



MAGSTRIPE AND CHIP TEST TOOLS FOR A SMART CARD WORLD

## Chip Application Tester

### CAT 3000v3

Version 3.51.0

November 2017

## User Manual

---

Barnes International Limited  
The Loft  
St. Clair's Farm  
Wickham Road  
Droxford  
Hampshire  
SO32 3PW  
UK

Tel: +44 (0)1730 231313  
Fax: +44 (0)1730 265353  
[support@barnestest.com](mailto:support@barnestest.com)

[www.barnestest.com](http://www.barnestest.com)

**Copyright © 2008-2017**

## **Barnes International Limited**

Information in this document is subject to change without notice. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Barnes International Limited.

*Windows® is a trademark of Microsoft Corporation.*

### **CE requirements (Europe)**

The CPT/CAT 3000v3 includes a hardware module which generates, uses and can radiate radio frequency energy. This equipment has been Declared to conform with the following regulations:

EEC-directive 89/336/EEC: "Electromagnetic Compatibility"

\*EN 50081-1 (Emission EN 55022 Class B/1994)

\*EN 50082-1 (Immunity IEC 801-2, -3, -4)

\*EN 61000-3-2+A12

\*EN 61000-3-3

### **FCC Requirements (USA)**

The CPT/CAT 3000v3 includes a hardware module which generates, uses and can radiate radio frequency energy. This equipment has been Tested in accordance with the procedure in ANSI C63.4 and declared to conform with the following regulations:

FCC Part 15 Class B

The operation is subject to the following two conditions:

- 1 This device may not cause harmful interference, and
- 2 This device must accept any interference received, including interference that may cause undesired operation.

The device tested is representative of subsequent units marketed; any changes to the device which could adversely affect the emission characteristics will require retest.



**Contents**

<b>INTRODUCTION TO THE CAT 3000V3 .....</b>	<b>7</b>
<b>CONTACTING BARNES.....</b>	<b>8</b>
<b>SOFTWARE AUTHORISATION.....</b>	<b>9</b>
<b>SOFTWARE UPDATE .....</b>	<b>10</b>
<b>LOGGING ON TO THE CAT 3000V3 .....</b>	<b>11</b>
<b>TESTING A CARD .....</b>	<b>12</b>
<b>THE CAT 3000V3 RESULTS DISPLAYS.....</b>	<b>13</b>
Test Report.....	14
Detailed Results Tree.....	16
Engineer's Test Log .....	17
Additional Screens .....	18
<b>CARD TESTING CONCEPTS .....</b>	<b>19</b>
<b>SCENARIO MANAGEMENT .....</b>	<b>21</b>
<b>SCENARIO VIEWER/EDITOR .....</b>	<b>24</b>
<b>THE SCENARIO STAGE EDITOR .....</b>	<b>27</b>
<b>SCENARIO AUTO SELECTION .....</b>	<b>29</b>
<b>SCENARIO SELECTION BY REFERENCE.....</b>	<b>33</b>
<b>ERROR CODING AND SUPPRESSION .....</b>	<b>36</b>
<b>SCENARIO SHORTCUT BUTTONS .....</b>	<b>37</b>
<b>SAVED CARD DATABASE .....</b>	<b>39</b>

<b>CARD GROUP MANAGEMENT .....</b>	<b>41</b>
<b>BATCH MODE TESTING.....</b>	<b>42</b>
<b>BATCH MANAGEMENT DIALOG .....</b>	<b>42</b>
<b>BATCH RESULTS DISPLAY .....</b>	<b>44</b>
<b>DATA EXPORT AND IMPORT .....</b>	<b>45</b>
<b>EXPORT FILE ENCRYPTION.....</b>	<b>48</b>
<b>CERTIFICATION AUTHORITY PUBLIC KEYS .....</b>	<b>49</b>
<b>EMV AID LIST EDITOR .....</b>	<b>50</b>
<b>SYMMETRIC KEY MANAGER .....</b>	<b>51</b>
<b>TERMINAL DEFAULTS.....</b>	<b>52</b>
<b>READER MANAGEMENT .....</b>	<b>53</b>
Currently Available Reader Types .....	54
<b>PROGRAM SETTINGS.....</b>	<b>56</b>
General Settings Tab.....	56
File Paths Tab .....	58
DataBase & Security Tab.....	60
Log In Settings .....	62
Report Settings .....	64
<b>USER CONTROL.....</b>	<b>65</b>
<b>USER PERMISSIONS.....</b>	<b>66</b>
<b>USAGE LOG .....</b>	<b>66</b>

CAT 3000v3

version 3.51.0

THE DAILY REPORT.....

66

BACKUP AND RESTORE .....

67

FILE ENCRYPTION .....

68

NEW FEATURES AND ENHANCEMENTS.....

69

REMOTE SYSTEM MANAGEMENT .....

70

ENGINEERING PANEL.....

71

TCL DEBUG UTILITY .....

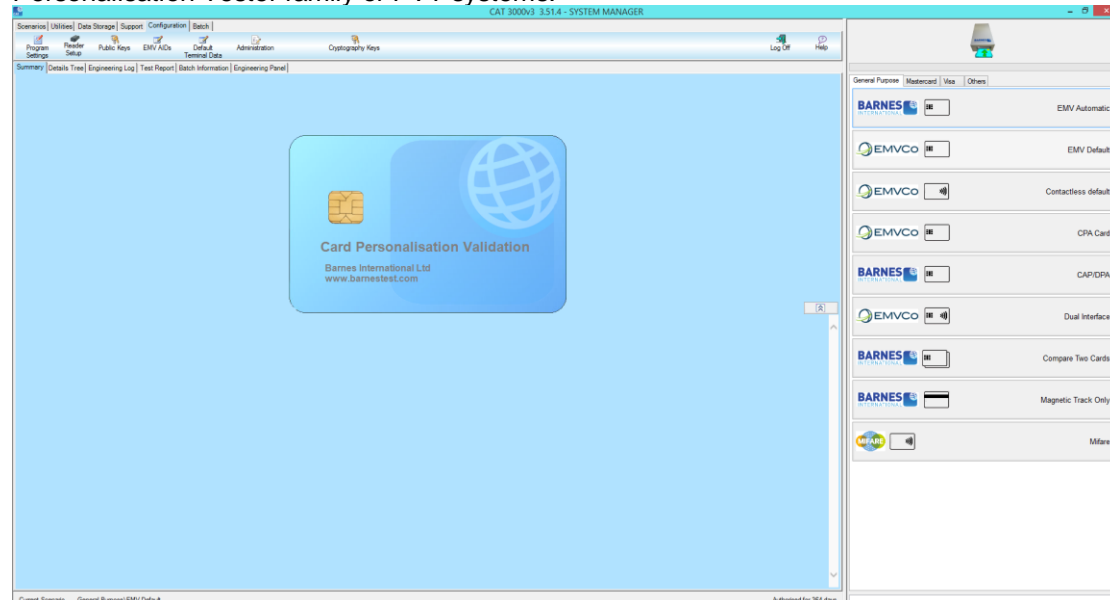
73

ANNEX A – EXTERNAL DATABASE CONNECTION.....

76

## Introduction to the CAT 3000v3

The CAT 3000v3 is a member of the third generation of Barnes International's Chip Personalisation Tester family of PVT systems.



The CPT 3000v3 and CAT 3000v3 range of products was developed with flexibility as a high priority, therefore, although the vast majority of units are used in the testing of EMV compliant financial cards the system is by no means limited to that area and can be applied to any chip card application. For this reason the aspects of the help system and manual that deals specifically with EMV cards (or any other specific type of card application) are in a separate document, this one deals with the CAT 3000v3 software and user interface itself.

For specific help on EMV card testing issues see the EMV manual and help document.

The CAT 3000v3 software is licensed and dongle protected and each installation must be authorised by Barnes International Ltd. before use. The dongle is normally embedded in one of the system's card readers, where this is not possible an external dongle will be provided.

## Contacting Barnes

Barnes International Ltd is a specialised and dynamic company based in Petersfield, Hampshire, in the United Kingdom. We produce a range of test tools covering both chip and magnetic stripe analysis.

Although every effort is made to keep CAT 3000v3 usage simple and error free, there may be times when it is necessary to contact Barnes to resolve problems or make enquiries. When contacting Barnes please provide as much information as possible about the installation and the nature of the problem in order to assist Barnes' engineers in responding quickly and effectively.

As well as providing support to our customers we are always glad to hear of suggestions for improvements in the products, indeed many of the features in the current product are the direct result of customer feedback from earlier versions.

Barnes International Limited  
The Loft  
St. Clair's Farm  
Wickham Road  
Droxford  
SO32 3PW  
United Kingdom

e-mail –

Technical enquiries - [support@barnestest.com](mailto:support@barnestest.com)  
Sales enquiries - [sales@barnestest.com](mailto:sales@barnestest.com)  
Authorisation codes – [authcodes@barnestest.com](mailto:authcodes@barnestest.com)

Tel. +44 (0)1730 231313  
Fax +44 (0)1730 265353

More information, including up to date contact details and updates to the latest software releases can be found on the Barnes International web site at [www.barnestest.com](http://www.barnestest.com).

## Software Authorisation

The first time the application runs it will request an authorisation code. A temporary code will have been included in the package shipped from Barnes, entering this code will enable the software for a limited period. Before the temporary code expires you must contact Barnes International for your permanent code. Select "Authorisation Codes" from the Administration menu on the Configuration ribbon to obtain your installation code and enter the new authorisation code. Use the e-mail address provided above, [authcodes@barnestest.com](mailto:authcodes@barnestest.com), quoting the installation code shown and an authorisation code will be returned.

This procedure will not be required again until the software license period expires. From two months before the expiry date a warning will be shown each time the software starts up. This warning includes the facility to enter a new code, but the software will continue to function normally without a new code until the actual expiry date (click "Continue Working" on the prompt dialog). At some point during the two-month warning period it will be necessary to contact Barnes again for a new code.

NB. Codes are normally issued annually, even if a multi-year license has been purchased, so it may not always be necessary to raise a purchase order for a license renewal.

The authorisation code provided by Barnes also enables certain optional features, if these features are purchased after installation then a new authorisation code will be required to enable them. The code entry dialog can be recalled from the "Administration" menu at any time to facilitate this.

## Software Update

It is very important to keep the CAT3000v3 up to date. We regularly add updates to the tool to support our customers' requirements , updates usually include :

- Test script updates to support newer specifications for all the supported schemes
- New features to help our customer test cards with flexibility and ease
- New standard profiles for all the schemes as and when the schemes release standard profiles: These are all available in the Scheme Standard profiles folder
- Bug fixes if any as reported by our customers or as discovered by the development / testing teams.

Procedure:

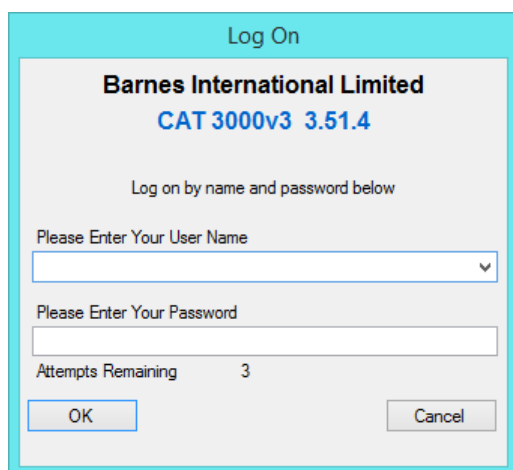
- Go to [www.barnestest.com/support](http://www.barnestest.com/support)
- Choose the product that you wish to download (CPT / CPV / CAT)
- Complete the details for your system
- Download and extract the file. It should be a file with the extension of ".bip"
- Open CPT and click Support > Package Installer button
- When prompted select the ".bip" file
- When installation is complete , the tool will prompt the user
- Restart CPT.

## Logging on to the CAT 3000v3

Before any user can operate the CAT 3000v3 he or she must log on to the system. The logon prompt is offered whenever the application starts up and the user is required to enter a name and password before continuing. This user remains 'logged on' until either the application is closed or the user logs off, in the latter case the log on prompt will be presented and the system may not be used again until another user logs on.

Note that both user names and passwords are case sensitive, that is "Fred" and "fred" will be regarded as two different user names.

The user is automatically logged off when the application is closed; alternatively you can log off using the button on the "Home" ribbon so that a different user may take over. It is also possible to configure the system to log off automatically following a pre-defined period of inactivity. The application will not function while there is no logged on user.



For convenience the names of the currently enrolled users are available in a drop down list, this is an alternative to typing the name, either method of input is equally effective. The user names are grouped by grade and ordered alphabetically within each grade. The password must always be typed in.

If the optional login card feature is enabled users can log in to the system by inserting their personal login card into the login card reader. The login card reader may be any PC/SC connected contact card reader, once the login card is inserted it must remain present until the user logs off, removing the card immediately logs the user off. Card login is available

regardless of whether or not the PC/SC interface is allocated for card testing.

If the user is logged off by another method while a login card is present, e.g. by shutting down the software or allowing the maximum inactive time to expire, then a prompt will be shown asking that the card be removed. There is an option to set up the system such that any login card left behind by an absent user can be invalidated after a predetermined time.

A further option allows logging in with the current Windows user name. This option must be specifically enabled in program settings, an extra button will appear on the login dialog when this is done. To use this feature the Windows user name must be enrolled as a CAT 3000v3 user, clicking the button will log the user straight in without the need for a password, it is assumed that all the security requirements have already been satisfied by the Windows login procedure.

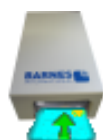
Refer to the user control and program settings sections for more details.

## Testing a Card

Once communications with the reader are established, the icon in the top right corner will indicate that the card reader is ready to accept a card. In the "out of the box" state CAT3000v3 will power up ready to test a standard EMV payment card application using the primary contact card reader, this default start up may be altered using the " Program Settings" dialogue accessed via the "Configuration" ribbon. Where possible the icon will illustrate the type of reader in use, this is helpful when multiple reader types are attached to the system. It is possible to have two readers selected for testing, in this configuration two icons will appear side by side, the card can be inserted into either reader.

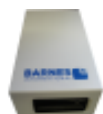


While the reader is being initialised the "No Reader" icon is shown, this should be replaced by the "Ready to Test" icon after a few seconds, if it remains then there is a problem with the reader or its connection to the PC.

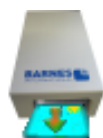


When the system is ready to test a card the icon will change as shown. A test card may now be inserted in the reader. When using a contactless reader the card must be placed on the coupler surface, and remain there for the duration of the test.

NB. Some reader types do not register the presence of the card immediately; there may be a delay of up to three seconds before the test starts.



During the test the main screen icon indicates that the card should not be removed. Some reader types will latch the card during this time, but if the card reader is not fitted with a latch (e.g. as in the case of a contactless coupler) then the operator is responsible for ensuring that card remains in place until the end of the test. A progress bar just below the icon indicates the progress of the test.



On completion of the test the icon will indicate that the card should be removed. A new test cannot be started until the reader has seen the card disappear. If the reader has a magnetic stripe reading capability and the active test requires magnetic stripe data then if the magnetic stripe could not be read during card insertion the system will request removal of the card before the progress bar has reached 100% so that a re-read can be attempted on the extraction stroke

**N.B. The images above depict the Barnes 3K7 reader, which is currently the most common type used with CPT 3000v3 systems, these images will change if a different reader is selected.**

Where two readers are configured the icon for the one which is not in use after a card has been inserted into the other one will disappear for the duration of the test.

