click to select **OP** or **OPc**. Enter the **OP/OPc value** and click **Update**.  
**For example:**  
**OPc value (in hexa):** CD 63 CB 71 95 4A 9F 4E 48 A5 99 4E 37 A0 2B AF
    - Select the **Constants** tab, enter the C1 to C5 and R1 to R5 parameters used by the 3G Milenage algorithm.  
 For example:  
**C1 (in hexa):** 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
**C2 (in hexa):** 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01  
**C3 (in hexa):** 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02  
**C4 (in hexa):** 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04  
**C5 (in hexa):** 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08  
**(In decimal) R1:** 64, **R2:** 0, **R3:** 32, **R4:** 64, **R5:** 96

---

**Note:** C1 to C5 and R1 to R5 are parameters used by the 3G Milenage algorithm. These values are only specific to each operator/card and cannot be chosen arbitrarily. Hence, you must enter the correct values defined for the card you are using.

---
  - 6 Select the **Identity** tab, enter an EAP identity and click **Send**. Your current identity will then be displayed in the card results.
  - 7 Select the **SIM/Start** tab, select the **Required Identity** to be used and click **Send** to send a SIM/Start request to the card. The network uses parameters entered previously to generate the EAP-SIM related keys.
  - 8 Select the **SIM/Challenge** tab, select the encryption algorithm from the drop-down list in the **Algorithm** box.
- 
- Note:** If the Milenage algorithm is selected, clicking on **Parameters** permits the personalization of the default algorithm set values.
- 
- 9 Click **Parameters >>** to enter the C1 to C5 and R1 to R5 values. Then click **Save** and **<< Parameters**.

**For example:**

**C1 (in hexa):** 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

**C2 (in hexa):** 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01

**C3 (in hexa):** 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02

**C4 (in hexa):** 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04

**C5 (in hexa):** 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08

**(In decimal) R1:** 64, **R2:** 0, **R3:** 32, **R4:** 64, **R5:** 96

You may take the same C1 and R1 values as given in the following **Parameters**.

---

**Note:** C1 to C5 and R1 to R5 are parameters used by the Milenage algorithm. Their values are specific to each operator/card and cannot be chosen arbitrarily. Hence, you must enter the correct values defined for the card you are using.

---

- 10** Enter the network's **Key Value**, **OPc Value** or **OP Value**, **Random** values and **IV**.

**For example:**

**Key value (in hexa):** 46 5B 5C E8 B1 99 B4 9F AA 5F 0A 2E E2 38 A6 BC

**OPC value (in hexa):** CD 63 CB 71 95 4A 9F 4E 48 A5 99 4E 37 A0 2B AF

**Random (in hexa):** 23 55 3C BE 96 37 A8 9D 21 8A E6 4D AE 47 BF35

**IV (in hexa):** 25 63 4A CB A5 37 A8 48 21 8A E6 4D AE 47 37 2B

- 11** Click **Send**.

The results such as SRES, KC, K\_encr, K\_aut, MSK and EMSK are sent to the card via the **Success** tab or **Failure** tab.

---

**Note:** If you are performing a re-authentication in the **SIM/Re-Authentication** tab, do not close the authentication viewer.

---

## EAP-SIM Re-Authentication

You may also choose to use the re-authentication process for the next EAP-SIM session instead of a full EAP-SIM authentication only if the SIM/Challenge request obtained previously contains a fast re-authentication identity. This fast re-authentication identity is a temporary identity which will be deleted after subsequent authentication is processed.

The steps are as follows:

- the network sends the SIM/Start request to the card.
- the card sends the SIM/Start response to the network using fast re-authentication identity without the Nonce MT component.
- the network sends the SIM/Re-authentication request to the card.
- the card sends the SIM/Re-authentication response to the network.

**To perform an EAP re-authentication using the EAP-SIM method for GemXplore Generations Flexible cards:**

- 1** In the GemXplorer Structure view, select the USIM and right-click **EAP-SIM Authenticate**.
- 2** Select the **SIM/Re-Authentication** tab, enter the **Nonce S** and **IV** values.
- 3** Click **Send**.

The results MSK and EMSK are sent to the card via the **Success** tab or **Failure** tab.

## EAP Authentication Using EAP-AKA Method

### A Full EAP-AKA Authentication

**Note:** The procedure described below is only available for GemXplore Generations Flexible card.

A typical EAP-AKA authentication basically involves the following steps:

- The network (in this case GemXplorer) sends an EAP request identity (permanent, pseudonym or re-authentication identity) message to the card to initiate the procedure.
- The card sends the EAP response (AKA/Identity packet) to the network.
- The network sends an AKA/Challenge request with the calculated MAC and the required parameters to the card.
- The card sends the EAP response (AKA/Challenge packet) to the network, which checks the validity of the RES, computes the MAC and compares it with the received MAC.
- If verifications are successful, the network sends the success packet to the card and the ME retrieves the key material (master session key MSK and extended master session key EMSK) from EF<sub>EAPKEYS</sub>. The ME uses the key material for security purposes such as the security for WLAN link layer.

**To perform a full EAP authentication using the EAP-AKA method for GemXplore Generations Flexible cards:**

- 1 In the GemXplorer Structure view, select the USIM and right-click **EAP-AKA Authenticate**.
- 2 In the GemXplorer File view, double-click **EF<sub>KEYOP</sub>**.
- 3 In the **Interpreted** tab, select the encryption algorithm from the drop-down list in the **Algorithm identifier** box.
- 4 Select the **3G** tab, enter the **Key value**.  
**For example:**  
**Key value (in hexa):** 46 5B 5C E8 B1 99 B4 9F AA 5F 0A 2E E2 38 A6 BC
- 5 If **Milenage** is chosen as the encryption algorithm:
  - Click to select **OP** or **OPc**. Enter the **OP/OPc value** and click **Update**.  
**For example:**  
**OPc value (in hexa):** CD 63 CB 71 95 4A 9F 4E 48 A5 99 4E 37 A0 2B AF

- Select the **Constants** tab, enter the C1 to C5 and R1 to R5 parameters used by the 3G Milenage algorithm.

**For example:**

**C1 (in hexa):** 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

**C2 (in hexa):** 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01

**C3 (in hexa):** 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02

**C4 (in hexa):** 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04

**C5 (in hexa):** 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08

**(In decimal) R1:** 64, **R2:** 0, **R3:** 32, **R4:** 64, **R5:** 96

You may take the same C1 and R1 values as given in the following **Parameters**.

---

**Note:** C1 to C5 and R1 to R5 are parameters used by the 3G Milenage algorithm. These values are only specific to each operator/card and cannot be chosen arbitrarily. Hence, you must enter the correct values defined for the card you are using.

---

- 6 Select the **Identity** tab, enter an EAP identity and click **Send**. Your current identity will then be displayed in the card results.
- 7 Select the **AKA/Identity** tab, select the **Required Identity** to be used and click **Send** to send an AKA/Identity request to the card. The network uses parameters entered previously together with the session keys from AKA mechanism to generate the EAP-AKA related keys.
- 8 Select the **AKA/Challenge** tab, select the encryption algorithm from the drop-down list in the **Algorithm** box.

---

**Note:** If the Milenage algorithm is selected, clicking on **Parameters** permits the personalization of the default algorithm set values.

---

- 9 Click **Parameters >>** to enter the C1 to C5 and R1 to R5 values. Then click **Save** and **<< Parameters**.

**For example:**

**C1 (in hexa):** 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

**C2 (in hexa):** 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01

**C3 (in hexa):** 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02

**C4 (in hexa):** 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04

**C5 (in hexa):** 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08

**(In decimal) R1:** 64, **R2:** 0, **R3:** 32, **R4:** 64, **R5:** 96

---

**Note:** C1 to C5 and R1 to R5 are parameters used by the Milenage algorithm. Their values are specific to each operator/card and cannot be chosen arbitrarily. Hence, you must enter the correct values defined for the card you are using.

---

- 10 Enter the network's **Key Value**, **OPc Value** or **OP Value**, **AMF**, **SQN**, **Random** values and **IV**.

**For example:**

**Key value (in hexa):** 46 5B 5C E8 B1 99 B4 9F AA 5F 0A 2E E2 38 A6 BC

**OPC value (in hexa):** CD 63 CB 71 95 4A 9F 4E 48 A5 99 4E 37 A0 2B AF

**AMF (in hexa):** B9 B9

**SQN (in hexa):** 55 F3 2F B4 35 77

**Random (in hexa):** 23 55 3C BE 96 37 A8 9D 21 8A E6 4D AE 47 BF35

**IV (in hexa):** 25 63 4A CB A5 37 A8 48 21 8A E6 4D AE 47 37 2B

**11 Click Send.**

The results such as AUTN, IK, AUTS, RES, CK, K\_encr, K\_aut, MSK and EMSK are sent to the card via the **Success** tab or **Failure** tab.

---

**Note:** If you are performing a re-authentication in the **AKA/Re-Authentication** tab, do not close the authentication viewer.

---

### EAP-AKA Re-Authentication

You may also choose to use the re-authentication process for the next EAP-AKA session instead of a full EAP-AKA authentication if the AKA/Challenge request obtained previously contains a fast re-authentication identity. This fast re-authentication identity is a temporary identity which will be deleted after subsequent authentication is processed.

The steps are as follows:

- the network sends the AKA/Identity request to the card.
- the card sends the AKA/Identity response to the network using fast re-authentication identity.
- the network sends the AKA/Re-authentication request to the card
- the card sends the AKA/Re-authentication response to the network
- If verifications are successful, the network sends the success packet to the card and the ME retrieves the key material (MSK and EMSK) from EFEAPKEYS. The ME uses the key material for security purposes such as the security for WLAN link layer.

#### To perform an EAP re-authentication using the EAP-AKA method for GemXplore Generations Flexible cards:

- 1 In the GemXplorer Structure view, select the USIM and right-click **EAP-AKA Authenticate**.
- 2 In the **AKA/Re-authentication** tab, enter the **Nonce S** and **IV** values.
- 3 Click **Send**.

The results MSK and EMSK are sent to the card via the **Success** tab or **Failure** tab.

## EAP Files

These files are involved in the management of EAP and are stored under ADFUSIM or ADFISIM.

To use the EAP functionality, information have to be contributed to some or all of these files to establish the security and authentication process.

### EAP Mandatory Files

- EAP Derived Key - 4F 01h
- EAP Authentication Status - 4F 02h

Please refer to the ETSI TS 102.310 standard for more details.

### EAP Related Files

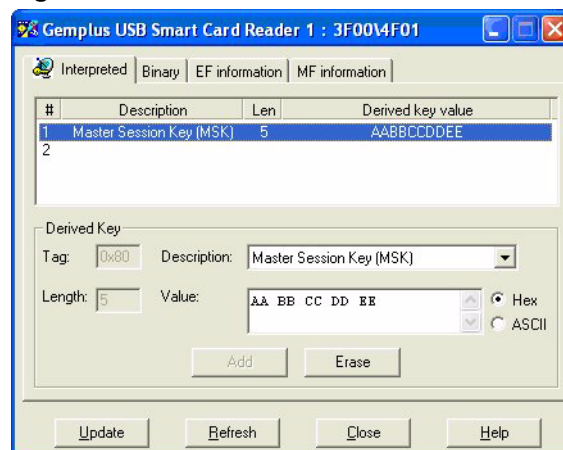
- EAP Permanent User Identity - 4F 03h
- Pseudonym - 4F 04h
- Pseudonym - 4F 41h

- User-Controlled PLMN WLAN - 4F 42h
- Operator-Controlled PLMN WLAN - 4F 43h
- User Preferred WLAN Specific Identifier (WSID) for WLAN - 4F 44h
- Operator Preferred WLAN Specific Identifier (WSID) for WLAN - 4F 45h
- WLAN Re-Authentication Identity - 4F 46h

### EAP Derived Key

EFEAP DERIVED KEY (4F 01h) indicates the key material (MSK and EMSK) that are derived after a successful EAP authentication. These keys in the form of TLV format may be used for subsequent authentications.

**Figure 62 - EFEAP DERIVED KEY**



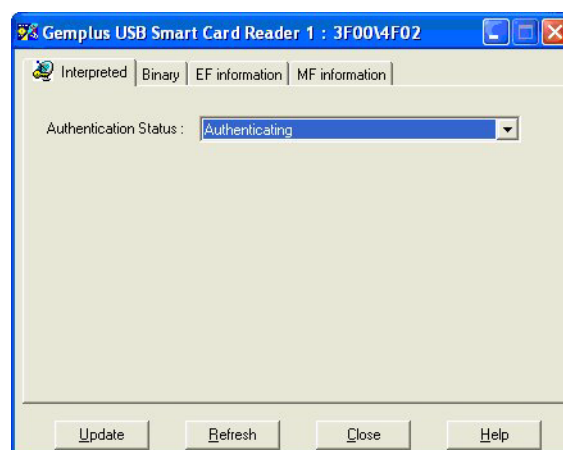
### EAP Authentication Status

EFEAP AUTHENTICATION STATUS (4F 02h) displays the authentication status supported by the EAP functionality.

The authentication statuses are coded as follows.

- 00h: No authentication started.
- 01h: Authenticating
- 02h: Authenticated
- 03h: Held (Authentication failure)

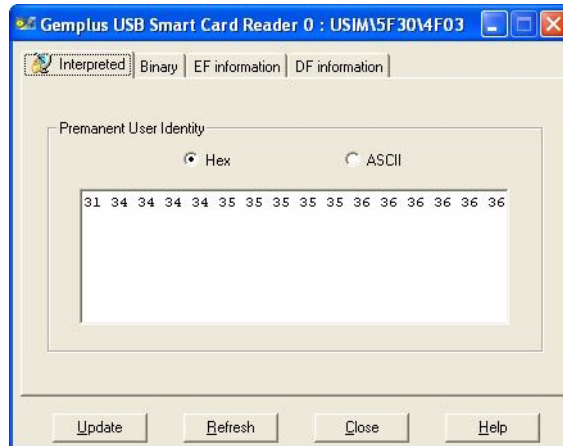
**Figure 63 - EFEAP AUTHENTICATION STATUS**



## EAP Permanent User Identity

EF EAP PERMANENT USER IDENTITY (4F 03h) contains the permanent user identity which may be used as the username part of the Network Access Identifier.

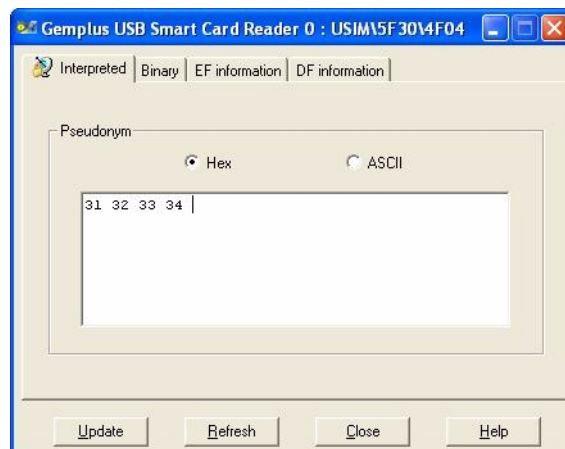
**Figure 64 - EF EAP PERMANENT USER IDENTITY**



## Pseudonym

EF PSEUDONYM (4F 04h) is used to store the temporary user identifier which is a pseudonym type. The pseudonyms obtained may be part of a previous authentication sequence and is used for the next EAP authentication. Pseudonyms are also used as the username part of the Network Access Identifier.

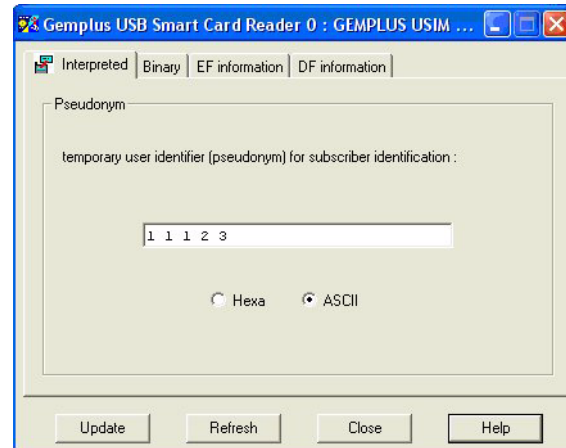
**Figure 65 - EF PSEUDONYM**



## Pseudonym

EFPSEUDONYM (4F 41h) contains a pseudonym, a temporary user identifier from a previous EAP authentication process, to be used for subscriber identification to gain entry to the WLAN.

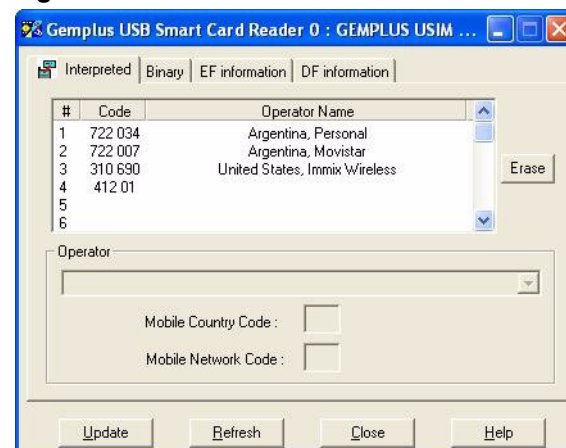
**Figure 66 - EFPSEUDONYM**



## User-Controlled PLMN WLAN

EFUPLMNWLAN (4F 42h) is a transparent file containing the coding of preferred PLMNs to be used for WLAN PLMN Selection. This information, set by the subscriber, defines the subscriber's preferred PLMNs in order of priority. The first PLMN entry in the list determines the highest priority and the nth PLMN entry indicates the lowest priority. PLMN codes identify GSM networks uniquely worldwide. They comprise a Mobile Country Code (MCC) and a Mobile Network Code (MNC).

**Figure 67 - EFUPLMNWLAN**



## Operator-Controlled PLMN WLAN

EFOPLMNWLAN (4F 43h) is a transparent file containing the coding of preferred PLMNs to be used for WLAN PLMN Selection. This information, set by the operator, defines the operator's preferred PLMNs in order of priority. The first PLMN entry in the list determines the highest priority and the nth PLMN entry indicates the lowest priority.

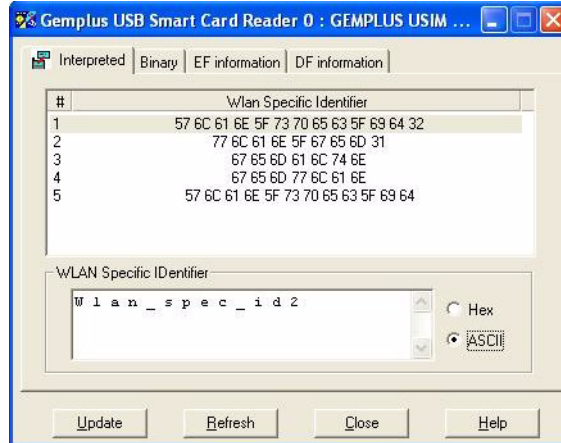
PLMN codes identify GSM networks uniquely worldwide. They comprise a Mobile Country Code (MCC) and a Mobile Network Code (MNC).



## User Preferred WLAN Specific Identifier (WSID) for WLAN

EFUWSIDL (4F 44h) contains a list of user's preferred WLAN specific identifier (WSID) for WLAN selection in order of priority. The first record in the list determines the highest priority and the nth record indicates the lowest priority.

**Figure 68 - EFUWSIDL**



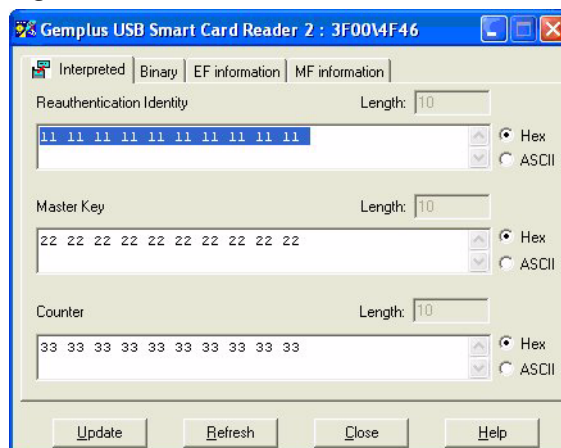
## Operator Preferred WLAN Specific Identifier (WSID) for WLAN

EFOWSIDL (4F 45h) contains a list of operator's preferred WLAN specific identifier (WSID) for WLAN selection in order of priority. The first record in the list determines the highest priority and the nth record indicates the lowest priority.

## WLAN Re-Authentication Identity

EFWRI (4F 46h) is a transparent file containing the list of parameters (WRI), which is used for fast re-authentication. The purpose of these parameters is to make use of the re-authentication identities and related parameters (such as the master key and counter values) generated from a previous authentication sequence as the user name part of the NAI for WLAN access re-authentication.

**Figure 69 - EFWRI**





# Working in the Card Manager Mode

This chapter describes tasks specific to cards that support the Open Platform (OP) framework. OP is a generic framework for the management of multi-application smart cards. It extends basic Java Card functionality by adding mechanisms for managing the applications on the card throughout their life, from installation through to eventual deletion or deactivation. The Visa Open Platform (VOP) is an extension of OP that supports additional sophisticated security features for use in security-sensitive business areas such as banking and other financial applications.

OP/VOP compatible cards support a predefined set of commands. You can use these commands to, for example:

- Load and install applications (Java Card applets) onto the card.
- Manage the card's security by, for example, setting up a secure channel between the card and the terminal then updating authentication keys.

GemXplorer automatically adds OP/VOP-related items to the card's contextual menus when an OP/VOP compatible smart card in a card reader is identified.

For example, Gemalto's GemXplore Xpresso V3 card is a Java card that is OP/VOP compatible and any compatible Java applet can be loaded into this card and run securely and independently.

The Card Manager applet is an applet that acts as a card administrator in an OP/VOP card. It provides services such as key handling, encryption and decryption of data, digital signature generation and verification, application loading, and general management of the card's contents. The Card Manager assumes responsibility for managing all application installation on the card, including, for example, SIM Toolkit applications.

In order to access the applets installed and functions available in the Card Manager via Card ADMIN, it is necessary to first select **Card Manager** in the **Select Mode** window. Refer to "Selecting the Card Manager Applet" on page 128.

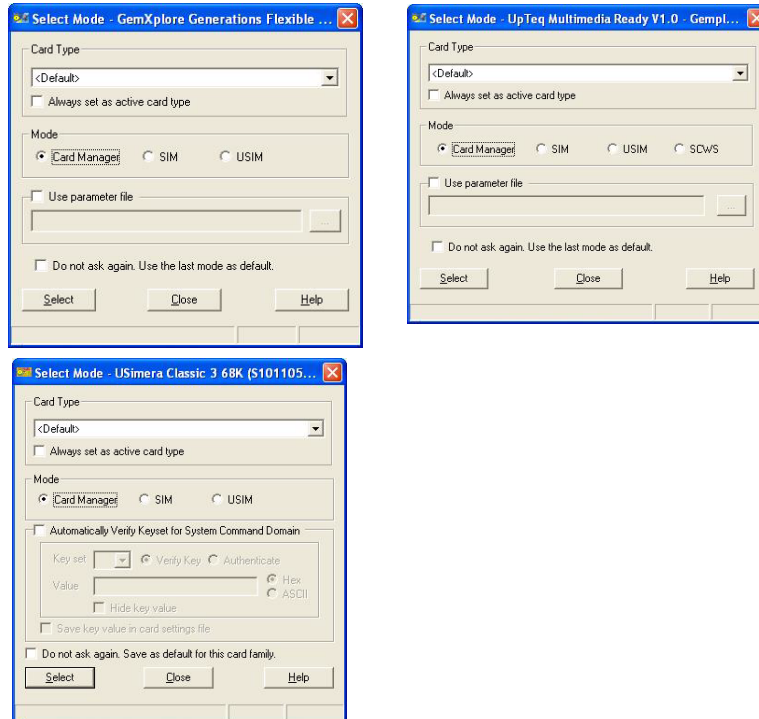
## Selecting the Card Manager Applet

To work with the Card Manager:

- 1 Insert a Java card into the smart card reader.

Card ADMIN will detect it and the **Select Mode** window will be displayed depending on the card inserted.

**Figure 70 - Examples of Select Mode — Java Card**



Select **Card Manager** to access the applets installed and functions available in the Card Manager.

The **Card Type** list displays the types of cards associated with the ATR of the card in the reader and highlights the card type in the reader. You can change the current card type associated to the card in the reader by changing the selection from the list. The active card type is displayed as the first in the list.

To modify the active card type and set it to the card type you have selected, check the **Always set as active card type** box and Card ADMIN will then associate the card to the new card type the next time the card is inserted. You can associate more card types to an ATR via the ATR Manager.

For some cards, there is an option to use a previously saved parameter (\*.out) file by selecting the **Use parameter file** box and browse to select the file.

To save the mode that you have just selected, select **Do not ask again. Save as default for this card family**. The next time you use a card from the same card family type, the Select Mode window will not appear to prompt you for a selection again.

The **Automatically Verify Keystore for System Command Domain** option may be available depending on the cards you are working with. You may deselect the 'Automatically Verify Keystore for System Command Domain' so that the key set verification for system command domain will not be automatically made.

You can check a card's default card type by accessing the Card Information window through the contextual menu of the top-level icon of the card media in the GemXplorer's Structure view.

Refer to "Viewing the File Structure of a Card" on page 26 for more information on how to view the contents of a card.

## The Card Settings File

In order to perform most operations such as scanning installed applets, managing keys and downloading an applet, it is necessary for Card ADMIN to set up a secure channel with the Card Manager. In order to do this, Card ADMIN uses keys that are defined in a ".card" card settings file. One card settings file is associated with each card type and the card settings file for predefined card types are stored in the *installdir*\Data directory. The key information in the card settings file is enciphered and you must use the editor provided in Card ADMIN to change its contents.

### To change the card settings file associated with a card type:

- 1 Right-click the top-level icon of the card media in GemXplorer's Structure view and select **Card Settings File** then **Select** from the contextual menu.
- 2 Select the card settings file (.card) to use.
- 3 Optionally, select **Set the file as default for the {Card Type}**. The card you select then appears as the default card settings file on all windows that require the card settings file for that card type to be specified.
- 4 Click **Open**.

### To change the card settings file parameters for the current card type:

- 1 Right-click the top-level icon of the card media in GemXplorer's Structure view and select **Card Settings File** then **Management** from the contextual menu.
- 2 The **Card Settings File Management** window is displayed. Here you can modify all the parameters held in the file and used by the current card type.

---

**Note:** Only the Card Settings file parameters supported by the current card type are displayed. Other parameters in the file that are not displayed.