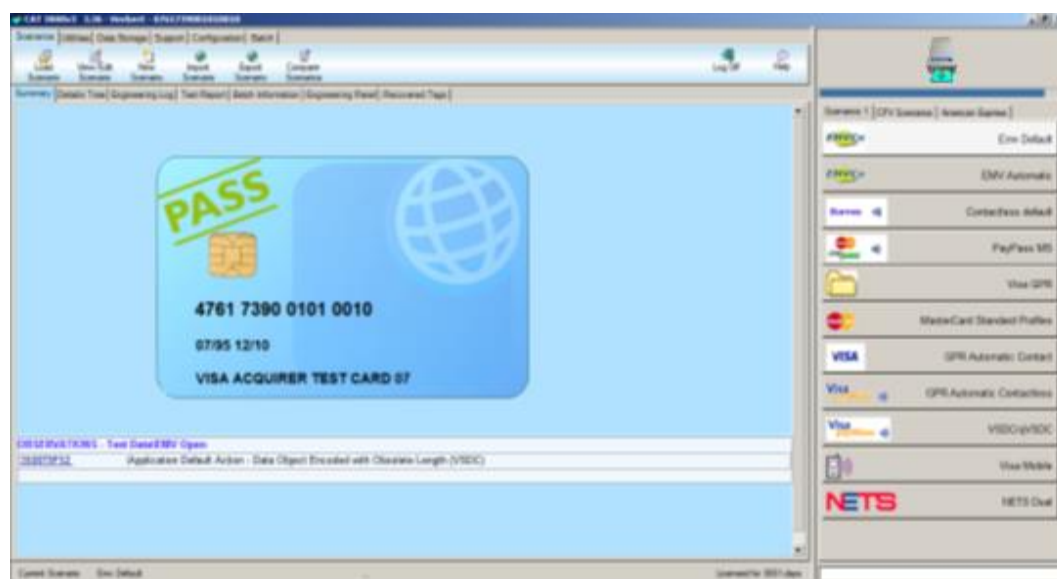
## The CAT 3000v3 Results Displays

Test results may be viewed in a number of ways as appropriate to different levels of operational need and technical understanding. The main screen may be switched between the "Pass/Fail Summary", the "Test Report", the "Detailed Results" tree structured display, and the "Engineer's Test Log" using the tabs at the top of the display.

**N.B. The uses of the various displays are described in terms of the EMV payment card test script shipped as standard with CAT 3000v3. This is the most common use of the CPT but it should be borne in mind that the layout and content of these screens are defined by the test scripts and the same philosophy will not necessarily be adhered to by all script programmers.**

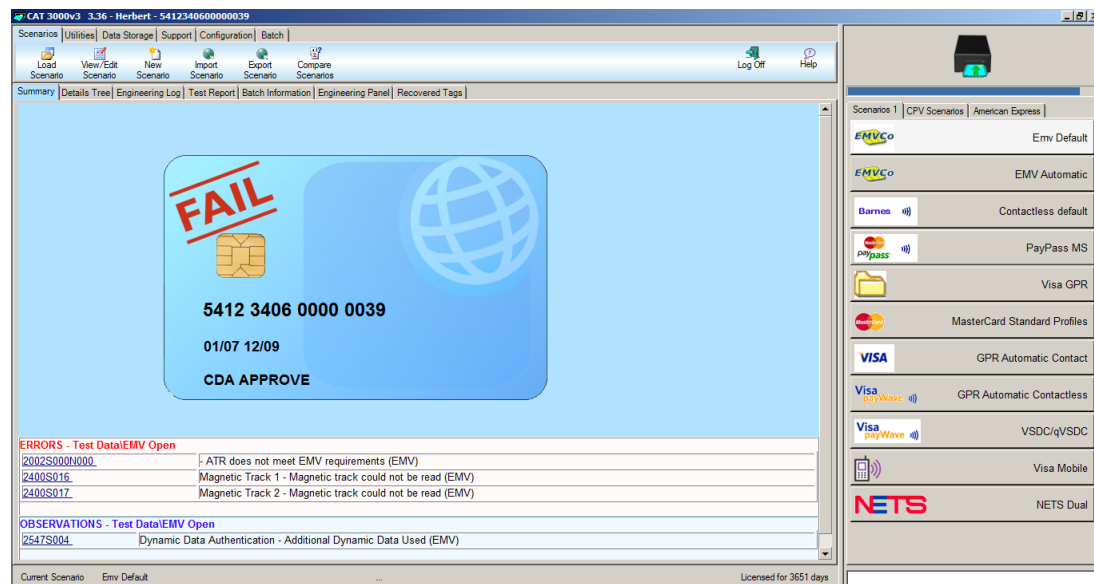
### Pass/Fail Summary

When a card has been tested the main display will show a stylised card outline with the chip represented along with the expected embossing. There may also be a pass or fail stamp to indicate the result of the test. There are also facilities to display the required card livery on this screen, see "Scenario Viewer/Editor" below.

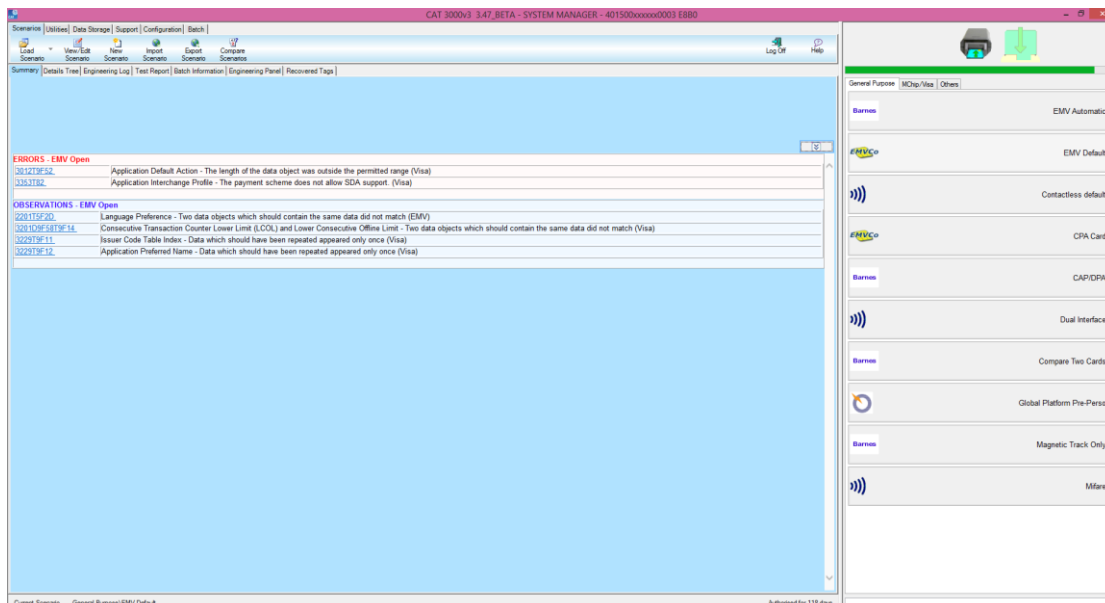


When the test has passed the "Pass" stamp is displayed as shown above, sometimes warnings or observations might appear below the card image, these are minor problems that do not cause the card to malfunction but may need attention by the issuer or manufacturer.

If the card has failed the test then the "Fail" stamp will be shown, see below. The area beneath the card image will show a list of the faults encountered. In most cases the error code is a hyperlink to another view of the error, clicking the mouse over this link will normally navigate to the Test Report where a more detailed explanation of the problem will be found. From the Report further links navigate to the tree and log displays where the problem area can be viewed in context with the rest of the card's data, and, where available (see below) to the page of the specification which has been contravened.



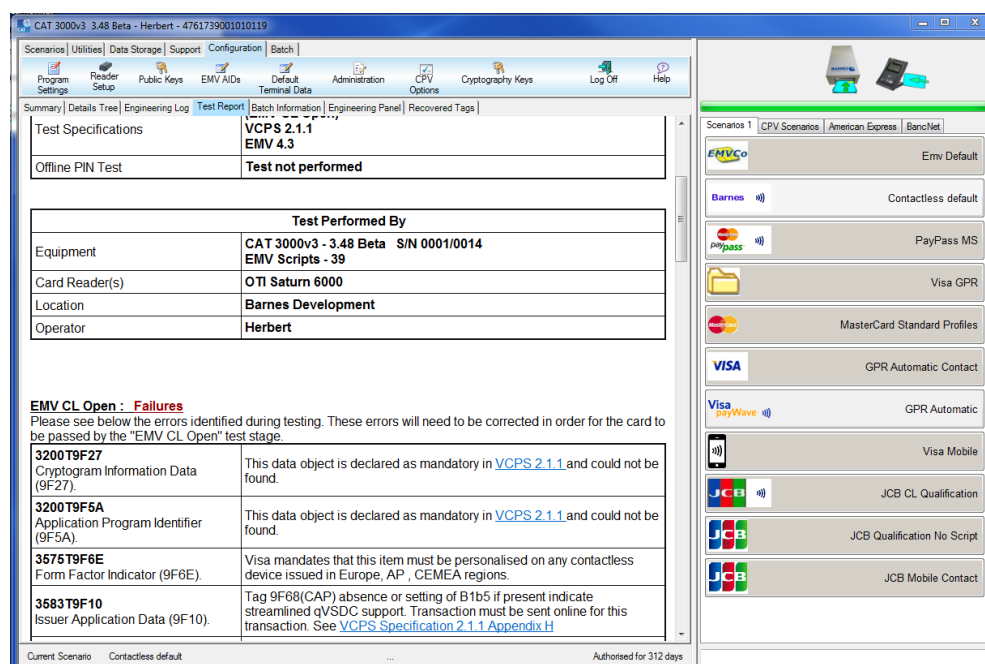
The pass/fail summary may be printed using the 'Print' button on the toolbar; the hard copy will be a single page showing a representation of the screen display. If there are failures and/or observations these will be listed beneath the card outline. In the most recent version of the software a button on the right side of the panel expands the error list to use more of the screen.



Since the summary display is also used for prompts and other progress information while a test is running, it will be shown automatically whenever a card test is initiated.

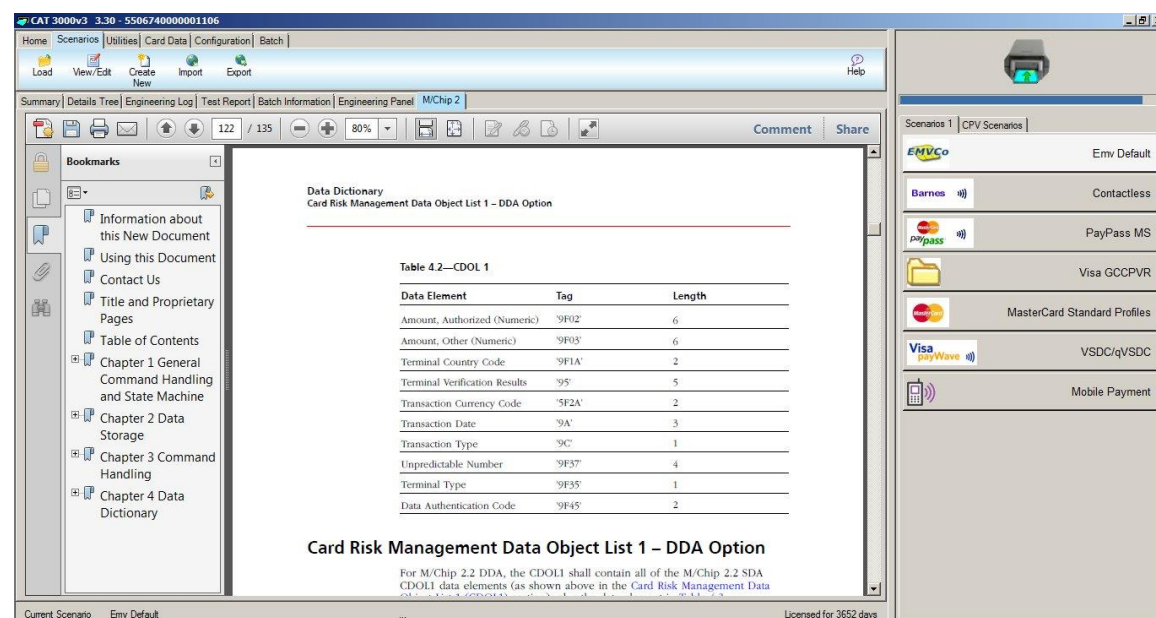
# Test Report

The report is a more formal way of displaying the test results. The first part is a table that summarises the tests performed, the relevant specifications, and the equipment used.



This is followed by up to three tables (per application tested) listing the errors, the suppressed errors, and observations as necessary. The descriptions of the errors etc. are explained in greater length than in the other displays, with reference to the specification clauses that have been contravened.

In the above example the specification references are hyperlinks, clicking one of these will open a new tab with the specification concerned open at the relevant page.

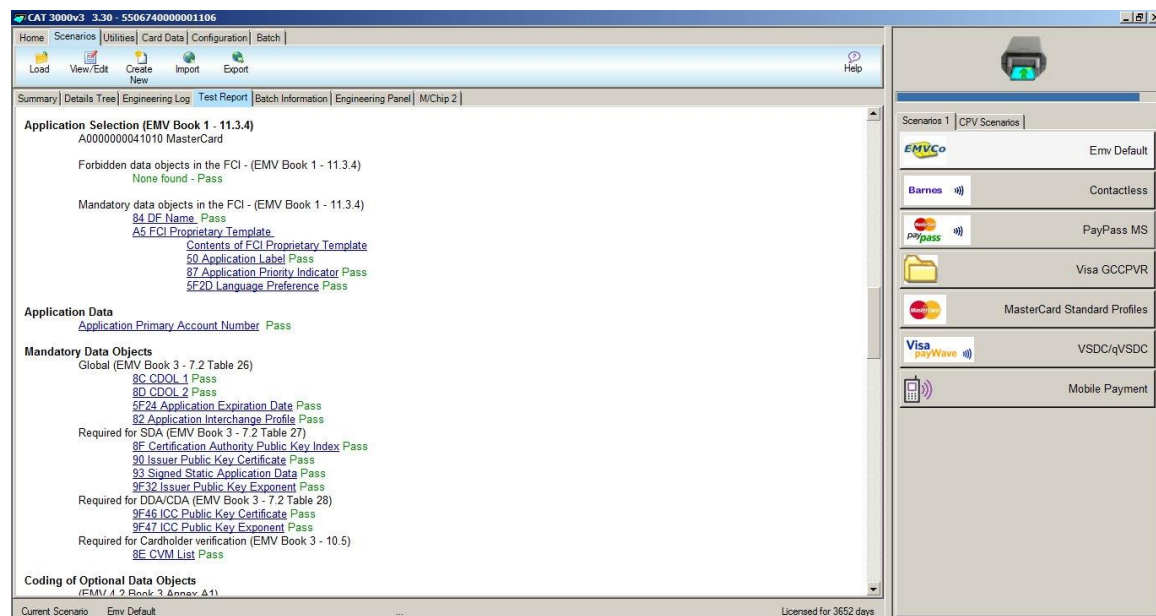


**NB.** For copyright and security reasons Barnes International Ltd is unable to re-distribute all of the specification documents that the tests refer to. Any organisation testing cards with this equipment is likely to be entitled to see the relevant specifications, but Barnes is unable to

make that assumption, so the documents, if not already available within the organisation, will need to be obtained directly from the issuing authority.

Where a specification is not available it will be replaced by a document explaining how to obtain a copy and integrate it with the CAT 3000v3 software.

The final part of the report is a commentary produced by data analysis script(s) which were used. Normally this commentary will list all the items checked, both pass and fail, and contain hyperlinks to navigate to the corresponding section of the tree. However, the report is produced by the test script, and so the content and layout of the commentary section may vary from script to script.



The test report can be customised by the user and exported in Rich Text (.rtf) format or in PDF format which are widely supported document formats.

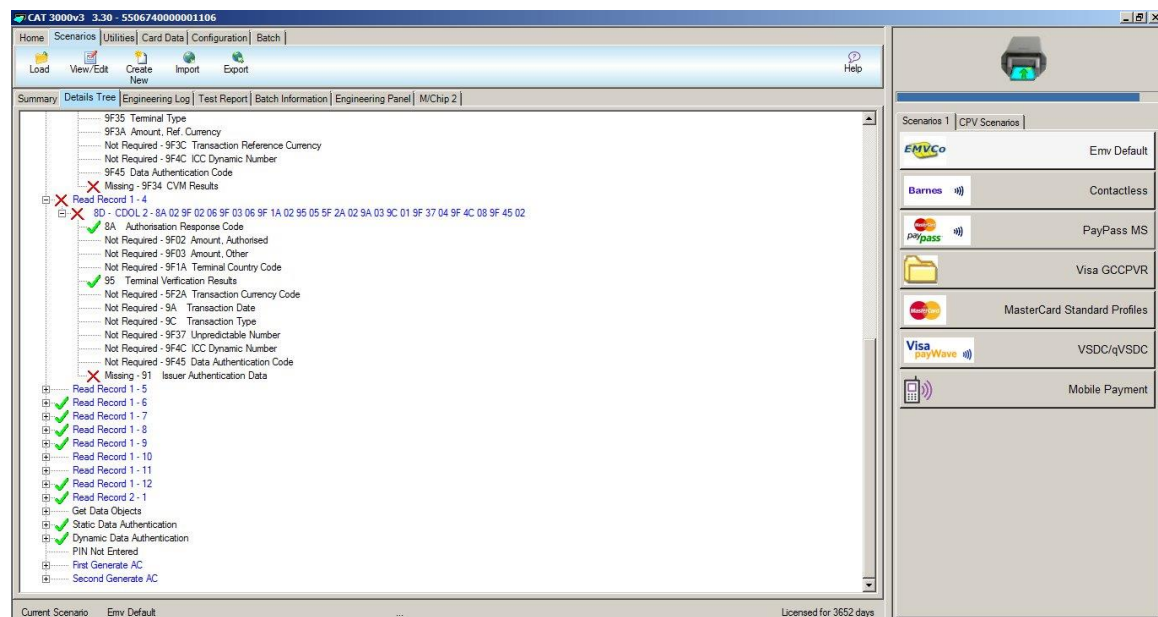
## Detailed Results Tree

The detailed results tree lays out the data content of the card using a tree structured display similar to that used by Windows™ Explorer. Each branch of the tree may be expanded or suppressed by clicking on the small '+' or '-' icon as appropriate alongside the entry. Green ticks (check marks) and red crosses indicate tests which have passed or failed respectively, these ticks or crosses are extended back up the tree so that overall categories are marked as 'pass' or 'fail' as appropriate. If the tree is expanded to a point where it is too big for the available display area then vertical and/or horizontal scroll bars will enable the view to be moved around.

Any branch having blue text is a hyperlink to the engineer's log, clicking on this branch will navigate the corresponding place in the log.

The exact layout of the tree is defined by the test script in use and may vary according to the type of card being tested, in the EMV scripts shipped with the standard system it reflects the

internal data structure of the card. The information held within it will be meaningful to anyone with a working knowledge of the data structures within the relevant type of card.



When the tree is first displayed following a card test it will be partially expanded to show details of any failed parameters. A card which passes all tests will have only the top level branches shown. Double clicking on the top line will fully expand all the branches of the tree, double clicking again on the top line will return the tree the expansion state it was in before the double click which expanded it.

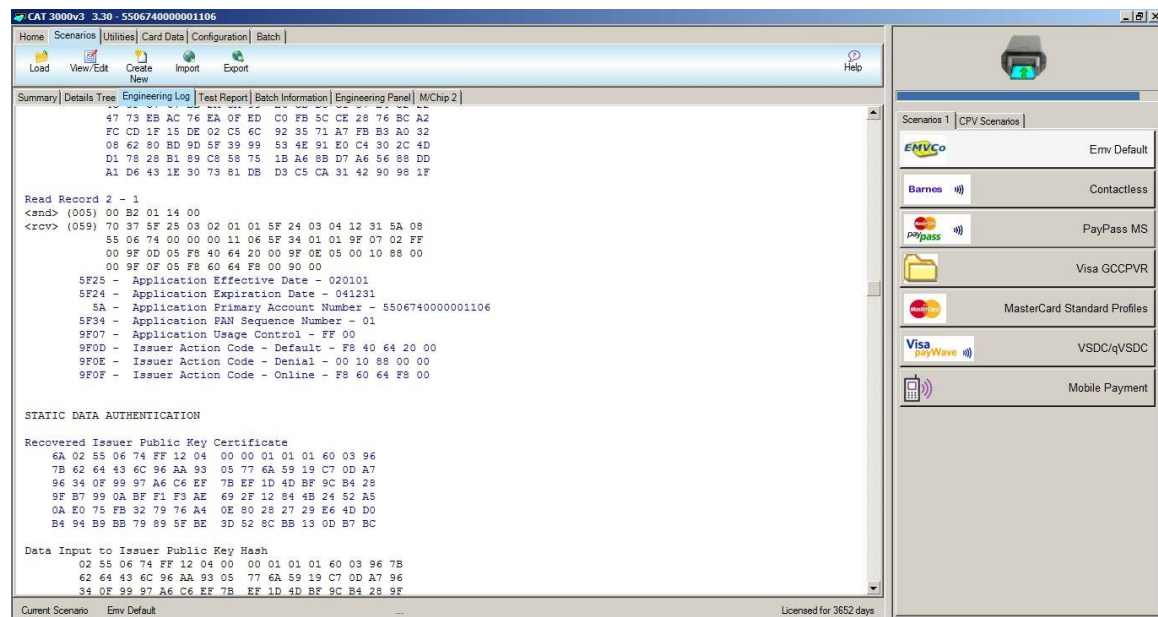
The tree may be printed using the 'Print' button on the toolbar. The hard copy will show the tree either fully expanded or as currently displayed. In the either case the hard copy will print all expanded branches regardless of whether or not they are currently scrolled into view.

The tree data may also be exported as an HTML document from the "Export" menu on the "Card Data" ribbon.

Right clicking on any branch will enable the text to be copied to the clipboard.

## Engineer's Test Log

The engineer's Test Log, as its name implies, is aimed at the more technical user. It is based on a log of the communications which occurred between the card reader and the card application. The data exchanged is given in hexadecimal representation with comments and analysis as appropriate. The additional (non communications) information is defined by the terminal simulation script and will be meaningful to anyone with a working knowledge of the low level card data objects and functions.



Many items in the log are hyperlinks to the details tree, clicking the mouse over these links will navigate to the tree branch corresponding to the log item.

The log data may be printed or exported in plain text or HTML formats.

## Additional Screens

Some test scripts produce an additional screen carrying either information not included in the other results screens, or the same information arranged in a different form. For instance the EMV script package produces the “Recovered Tags List”, a list of the data objects retrieved from the card arranged in alphabetical order.

## Card Testing Concepts

The process of testing a card may be divided into two stages, terminal simulation, which is the operation on the card itself to extract the data from it, and data analysis, which is the verification of that extracted data against the appropriate test criteria.

Each of the operations is controlled by a "test script", which translates the user's requirements into operations on the card or on the extracted data.

The test criteria and the decision as to which script(s) must be run on a particular card are defined by the test scenario.

### Test Scripts

Test scripts are written in Tcl (Tool Control Language) which is a well established, public domain scripting language, the interpreter for which is embedded in the CAT 3000v3 application. In addition to all the standard features of Tcl the CAT 3000v3 software adds a number of application specific language extensions which allow the test script to access to the card readers and the results displays, and to efficiently process card data.

The use of a scripting language in preference to an embedded test sequence enables CAT 3000v3 to be quickly and easily upgraded to meet the ever changing needs of the chip card industry. New test scripts will be prepared by Barnes International both as part of the ongoing development of the product and to meet individual customer requirements.

The CAT 3000v3's sister product, the CPT 3000v3, is fully compatible with CAT 3000v3 so that this product also serves as the development environment for CPT 3000v3 scripts.

Test scripts are stored in plain text files but are protected against tampering by the use of secure checksums. Under normal operation any script file which fails its checksum test will cause the test to stop with an error; if this occurs the error message will identify the offending file which may then be restored from the system back up.

One exception to this is that if the user logged on to the CAT 3000v3 has script development permission, then the checksums are ignored. This allows script development to take place without the need to continuously update checksums

### Scenarios

The scenario defines the entire test, from powering up the card when it is first detected to presenting the test results and generating the reports. The scenario does this by defining a number of test stages, which may be terminal simulations, responsible for communicating with the card and extracting the data, or data analysis, for checking the extracted data against the appropriate criteria. Each scenario stage definition is associated with a test script, and allows the user to define the conditions and criteria required by that script.

Since the CAT 3000v3 is designed for flexibility and can test a wide variety of card types, this document will not go into details of specific test scripts and scenario layouts. The user should consult the specialist help files associated with the script package in use. These are most easily invoked by the use of the "Help" button on the stage viewer/editor screens. This document only contains information which is applicable to all test environments.

### Basic Testing Process

In general, the following process should be followed to test any card:

- Choose a scenario from the set of reference scenarios provided in the tool. For example if a user wishes to test a Visa contact card, select one of Visa 1.5.X / Visa 1.6 scenario depending on the specification to be tested against. Scenario can be selected through shortcut buttons or by clicking "Load Scenario" buttons or by selecting a scenario from the list of "Recent Scenarios" which are displayed when user clicks on the small black arrow on the "Load Scenario" button.
- Edit the Scenario to simulate the required transaction and to analyse the data received. See Scenario Viewer/Editor for details
- Save stages and scenario
- Insert card in the reader.

Results will be displayed

## Scenario Management

A scenario is described by an XML file, which itself refers to other XML files containing the test stage definitions. These files are held in the PC's filing system, they may be local, i.e. on the same PC as the software is running, or remote, i.e. somewhere out on the network. In either case a number of CPT3000v3 and/or CAT3000v3 systems on the same network can share a scenario store, e.g. the local scenario store for one installation may also be the remote scenario store for another.

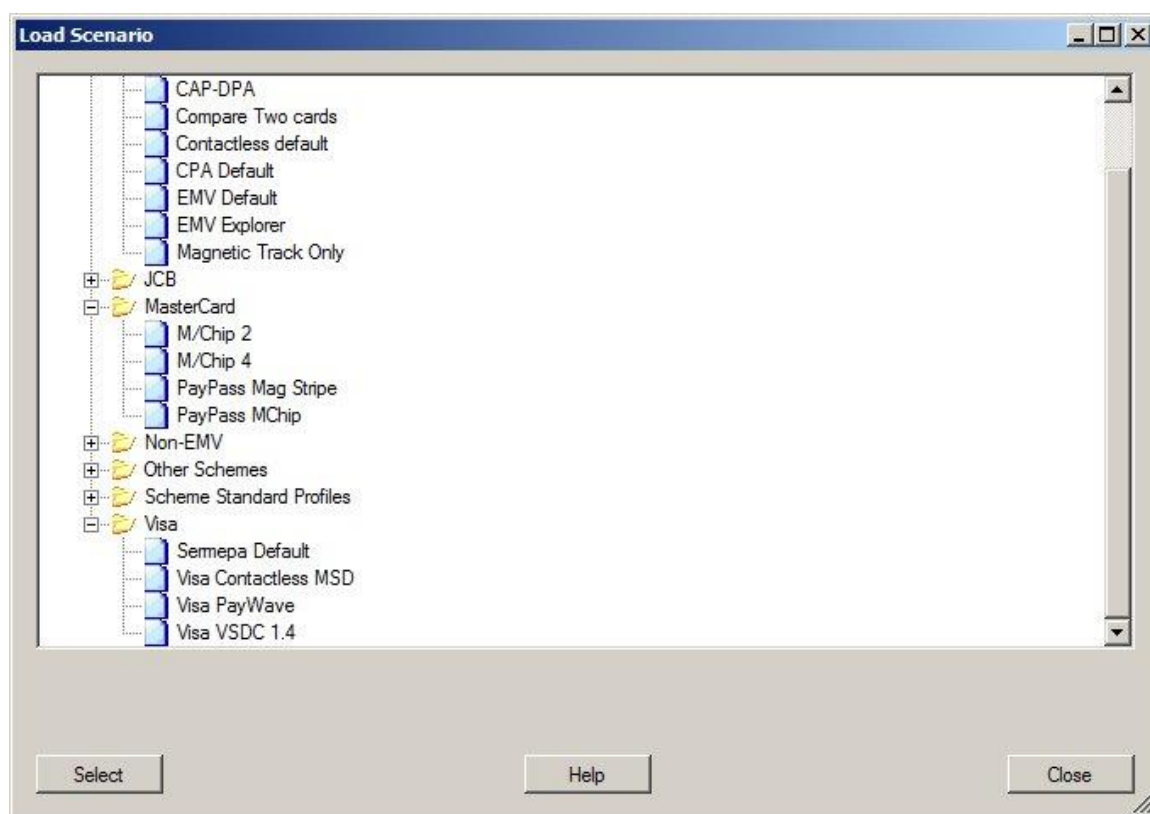
As a general rule, if Windows™ Explorer can access a folder then that folder can be used for the CAT 3000v3 to store its scenarios.

The main folder for scenario storage is defined in the Program Settings dialog, beneath this "Default Scenario Folder" there must exist three folders named "Profiles", "Terminals" and "Analysers". Each folder will hold files relating to scenarios, terminal simulator stages and data analysis stages respectively. Each of these folders may contain further sub folders in any arrangement convenient to the individual user. NB. In earlier versions of the software scenarios were known as profiles, the terminology was changed to avoid confusion with the many other uses of the word "profile" in the payment card industry, the naming of the folder was left unchanged to ease the process of upgrading existing systems.

Scenario files have the extension ".xrm", terminal simulator stage files use the extension ".xrt" and analysers ".xra".

Please note that the above information is provided only for the purpose of setting up remote folder structures for use as a scenario store. Because the scenario files contain information about the whereabouts in the folder structure of the stage files they refer to, manipulating these files using Windows™ Explorer will cause errors to occur. The Scenario Management facilities within the CAT 3000v3 software provide all the means necessary to manipulate the scenarios and stages, and will automatically update all cross-referenced information.

The Scenario Management and Scenario Editor dialogs provide the means to manipulate these files and folders. When opened, from the "Load Scenario" button on the "Home" ribbon or the "Load" button on the "Scenarios" ribbon, the scenario management dialog will configure itself according to the permissions settings of the logged on user such that only those functions appropriate to that user will operate. User grade permissions may be configured using the User Control dialog.



### Scenario Loading

To use the scenario management dialog to load a scenario ready for use, simply select the desired scenario in the tree window and click OK.

### Create a New Folder

Select the folder under which you wish to create the new folder then right click and select Create New Folder from the pop-up menu.

### Create a New Scenario

To create a new scenario click the "Create New " button on the "Scenarios" ribbon, this will create a new empty scenario and open the scenario editor dialog. Alternatively, load an existing scenario, open the scenario editor and use the "Save As" button to save a copy under a different name, then edit it as required. Scenarios may also be copied within the tree window by using the right click pop-up menu (select a scenario, right click and select "copy", then select a folder, right click again and select paste) or by dragging a scenario to a folder with the control key held down. With both of these methods you will be prompted to enter a name for the new scenario

### Creating a scenario from exiting scenario

It is possible to click on "Save As" button on the scenario editor and create copies of existing scenario and edit them. Two possible options are available:

- Create copy of the scenario and re-use some of the same Terminal and analyser files. This method allows creation of scenarios with multiple applications or interfaces using existing terminal / analyser stages which are already created.
- Create a copy of the scenario and create copies of the stages as well. This option should be used when Terminal / Analyser settings need to be edited as well.

**Scenario Comparison**

Tool allows the user to compare two scenarios, so that user can easily analyse changes he made to the scenarios. To use the comparison tool, select the first scenario , click "Compare Scenarios" , and then select the second scenario. The identical settings will be shown in green and the differences will be highlighted in Pink.