---

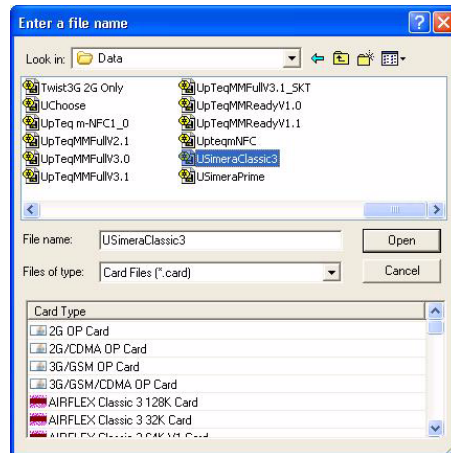
For more information about the parameters and settings, click the **Help** button.

- 3 Click **Update** to save the changes to the settings file.

To change the card settings file parameters with no card selected:

- 1 Select **Tools > Card Settings Management** from the GemXplorer menu bar. The **Card Settings File Selection** window is displayed.

**Figure 71 - The File Selection Window**



- 2 Select the Card Settings file that you want to update and select the **Card Type** parameters that you want to change. Click **Open** to continue.
- 3 The **Card Settings Management** window is displayed. Here you can modify all the parameters held in the file and used by the selected card type.  
For more information about the parameters and settings, click the **Help** button.
- 4 Click **Update** to save the changes to the settings file.

## Getting Card Manager Properties

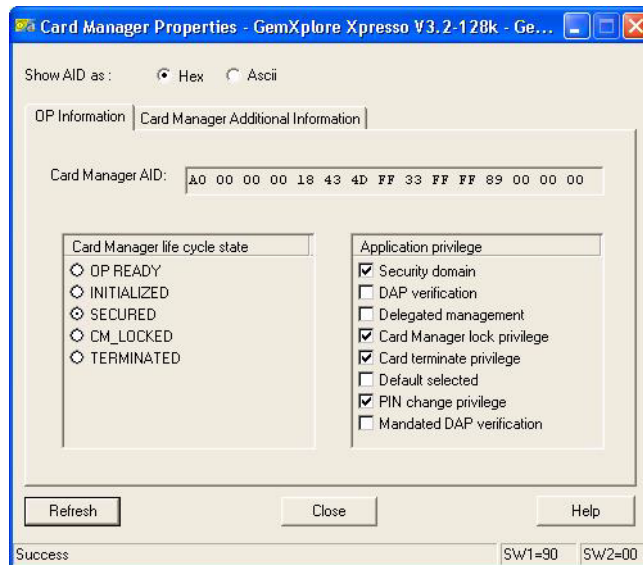
The Card Manager applet is always in one of a set of defined life cycle states, which in turn determine the level of card functionality that is available. You can use GemXplorer to view the current life cycle state of the Card Manager applet together with other relevant information.

**To view the Card Manager's current life cycle state:**

**Note:** Ensure that the card media you are using is OP/VOP compatible for example, the GemXplore Xpresso V3 card.

- 1 Right-click on the card's top-level icon in the Structure view and select **Card Manager Properties**. The **Card Manager Properties** window is displayed:

**Figure 72 - The Card Manager Properties Window**



The **Card Manager AID** and current **Card Manager life cycle state** are displayed in the left-hand column.

The right-hand column displays the current **Application privilege**, which the Card Manager applet uses to control the access rights and runtime behavior of applications installed under the Card Manager applet's control. You cannot modify any of the values displayed.

Click **Refresh** to update the display at any time.

- 2 If you are working with Gemalto OP/VOP compatible media (for example, a GemXplore Xpresso V3 card), click the **Card Manager Additional Information** tab to access additional Gemalto proprietary card manager information about the number of applets installed on the card and the amount of volatile and non-volatile memory available on the card.
- 3 Click **Close** to close the window.

**Note:** The **Card Manager Additional Information** and **Security Domain** tabs are available only on certain Gemalto OP/VOP compatible cards.

## Card Manager Commands

The following lists the types of commands available when the card is in the Card Manager mode. For more information about the use of the commands, click the **Help** button in the command window.

### Setting Up an OP Secure Channel

A secure channel to an applet must be established before any OP-specific commands (for example, creating cryptographic key sets) can be sent to the applet. Normally you define the settings required to establish a secured channel in a Card Settings file and this is processed automatically to establish the secure channel when the card media is first accessed.

### Secured APDU Exchange

After a secured channel has been established, you can send APDU commands to the card using the secured exchange mode.

### Secured ATF Trace

To enable multiple commands to be monitored and replayed through the secured channel, a Secured ATF Trace mechanism is provided. This works in exactly the same way as the standard ATF trace mode but has support for the security mechanism.

### Putting Key Sets

This command is only available on OP-compatible cards. The Put Key command allows you to work with cryptographic keys for the card.

### Getting and Putting Data Objects

The OP 2.0.1 commands **Get Data** and **Put Data** manage tag-length-value (TLV) objects associated with a card by retrieving or setting the value of the TLV. You can identify the TLV object either using predefined tags, or a 2-byte custom tag value.

---

**Note:**

- On certain Gemalto cards, the **Get/Put Data** command may appear as **Get Data** on the contextual menu.
  - On Avisa cards, the **Get Data** command operates in the SIM mode.
  - On Avisa, Simera and USimera cards, the **Key Management** command is used instead of the **Put Key** command.
- 

### Select

This command is used in order to select an applet for use and only one applet on a card can receive, execute and respond to APDU commands at any one time. This is the “selected” applet. One applet is selected by default. In the early stages of a card’s life, the Card Manager applet is typically selected as the default applet. In later stages of the card’s life, a custom Java Card or SIM Toolkit applet may be specified as the default applet.

Before exchanging APDU commands with a custom applet, you must select the applet for use. For example, before issuing any GSM-specific commands, you must explicitly select the GSM Application for use.



## Get Status

The Get Status OP command is used to display information about applets resident on a card using specified search criteria such as the application identifier (AID) or life cycle state. For example, you can display a list of all custom applications on a card that are in the SELECTABLE status.

## Set Status/Set Privilege

The Set Status/Set Privilege OP commands are used to update the life cycle state/status of applets resident on a card using their application identifiers (AIDs).

## PIN Change/Unblock

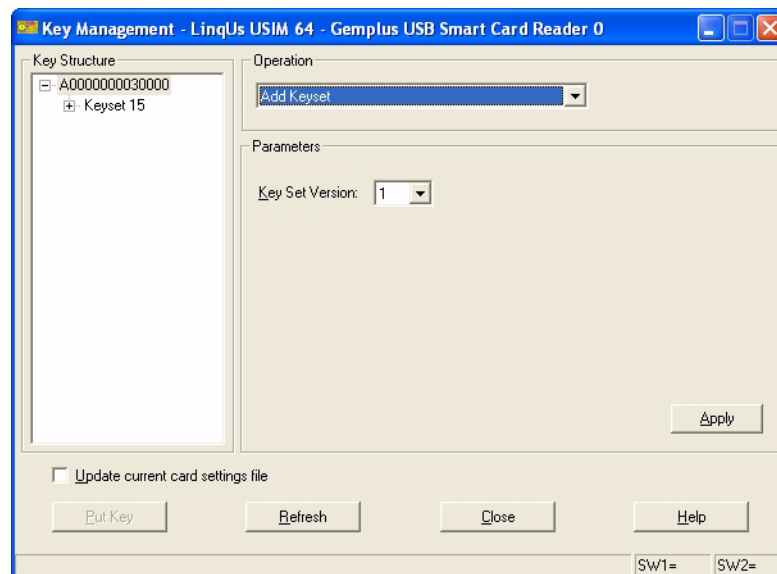
This command is used to create, update or unblock the card Global PIN. The 8-byte PIN structure is defined in accordance with Visa Open Platform specifications. This PIN is not related to the CHV or PIN codes used by GSM or any other telecom technology applications that may also be present on the card.

# Managing Key Sets

This feature allows you to control the use of key set versions and its keys. These controls enable you to:

- Add and update existing key set information.
- Load information such as the key index, algorithm ID, key values and status of the key from the card settings file (\*.card) created in the Card Settings File Management window.
- Rename an existing key set version with a new one.
- Modify the security level of selected key sets.
- Reset the setting in the command domain.
- Modify the access domain that is granted with the selected key set.

**Figure 73 - An Example of Key Management**



Secure methods of key management are performed depending on the current state of the card and the access right granted.

- When the card state is in the **OP READY** state and **Key Admin** command domain access is granted, you can create new key sets and update the key values of existing key sets. In addition, the key set version can be modified by checking the **Rename this key set version with new key set version box**.
- If the card state is in the **OP READY** state and **Perso** command domain access is granted, you can update the **Security level**, **Access Domain** and **Command Domain** fields.
- If the card is in the **SECURED** state and **Key Admin** command domain access is granted, you can update the key values and the key set version can be modified by checking the **Rename this key set version with new key set version box**.

## Using the Application Manager

This section outlines how to use the Application Manager tool supplied with the Card ADMIN.

For more information on Application Manager tool, check with your Gemalto Technical Consultant.

## Introduction

The main features of the Application Manager are:

- Provides an easy to use “application repository” in which to store information about the applications that are ready to be loaded onto cards. You can create, copy, import, export, and delete applications and modify their properties.
- Supports downloading applications to real cards.
- Supports two loading modes:
  - “Over-the-air” (OTA) mode, which uses the 3GPP TS 23.048 Short Message Service (SMS) facility to remotely download applications. The Application Manager generates the appropriate envelope commands and parameters and sends the application to the target card encapsulated within one or more SMS point-to-point data download messages.
  - “Input/Output” (I/O) mode, where the Application Manager sends Open Platform commands directly to the Card Manager applet on the target card.
- Uses *card profiles* to configure all the parameters necessary to send applications to specific card types in I/O or OTA mode. Each card profile is based on a template. A preconfigured and tested template is supplied for each of the sample card types delivered with the product you have purchased, for example, the GemXplore Xpresso V3”. You can create, copy, import, export and delete card profiles and modify their properties as necessary.
- Provides flexibility in terms of the tasks you can perform. For example, you can load packages that contain only Java library classes referenced by other applets, load packages and install several different applets from the package, or create multiple instances of an applet that has already been loaded onto the card. You can also choose to perform separate load and install operations. For example, you load a package initially, then install the applets it contains at some later time.
- Allows you to debug the load and install process by means of an easy to understand trace window.
- Allows you to play an ATF or CSV script after a successful installation of an applet.
- Improves transport management in supporting SMS concatenation.

## Overview of Defining and Running an Application

*To define and run an application:*

- 1 Start the Application Manager.
- 2 Configure the terminal profile settings (if working in the OTA mode).
- 3 Select the terminal containing the target card.
- 4 Create, configure, or select the application to load into the target.
- 5 Select the loading mode.

- 6 Create, configure, or select a suitable target card profile for the card.
- 7 Select the action to perform on the application.
- 8 Execute the selected action.
- 9 Optionally, analyze the results in the **Trace** panel.

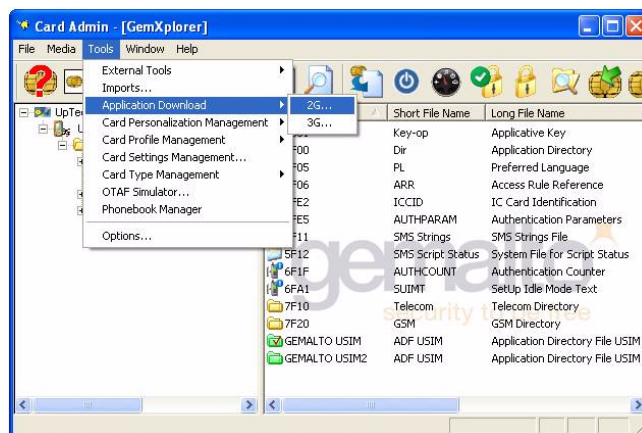
## Starting the Application Manager

### To start the Application Manager:

In GemXplorer Structure view, right-click the icon representing the card type, together with the card's name and card reader type and select **Application Download...** .

Alternatively, the Application Manager can be launched from **Tools > Application Download > 2G** or **3G**. In this case, selecting a terminal is possible.

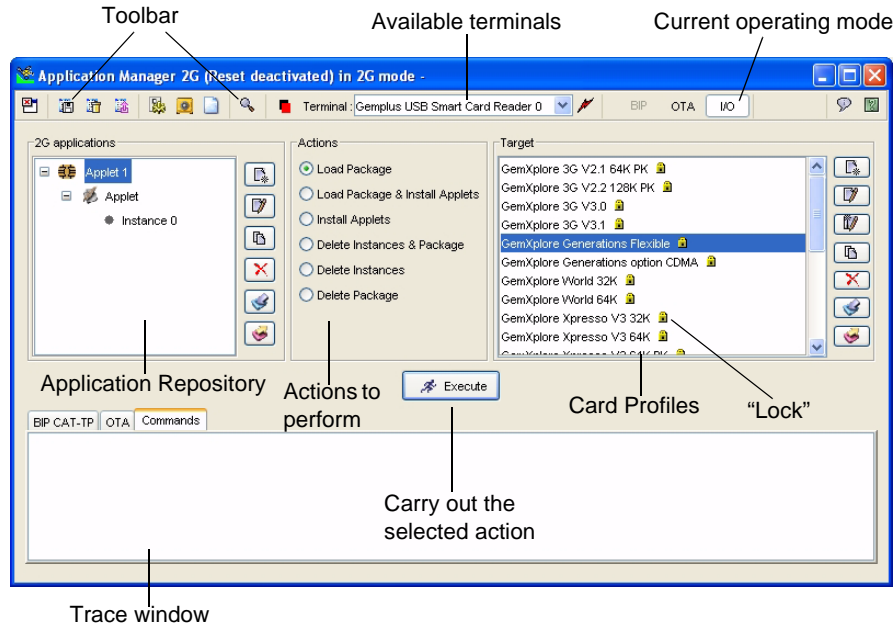
**Figure 74 - Starting the Application Manager**




## The Application Manager Window

When first started, the main window of the Application Manager is displayed, as shown in “Figure 75”:

**Figure 75 - The Application Manager Main Window**



Refer to the online help for further information on the meaning of each of the controls on the main window (click  in the top right-hand corner of the window).