**Move a Scenario to a Different Folder**

Select the scenario in question, and, holding down the left mouse button, drag it to the new folder, or right click and use the pop-up menu to select "Move", then select the destination folder, right click again and select "Paste".

**Delete a Scenario or a Folder**

Select the scenario or folder in the tree window and right click, select "Delete Item" from the pop-up menu. NB. Folders may only be deleted when they are empty.

**Scenario Access Codes**

Scenario access codes provide an efficient and flexible way to restrict access to scenario sets for selected users. An access code may be applied to any folder in the scenario storage system, and if that same access code is also associated with a user grade then that folder becomes the root scenario folder for users of that grade.

Using this technique it is possible to set up a hierarchical system of folders such that users of increasing status have access to more and more scenarios, or a 'flat' arrangement whereby users from, say, different departments, have independent scenario sets.

**NB.** The Scenario Shortcut Buttons on the right of the main screen by-pass these restrictions, any scenario assigned to a shortcut button is available to all users at all times.

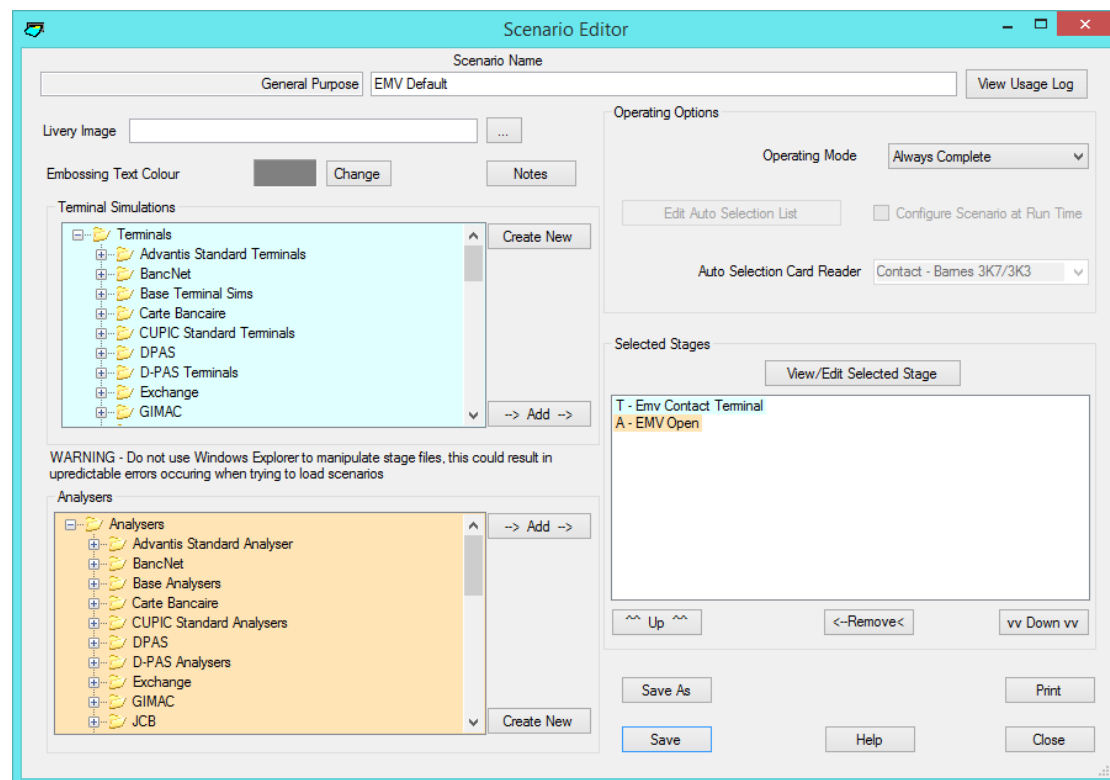
When an access code is assigned to a folder it is shown in brackets following the folder name. To assign or remove an access code associated with a folder, select the folder and right click, then select the desired option from the pop-up menu. To assign an access code to a user grade, use the "User Permissions" dialog where it is part of the permissions setup for user grades.

**NB.** This facility is not available on the terminal simulator and data analyser stage folders; therefore any user grade that has an access code assigned to it is automatically disallowed from editing scenarios.

## Scenario Viewer/Editor

The main dialog for scenario editing consists of linking together the required test stages so that they run in the required order.

The list window to the right of the dialog contains the current list and this may be amended by adding or removing stages and by altering their order. To the left of the dialog are two windows containing the available terminal simulation and data analysis stages.



The two types of stage may be freely mixed provided one simple and obvious rule is observed: a data analysis stage must be preceded by a terminal simulation in order to have some data to analyse. Two or more data analysis stages may be strung together following a single terminal simulation e.g. if it is desired to assess a single set of data against differing criteria. The data analysis scripts contain code to verify that the most recent terminal simulation is compatible with them.

### To Add a Stage to the Scenario

Select the desired stage in one of the left hand windows and either click the "--> Add -->" button or drag it with the mouse into the scenario window. It will then be added to the end of the list.

### To Remove a Stage from the Scenario

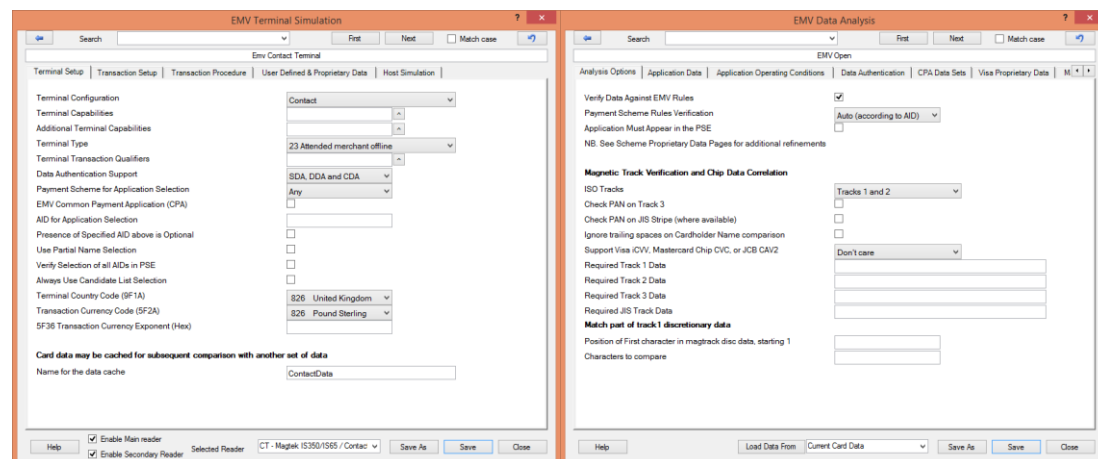
Select the desired stage in the scenario window and click the "<- Remove <-" button.

### To Alter the Order of the Stages

Select a stage in the scenario window and click the "^" or "V" buttons below the window to move it up or down the sequence as appropriate.

### To Edit a Stage

Either select the stage in the scenario window and click the edit button, or double click on the stage in the scenario window. This will open the stage editor as a new dialog. Click the "Help" button on the stage editor for information specific to the scenario being edited.



### To Create a new Stage

Click the "Create New" button in either the terminal simulator or data analysis section. This will open a selection window with the available test scripts, choose one and the stage editor appropriate to that script will be opened with empty or default data. Enter the required criteria, choose a name for the new stage and save it. The new stage will appear in the "available" window and may then be added to the scenario.

**NB.** The stage editor has a "Save As" button which enables a copy to be made of an existing stage, this may be more convenient than creating a new one from scratch. The data analysis stage editor also has an auto-populate facility by means of which the scenario may be loaded with data from an external source, a drop down list provides a means of selecting the data source, which may be the data from the last card read or imported, or the output from some other software package such as the Visa VPA tool. Additional data import scripts can be added, please contact Barnes International for details.

### Livery Image

If desired, an image of the card livery may be overlaid on the Pass/Fail Summary screen when the scenario is first selected and after a card test. The image file name is entered in the box in the scenario editor and the image file must reside in the folder designated for liveries in Program Settings, by default this will be the folder named "Liveries" under the main CPT folder. The system will accept files in "bmp", "jpg", "gif", or "png" formats. Just below the panel that defines the livery image file there is a facility to change the colour of the text used to represent the card's embossing data on the summary screen. The default colour may not always show up well against the chosen livery, and it can be changed here. The current colour is shown in the small panel to the left of the change button, clicking the "Change" button opens a colour chooser dialogue which allows any colour to be substituted.

**Test Operating Mode**

There are several modes of operation available.

**"Always Complete"** will ensure that every stage in the scenario is performed on every card, the result of the test will be a pass only if all the stages returned a pass.

**"Stop on Fail"** will truncate the test and report a failure after the first occurrence of a fail result from any stage.

**"Stop on Pass"** will truncate the test and report a pass on the first occurrence of a pass result from any analysis stage.

**"Auto Select"** will select a scenario from a list based on data read from the chip or from the magnetic stripe. The "Auto Selection List" button allows the Auto Selection List Manager to be opened whenever the "Auto Select" mode is active.

**"MasterCard CPV"** If the CPV module is installed then this option sets up the scenario to perform a MasterCard CPV card qualification test. Please note that only CPV test stages may be used when this mode is selected, and CPV test stages will not work correctly in any other mode.

**"Visa GPR"** If the GPR module is installed then this option sets up the scenario to perform a Visa GPR card qualification test. Please note that only GPR test stages may be used when this mode is selected, and GPR test stages will not work correctly in any other mode.

**Auto Selection Card Reader**

In auto selection mode it is necessary to define which card reader is used to obtain the information required for auto selection to take place. Normally this will be the same reader as is used to conduct the test itself, but there may be circumstances where this is not so, for instance where independent contact and contactless readers are installed and it is desired to select a scenario for a contactless card based on magnetic stripe data.

**Configure Scenario at Run Time**

When this box is checked then a dynamic scenario will be created to suit the card under test. This feature is only available in certain operating modes, when not available the check box is greyed out. In this mode a specific test script will be run that will examine the card to determine what applications are present, and will generate a test scenario which will then be applied to the card. Any test stages in the "Selected Stages" window will be ignored, except for the first terminal simulator which will be used to provide such static information as country and currency codes, keys for host simulation, etc. Please note that the data analysis stages used in the dynamic scenario will test against EMV and payment scheme requirements without adding any user specific requirements. This feature makes use of the EMV AID list to recognise valid payment applications. It is a convenient way to explore an unknown card but is not recommended for quality control purposes.

**Notes**

Clicking the Notes button will open a text editing screen which will allow notes and comments to be added to the scenario, the text is stored with the scenario and can be viewed using the scenario editor dialog. It is intended for use by personnel editing scenarios and is not included in any test results.

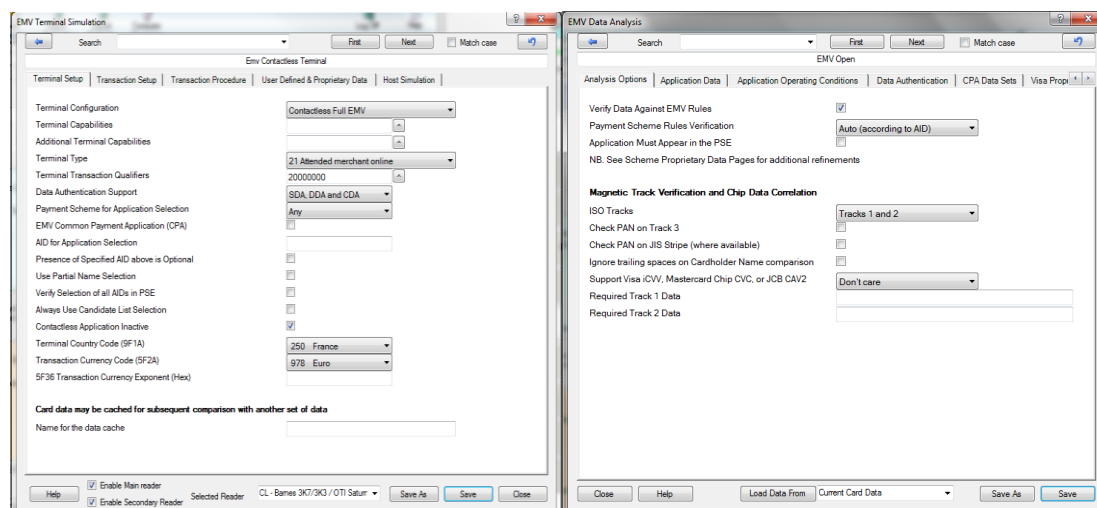
**Scenario Usage logs**

Tool logs the user actions of editing a stage, modifying scenario Auto-selection list, configuration changes etc. for as long as the period specified for usage logs (default 30 days). It can be viewed by clicking the "View Usage Log" button on the scenario editor screen.

## The Scenario Stage Editor

The bulk of the setup and editing for a test scenario takes place in the stage editors. To edit a stage, select it in the scenario editor screen and either click the edit button or double click the stage name.

The main area of the editor dialog is occupied by a series of tabbed pages. The number and content of these pages is dependent on the type of stage being edited.



The rest of this topic describes the controls which are common to all stage types, for information on individual pages click the help button at the bottom of the editor while the page of interest is open or consult the accompanying manual for that test type.

### Reader Selection

If the stage being edited is a terminal simulator and the system has more than one reader attached then the card reader to be used may be selected from the drop down list at the bottom of the dialog. For any terminal stage, two readers can be used for testing, both can be enabled or disabled by using the checkbox against “enable main reader” / “enable Secondary reader”.

### Data Import

If the stage is a data analyser then the drop down box at the bottom is used to select the source of data used to auto-populate the stage data. The content of this list is dependent upon the stage type and the options enabled in the system, but typically will include such possibilities as using the data currently held following the last card to be tested, or importing data from an external software package such as the Visa VPA tool.

The button beside the drop down list performs the actual import action, the entire stage will be populated immediately with the imported data, which can then be edited if required. It is possible to provide additional data import scripts to use with this facility, please contact Barnes International for more details.

### Back and Undo Controls

At the top of the dialog there are two buttons which may be used to reverse recent edits. The button on the left reloads the stage data with the values that existed before the last save to disk. The button on the right reloads the data to that which existed when the dialog was

opened, i.e. to the state after the last save to disk and before any changes were made in the current session.

The left hand button will be disabled if the stage has not been saved before, as in the case of a new stage.

### **Save and Save As**

The "Save" button saves the edited data to disk, and the "Save As" button allows the edited stage to be saved under another name. If the stage already exists and is being edited then the original stage will be unchanged; if a new stage is being created then it will be saved under the new name only.

Both of these buttons close the dialog.

### **Bit Allocation View**

The Bit Allocation View is a pop-up dialog which is available for selected items in some stages. Generally it is used where the data item being defined is a bit field rather than a numeric or string value, and provides a more convenient way of editing than typing hexadecimal values manually. The dialog contains a tabbed page for each byte of the object, with the bits listed MS at the top, LS at the bottom.

On first opening, the check boxes will reflect the currently set up hexadecimal or binary value in the main edit box. Any changes made using the check boxes will be transferred back to the edit box when the "Apply" button is clicked. The check boxes have three states, checked, unchecked, and indeterminate (greyed out), and will cycle round these three states with each click. The indeterminate state represents a wildcard, or "don't care" value, if wildcard characters are not available for the field being edited (as in a terminal simulator stage) then the indeterminate state will not be available.

There is a check box labelled "Binary" which indicates whether the setting in the edit box uses binary or hexadecimal notation. If there are no wildcard characters in use it will be preset to whatever notation was in use before the dialog was opened, and may be changed if required. This means that the Bit Allocation View dialog may be used as a convenient way for converting values between hexadecimal and binary.

If any of the checkboxes are in the indeterminate, or wildcard, state when the "Apply" button is clicked then the output will be in binary form regardless of the setting of the "Binary" check box.

When first invoked the Bit Allocation View will handle the single character wildcards ('?' and 'X') correctly but the results when using the multiple character wildcard, '\*', will be unpredictable.

### **Text Search Facility**

This facility searches for text within the currently open stage. The "First" button begins searching from the top of the first tab, and the "Next" button starts at the item below the point at which the last successful search stopped. The search covers the labels and the content of each item. When the text is found the relevant tab will be opened and the label of the item containing the text will be highlighted (even if the text was found within the requirement setting).

The "Next" button will always start searching from the next item, even if the text appears twice in the original found item, and even if the search text is changed in the mean time.

The text entry box features a drop down list which retains the last ten search strings entered. This history is global, i.e. there is not a separate history for each scenario and/or stage.

## Scenario Auto Selection

In a production or QC environment it may be convenient to automate the task of scenario selection, this facility is activated by setting the scenario operating mode to "Auto Select". When this is done the scenario used for the test will be chosen according the BIN read from the magnetic stripe OR tag value from the chip data.

When the selected scenario is in "Auto Select" mode the CAT will look up a list of alternative scenarios stored within the active scenario. Associated with each scenario is a data value. The source for the data value can be either the "BIN" read from the magnetic stripe, in which case the data value associated with each scenario will be the beginning of the PAN read from the stripe, or an AID/Tag combination, in which case the data will be read from the chip.

The CAT will check each entry in the order specified until it finds a BIN that matches the beginning of the account number read from the magnetic stripe on the card, then the associated scenario will be loaded and used for the test.

e.g.

When using mag stripe data :

```
449900 Vis 1.4
558811 M\Chip 4
332211 Amex Scripts\ExpressPay
```

or when using chip data :

```
A000000003 Vis 1.4
A000000004 M\Chip 4
A000000025 Amex Scripts\ExpressPay
```

When using mag stripe data it is permissible to use more or fewer than the six characters that normally form a BIN, the number of characters extracted from the magnetic stripe data will be geared to the length of the "BIN" in the selection list. The scenario used will be the first positive comparison found, so the order of the entries in the list is important, for instance:

```
5588    scenario 1
558811  scenario 2
```

will never choose scenario 2, but

```
558811  scenario 2
5588    scenario 1
```

will select scenario 2 if the BIN is 558811 and scenario 1 for all other BINs beginning 5588.

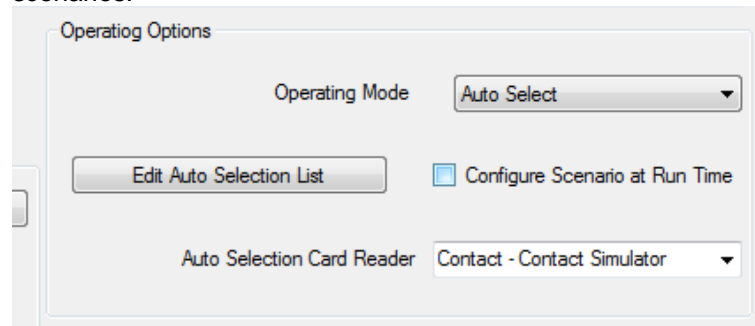
Similarly, when using chip data wildcard characters can be used so that an exact match will not always be necessary, again, it will be the first positive match that will determine the scenario to be used.

The scenario which has the auto select mode set should itself contain test stages just like any other scenario. These stages will then be used as a fallback, or default scenario, to be run if the auto selection list does not yield a valid choice. This could happen, for instance, if the magnetic stripe read fails, or the selection list does not contain a data value matching the card under test. When this happens the scenario will be run in "Always Complete" mode.

Auto selection is now recursive, in earlier versions of the software it was not. So if the scenario selected by this method also has the "Auto Select" mode set then a further scenario selection process will take place, and so on. This allows quite complex decision paths to be implemented but requires care in setting up because if a scenario is able to auto select the scenario that selected it then an endless loop will be created.

### Creating "Auto Select" scenario

A template scenario called "EMV Automatic" has been provided to aid the user in creating the auto selection scenario. The operating options for this scenario are different from the standard scenarios:



The screenshot shows a dialog box titled "Operating Options". Inside, there is a section for "Operating Mode" with a dropdown menu set to "Auto Select". Below this is a button labeled "Edit Auto Selection List" and a checkbox labeled "Configure Scenario at Run Time" which is currently unchecked. At the bottom, there is a section for "Auto Selection Card Reader" with a dropdown menu set to "Contact - Contact Simulator".

The drop box for operating mode must indicate "Auto Select". The Auto selection list can be edited by clicking on the button "Edit Auto Selection List" as described below.

[illegible]

## Editing the Auto Selection List

Whenever the scenario is in Auto Select mode the "Auto Selection List" button immediately below the operating Mode selection window will be enabled. Clicking this button opens the Auto Selection List Manager. The "Auto Selection List" allows user to enter values that help CAT in making the decision to choose appropriate scenario. It can be used to implement any of the following functionality:

- Read Magnetic Stripe data, and choose a scenario based on the BIN.
- Read chip data, find a particular tag value and choose a scenario based on that value.
- Read PSE / PPSE data and choose a scenario based on tag from the FCI. Currently the CAT only supports tags within the first level of PPSE FCI. It does not support reading / analysing the tags under "BF0C" template. For both PSE / PPSE currently no support is provided for reading tags under the directory entries. However, if you need this feature, please let us know and we can explore the possibility.
- Read AID of card and choose a scenario based on the AID / RID.

**Data Source**

This can be the BIN from the magnetic stripe or an AID/Tag combination read from the chip.

**AID**

This box is only active if the data source is chip data, it has no function when using mag stripe data. Enter here the AID to be selected in order to obtain the data to choose the scenario. Since virtually all cards nowadays support partial name selection, this can be just a RID. It is also permissible to enter a sequence of AIDs separated by vertical bar characters('|'), in this case the first AID in the list to return a positive response will be the one used. The keyword "PSE" or "PPSE" may be used to specify that the PSE or PPSE respectively be used, in this case only a Select command will be issued, there will be no Read Record or Get Data commands issued if the tag cannot be found in the selection FCI. This means that PSE directory entries will not be accessed, but the PPSE directory entries will be available. If the defined tag occurs more than once then the last occurrence will be the one used for scenario selection.

**Tag**

This box is only active if the data source is chip data, it has no function when using mag stripe data. Enter here the hexadecimal tag for the data item to be read to obtain the data to select the scenario. When a number of alternative AIDs have been listed in the AID box it is possible to leave the tag field empty.

**The Value Field**

The data value associated with each scenario. When using mag stripe data this is the BIN read from the stripe, in this case the number of characters in the value field determines how many characters will be matched in the card data, see above for examples. When using chip data it may be the value of the tag defined in the AID/Tag fields or, if the tag field is blank, one of the multiple AIDs listed. In the latter case the system will choose the scenario which corresponds to the first AID which responds. The value field can contain the wildcard characters '\*' and '?' where '\*' represents any group of characters and '?' represents a single character. So, for instance, a tag of "50" and a value of "\*DEBIT\*" will match any application with the word "DEBIT" in its label.

**The Note Field**

Associated with each value/scenario pairing there is a note field. Any text entered in this field will be displayed on the summary screen at the end of the test. It may be used to convey additional information or instructions to the operator.

**To Add a New Entry**

Type the data value into the leftmost text box at the top of the manager, then either type the scenario name into the rightmost box or use the "Browse" button to open the Scenario Manager and choose one from those available.

Ensure that no existing entry is highlighted in the main list box (if one is already highlighted then select the blank entry immediately below the last entry in the list) and click the "Insert" button.

**To Replace an Entry**

Follow the procedure above but select the entry which is to be replaced before clicking the "Insert" button.

**To Edit an Entry**

Select the required entry and click the "Edit" button. The entry will be copied to the text boxes at the top. After making the required changes click the "Insert" button.

If it is desired to add the changed entry as a new entry, leaving the original entry as it was, simply select the blank entry at the bottom before clicking "Insert".

**To Delete an Entry**

Select the entry or entries to be deleted and click the "Delete" button.

**To Change the Order of Entries**

Select the entry to be moved and click the "Move Up" or "Move Down" button as necessary.

**Import from CSV**

User can prepare the list of entries in a CSV (Comma separated values ) file and import them all using this button. The existing entries will be overwritten by the whole list, tool checks if the scenario exists before importing.

**Export to CSV**

User can export the whole list to a CSV file for analysis and storage

**Sort and Search of list**

The list can be sorted by clicking on column header that the user wants to sort the list for. Care must be taken while sorting, as the list is a "prioritised" list of values. Sorting may change the priority order. List can be searched for a string, if multiple matches are found the tool will allow user to "select" the entries one by one by clicking "Search Next" . The search is cyclic, i.e. when it reaches the end of list it will again start from the top of the list.

**Closing the Auto Selection List Manager**

The "Save" button copies the amended list back into the scenario and closes the manager. The "Cancel" button closes the manager without making any changes to the scenario.

## Scenario Selection by Reference

In a production or QC environment it is often convenient to select a scenario using machine readable data such as a barcode. This facility exists to facilitate that option.

Since a wide variety of automatic data entry devices such as barcode readers can be interfaced to a PC as a keyboard emulator the input of the reference data into the CAT 3000v3 is implemented as keyboard input, although it is not anticipated the actual keyboard will be widely used.

The reference data is input as text into the reference text box in the bottom right corner of the main screen, on receipt of a user defined termination character the reference is used to look up and load a scenario from a user prepared list.

**Setting up the Scenario Reference List**

The scenario reference list editor is invoked from the Administration menu on the Config Ribbon.

Scenario Reference Code Setup

Terminator Character (Hex) 0D Interpretation Script

Value	Scenario
-------	----------

Edit Insert ☐ Reference Input is Literal Scenario Name ☐ Use Wildcard Characters

Save Delete Help Cancel

**The Value Field**

The reference associated with each scenario. This is either the complete reference (e.g. barcode) string, or the output from the interpretation script.

**Terminator Character**

This is the character sent by the input device to denote the end of the reference string, it is entered in hexadecimal so that non-printing characters can be used. The default value is "0D" which is the "New Line" character sent by the "Enter" key on most keyboards.

**Use Wildcard Characters**

If this check box is checked then the value field can contain the wildcard characters '\*' and '?' where '\*' represents any group of characters and '?' represents a single character.

**Reference Input is Literal Scenario Name**

It may be convenient to either name the scenarios with the reference string or to have the interpretation script perform the lookup, in which case this box can be checked and the Value/Scenario list will not be used.

**Interpretation Script**

If the reference string is long and complex, and only a small part of it defines the scenario to be used (e.g. in the case of a 2D code) then a Tcl script can be provided to extract a manageably sized reference string from the input data. This script can be produced in-house if desired, or can be provided by Barnes International.

**To Add a New Entry**

Type the data value into the leftmost text box at the top of the manager, then either type the scenario name into the rightmost box or use the "Browse" button to open the Scenario Manager and choose one from those available.

Ensure that no existing entry is highlighted in the main list box (if one is already highlighted then select the blank entry immediately below the last entry in the list) and click the "Insert" button.

**To Replace an Entry**

Follow the procedure above but select the entry which is to be replaced before clicking the "Insert" button.

**To Edit an Entry**

Select the required entry and click the "Edit" button. The entry will be copied to the text boxes at the top. After making the required changes click the "Insert" button.

If it is desired to add the changed entry as a new entry, leaving the original entry as it was, simply select the blank entry at the bottom before clicking "Insert".

**To Delete an Entry**

Select the entry or entries to be deleted and click the "Delete" button.

**Closing the Scenario Reference Manager**

The "Save" button writes the amended list to disk and closes the manager. The "Cancel" button closes the manager without making any changes.

## Error Coding and Suppression

### Errors and Observations

An **error** is a defect in the card's data or responses which causes the card to fail the test. An error might be caused by a violation of one or more of the various specifications the card must comply with, or by a deviation from the user defined test scenario criteria. The vast majority of errors will be produced by the data analysis stage(s), terminal simulators will normally only report the sort of gross error that prevents the test from being completed.

An **observation** is an anomaly of the data which, while not being serious enough to cause a test failure, may need to be brought to the attention of the card issuer. It may also indicate that for some reason, not under the control of the card, the test could not be fully carried out. If desired, observations may be hidden from the summary screen so as not to confuse the non-technical operator - this feature is available on Program Settings, accessed from the "Configuration" ribbon.

Observations are sometimes included at the specific request of payment scheme authorities when they wish to draw their members' attention to some point.

**Error coding** schemes are dependent upon the test script being used, information on them will be found in the help documents associated with the test scripts. The standard EMV test scripts use the Barnes scheme which is described in the EMV help document, qualification test packages will often use error code arrangements defined by the payment schemes or the test plan provider.

### Error Suppression

Some tests have error suppression facilities available. Where error suppression is available there will be an error suppression tab in the stage editor and information about how to use it will be found in the stage editor help topic.

## Scenario Shortcut Buttons

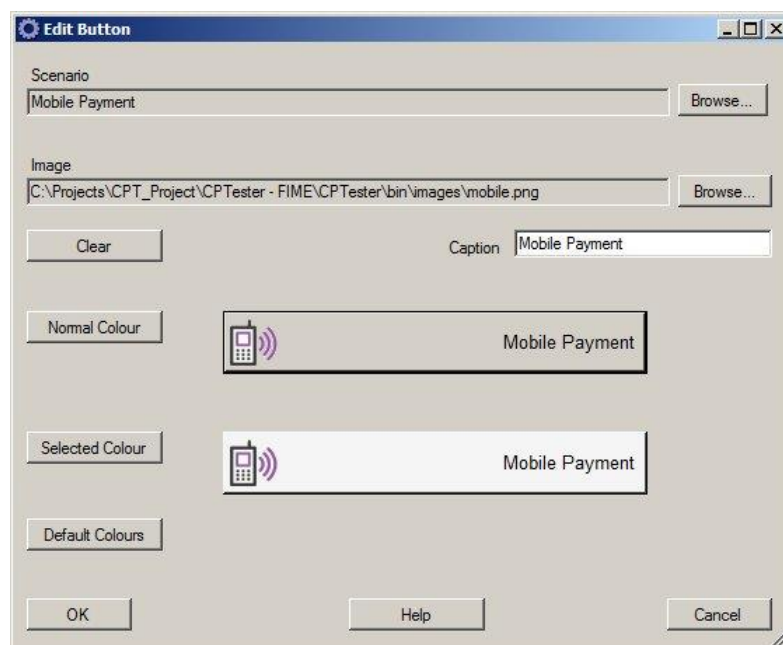
The scenario shortcut buttons on the right of the main screen provide a quick way to select frequently used scenarios. Although the system is shipped with these buttons pre-programmed, this is only intended as an illustration, and it is expected that users will set the buttons up to suit their own operations.

The button panel is tabbed, and users may add and remove tabs as required.

**To change the scenario allocated to an existing button**, right click on the desired button and select "Edit Button" from the pop-up menu. Note that this option is only available to users with the appropriate grading.

Select the scenario using the upper browse button, this will open the scenario management window from which a scenario may be chosen. Note that choosing a scenario this way does not load the scenario for use, it only allocates it to the chosen button. If an image is required on the button then it is chosen from the currently available image files using the lower browse button. Additional images may be added to the system by placing files in the local "Images" folder. Note that the images are not scaled so they must be saved as the actual size required on the screen. Image formats accepted are .jpg, bmp or png.

As an alternative to a specific scenario a button can be attached to a folder within the scenario storage system. In this case clicking on the button will open the scenario management screen with just the scenarios in that folder, and any sub folders beneath it, visible.