**Note:** The “lock” displayed beside a card profile denotes that it is a generic profile and cannot be modified (in I/O mode).



# Working in the SCWS Mode

This chapter describes GemXplorer's SCWS-specific features.

Service providers deploy multimedia services via the use of Smart Card Web Server (SCWS) to facilitate user interaction over the wireless communication networks.

SCWS uses the application protocol — hypertext transfer protocol (HTTP) as defined in the Open Mobile Alliance (OMA) specifications to establish the connection via the static pages stored in the SCWS. These static pages contain links to the external sites which are controlled by the service providers.

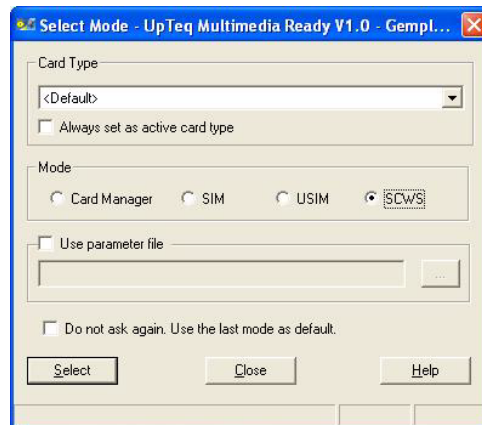
## Selecting the SCWS Application

To work in the SCWS mode:

- 1 Insert a multimedia card in the smart card reader.

The **Select Mode** window is automatically displayed.

**Figure 76 - Selecting SCWS Mode**



**Note:** You can access the SCWS functions and its file system only after setting up a secure communication channel with successful authentication to the Card Manager. Otherwise, an error message will be displayed after selecting the SCWS mode. Refer to the **Help** button for information about establishing a secure communication channel.

- 2 The **Card Type** list displays the types of cards associated with the ATR of the card in the reader and highlights the card type in the reader. You can change the current

card type associated to the card in the reader by changing the selection from the list. The active card type is displayed as the first in the list.

- 3 To modify the active card type and set it to the card type you have selected, check the **Always set as active card type** box and Card ADMIN will then associate the card to the new card type the next time the card is inserted. You can associate more card types to an ATR via the ATR Manager.
- 4 Select **SCWS** to access the SCWS file system and functionality.  
To save the mode that you have just selected, select **Do not ask again. Use the last mode as default**. The next time you use a card from the same card family type, the **Select Mode** window will not appear to prompt you for a selection again.
- 5 For some cards, there is an option to use a previously saved parameter (\*.out) file by selecting the **Use parameter file** box and browse to select the file.
- 6 You can check a card's default card type by accessing the Card Information window through the contextual menu of the top-level icon of the card media in the GemXplorer's Structure view.

## Working with SCWS application

You can view the SCWS application and its file system depending on:

- Whether the appropriate multimedia card is used.
- Whether or not the appropriate permissions to users and realms have been acquired.
- Whether URLs are registered.

## Browsing SCWS File Systems

Refer to “Managing Card Data” on page 26 for information such as viewing the contents of a card, protection commands and viewing the contents of a file.

## Configuring SCWS

The ota.conf file in the **Static Pages > SCWS** allows you to configure the network connectivity parameters that are used between the Smart Card Web Server (SCWS) and the server.

To access this file, right-click ota.conf in the file view and select **Open**. The Open window contains the four tabs that are configurable in SCWS:

- Connection
- Security
- Retry Policy
- Agent Http Post

For a detailed description of each setting, refer to the contextual help displayed by clicking the Help button in the respective tab.



## Connection

This tab allows you to establish a point-to-point TCP connection between the Smart Card Web Server and the server.

You can choose to activate this connection or disable it. Additionally, you can set the **Bearer Description** and **Data Destination Address** so that retrieval of these information is possible.

## Security

This tab allows you to configure the Transport Layer Security (TLS) layer. You can choose to enable or disable the check for **PSK-Identity** and **Card Key-Identifier** whenever a SCWS application is connected.

If PSK-Identity is enabled, Card ADMIN will authenticate the keys specified in the SCWS and if Card Key-Identifier, Card ADMIN will verify key value used. Only successful authentication of the keys will establish the connection to the service provided.

## Retry Policy

This tab allows you to reconnect the terminated session due to administrative failures such as network coverage failure or when the server is not responding.

## Agent Http Post

This tab allows you to send a **Post** request to the SCWS. It contains the **Administration Host**, **Agent ID parameter** and **Administration URI parameter** which defines the parameters to be used in the **Post** request.

# SCWS Management in GemXplorer

In GemXplorer, you can manage the SCWS sessions via the contextual menu.

### To manage SCWS sessions via the contextual menu:

In the GemXplorer Structure view, right-click the **SCWS Administration Application** and select **Manage Users and Protection Sets** in the GemXplorer Structure view.

For more information about the use of the SCWS commands, click the **Help** button in the command window.

## SCWS Commands

This group of commands enables you to manage the directories and files, and protections under the SCWS application. The following commands, sorted in alphabetical order, are available depending on the level that you have selected.

<b>Card Content Report</b>	Use this command to generate content report for the card.
<b>Create Directory</b>	Use this command to add new directories.
<b>Delete</b>	Use this command to remove a file or a directory.
<b>Delete Multiple</b>	Use this command to remove several files from the same directory at a time.
<b>Map</b>	Use this command to connect a registered application to an incoming request via the URI. If there are no available registered menu items to be mapped, this context menu will not be displayed.
<b>Unmap</b>	Use this command to disconnect a mapped application which is linked to an incoming request via the URI.
<b>Manage Users and Protection Sets</b>	This command is only accessible by the server administrator. Use this command to manage the security parameters (such as the user accounts and setting permissions to domains) accessing the realms.
<b>Manage Users and Realms</b>	This command is only accessible by the server administrator. Use this command to create realms and manage the security parameters (such as the user accounts and setting permissions to domains) accessing the realms.
<b>Navigate</b>	Use this command to navigate from one Web page to another.
<b>Open</b>	Use this command to open a configuration file.
<b>Protect</b>	Use this command to protect the selected file. If an existing protection set is available, the existing protection set is displayed as the sub-menu item on the same level with the "New Protection set" under this command.
<b>Unprotect</b>	Use this command to unprotect the selected file. A message will be returned when this command is executed successfully.
<b>Properties (of Security Domain)</b>	Use this command to view the capacity (used and free space) of the Smart Card Web Server application.
<b>Properties (of File)</b>	Use this command to view the property information of the selected file.
<b>Put File</b>	Use this command to add or modify files.
<b>Put Directory Content</b>	Use this command to add or modify directories.
<b>Security Domain Settings File</b>	Use this command to view Security domain settings data and to create custom settings.  <b>Note:</b> If SCWS and Card Manager contain the same applet instances, you will need to manually add the Security domain settings file again after selecting the SCWS mode and reuse the same keys as in the card settings file.

<b>Site Extraction Wizard</b>	Use this command to perform an extraction of the contents from the SCWS and store them in your PC.
<b>Refresh</b>	Use this command to update the currently displayed view.
<b>Register URI</b>	Use this command to connect a security domain to a URI.
<b>Unregister URI</b>	Use this command to disconnect a security domain which is linked to a URI.
<b>Resize Static Pages Container</b>	Use this command to increase or reduce the size of static pages.
<b>View</b>	Use this command to view the selected file.



# Working In the CDMA Application Mode

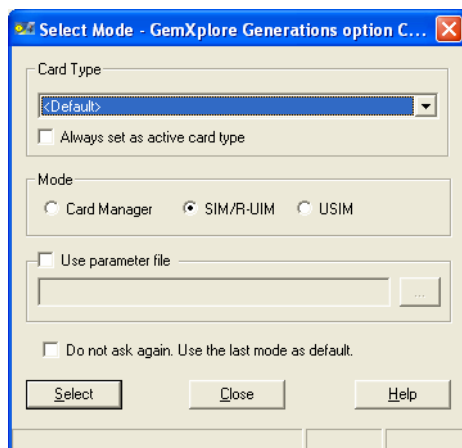
This chapter describes GemXplorer's CDMA-specific features. For 2G and Card Manager-specific features, refer to the *Card ADMIN Getting Started* document for more information.

## Selecting the CDMA Application

To work in the CDMA mode:

- 1 Insert a card into the smart card reader.  
The **Select Mode** window is automatically displayed.

**Figure 77 - Selecting the CDMA Mode**



- 2 Select **SIM/R-UIM** to access the CDMA application and the GSM functions and file system available for use or select **Card Manager** to access the applets installed and functions available in the Card Manager. Select **USIM** to access the USIM functions and file system available for use.

The **Card Type** list displays the types of cards associated with the ATR of the card in the reader and highlights the card type in the reader. You can change the current card type associated to the card in the reader by changing the selection from the list. The active card type is displayed as the first in the list.

To use a previously saved parameter (\*.out) file, select the **Use parameter file** box and browse to select the file. The \*.out file is a Gemalto production text file that stores a card's diversified data such as PIN codes and key values. When this

option is selected, the data stored in the \*.out file is retrieved and used during the setting up of a secure session with the Card Manager and during secret code verification.

To save the mode that you have just selected, select **“Do not ask again. Save as default for this card family”**. The next time you use a card from the same card family type, the Select Mode window will not appear to prompt you for a selection again.

## CDMA Commands

The following provides a brief description of the CDMA Commands. Refer to the CDMA Option online help for the steps to execute the commands or the card operating system’s reference manual for command details.

### Authentication Management Commands

The following authentication commands are used to verify that communication occurs only between validated entities, namely the mobile equipment and the network.

#### Authentication

The authentication command provides for the authentication of the base station and the mobile station. Refer to “Base Station Authentication” on page 152, “Mobile Station Authentication” on page 153, “SimpleIP Authentication” on page 160, and “MobileIP Authentication” on page 161 for details.

#### Store MEID

While Store ESN\_ME enables the electronic serial number (ESN) that is held in the mobile equipment to be saved and stored in the EFESN, Store ESN\_ME/MEID enables the MEID that is held in the mobile equipment identifier to be saved and stored in the EFESN. Refer to “Store ESN\_ME” on page 157 and “Store MEID” on page 157 for more details.

### Secret Code Management Commands

Sensitive files on a card are protected by security mechanisms. These require that one or more secret codes be provided before carrying out certain operations (for example, reading the content of a file, modifying a file or deleting a file). The secret code required for a given command is specified when the file is created. The conditions for accessing a file are available in the file’s properties.

For some cards, there is a Key set option available to allow you to choose the version to be used for the ADM codes before entering the code value.

#### Verify

This is used to perform verification of the PIN value. After a successful PIN entry, the associated authentication object is unlocked and any files protected by it will be accessible. When an incorrect PIN code is entered multiple times, the PIN code will be blocked. Depending on the authentication object settings, it may not be possible to unblock the PIN.

#### Change

This is used to change the value of an application/file code. Depending on the authentication object settings, it may not be possible to change a PIN value.

### Unblock

This is used to unblock a PIN value that has become blocked due to multiple incorrect submissions. Depending on the authentication object settings, it may not be possible to unblock a PIN value.

### Enable PIN

This is used to reactivate the PIN code protection mechanism for a particular PIN value. It is not always possible to reactivate a PIN and it depends on the specific setting in the application or file.

### Disable PIN

This is used to deactivate the PIN code protection mechanism for a particular PIN value. Once it is disabled, all objects and files protected by the associated authentication object will be unlocked. It is not always possible to deactivate a PIN and it depends on the specific setting in the application or file.

### Update Keys

This command allows you to update the secret key values of A-Key, SSD\_A and SSD\_B which are used in the authentication process.

---

**Note:** This feature is currently available for Simera Airflex Classic cards only.

---

## File and Application Management Commands

These commands are related to the activation of an application or file to be responsive to a set of commands.

### Select

Before communication can begin, an application or file must be targeted. The Select command does this by opening the communication with the application or file.

### Invalidate

Once an application or file is selected, you can limit the possible commands using the Invalidate command.

### Rehabilitate

This command is used to restore a previously invalidated application or file.

## EF Management Commands

The following commands allow you to adapt the EFs contained in the selected application.

### Create

This command is used to create a new transparent, linear fixed or cyclic EF.

### Delete

This command is used to delete an existing EF.

### Extend/Resize

This command is used to extend or resize a specified EF, with the exception of cyclic files.

### **Lock**

This command sets the access conditions of an EF to NEVER and is an irreversible command.

### **Terminate**

For GemXplore Generations Option CDMA cards only. Use this command to change the state of the DF/EF to terminated. This action is irreversible and will make a DF/EF unusable.

## **OTAPA/OTASP Commands**

Using the Over-The-Air (OTA) mechanism to transfer new data to a Gemalto CDMA card can be initiated by two sources: by the mobile in response to a user action (OTASP), or by the network in order to read or update parameters in the card (OTAPA). The OTA commands may be one of the six types:

### **Configuration Requests**

These commands — SSPR Configuration Request, Configuration Request and 3GPD Configuration Request retrieve parameters in the card.

### **Download Requests**

These commands — SSPR Download Request, Download Request and 3GPD Download Request update the OTA parameters in the card with new values.

### **SPC Change**

This command changes the Service Programming Code (SPC) value used for an on-card protection of parameters.

### **Commit Request**

This command stores and saves the downloaded parameters and SPC.

### **A-Key Generation**

This command executes the procedure to update the secret key in the card.

### **Secure/Fresh**

This command enhances the security between the network based Over-The-Air Service Provisioning entity and the mobile station, and protects sensitive subscriber information when the Fresh value and the message are encrypted together.



## Overview of CDMA Security Mechanisms

The security of the CDMA application environment is controlled by:

- Authenticating the base station, with the base station menu of the **Authentication** command. This is used by the mobile station (MS) to validate the network (the base station) as described in “Base Station Authentication” on page 152.
- Authenticating the mobile station, with menus of the **Authentication** command. This is used by the network to validate the MS at any time within the network (a global challenge) or when in a visiting network (a unique challenge). See “Mobile Station Authentication” on page 153.
- Authenticating the voice and message encryption keys with the Key\_VPM menu of the **Authentication** command. This is launched after authentication of the base station or the mobile station. See “Voice Privacy Mask” on page 155.
- Authenticating the access to high rate packet data (HRPD). This authentication is an access authentication function for 3G packet data service. See “HRPD Access Authentication” on page 159.
- Authenticating the user using SimpleIP. The access provider network assigns an IP address and supplies an IP routing address to a mobile station. See “SimpleIP Authentication” on page 160.
- Network authenticating the user via MobileIP. See “MobileIP Authentication” on page 161.
- Protecting CDMA application files by secret codes.

---

**Note:** CDMA authentication is possible only after correct presentation of CHV1 and when the current DF is DFCDMA (7F 25) or its subdirectory.

---

## CDMA Authentication Procedure

Authentication is a process by which one communicating party, the mobile station (MS) or base station (BS) proves its authenticity to the other. This proof is accomplished by:

- 1 Calculation of an authentication signature based on some secret data shared between the two and a mutually-known algorithm.
- 2 Exchange and then a comparison of the resulting signature for verification.
- 3 Authorization to communicate only if the signatures match.

The algorithm used in the Gemalto CDMA cards is the Cellular Authentication and Voice Encryption (CAVE) algorithm. The shared secret data is called SSD\_A and SSD\_B.

## Authentication Management Commands

The GemXplorer contextual menu in CDMA Option, has two commands concerned with CDMA authentication mechanisms:

- **Authentication**, containing windows for the authentication of:
  - the base station (BS)
  - the mobile station (MS), with two global challenge authentication mechanisms. Mobile Station Originating (MSO) and Mobile Station Registration Termination (MSRT), and one unique challenge authentication mechanism, Mobile Station Unique Challenge (MSUC)
  - Voice and message encryption, Key\_Voice Privacy Mask (VPM)
- **Store ESN\_ME/MEID**, which enables you to save the electronic serial number (ESN) or the MEID held in the mobile equipment into a specific card file (EFESN). Refer to “Store ESN\_ME” on page 157 and “Store MEID” on page 157.
- **Authentication Packet Data**, which is an authentication mechanism used by the access network authentication, authorization and accounting entity to validate the mobile equipment. This includes the HRPD, SimpleIP and MobileIP authentication.

## Authentication

The Cellular Authentication and Voice Encryption (CAVE) algorithm is used in calculating the authentication signatures and generation of encryption keys. This algorithm remains transparent to the user, but requires certain input parameters depending on the command.

### CAVE Input Parameters

The following variables are used by the CAVE algorithm to calculate signatures:

- **ESN**, the 7-byte electronic serial number assigned by the mobile station (MS) manufacturer which uniquely identifies the mobile equipment. The MS automatically supplies this value. The ESN\_ME is stored in the EFESN (6F 38). Refer to “Store ESN\_ME” on page 157 for details.
- **UIM\_ID**. The ESN value can be replaced with the UIM\_ID, the unique identity number of the user identity module, held in the EFUIMID (6F 31). The UIM\_ID emulates many of the functions of the ESN.

The flag which indicates which value to use in the ESN\_ME field (UIM\_ID or ESN\_ME) is held in the EF\_USAGE\_IND and is set with the Store ESN\_ME command.

- **SSD**, the shared secret data stored in the MS and known by the BS. It is composed of two calculated 8-byte sets: SSD\_A, used in generating the authentication signature and SSD\_B, used for generating the encryption mask.

The true SSD\_A and SSD\_B values are only displayed when recalculated during the base station authentication command. At other times, these values are displayed in the menu windows as a string of FFh values. The values of SSD\_A and SSD\_B must be known in advance or a base station authentication must be performed to automatically insert the correct values.

- **A-Key**, an 8-byte secret pattern used to generate and update the SSD stored in the MS. This secret key is stored in the MS and the Home Location Register (HLR). The A-Key value must be manually entered.

- **IMSI\_M/IMSI\_T**, two versions of the IMSI (International Mobile Station Identity):  
**IMSI\_M**: is based on the mobile identification number (MIN) for IMSI\_M. Two parts of the IMSI values are used in authentication: IMSI\_M\_S1 (bytes 4, 5 and 6) and IMSI\_M\_S2 (bytes 2 and 3). The MS automatically supplies this value.  
**IMSI\_T**: is the 'true' IMSI which does not store or use the MIN. If IMSI\_M is not programmed, the CAVE algorithm is calculated with the IMSI\_T value which has two parts, S1 (bytes 4, 5 and 6) and S2 (bytes 2 and 3) as does IMSI\_M.
- **Digits** of a dialed number. Its length must be indicated.
- **RAND**, a randomly generated number. Different random numbers are generated depending on their use.
- **RANDU**, a unique random challenge sent by the network.
- **Pseudo ESN**, a 32-bit number hashed from MEID.

#### Verification

The results of the authentication calculations of both parties is the authentication signature called AUTH. The AUTH of the challenged station is compared with that held by the validating station. If these values match, authentication is verified, and authorization to communicate is granted.

## Base Station Authentication

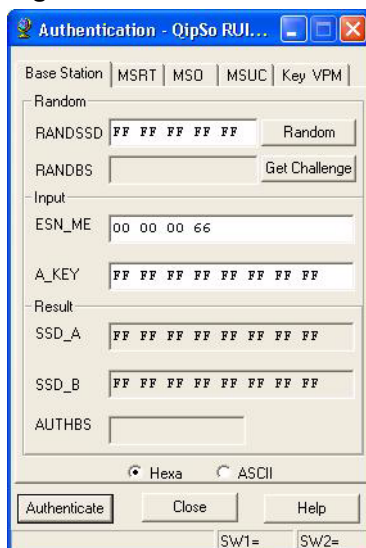
The Base Station Authentication process is as follows:

- 1 The RANDSSD is generated by the base station and sent to the card. The card then generates the RANDBS (initiated by the Base Station Challenge command). This value is sent to the base station via the mobile equipment for the base station to compute its AUTHBS.
- 2 The mobile equipment instructs the card to generate a new set of SSD keys via the CAVE algorithm with the ESN\_ME or UIM\_ID, the A-Key and the RANDSSD. With the new SSD\_A, the card calculates its AUTHBS via the CAVE algorithm with the ESN\_ME or UIM\_ID supplied by the UIM.
- 3 Authentication is verified if the signature AUTHBS matches the card's signature AUTHBS.

**To perform the AUTHBS calculation:**

- 1 In GemXplorer, right-click DFCDMA (7F 25) or one of its directories and select **Authentication**. You must have first correctly presented CHV1.
- 2 Select the **Base Station** tab and the following window is displayed.

**Figure 78 - Base Station Authentication**



- 3 Click to select the display mode: **Hexadecimal** or **ASCII**.
- 4 Click the **Random** button to display the randomly generated number RANDSSD.
- 5 Click the **Get Challenge** button to launch the generation of the random number, RANDBS, which is displayed. When this action is completed, the status bar displays "Success".
- 6 Type or modify the A-Key value (eight bytes). The ESN\_ME or UIM\_ID is supplied by the UIM.
- 7 Click **Authenticate**. If the card's AUTHBS and the AUTHBS from the base station match, the authentication is successful and a confirmation window is displayed.
- 8 Click **OK** in the confirmation window. The resulting AUTHBS, new SSD\_A and SSD\_B values are displayed.

**Note:** If you want to perform another base station authentication, you must re-launch the Get Challenge command by clicking the **Get Challenge** button.

## Mobile Station Authentication

There are three types of Mobile Station Authentication, depending when and where the challenge is made. These correspond to the three commands available under the GemXplorer **Authentication** contextual menu:

- **MSRT** (Mobile Station Registration or Termination) when the global (within the network) challenge procedure occurs at mobile station registration or call termination.
- **MSO** (Mobile Station Originating) when the global (within the network) challenge procedure occurs at call origination.
- **MSUC** (Mobile Station Unique Challenge) when the unique challenge procedure occurs when the subscriber is visiting in another network.

### MSRT (Mobile Station Registration or Termination)

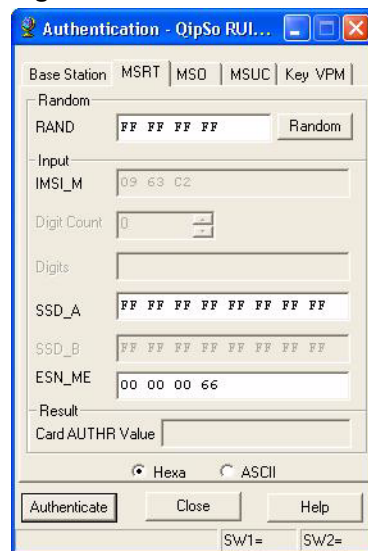
The following steps outline the mobile station authentication process for MSRT:

- 1 The network sends a RAND to the mobile station.
- 2 The card launches the CAVE algorithm to generate the resulting AUTH signature (called AUTHR) using the RAND, the card's SSD\_A, the IMSI\_M or IMSI\_T and the ESN or UIM\_ID.
- 3 Authentication is verified if the mobile station's AUTHR value (from the card) matches the network's AUTHR value (that is, from the base station).

#### To calculate the card's AUTHR value:

- 1 In GemXplorer, right-click DFCDMA (7F 25) or one of its directories and select **Authentication**. You must have first correctly presented CHV1.
- 2 Select the **MSRT** tab and the following window is displayed.

**Figure 79 - MSRT Authentication**



- 3 Click to select the display mode: **Hexadecimal** or **ASCII**.
- 4 Click the **Random** button to display the randomly generated number RAND. The IMSI\_M and ESN\_ME or UIM\_ID are supplied by the UIM (according to EFUSAGE\_IND (6F 42). The SSD\_A and SSD\_B values are displayed as a string of FFh values.

**Note:** The correct value of SSD\_A must be entered as incorrect values will cause the authentication to fail.

- 5 Click **Authenticate**. If the AUTHR calculated by the network matches that of the card, the authentication is successful and a confirmation window is displayed.
- 6 Click **OK** in the confirmation window. The resulting AUTHR is displayed.

### MSO (Mobile Station Originating)

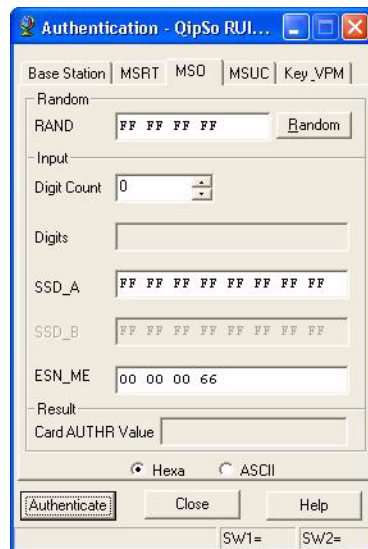
The following steps outline the mobile station authentication process for MSO:

- 1 The network sends a RAND to the mobile equipment.
- 2 The card uses the CAVE algorithm to generate the resulting AUTH signature called (AUTHR) using the RAND, the card's SSD\_A, dialed digits of the specified length (maximum three bytes) and the ESN or UIM\_ID (seven bytes).
- 3 Authentication is verified if the mobile station's AUTHR signature (from the card) matches the network's AUTHR signature, that is, from the base station.

#### To calculate the card's AUTHR value:

- 1 In GemXplorer, right-click DFCDMA (7F 25) or one of its directories and select **Authentication**. You must have first correctly presented CHV1.
- 2 Select the **MSO** tab and the following is displayed.

**Figure 80 - MSO Authentication**



- 3 Click to select the display mode: **Hexadecimal** or **ASCII**.
- 4 Click the **Random** button to display the randomly generated number RAND.
- 5 Set the number of digits (maximum is six, three bytes) and type the complete number.

The ESN\_ME or UIM\_ID is supplied by the UIM (according to EFUSAGE\_IND (6F42)). The SSD\_A and SSD\_B values are displayed as a string of FFh values.

**Note:** The correct value of SSD\_A must be entered as incorrect values will cause the authentication to fail.

- 6 Click **Authenticate**. If the AUTHR calculated by the network matches that of the card, the authentication is successful and a confirmation window is displayed.
- 7 Click **OK** in the confirmation window. The resulting AUTHR is displayed.