The "Caption" box sets up the words which will appear on the button, this will initially default to the scenario name, but may be edited if required, e.g. if the full scenario name is too long to fit comfortably on the button. The two "buttons" below the caption box are an indication of how the shortcut button will appear in its unselected (upper) and selected (lower) states, these are not real buttons and clicking on them will have no effect. The button will take on the

selected state when the scenario attached to it is loaded and in use, this will happen even if the scenario was loaded by some means other than clicking on the button, e.g. by using the scenario management screen. Buttons with folders attached will never enter the selected state.

The two buttons to the left of the sample buttons may be used to define the button colours for the two states. It may be useful to use colour coding to identify groups of buttons or to distinguish profile buttons from folder buttons.

The "Clear" button removes all settings from the shortcut button, which will then appear blank and clicking on it will have no effect. The clear button does not affect the button's colour setting.

**To delete a button when it is no longer required**, right click on the button and select "Delete Button" from the pop-up menu.

**To create a new button** right click on the space below the buttons and select "New Button" from the pop-up menu. A new button will be added to the bottom of the panel and the button editing dialog will be opened. See above for allocating a scenario etc.

**To create a new tab** right click on the space below the buttons or on one of the existing tabs and select "New Tab" from the pop-up menu. You will be prompted to enter a name for the new tab. Once the tab is created buttons can be added using the techniques described above.

**To delete a tab no longer required** ensure the tab to be deleted is selected, right click on the tab and select "Delete Tab" from the pop-up menu

**To rearrange the buttons on a tab** right click on any button and choose "Move Up" or "Move Down" from the pop-up menu, the button will move one slot in the chosen direction.

## Saved Card Database

Individual card test results may be stored in the card test result database. This database is separate from the storage of batch test results. Although the data saved for each card is the same in both cases, the management of the storage is handled differently.

The Card Database Dialog brings together all the functions required to manage the individual card test results in one convenient screen. **NB. The features on this dialog are subject to user permission control, and so may not all be available to all users.**

ID	Date Stored	Card Ven...	Chip Vendor	Encoder	Product C...
4547 4240 0000 0038	09/03/2007 15:19:29	Visa MFC...			
4579611500039000	03/12/2007 18:28:01	Visa		Amanda	
4761739001010358	03/12/2007 18:22:28	Test Save			
4917330048445378	03/12/2007 18:12:54	Woolwich			Electron
541234xxxxxx612	24/09/2007 15:42:13	Mastercard	Butterfly		Dual Interf...
5413 3390 0000 1513	09/03/2007 15:30:14	Mastercar...	M/Chip 4	CDA Ena...	
5413339000001513	29/10/2007 10:04:31	mchip 4 a...			

Save New Card Recall Card Delete Card Save Changes Card Groups Last Card

Selected Card Data

Card Vendor: Test Save

Chip Vendor: Encoder: Date Stored: 03/12/2007 18:22:28

ID: 4761739001010358

Product Code: Help Exit

### Concepts

Each test results item consists of a complete record of the test as it was performed on the CAT 3000v3, recalling the result will produce exactly the same set of screens as were shown when the test originally took place, regardless of any changes made since that time to the test scripts or scenario used. By default all the stored card data is encrypted, so can only be seen by a user logged on to the CAT with card recall permission.

For the purposes of this topic, the term "Card" will be used to represent a set of test results stored in the database.

Each card is identified by an identifier, for an EMV card this will default to the card's PAN, but this can be changed when the data is saved. Associated with each card is the date and time of the test and four user definable information fields. Every card stored is a member of a "Card Group".

Card groups allow stored cards to be subdivided into more manageable blocks, this will be most useful where large numbers of cards are being stored and batch mode is not a convenient way of managing the tests.

**Action Buttons**

Five action buttons are provided just below the card and group list windows, these will be enabled and disabled according to whether their function is currently available.

**Save New Card**

This button is available if there is a set of unsaved test results available within the CPT 3000v3. This normally occurs when the dialog is first opened following a card test. The default id supplied by the test script will be already inserted in the "ID" box (the generation of this ID is a function of the test script, so may vary according to the type of card tested), this may be altered if required. The four information fields are available for text entry, or may be left blank. The titles of these four information fields can be tailored to individual user requirements in the Program Settings dialog, these titles do not affect the content or use of the fields in any way, and changing them will not affect any of the data already saved.

Clicking the "Save" button will install the card in the database, as a member of the group currently selected in the "Card Group" window.

NB. Automatic saving of every card tested, or every card that fails a test, is available as a set up option in the Program Settings dialog.

**Recall Card**

This button becomes available whenever a card is selected in the cards list window, clicking this button will recall that card to the main screens and close the dialog.

**Delete Card**

This button becomes available whenever a card is selected in the cards list window and the logged on user has permission to delete saved cards, clicking this button will delete the selected card from the database. To guard against accidental loss of data an extra confirmation dialog will be presented before the deletion takes place.

NB. Automatic deletion of cards over a defined age is available is required, this can be set up on the Program Settings dialog.

**Save Changes**

When this button is clicked any changes made to the information fields, or the group the currently selected card is allocated to, are written to the database.

**Card Groups**

Opens the Card Group management dialog.

**Last Card**

Restores to the main screen the last card tested, regardless of whether it was specifically saved or not.

**Cards Window**

Cards in the currently selected group are listed in the cards window. When the dialog opens they are sorted in order of their ID, but may be re-sorted using any of the other fields simply by clicking on the column header. Clicking on the column header of the field already in use will reverse the order.

### Card Group Window

Each card saved in the database is a member of a group. The cards shown in the cards window are only those which are members of the group currently selected in the Card Groups window, to see cards in other groups, simply select the required group in the Card Groups window.

When saving a new set of card results that card is saved into the currently selected group. To move a card from group to group after it has been saved simply use the mouse to drag it from the cards window onto the required group in the Card Groups window. To make a copy of a card in another group hold the control key down while dragging.

Groups may be created and deleted using the Card Group management dialog, activated by the "Card Groups" button.

## Card Group Management

Card Groups are a means of managing large numbers of saved cards by dividing them into smaller packets, they can be thought of a bit like folders in the filing system. The main difference between a card group and a folder is that a card group can only contain saved cards, it cannot contain other groups.

The system is shipped with a single card group, named "General", and if only small numbers of cards are being saved then this will probably be adequate. A second predefined group, named "AutoSave" will be created by the system if the "save all cards" option is enabled in program settings, the automatically saved cards will be placed in the AutoSave group. In addition to this, there is an option to categorise automatically saved cards into groups identified with the card's BIN, so there may be a number of "AutoSave" groups, each one being appended with the first six characters of the card's identifier (the BIN for EMV cards). When this option is active any cards for which an identity cannot be derived by the test script (e.g. in the case of a gross card failure) will be placed in the AutoSave group.

The Card Group Management dialog is accessed from the Saved Card Database dialog.

To create a new group, type a name for it into the box at the top of the group management dialog and click the "Add Group" button. Group names can contain any alpha-numeric character, and spaces, but no punctuation; in addition the first character cannot be numeric. The edit window will prevent invalid names being typed in but care must be taken if using copy and paste techniques.

The window below this contains a list of all current groups. To delete a group, select it in this window and click the delete button. **NB. If a group is deleted then all cards within it will also be deleted**, use this function with care.

Moving and copying cards from group to group is carried out using the Saved Card Database dialog.

## Batch Mode Testing

Batch mode provides a means of testing cards in an ordered environment and of keeping automatic records of the results. It is primarily aimed at the Quality Control function but may also be used in any situation where this method of result recording is convenient.

A batch is a group of cards all tested to the same scenario either during a single session or in a series of sessions spread over time. Once created, a batch can be closed and re-opened any number of times to add new tests.

### Open or Create a Batch

This is carried out using the Batch Management dialog opened using the Batch toolbar button at the top of the main screen, see below for more details

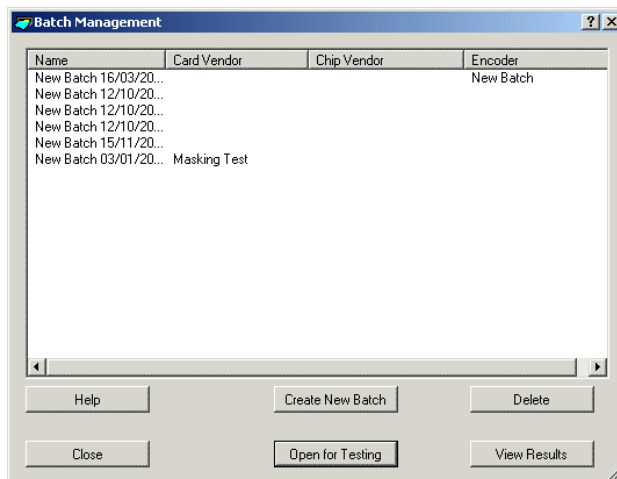
### Testing cards in batch mode

Testing cards in batch mode is exactly the same as testing them in normal, single card, mode. The only difference is in the way the results are stored. After each test all the normal displays and reports are available for inspection.

### Close a Batch

When the system is operating in batch mode the batch button at the top of the screen becomes a "Stop" button. Clicking this will close the batch and display the results to date. In addition a batch can be set up to close automatically after a preset number of cards.

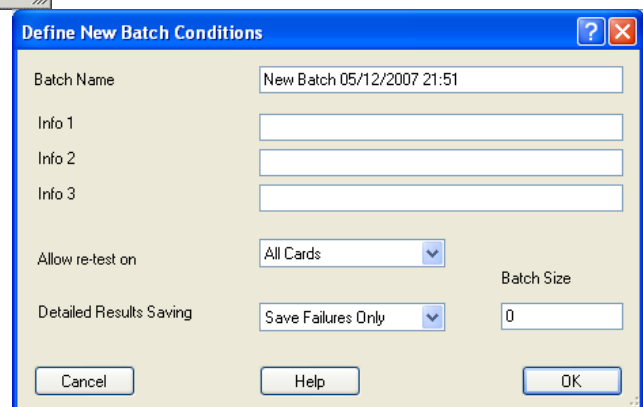
## Batch Management Dialog



The batch management dialog is opened using the "Manage Batches" button on the "Batch" ribbon. It shows a list of the batches currently in existence and has a series of action buttons at the bottom, these enable the user to create a new batch, open an existing batch to test more cards, open an existing batch to view the results, or delete a batch. Some user grades may not have access to all of these functions; in this case the unavailable buttons will be greyed out.

### Create a New Batch.

This button opens the new batch dialog into which the batch name may be entered, along with up to three information fields. The titles of these four fields are the same as the first three of the four information fields used for individual saved card data and may be set up in the Program Settings dialog.



The size of the batch may be set up here also. If a value is put into the size field then the batch will be automatically closed when that number of cards have been tested, if it is left at zero then the batch can only be closed manually.

The card data saving option is set up using the drop down list. This controls the saving of the complete results for the cards. Note that the card id and the pass/fail status is always recorded for every card tested, the data saving option controls the saving of the detailed data for the cards. The options are “save nothing”, “save only failures”, or “save everything”.

When all these details are entered the OK button will open the scenario loading dialog. The scenario for the batch is chosen now. Once chosen a copy will be made of the scenario which will be stored with the batch data; and this copy will be used whenever the batch is opened for more testing. In this way, even if the scenario is edited during the lifetime of the batch, all the cards in the batch will still be tested to the same set of conditions as the first one.

Once the scenario is selected the system is ready to test cards.

### **View Batch Results**

This button will load the results to date of the selected batch into the batch results main screen and close the dialog.

### **Open a Batch for More Testing**

Select the desired batch in the batch in the batch management screen and click the open for testing button. The dialog will be closed, the test scenario for that batch will be loaded, and the system will be immediately ready to test cards.

### **Delete a batch**

Select the batch(es) required for deletion in the list window and click the delete button, a confirmatory warning will be shown to prevent accidental deletion. Please note that when a batch is deleted **all the card test data saved with it is deleted also**. Use this function with care.

## Batch Results Display

The batch results screen is essentially a list of all the tests carried while that batch was active. At the top there is some general information, applicable to the entire batch, then each test is listed below. If the same card is tested more than once, then each test of that card is shown, but grouped together, the number of individual cards is shown at the top of the display as well as the number of total tests and the number of failures.

**BARNES INTERNATIONAL**  
Batch Test Information

**New Batch 16/03/2007 14:58**

Test started 16/03/2007 14:58  
 Completed 05/12/2008 10:52  
 Equipment CAT 3000v3 Ser. No. 12/12 Software Ver 3.18  
 Profile Emv Default  
**Tests Performed** 6  
**Unique Cards Tested** 5  
**Cards Failed** 2

**Test Results**

Card	Card id	Operator	Time	Result
1	123456789098	Melanie	16/03/2007 14:59	Pass
2	<a href="#">123456789000</a>	Melanie	16/03/2007 14:59	Fail
	123456789000	Melanie	16/03/2007 15:00	Pass
3	<a href="#">123456789123</a>	Robert	16/03/2007 16:04	Fail
4	123456789099	Robert	16/03/2007 16:05	Pass
5	<a href="#">5412340600000039</a>	Herbert	05/12/2008 10:52	Fail

Current Scenario: Emv Default  
Licensed for 3652 days

The pass/fail result of each test is shown alongside the time of that test, as is the operator logged on at the time. Where a card is tested more than once it is only considered a failure if all its tests failed, if one of them passed then it is considered a pass. This philosophy stems from the relative unreliability of magnetic stripe reading; especially if a hand operated dip reader is in use, a test might fail due to a poor magnetic stripe read on one occasion through no fault on the card. If a chip data problem causes a failure it is unlikely to pass on a subsequent test.

The card results are shown in chronological order of the first test on each card. Re-tests are grouped with the first test on the card even if they took place days later.

Where the full tests results for a card have been saved the card identity will appear blue and clicking on it will recall those results to the main displays.

The card identity is normally taken from the account number, which is unique to the card, but sometimes this has to be masked for security or privacy reasons. In this case a hash value is calculated from the number and used instead as the card id. It is impossible to derive the account number from the hash and there is a vanishingly small probability of two different account numbers producing the same hash. Where the card number is partially masked, then the masked value is shown with a four character hash appended to it, when the number is fully masked then an eight character hash is used alone.

## Data Export and Import

The CAT 3000v3 provides a number of ways in which the data it produces and uses can be moved in and out of the system. This enables test result information to be passed to external interested parties and results from other installations to be viewed. Also test scenarios may be exported and imported as files so that they can be shared between non-networked installations.

All of these features can be accessed from "Export" and "Import" menus on the "Card Data" ribbon.

### Complete Test Results

The complete test result set can be exported as an XML file which can be imported by another CPT/CAT 3000v3, the imported file will exactly reproduce the displays from the exporting system, regardless of what scenarios are loaded on the import machine. These files, which include the information necessary to reproduce the hyperlinks as well as the results text, are in a format specific to Barnes. From software version 3.17 onwards the scenario data is also saved into this file, and after the file has been imported this scenario data may be viewed using the "Embedded Scenario" button on the scenario tool bar. This option is only available when there was scenario data in the imported file, at all other times, and when the imported data did not include the scenario (i.e. was exported by an earlier version of the software) then this menu option is disabled. If it is desired to use the scenario saved in the results export file then it can be imported using the scenario import facilities explained below.

These files may optionally be encrypted using the inbuilt 3DES encryption engine. In this case, the encrypted file has ".bir" extension. The ".bir" file can be directly imported into the CAT or a CPT 3000v3.

**NB. Complete Test Results is the preferred way to send data back to Barnes when technical is required. It contains the maximum amount of information to allow Barnes' engineers to help you.**

### Barnes Card Image File

The card image of any card can be exported in Barnes proprietary format. This file can later be imported in another CPT (3.47 or above) and re-tested. This feature enables users to store card data at one location and test the same card data at another location without the need to transfer a physical card.