### MSUC (Mobile Station Unique Challenge)

There are three main steps in the MS authentication process:

- The network sends a RANDU to the mobile equipment.
- The card uses the CAVE algorithm to generate the resulting AUTH value (called AUTHU) using the RANDU, the card's SSD\_A, the IMSI\_M and the ESN or UIM\_ID (according to EFUSAGE\_IND (6F 42)).
- Authentication is verified if the mobile station's AUTHU value (from the card) matches the network's AUTHU value (that is, from the base station).

#### To calculate the card's AUTHU value:

- 1 In GemXplorer, right-click DFCDMA (7F 25) or one of its directories and select **Authentication**. You must have first correctly presented CHV1.
- 2 Select the **MSUC** tab and the following is displayed.

**Figure 81 - MSUC Authentication**

- 3 Click to select the display mode: **Hexadecimal** or **ASCII**.
- 4 Click the **Random** button to display the randomly generated number RANDU.
- 5 Set the number of digits (maximum is six) and type the complete number.

The ESN\_ME or UIM\_ID is supplied by the UIM (according to EFUSAGE\_IND (6F42)). The SSD\_A and SSD\_B values are displayed as a string of FFh values.

**Note:** The correct value of SSD\_A must be entered as incorrect values will cause the authentication to fail.

- 6 Click **Authenticate**. If the AUTHU calculated by the network matches that of the card, the authentication is successful and a confirmation window is displayed.
- 7 Click **OK** in the confirmation window. The resulting AUTHU is displayed.

## Voice Privacy Mask

This command is used to calculate the following keys used in the encryption processes:

- The cellular message encryption algorithm (CMEA) used for message encryption/decryption.
- The voice privacy mask (VPM) used for voice encryption.

These keys are used to calculate the AUTH value for the base and mobile stations.

The command calculations that produce the resultant AUTH vary depending when the command is launched: after a mobile station authentication (global or unique challenge) or after a base station authentication.

---

**Note:** This command relates to both global (made within the network) and unique (made from a visited network) challenges. In accordance with the CDMA terminology, RAND and AUTHR fields relate to a global challenge, and RANDU and AUTHU refer only to a unique challenge.

---

**To perform the AUTHR/AUTHU calculation for the encryption keys:**

- 1 In GemXplorer, right-click DFCDMA (7F 25) or one of its directories and select **Authentication**. You must have first correctly presented CHV1.
- 2 Select the **Key\_VPM** tab and the following is displayed.

**Figure 82 - Key VPM Authentication**

- 3 Click to select the display mode: **Hexadecimal** or **ASCII**.
- 4 Select the type of random number: **RAND**.
- 5 Click the **Random** button to display the randomly generated number RANDU/ RAND.

The ESN\_ME or UIM\_ID is supplied by the UIM (according to EFUSAGE\_IND (6F42)).

- 6 Set the number of digits (maximum is six) and type the complete number. The SSD\_A and SSD\_B values are displayed as a string of FFh values.

---

**Note:** The correct value of SSD\_A must be entered as incorrect values will cause the authentication to fail.

---

- 7 Define the length of the VPM displayed by first setting P2 (to define the last byte displayed) and P1 (to define the first byte displayed).
- 8 Click **Generate**. If the AUTHR calculated by the network matches that of the card, the authentication is successful and a confirmation window is displayed.
- 9 Click **OK** in the confirmation window. The resulting AUTHR is displayed with the CMEA key (eight bytes) and VPM key (length defined by P1 and P2 values).



## Store ESN\_ME

This command is used to store the electronic serial number from the mobile equipment into the card file EFESN. The ESN is one of the input parameters to the CAVE algorithm. The UIM\_ID emulates many of the functions of the ESN and can be used in place of the ESN\_ME input parameter in the CAVE algorithm.

The **Store ESN\_ME** window contains the following fields:

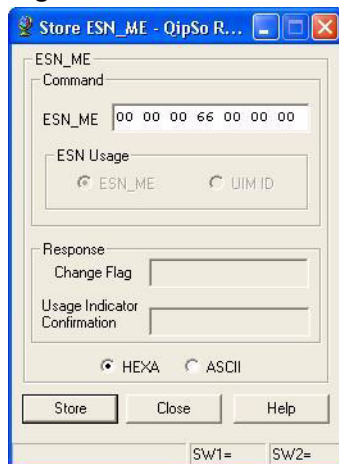
- **ESN Usage**, updates the EFUSAGE\_IND (6F42), the flag which indicates which value is used for the ESN, the value stored in EFESN (6F38) or that in the EFUIMID (6F31).
- The **Usage Indicator Confirmation** field which shows if the ESN in EFESN or the UIM\_ID held in the EFUIMID is used, as indicated in EFUSAGE\_IND (6F42).

**To save the ESN:**

- 1 In GemXplorer, right-click DFCDMA (7F 25) or one of its directories and select **Store ESN\_ME**. You must have first correctly presented CHV1.

The following is displayed.

**Figure 83 - Store ESN\_ME Parameter Window**



- 2 Click to select the display mode: **Hexadecimal** or **ASCII**.
- 3 Type the **ESN\_ME** value (7 bytes).
- 4 Click **Store**.

## Store MEID

**Note:** This feature is currently available for GemXplore Generations Option CDMA and Simera Airflex Classic cards only.

This command allows the management of the mobile equipment identifier in the card file EFESN. The Pseudo ESN, a 32-bit number hashed from MEID, is one of the input parameters to the CAVE algorithm. The UIM\_ID emulates many of the functions of the ESN and can be used in place of the MEID input parameter in the CAVE algorithm.

The **Store MEID** window contains the following fields:

- **Change Flag**, the flag which indicates if the parameter is the same as the identifier (ESN\_ME or MEID) stored in EFESN (6F38).
- The **Usage Indicator Confirmation** field which shows if the ESN in EFESN or the UIM\_ID held in the EFUIMID is used, as indicated in EFUSAGE\_IND (6F42).

**To save the MEID:**

- 1 In GemXplorer, right-click DFCDMA (7F 25) or one of its directories and select **Store ESN\_ME > MEID**. You must have first correctly presented CHV1.

The following is displayed.

**Figure 84 - Store\_MEID Parameter Window**

Store ESN\_MEID\_ME - QipSo RUIM 6...

ESN\_MEID\_ME

MEID

Manufacturer Code

Serial Number

MEID

☒ HEXA ☐ DIGIT

Command Parameter

Storage Format ☒ MEID ☐ Pseudo ESN

Current Value

MEID

ESN 66 00 00 00

Response

Change Flag

Usage Indicator Confirmation

Store Close Help

SW1= SW2=

- 2 Click to select the display mode: **Hexadecimal** or **Digit**.
- 3 Enter the **Manufacturer Code** and **Serial Number**.
- 4 Click to select the storage format: **MEID** or **Pseudo ESN**.
- 5 Click **Store**.

## HRPD Access Authentication

The High Rate Packet Data (HRPD) access authentication is an access authentication function for 3G packet data service. It is a procedure by which the access network authentication, authorization and accounting entity authenticates the mobile equipment.

The HRPD access authentication process is as follows:

- 1 The network generates a random challenge and sends it to the mobile equipment in the form of a CHAP Challenge message.
- 2 The mobile equipment forwards this message to the R-UIM using the Compute IP authentication command.
- 3 The R-UIM computes the CHAP Response and passes it to the mobile equipment which in turn will forward it to the network.
- 4 If the CHAP Response sent by the mobile equipment matches the network's calculated CHAP Response, the network returns an indication that the authentication is successful.

### To perform the HRPD access authentication:

- 1 In GemXplorer file view, select the EFHRPD AA CHAP SS available on the card, enter the Algo ID, length of SS and the HRPD Shared Secret.  
If EFHRPD AA CHAP SS is not in listed in your card, use the **Create...** feature to create EFHRPD AA CHAP SS.

---

**Note:** Different file IDs are used for different EFHRPD AA CHAP SS.

- For GemXplore Generations cards, EFEE6 is used.
  - For Simera Airflex Classic 64K cards, EF6F13 is used.
  - For Simera Airflex Classic 128K cards, EF1F13 is used.
- 

- 2 In GemXplorer structure view, right-click DFCDMA (7F 25) and select **Authentication Packet Data > HRPD**.  
The HRPD access authentication window is displayed.

**Figure 85 - HRPD Parameter Window**

- 3 Click to select the display mode: **Hexadecimal** or **ASCII**.
- 4 Enter the **CHAP ID** which is to be sent to the RUIM in the Compute IP command.

- 5 From the **Algorithm** list, select **MD5**.
- 6 Select the length of the **CHAP Challenge** and click **Random** to generate the random number.
- 7 Under the **HRPD Shared Secret**, select the length required and enter the **HRPD Shared Secret** that was stored in the card.
- 8 Click **Authenticate**.

## SimpleIP Authentication

**Note:** This feature is currently available for GemXplore Generations Option CDMA, Simera Airflex Classic 64K and Simera Airflex Classic 128K cards only.

SimpleIP refers to a service in which an access provider network assigns an IP address and supplies an IP routing address to a mobile station. The SimpleIP CHAP authentication is used to authenticate the user.

### To perform the SimpleIP authentication:

- 1 In GemXplorer file view, select the EFSIMPLEIP CHAP SS available on the card. If EFSIMPLEIP CHAP SS is not in listed in your card, use the **Create...** feature to create EFSIMPLEIP CHAP SS.

**Note:** Different file IDs are used for different EFSIMPLEIP CHAP SS.

- For GemXplore Generations cards, EFEE5 is used.
- For Simera Airflex Classic 64K cards, EF6F51 is used.
- For Simera Airflex Classic 128K cards, EF1F11 is used.

- 2 In GemXplorer structure view, right-click DFCDMA (7F 25) and select **Authentication Packet Data > SimpleIP**. The SimpleIP authentication window is displayed.

**Figure 86 - SimpleIP Parameter Window**

- 3 Click to select the display mode: **Hexadecimal** or **ASCII**.
- 4 Enter the **CHAP ID** which is to be sent to the RUIM in the Compute IP command.
- 5 From the **Algorithm** list, select **MD5**.

- 6 Enter the **NAI Entry Index** and **SS Length**.
- 7 Enter the **SimpleIP CHAP Shared Secret** that was stored in the card.
- 8 Select the length of the **CHAP Challenge** and click **Random** to generate the random number.
- 9 Click **Authenticate**.

## MobileIP Authentication

**Note:** This feature is currently available for GemXplore Generations Option CDMA, Simera Airflex Classic 64K and Simera Airflex Classic 128K cards only.

MobileIP refers to a service where the network provides the user with an IP routing service to a public IP network and/or secure IP routing service to private networks. MobileIP authentication is used for the network to authenticate the user.

To perform the MobileIP authentication, it is required of the user to input the parameters in the MN-HA, MIP-RRQ and MN-AAA tabs.

In GemXplorer file view, select EFMOBILEIP SS, enter the Algo, NAI Entry Index, length of SS and the MN-HA Shared Secret and the MN-AAA Shared Secret.

If EFMOBILEIP SS is not in listed in your card, use the **Create...** feature to create EFMOBILEIP SS.

**Note:** Different file IDs are used for different EFMOBILEIP SS.

- For GemXplore Generations cards, EFEE4 is used.
- For Simera Airflex Classic 64K cards, EF6F52 is used.
- For Simera Airflex Classic 128K cards, EF1F12 is used.

In GemXplorer structure view, right-click DFCDMA (7F 25) and select **Authentication Packet Data > MobileIP**.

**In the MN-HA tab:**

- 1 The MobileIP authentication window is displayed.

**Figure 87 - MobileIP (MN-HA Tab) Authentication Parameter Window**

- 2 Click to select the display mode: **Hexadecimal** or **ASCII**.

- 3 From the **Algorithm** list, select **MD5**.
- 4 Enter the **NAI Entry Index** and **SS Length**.
- 5 Enter the **MN-HA Shared Secret** that was stored in the card.
- 6 Under the **Registration Data**, fill in the length and the registration data.
- 7 Click **Authenticate**.

In the **MIP-RRQ Hash** tab:

**Figure 88 - MobileIP (MIP-RRQ Hash Tab) Authentication Parameter Window**

The screenshot shows the 'Authenticate Packet Data Mobile...' window with the 'MIP-RRQ Hash' tab selected. The 'Input' section contains an 'Algorithm' dropdown set to 'MD5'. Below it, the 'Preceding MIP-RRQ Data' section has a 'Length' spinner set to '1' and a text field containing 'FF'. The 'MN-AAA Extension Header' text field contains 'FF FF FF FF FF FF FF FF'. At the bottom, there are radio buttons for 'Hexa' (selected) and 'ASCII', and buttons for 'Compute Hash', 'Close', and 'Help'. A status bar at the very bottom shows 'SW1=' and 'SW2='.

- 1 Click to select the display mode: **Hexadecimal** or **ASCII**.
- 2 From the **Algorithm** list, select **MD5**.
- 3 In **Preceding Data**, input the length and the preceding MIP-RRQ data.
- 4 Enter the **MN-AAA Extension Header**.
- 5 Click **Authenticate**.