### Engineer's Log

The engineer's log may be exported in either plain text or HTML. In HTML format it will display exactly as it appears on the CAT 3000v3 screen, in text format it is compatible with the engineer's log files from the CPT 2000 and CPT 3000 products. The text form can be imported into the CAT 3000v3, as can files from the earlier two incarnations of the tool.

Please note an important difference between the import of an engineer's log and the complete results mentioned above, which includes the engineer's log as well as all the other displays. When an engineer's log is imported the other displays are derived from the card data it contains based upon the first (or only) analysis stage of the current scenario, this is similar to the way in which engineer's logs were imported into CPT 3000, and means that the results displayed after import will not necessarily be the same as they were on the system that exported the file. This feature provides a limited means of checking card data against scenarios other than the one against which the card was originally tested. Please note especially that if sensitive data is masked in the log file then checks requiring access to that data, such as SDA and DDA, will inevitably fail.

The text format files may optionally be encrypted using the inbuilt 3DES encryption engine. In this case, the encrypted file has “.bil” extension. The “.bil” file can be directly imported into the CAT or a CPT 3000v3. If decrypted through the “File Encryption utility”, a text file can be recovered which can be viewed directly using any text editor. It can also be imported into the CAT or CPT 3000v3 if required to check the card data against another scenario.

Engineer's log data may also be imported in two other forms, the XML format used for card data saving on the CPT 3000 and CAT 3000v2, and the "Raw Card Data" format. The data may also be exported in the latter form. The Raw Card Data format is an encrypted file that can only be opened by another (or the same) CPT/CAT 3000v3, it differs from the text form of the log in that the data masking is not applied before saving. Thus, when displayed, the data is masked according to the settings on the importing system, not the exporting system.

### **Detailed Results Tree**

The tree display can be exported as an HTML file. This format will show the tree fully expanded, regardless of its expansion state on the screen. The resultant display will show the layout of the tree, but without the lines connecting the branches to their parents.

These files may optionally be encrypted using the inbuilt 3DES encryption engine. In this case, the encrypted file has “.bit” extension. The “.bit” file cannot be directly imported into the CAT, but needs to be first decrypted using the “File encryption utility”. After decryption a standard HTML file is recovered which can be viewed in an html browser.

### **Test Report (RTF)**

The test report is exported in Rich Text Format (rtf). This format is widely accepted and can be imported into all major word processing systems. The appearance of the RTF version is very similar to that shown on the screen.

### **Test Summary**

The test summary can be exported as a simple HTML file without the images, but including all the embossing and failure/observation notes and the Pass/Fail stamp.

These files may optionally be encrypted using the inbuilt 3DES encryption engine. In this case, the encrypted file has “.bis” extension. The “.bis” file cannot be directly imported into the CAT, but needs to be first decrypted using the “File encryption utility”. After decryption a standard HTML file is recovered which can be viewed in an html browser.

### **Zipped Report Set**

The summary, tree, test report and engineers log described above may be exported in a single operation and saved in a zip file. This provides a convenient means of exporting all the test result data in a form that can be read without requiring the use of another CPT or CAT. Optionally the zip file can be password protected. NB. this encryption uses the standard zip file encryption method, not the CPT's inbuilt encryption engine.

### **Test Results (PDF)**

This option appears when a card has been tested. By default, the tool will export Test Report, Details Tree and Engineering log. The user can disable the PDF report completely or remove the details tree and/or engineering log from the exported file.

### **Test Scenarios**

Scenarios are exported in a format that combines all the stages into a single file and allows an identical scenario to be set up on another system. Note that where systems are on a

common network it may be more convenient to simply set them up to share a single scenario set (see program settings), the scenario export file is intended to transfer scenarios between sites and organisations, such as issuers and bureaux, or payment schemes and issuers, etc.

From software version 3.17 onwards, scenario information is also stored in the complete test results file, so these files may also be used as a source for importing scenarios. Obviously an attempt to import a scenario from a file saved by an earlier version of the software will not be successful.

Scenarios may also be imported from CPT 2000, CPT 3000 and CAT 3000v2 scenario export files, this option is available using the "Files of Type" drop down list on the file open dialog. Please note, that due to significant differences in the make-up of test scripts and scenarios between CPT/CAT 3000v3 and the previous versions of the tool the conversion utility makes a number of assumptions, it is recommended that each converted scenario be manually checked before use.

The file open dialog used for scenario import has the multi-select option enabled, so that a number of files may be selected and imported in one go. Imported scenarios are placed in a specific folder, from where they may be moved, renamed, etc using the scenario management facilities. Scenarios from CPT3000v3 or CAT3000v3 are placed by default in the "Imported Scenarios" folder, this folder can be changed in "Program Settings". Scenarios converted from earlier software versions are placed in the "V2 Imports" folder.

Scenario data may optionally also be imported from external sources, such as the Visa VPA tool, or the last card tested. In these cases the import is handled from within the data analyser stage editor, and not by the scenario import mechanism.

### **Daily Test Reports**

A summary of a day's tests can be generated automatically and stored in a folder. Alternatively it can also be viewed through CPT Administration menu. To auto-generate the daily test reports, please set the folder paths in the Program Settings > File Paths

## Export File Encryption

It is in the nature of the CAT 3000v3 that much of the data handled by the system is confidential, and when transmitting this data from one location to another by electronic means it will be desirable, if not essential, to encrypt that data.

Several of the data export functions include the option to encrypt the file, where this is available an encryption dialog box will appear after the export file name and location have been chosen.



The dialog contains two password entry boxes, both must be filled in with the same password to eliminate typing errors. Passwords must be at least four characters long, but longer passwords, up to the maximum of sixteen characters, will be more secure.

Once both copies of the password have been entered, click the encrypt button to save the encrypted file.

NB. The file extension will be changed when the file is encrypted, complete test results files

will have the extension ".bir", engineer's log files ".bil", and HTML files ".bih".

Engineer's log and complete test results files can be directly imported back into a CAT 3000v3 or CPT 3000v3 after entering the correct password.

To skip encryption and save the file in plain text, simply click the plaintext button, no password is required for this.

The encrypted file includes a checksum which is verified on decryption, this allows the system to detect errors in the password entry or invalid files (i.e. files which were not encrypted by a CPT/CAT 3000v3 or which have been corrupted in transit).

NB. Only files which have been encrypted by a CAT 3000v3 or CPT 3000v3 can be decrypted by this facility, and files encrypted here can only be decrypted by a CAT 3000v3.

There is an offline file encryption facility on the administration menu which can be used on any file, including the ".bih" encrypted HTML files.

## Certification Authority Public Keys

In order to carry out data authentication tests on a chip card CAT 3000v3 requires access to the relevant public keys from the Certification Authority. The system is shipped with a set of current keys for Visa, MasterCard, American Express and JCB cards but from time to time the authorities issue new keys which will need to be added to the system. In addition test cards

are personalised using test keys, and, while there are a number of these available to Barnes and are therefore included with the standard system, these are not all the keys that may be around.

Because of this the 'Public Keys' menu, accessed from the "Configuration" ribbon, contains options to manage the public keys in the system, these functions are available only to higher grade users.

### Importing a New Public Key

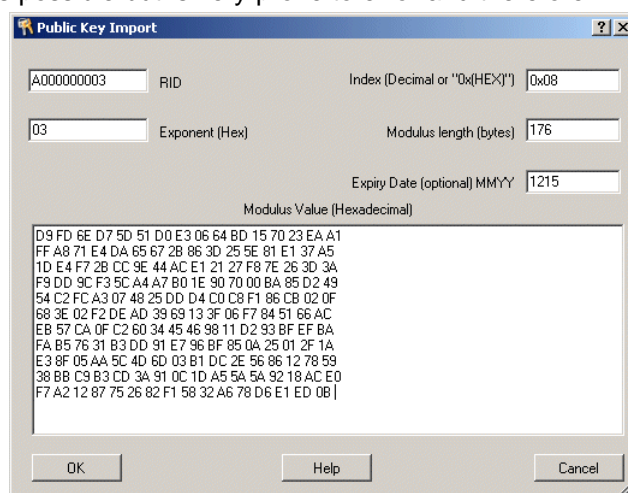
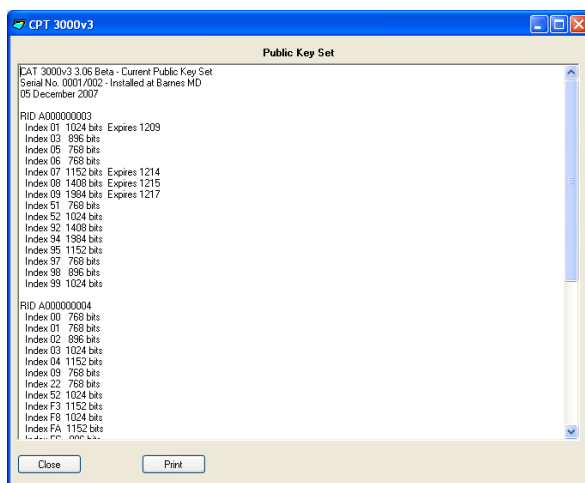
When 'Import Public Keys' is selected the user is presented with a dialogue which enables a new public key to be entered. The public key itself consists of

an exponent, which is normally "3" or "0x10001", and a modulus, which is a block of data containing the same number of bytes as the encrypted Certificate on the card. The new modulus must be entered into the text box in hexadecimal form. In order to make this easier the text box has full text editing facilities, with an 'Edit' menu available by right clicking. The normal method of entering a modulus will hence be via a 'copy and paste' operation from another document, typing it in byte by byte is possible but is very prone to error and therefore

not recommended. The length of the modulus is entered as a check that the data has been correctly entered. This box will accept the length in either bytes or bits. Key lengths are usually quoted in bits, this number must be divided by eight to obtain the number of bytes, so a key length of 1152 bits will be represented by 144 bytes.

In order to identify the correct key for the card under test the key is stored with a RID and an index number. The RID, which is the first ten characters of the card's application identifier (AID), is used to identify the Certification Authority, and the index, which is also read from the card, identifies which of that Authority's keys to use. Thus a MasterCard key with a RID of A000000004 and an index of 3 is distinct and different from a Visa key with RID A000000003 and index of 3.

Optionally an expiry date may be entered. Many live public keys are published with expiry dates after which they are not permitted to be used. If the card's data specifies the use of a public key that has an expiry date associated with it the test scripts will verify that the key will not expire before the card's application expiry date.



When the new key has been checked it is entered into the internal public key database and may be used immediately. It is not saved permanently until the 'Save Public Keys' option is chosen from the 'Public Keys' menu. This enables new keys to be tested before being permanently stored. A reminder will be issued to the user if any public keys have been imported but not saved when the application is closed down.

**Editing a Public Key.**

Another item on the public keys menu allows an existing key to be edited. In this case the user will be presented with a list of the current keys and when one is chosen the dialog described above will be opened populated with the data relating to that key. Any of the fields may be edited and the key re-saved.

**Importing Keys from Another System**

The entire key set may be imported from an external source, this can be either an XML format key file from another CAT 3000v3 or a CPT 3000v3, or a "pubkeys.ini" file from a CPT/CAT 2000/3000/3000v2. The new keys may either completely replace the existing keys or merge with them; in the latter case only keys that do not already exist will be imported.

**Deleting a Key.**

The final option allows a key to be deleted from the system.

## EMV AID List Editor

Since Most installations of CAT 3000v3 are used to test EMV payment applications, a user interface has been provided to edit the list of known EMV AIDs so that valid payment applications can be recognised by the test scripts. It is particularly important to keep this list up to date when using Dynamic Scenario Generation.

The AIDs are divided into groups for ease of management and so that the list can be easily subdivided to save time when only one scheme's cards are undergoing test. The group is selected from the drop down list box at the top.

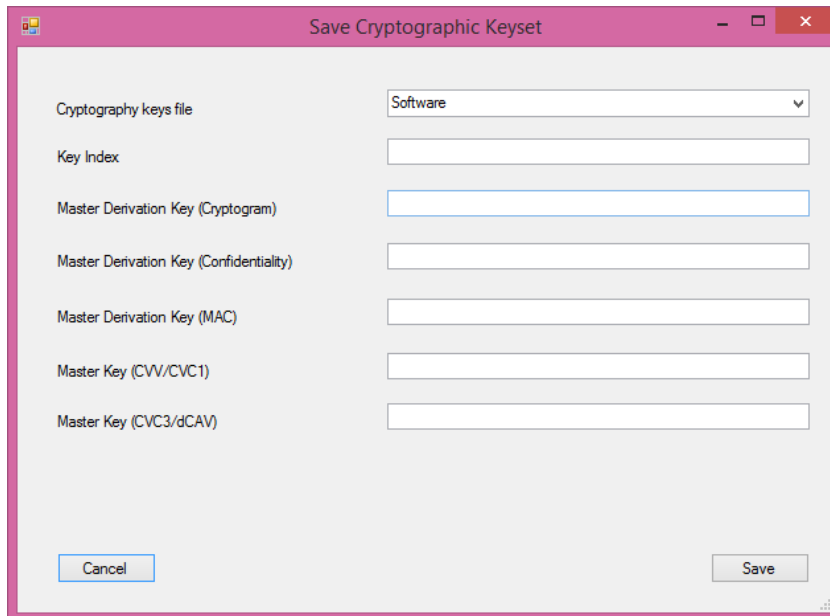
Right click in the main list box for the editing options, which are largely self-explanatory. New AIDs can be added, existing AIDs can be edited or deleted, and new groups can be added.

## Symmetric Key manager

The index file used to maintain the library of symmetric encryption keys can be managed by clicking the Cryptographic Keys button on the Configuration toolbar

Possible options:

1. List Key Indices: When clicked CPT will list all the indices already present in the Index file.
2. Add / Edit / Delete Key: Allows changes to a specific key:



The screenshot shows a dialog box titled "Save Cryptographic Keyset". It contains several input fields and two buttons at the bottom. The fields are labeled as follows:

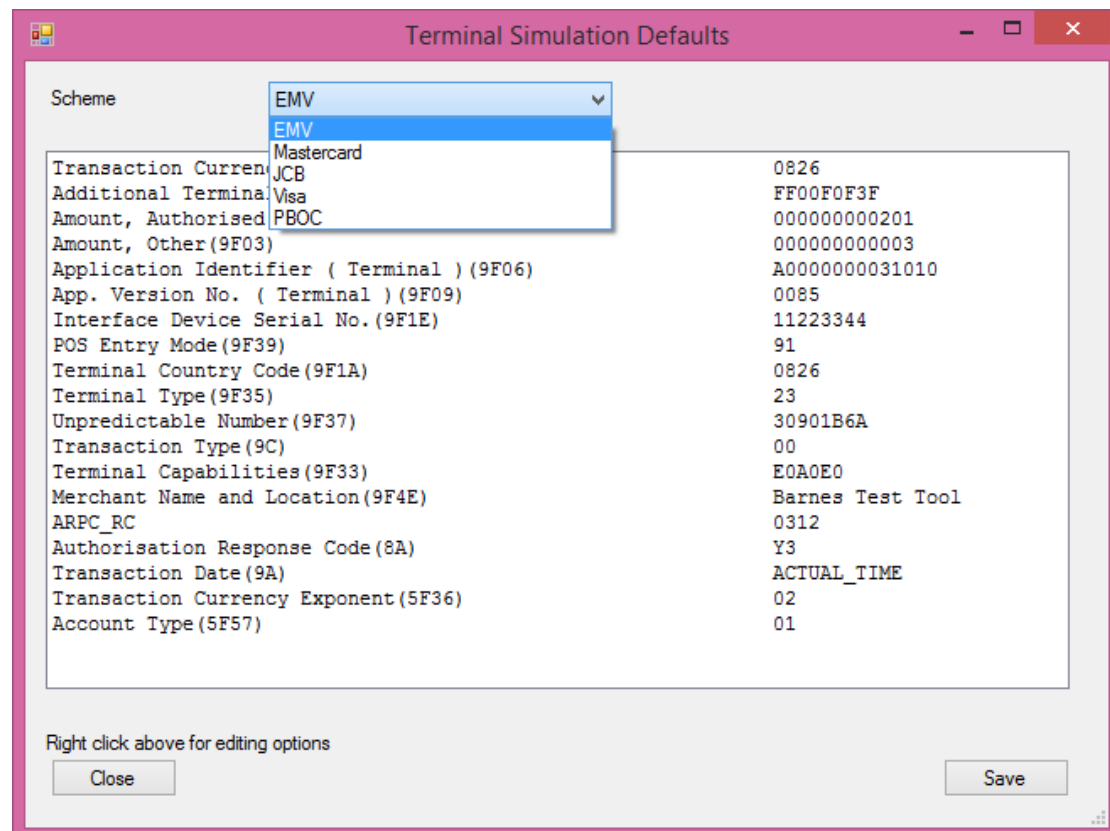
- Cryptography keys file: A dropdown menu currently showing "Software".
- Key Index: A text input field.
- Master Derivation Key (Cryptogram): A text input field.
- Master Derivation Key (Confidentiality): A text input field.
- Master Derivation Key (MAC): A text input field.
- Master Key (CVV/CVC1): A text input field.
- Master Key (CVC3/dCAV): A text input field.