In the **MN-AAA** tab:

**Figure 89 - MobileIP (MN-AAA Tab) Authentication Parameter Window**

The screenshot shows the 'Authenticate Packet Data Mobile...' window with the 'MN-AAA' tab selected. The 'Input' section contains an 'Algorithm' dropdown set to 'MD5'. Below it, the 'MN-AAA Shared Secret' section has an 'NAI Entry Index' spinner set to '0' and an 'SS Length' spinner set to '1'. The 'MN-AAA SS' text field contains 'FF'. The 'MN-AAA Extension Challenge' section has a 'Length' spinner set to '1' and a text field containing 'FF'. At the bottom, there are radio buttons for 'Hexa' (selected) and 'ASCII', and buttons for 'Authenticate', 'Close', and 'Help'. A status bar at the very bottom shows 'SW1=' and 'SW2='.

- 1 Click to select the display mode: **Hexadecimal** or **ASCII**.
- 2 From the **Algorithm** list, select **MD5**.
- 3 Enter the **NAI Entry Index** and **SS Length**.
- 4 Enter the **MN-AAA Shared Secret** that was stored in the card.
- 5 Select the length of the **MN-AAA Extension Challenge** and click **Random** to generate the random number.
- 6 Click **Authenticate**.

## CDMA OTAF Simulator

The CDMA Over-The-Air Functionalities (OTAF) Simulator contains the commands required for transferring data Over-The-Air between a Gemalto CDMA card and a configured CDMA OTA server database.

You can use the CDMA OTAF Simulator to create a new user in a CDMA OTA database, then define the target card/mobile (subscriber) parameters and view the card variables that can be modified.

---

**Note:** CDMA OTAF is available only in the CDMA mode.

---

## OTA Concepts

### OTA Data Transfer

Certain variables held in the UIM of Gemalto CDMA card can be updated or uploaded to the server database using Over-The-Air (OTA) functionality. This data transfer can be initiated by a request from:

- The network, for example, to update existing variables held in a card.
- The user, for example, to request the configuration parameters from the card.

The CDMA OTA data transfer is concerned with providing mobile station with operational parameters over the air interface and is either:

- Over-the-Air Service Provisioning (OTASP) which is the general process; initiated by the network or mobile station, or,
- Over-the-Air Parameter Administration (OTAPA), which is specifically the network initiated process.

### OTA in Local Mode

In local mode, with CDMA Option installed on a PC and an attached card reader, the OTA uploading and downloading mechanisms (OTAPA/OTASP) are simulated, to and from a simulated CDMA OTA server.

### CDMA OTA Server

Normally data is held in a database on a CDMA OTA server and then transmitted Over-The-Air to a specified target.

The CDMA OTAF Simulator simulates the processes that would realistically occur in a CDMA OTA server, with an actual database built on your PC. The CDMA OTA server sends blocks of data including subscriber information to identify this target card/mobile. To use OTAPA/OTASP locally, you use the information held in your local (PC) database.

The CDMA OTAF Simulator provides:

- A database which simulates a subscriber database installed on an CDMA OTA administration server
- Processing of data, to formulate the data (into blocks) and simulate sending data Over-The-Air by sending it to the card in an attached reader.



### Database Details

An OTA subscriber is made up of a set of Users, where each user is essentially a user-card identification profile composed of:

- **Subscriber Parameters**, which define the target card/mobile (for example, by ESN\_ME (mobile electronic serial number), R-UIM\_ID)
- **OTA Parameters**, which indicate the UIM card values that can be modified by OTA (for example, Mobile Directory Number (MDN), Preferred Roaming List (PRL)). Any of the variables from the list can be sent by OTA to the associated user.

### OTA Processing

Processing of the data depends on the action required. For example, the database parameters may be updated (configured) with data held in the card or alternatively, a database value downloaded into the card.

---

**Note:** Any CDMA OTA data processing must be fully completed and stopped before a subsequent OTA data transfer is possible.

---

## Creating a New User with Database Values

To set or confirm the database parameters you need to do the following:

- 1 Set or validate the subscriber parameters that identify the target card.
- 2 Check the corresponding card file values via the GemXplorer module.
- 3 Optional: Note the original IMSI\_T parameters for later comparison with the new value in the database after OTA processing.
- 4 Display the OTA parameter list indicating the parameters that can be transferred into or from the card.

---

**Note:** Ensure that a Gemalto CDMA card is inserted in the reader.

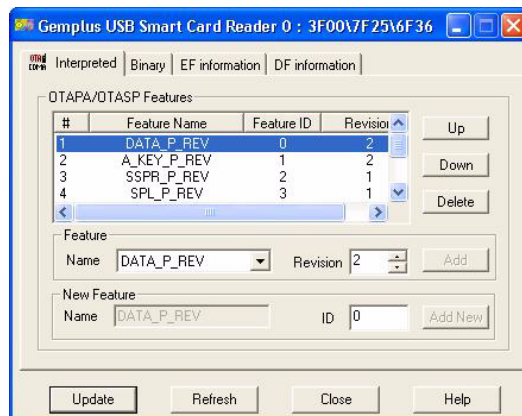
---

### To create a new database and new user:

- 1 In GemXplorer, right-click **DFCDMA (7F 25) > OTAF Simulator...**
- 2 Click on the **Database** tab.
- 3 Create a new database directly from **File > New Database**.
- 4 Specify the file name for the new database in the File Open window. Change the path if necessary.
- 5 Click **Save** to store the new database.
- 6 Select **File > Data > Create User**.
- 7 Enter a name for the user for the card entered in the reader. This name is associated with all the parameters available for identifying and downloading to a specific CDMA card. This allows one or more settings to be created, each setting associated with specific information, and allows many different cards to be updated through this procedure.

**To set the Subscriber parameters in the database:**

- 1 In OTAF Simulator, select **File > Data > Secret codes**.
- 2 Select the card type from the media list, using the drop-down list box if necessary > **OK**.
- 3 In the window that appears next, specify and validate CHV1, ADM1 and ADM4.
- 4 In GemXplorer file view, click to open **EFOTASP/OTAPA FEATURES (6F 36)** on the card. The following window is displayed.

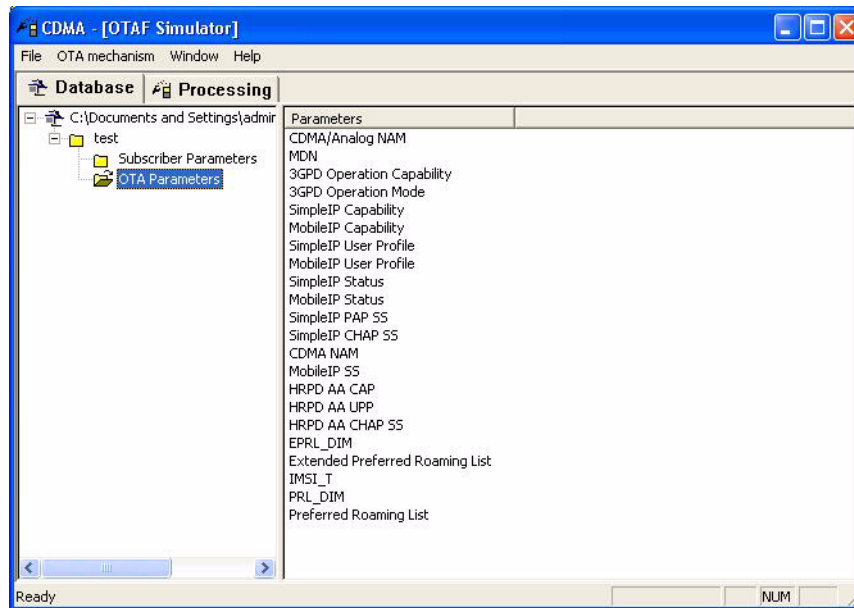
**Figure 90 - OTASP/OTAPA Features Window**

- 5 Ensure that the **SPL\_R\_REV** and **OTAPA\_P\_REV** displayed are of the correct version. If not, select them from the scroll list in the **Feature Name** list.
- 6 Click **OK**.
- 7 In GemXplorer file view, double-click to open **EFNAM\_LOCK (6F 35)**.
- 8 Ensure that **NAM\_LOCK STATE** and **NAM\_LOCK** are checked.
- 9 In OTAF Simulator, select the **Database** tab, right-click on a database and click **Load data from card...**
- 10 Select the corresponding user > click **OK**.
- 11 Select the corresponding media and click **OK**.
- 12 In **OTAF Simulator > Subscriber parameters** folder, double-click on **CHV1**.
- 13 Select the **Interpreted** then **Binary** tab. You can modify the value displayed with the actual CHV1.
- 14 Click **OK**.
- 15 Repeat steps 13, 14 and 15 for **A-Key** and **SSD\_A**.

**To view the OTA parameters:**

Click to open the **OTA Parameters** folder, a list of values that can be modified in the card is displayed as follows:

**Figure 91 - OTA Parameters Window**



## OTA Processing: Retrieving IMSI\_T

In the following example, the Configuration Request process is initiated by the network and requires the following steps:

- 1 Start the network session.
- 2 Setup the Secure Mode parameters.
- 3 Setup the Configuration Request parameters.
- 4 Launch the Configuration Request process.
- 5 Optional: To compare the new and original values for IMSI\_T.

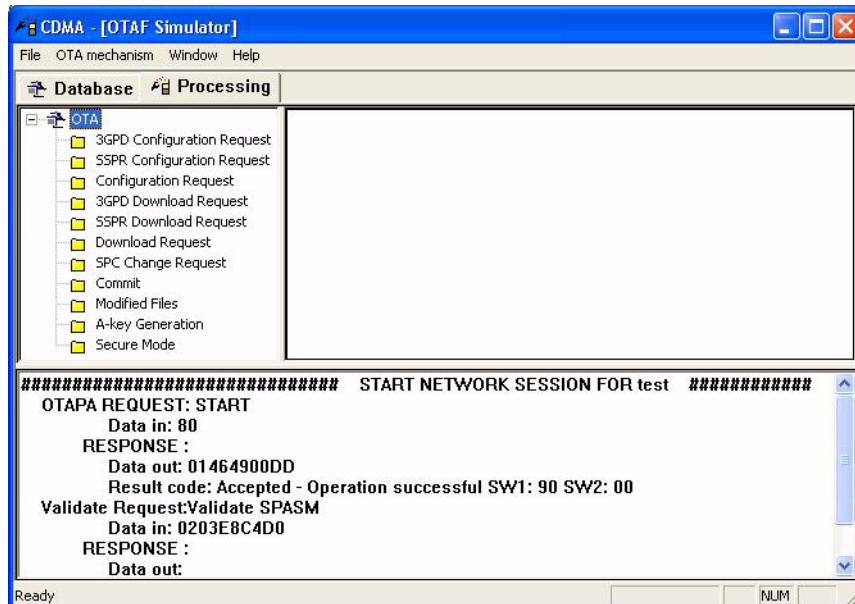
---

**Note:** Ensure that a Gemalto CDMA card is inserted in the reader.

---

**To start the network session:**

- 1 With the CDMA OTAF Simulator window displayed, click the **Processing** tab. The window is divided into three panes. The lower pane displays the processing status messages.
- 2 Click **OTA**.  
A list of available processing requests are displayed as follows:

**Figure 92 - Processing Request List**

- 3 From the menu bar select **OTA Mechanism > Start > Network Initiated**. The window displays the name of the Users and the media.
- 4 Select the correct values from the list and click **OK**.  
As soon as the OTA session is started, all database values are locked and the card is in the receptive state.

---

**Caution:** To return the card to normal and quit CDMA OTAF Simulator or to process another OTA transfer, any started OTA session must be fully completed and stopped with the menu command **OTA Mechanism > Stop**.

---

- 5 The SPC and SPASM are validated and the status window displays that the network session is started successfully. If an error occurs, check that you have correctly presented the CHV1, SSD\_A and A-Key and repeat the procedures detailed previously.

---

**Note:** The SPC, SSD\_A and A-Key of the card and database must match. If not, validation fails and an error occurs.

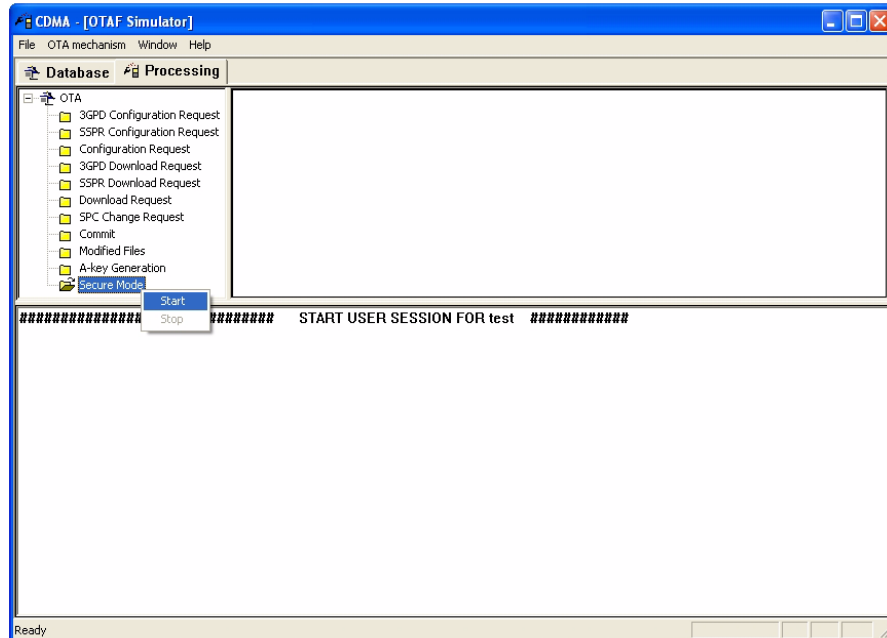
---

**To set up the Secure Mode parameters:**

The Secure Mode menu will have either a **Start** or a **Stop** sub-menu depending on whether the secure mode is currently active. To discontinue an active secure mode, select **Secure Mode > Stop**.

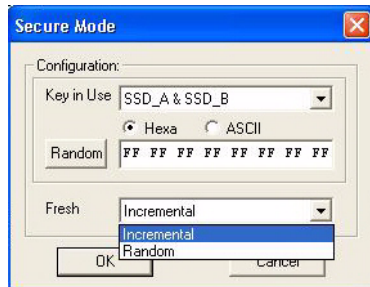
- 1 To initiate Right-click on **Secure Mode** and select **Start** from the contextual menu.

**Figure 93 - Setting Up Secure Mode**



- 2 The window displays the possible parameters to be selected for a secure mode.

**Figure 94 - Secure Mode Parameters Window**



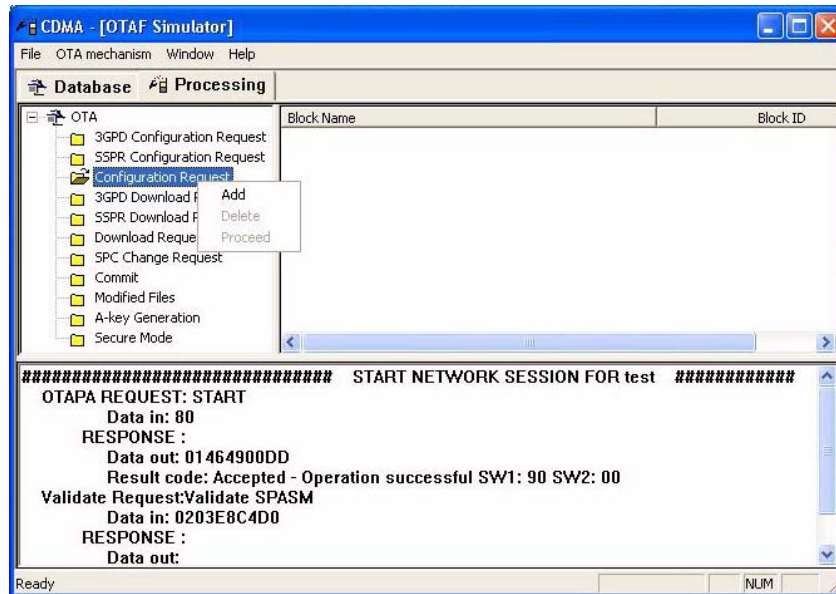
- 3 Click to select the display mode: **Hexadecimal** or **ASCII**.
- 4 Select the desired key — **3G Root Key** or **SSD\_A & SSD\_B** to generate the SMCK.
- 5 Click **Random** to generate the random number.
- 6 Select to set the Fresh field generation mode when the Secure Mode is active: **Incremental** or **Random**. When Secure Mode is active in the Download request, the CDMA OTAF Simulator will include the Fresh field and the 15-bit fresh value.
- 7 Click **OK**.

**To set up the Configuration Request parameters:**

You must first define the parameter to retrieve from the card.

- 1 Right-click on **Configuration Request** and select **Add** from the contextual menu. The window displays the possible parameters retrieved with a Configuration Request.

**Figure 95 - Configuration Request Parameters**



- 2 Select **IMSI\_T** and click **OK**.

**To launch the Configuration Request:**

- 1 Right-click on **Configuration Request** and select **Proceed** from the contextual menu.
- 2 The status window displays that the parameter value was successfully retrieved from the card.
- 3 Click to open the **Subscriber Parameters** folder under the **Database** tab.
- 4 Double-click on **IMSI\_T** to launch the viewer. Take note of the value and close the viewer.
- 5 In the **Processing** tab, click on **Configuration Request** and open **IMSI\_T** to compare the database value.
- 6 From the menu bar, select **OTA Mechanism > Stop**.  
The parameters are locked until the OTA session is manually stopped.  
This action returns the card to its normal state and card files can now be viewed and modified via the GemXplorer or CDMA OTAF Simulator.

**Note:** Refer to the contextual help within CDMA OTAF Simulator for more OTA menus and commands.

# Wireless Application Protocol (WAP) Content Provisioning

## WAP Content Provisioning

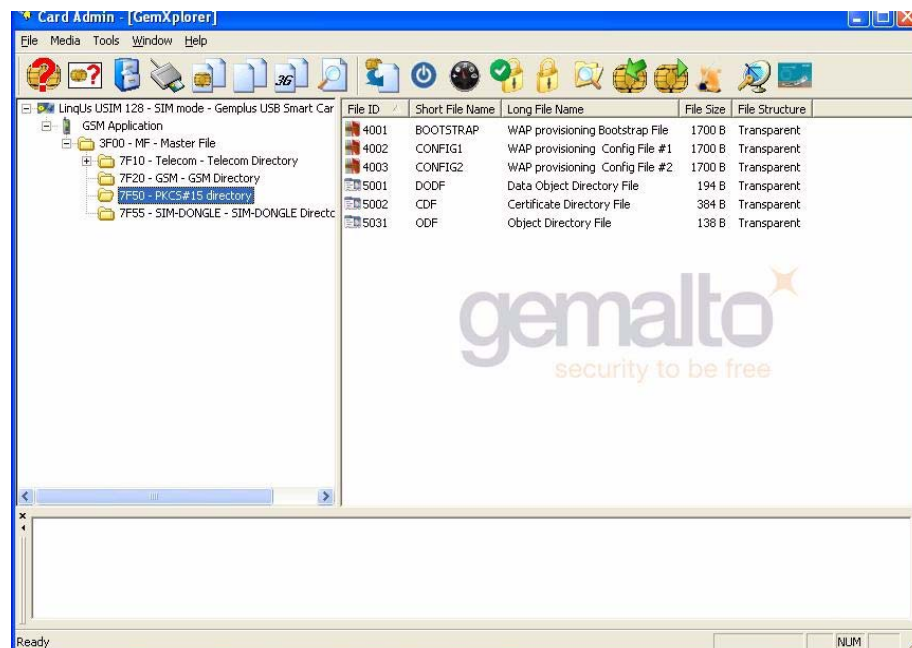
The WAP Provisioning framework specifies that each bearer network has unique provisioning mechanisms which provide mobile equipment with connectivity and application information. With WAP Provisioning, the mobile network operator is able to pre-configure the Universal Subscriber Identity Module (USIM) with appropriate information such as login and passwords so that the mobile subscriber is able to gain direct access to web browsing and email when the USIM is inserted into the mobile equipment. The WAP Provisioning data is stored in the USIM as PKCS#15.

Card ADMIN addresses the administration needs such as scanning and editing of WAP Provisioning data stored under PKCS#15. The PKCS#15 application ensures secure and safe e-services by providing secure digital generation for authentication and non-repudiation of transactions. It provides facilities for extremely high security 1024-bit RSA public key cryptographic operations and secure storage of digital signatures.

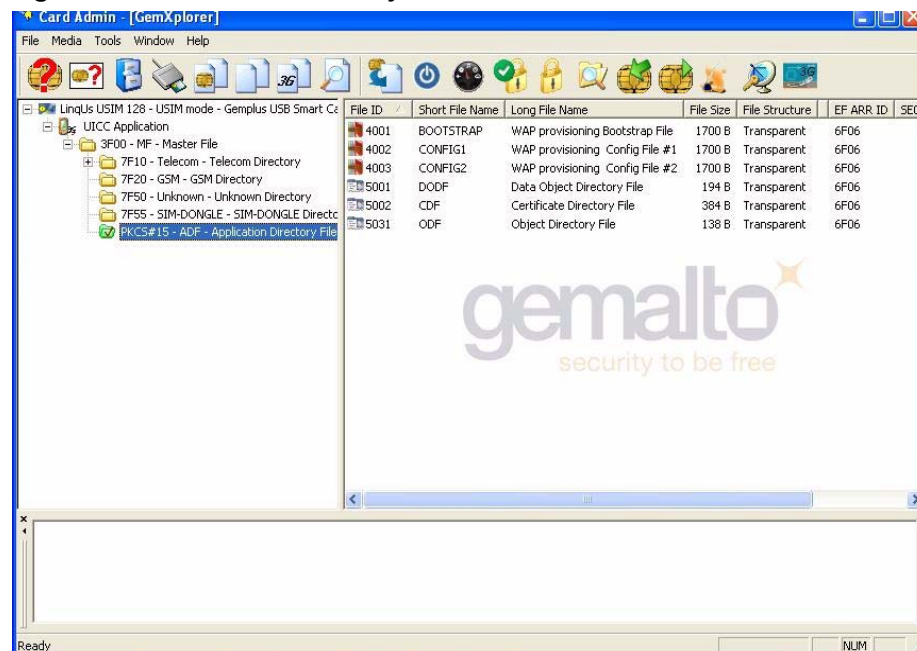
Within PKCS#15, files are accessed via EFODF which contains pointers to other directory files. These directory files contain information on different types of objects such as keys, certificates and authentication objects (PIN).

To scan the WAP Provisioning files while you are in the 2G or 3G mode, in GempXplorer, right-click **3F00 Master File > Scan WAP Provisioning**. The PKCS#15-related files are displayed.

**Figure 96 - DF PKCS#15 Directory in 2G Mode**



**Figure 97 - PKCS#15 Directory in 3G Mode**





## WAP Content Provisioning Creation Wizard

Card ADMIN provides a wizard to help you create WAP content provisioning files such as DODF and CDF and provisioning text documents such as Bootstrap, Configuration 1 and Configuration 2. In addition, you can specify if the new content provisioning files are to be protected by an existing EFARR (Access Rule Reference) or a new EFARR is to be created for these files. Optionally, you can also use this wizard to create Certificate Files and Trusted Certificate Files.

---

**Note:**

The WAP Content Provisioning Creation Wizard can only be launched when you are working in the 3G mode.

When this wizard is used, it automatically creates a link to DF PKCS#15 (7F 50) in the 2G mode. This enables the PKCS#15 files to be accessible via DF PKCS#15 in the 2G mode.

---

An PKCS#15 must exist before this wizard can be launched to help create content provisioning objects. If PKCS#15 does not exist, use Application Manager to instantiate a USIM with the PKCS#15 AID. When PKCS#15 is created, the wizard automatically creates a link to DF PKCS#15 (7F 50) so that it is accessible in the 2G mode.

If this wizard detects that the existing PKCS#15 is complete with all the content provisioning-related files, it will stop the process. Otherwise, it prompts you of the content provisioning-related files you can create. When a content provisioning object is successfully created, a report will display its status and it will appear under PKC#15.

All necessary file access conditions must be met. Otherwise, the Secret Code Verify window will appear for you to enter the secret codes.

Refer to the online help for details.



# Test Card Specifications

The following are the code values for the sample card that is included in the Card ADMIN kit.

**Table 8 - Code Values of Sample Card in Card ADMIN Kit**

PIN1	31313131FFFFFFFF
PIN2	32323232FFFFFFFF
Unblock PIN1	3131313131313131

---

**Note:** The values of the codes may vary according to the cards, please contact your Gemalto representative person for assistance and for more information.

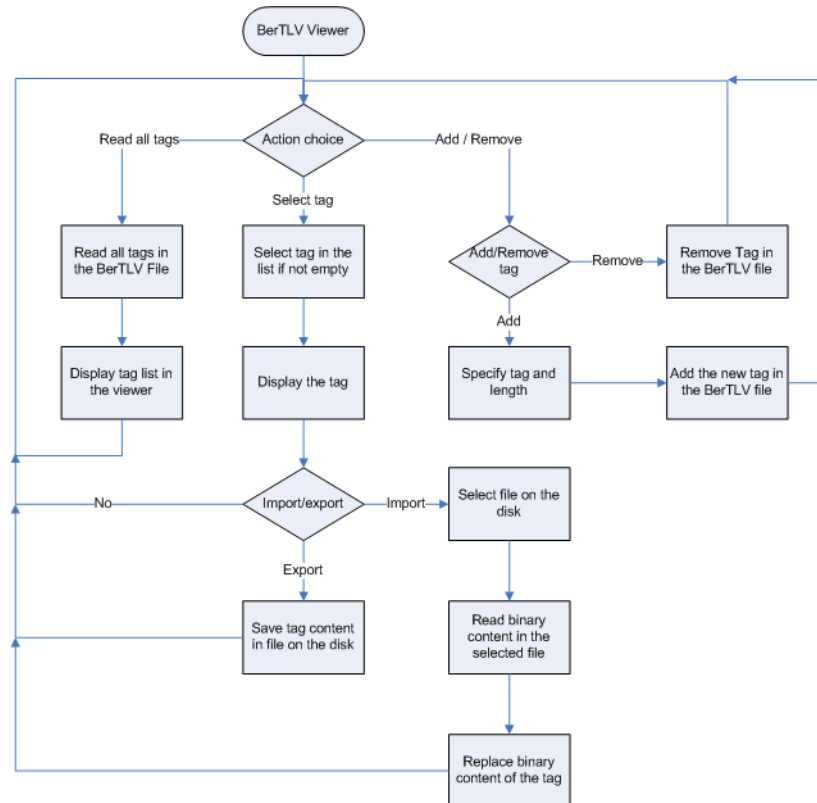
---



# BER-TLV Files

## Generic Behavior of BER-TLV Viewer

**Figure 98 - Generic Behavior of BER-TLV Viewer**



## Relationship between EFmML (Multimedia Message List) and EFmMDF (Multimedia Data File)

**Figure 99 - Relationship Between EFmML and EFmMDF**