At the bottom left is a "Cancel" button, and at the bottom right is a "Save" button.

The keys file selection allows the same process to be used with any of the key index files present in the scripts folder, only the nature of the keys themselves will vary between the software and HSM options.

## Terminal Defaults

CPT uses static default values for all the terminal tags such as Country code (9F1A), Transaction currency code (5F2A), Amount authorised (9F02) etc. the user can edit the default values used by the terminal simulator globally through the Terminal Defaults Editor:



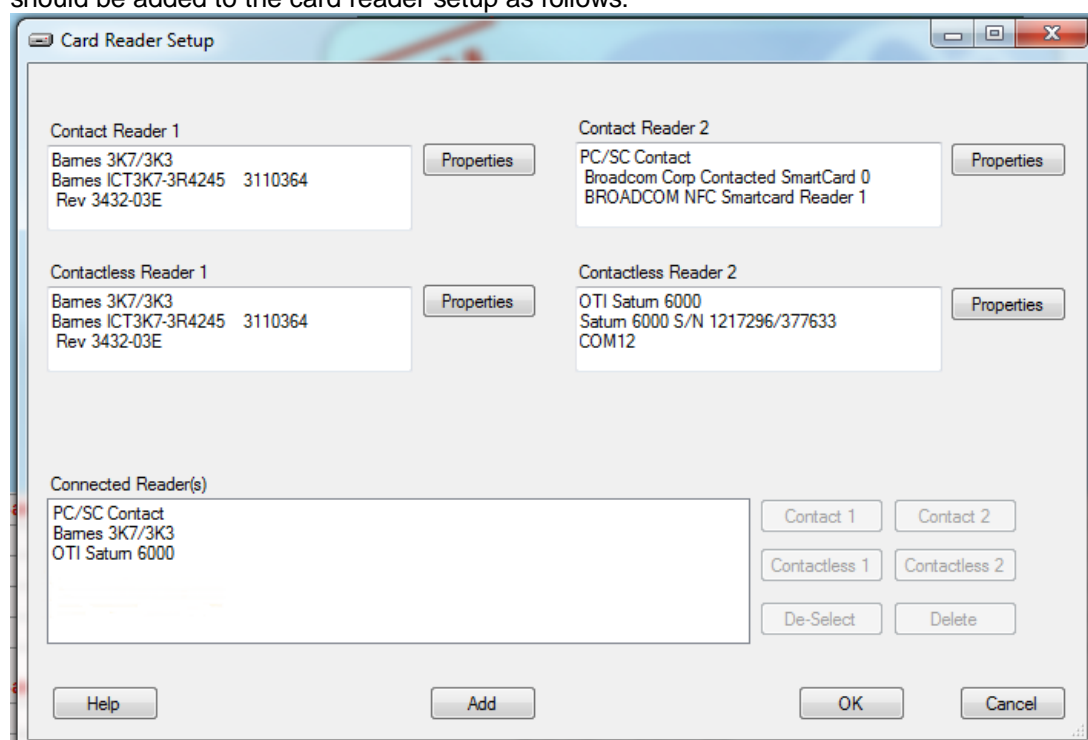
Tags can be added / deleted / edited by selecting them and then using the “right-click” button. Tags are arranged as per the schemes and they are displayed by selecting the appropriate scheme in the drop down menu as shown above.

## Reader Management

CAT 3000v3 is set up to support a number of commercially available card reader types. The reader management dialog is used to allocate these readers for use on a particular CAT 3000v3 installation.

One of the readers will usually be fitted with a Barnes International dongle. Barnes fits dongles inside the readers for the convenience of the user, the reader has to be present for the system to test cards so having it act as the dongle as well saves any need for additional tokens to be attached to the PC. Where this is not possible a separate dongle token can be provided.

Where two or more readers are enabled, usually a contact and contactless reader, they should be added to the card reader setup as follows:



The lowest window in the dialog shows the readers currently connected to the PC and recognised by the CAT 3000v3 software. The upper windows show information about the contact readers and middle window shows information about the contactless readers that can be used for testing. Card can be inserted in either "reader 1" or "reader 2", CPT will auto-detect the card and test it.

To allocate a connected reader to be the contact or contactless reader, select it in the "connected readers" list and click the "Contact" or "Contactless" button as desired. The selected reader will be allocated to that function.

To add a new reader click the "Add" button, this will bring up a list of the currently supported reader types. The new reader must already be connected to the PC and have had any necessary Windows™ drivers installed. Select the new reader from the list and, provided it can be initialised by the CAT 3000v3 software, it will be added to the "Connected Readers"

list. It will then be available to be allocated to the primary or alternate function.

The lowest window in the dialog shows the readers currently connected to the PC and The list of available readers will increase as time goes on and more devices are supported. Support for additional readers will be added as and when they become available and will be distributed as part of the standard software upgrade procedure.

The "De-Select" button will remove the reader selected in the lower box from the Contact 2 or Contactless 2 position. After this the interface will only have one reader allocated.

The Delete button removes the reader selected in the lower box completely. Note that if the reader containing the dongle (usually the main contact reader) is removed then the software will cease to operate.

## Currently Available Reader Types

**Barnes 3K7** – (Mag stripe/Contact/Contactless) - The Barnes 3K7 simplifies the testing of dual interface cards due to its ability to perform contact and contactless testing, together with a mag stripe read, with a single insertion. It is shipped as the standard reader on all CAT 3000v3 systems. It is only available with an RS232 interface, but comes with a USB/Serial converter and can be dangled.

**Barnes 3R1** – (Mag stripe/Contact) – This is a manual insertion reader useful in situations where it is required to test significant numbers of the metal cards which cause undue wear on motorised readers. It has a serial interface and can be dangled.

**MagTek IS350/IS65** - (Mag stripe/Contact) The MagTek IS350 was the standard motorised reader for CAT 3000v3 systems before the Barnes 3K7 was introduced. The IS350 is actually a model IS320 with a desktop case, so it will always appear to the CAT software as an IS320. The interface is also capable of supporting the manual insertion IS65. Because of different positioning of the card present sensor the IS65 works better with cards that do not meet the standard ID-1 outline. Both the IS320 and the IS65 can be dangled. The readers must be configured in ASCII mode and use the serial interface to work with the CAT 3000v3. The RS232 version is supported on all Windows versions. A USB serial converter is also supplied.

**PC/SC Contact** - (Chip only contact) PC/SC is Windows' inbuilt chip card reader interface. It supports contact chips only and has no facility for handling mag stripe data. The CAT 3000v3 PC/SC Contact interface monitors any connected PC/SC contact devices and will conduct the test on the first one that detects a card, the others are locked out for the duration of the test.

One PC/SC contact reader may be utilised to hold a dongle and/or one PC/SC reader can be used for card login. Please contact Barnes for more details.

**PC/SC Contactless** - (Chip only contactless) PC/SC is Windows' inbuilt chip card reader interface. Although it was designed only to support contact chips, many contactless card reader suppliers provide PC/SC drivers for their products, these readers appear to Windows as contact readers. The CAT3000v3 software is able in most cases to identify these readers as contactless, and this is backed up by facilities in the scenario editor to specify that the PC/SC reader is contactless. The CAT 3000v3 PC/SC Contactless interface monitors any connected contactless PC/SC devices and will conduct the test on the first one that detects a card, the others are locked out for the duration of the test.

**ViVotech** (Chip only contactless) This interface supports any ViVotech device that has "Pass-Through" mode enabled in its firmware. These are RS232 connected devices and

cannot be dangled. NB. Only readers having firmware version GR 1.0.0 will work with all card types. Due to recent design changes by the manufacturer the current versions of these readers will not work with the CAT 3000v3.

**OTI Saturn 5000** - (Chip only contactless) this interface supports the OTI Saturn 5000 in RS232 mode only. These devices cannot be dangled. These readers are no longer available and are supported only as a legacy feature.

**OTI Saturn 6000** - (Chip only contactless) this interface supports both the RS232 and USB variants of the OTI Saturn 6000. Some versions can be dangled, please contact Barnes for details.

**QPROX 3000** – (Contactless Only) A USB connected contactless reader with the option to carry the dongle.

**MagTek IS380** – (Mag stripe/Contact) The IS380 is similar to the IS320 but has the capability to write to the magnetic stripe on the card. NB. In order to make use of this feature specific test scripts and options are required, please contact Barnes International for details. The IS380 can be dangled.

**Barnes 3K3** – (Mag stripe (JIS and ISO T1 & T2) /Contact Chip). This reader is used primarily for the Japanese market because of its ability to read the JIS 2 magnetic stripe on the front face of Japanese financial cards as well as the ISO stripe on the back. It simplifies testing by reading the contact chip, together with a mag stripe of both magnetic stripes read, with a single insertion. It is being shipped as the standard reader to Japan only. It is only available with an RS232 interface and can be dangled.

**Omron V2BF Series** - (Mag stripe/Contact) These RS232 connected readers are used primarily for the Japanese market because of their ability to read the JIS 2 magnetic stripe on the front face of Japanese financial cards. They cannot be dangled.

**Micropross MP65** - (Chip only Contact ID-1/SIM/SWP) The MP65 is a contact chip only device which has facilities to communicate with the card using the SWP contact used by UICC resident mobile payment applications. The use of this reader and the test scripts that make use of its facilities requires the Mobile Device Testing module to be activated.

**XAC P89** - (Mag stripe/Contact) The P89 is a hand insertion reader that was shipped with most CPT3000/CAT3000v2 products. The P89 can be dangled. Only the USB version is supported and its use is now deprecated.

**XAC P88** - (Mag stripe/Contact) The P88 is no longer in production, but was shipped with most CPT2000 systems, so there may still be some in use, it is an RS232 device, and if it was supplied by Barnes then it is dangled. Its use is now deprecated.

## Program Settings

This screen allows the CAT 3000v3 software to be customised to suit the individual user. The various setup items are described below. The dialog is opened using the Program Settings button on the Configuration ribbon. The settings are divided functionally into four tabbed pages.

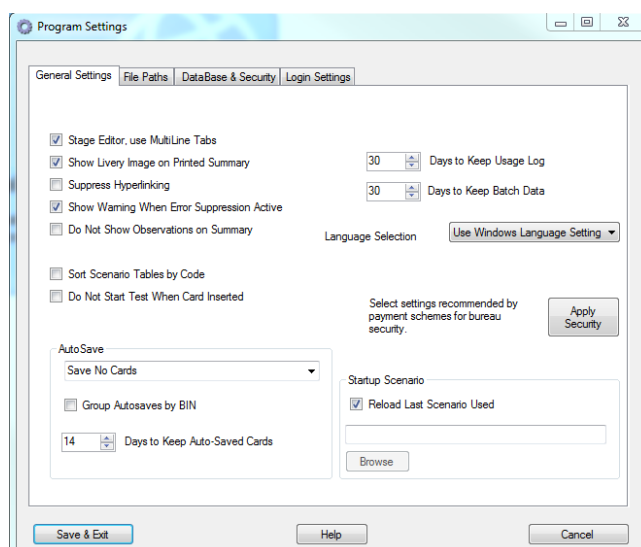
### General Settings Tab

#### Stage Editor, Use Multiline Tabs

The scenario stage editor displays its settable options in a series of tabbed pages, when there are too many of these to fit across the display area they will normally scroll horizontally. If this check box is checked then the tabs will be arranged in multiple rows so they are all in view all the time.

#### Show Livery Image on Printed Summary

When the Pass/Fail summary is printed and the test scenario includes a livery image, then that image can optionally be printed on the hard copy. However, due to printer characteristics and other presentation concerns this may not always be desirable, so this check box allows the livery print to be enabled or disabled as required.



#### Suppress Hyperlinking

The hyperlinks which enable single click navigation between related points on the various results displays were introduced primarily to enable users unfamiliar with the card and transaction data to quickly locate areas of concern. However, some experienced users have found that at times the links could be a nuisance, particularly when trying to copy and paste extracts from the report or the engineer's log. Checking this box will disable all hyperlinks within the CAT 3000v3 results displays.

#### Show Warning When Error Suppression Active

Checking this box causes a warning to appear at the top of the Results Summary Screen after a test has been completed.

#### Do Not Show Observations on Summary

Checking this box causes any observations or suppressed errors that would normally be displayed on the summary screen to be hidden when the test has passed. They will still be shown in the report and the details tree. If the test fails the observations and suppressed errors will be shown as well as the errors on the summary.

#### Auto Save

This list gives three options for the automatic saving of card data, either save no cards at all, save every card tested, or save only those cards that failed their test. The cards will be saved under their account number, or whatever card identity is used in its place for non-payment card applications. They will all be saved in the card group "AutoSave". For an explanation of saved card groups see the Saved Card Database topic.

**NB.** It is recommended that the automatic card deletion option be enabled with auto save, to prevent the saved card database from becoming too large.

#### **Group Autosaves by BIN**

This checkbox is only relevant if automatic card data saving is enabled. If this option is enabled then the group used to save the auto saved data will be named "AutoSavennnnnn", where the "nnnnnn" will be the first six characters of the card's identifier as supplied by the test script, in the case of EMV cards this represents the card's BIN (or a hash of it if masking is being used). If a group does not already exist for the card being saved then it will be created automatically.

#### **Days to Keep Auto-Saved cards**

Cards in the saved card database will be automatically deleted after the defined number of days. If the value is set to zero then no cards will be automatically deleted. It is recommended to use this feature if auto-saving is enabled, to keep the card database to a manageable size.

#### **Days to Keep Usage Log**

The usage log files are automatically deleted after the defined number of days.

#### **Days to Keep Batch Data**

Batches will be automatically deleted after the defined number of days. If the value is set to zero then no batches will be automatically deleted. The timing is taken from when the batch was created, regardless of when it was last used. When a batch is deleted then all the saved card data associated with it is also deleted.

#### **Startup Scenario.**

This section defines the test scenario that is loaded automatically when the software starts. If the "Reload Last Scenario Used" check box is checked the CAT3000v3 will remember the last scenario loaded each time it is shut down and will reload that scenario automatically next time it starts up. If the box is unchecked then desired start-up scenario can be specified using the adjacent text box and/or browse button. The browse button will open the scenario management dialog.

#### **Language Selection.**

The CAT 3000v3 GUI supports alternative languages, normally these are set up automatically according to the International settings in Windows, however, it is possible to manually select any of the available languages if that is the user's preference.

#### **Show Warning When Error Suppression Active**

Checking this box causes a warning to appear at the top of the Results Summary Screen after a test has been completed if the scenario includes suppressed errors.

#### **Apply Security.**

The payment schemes increasingly mandate minimum security settings covering data storage, password regimes, etc. for use in situations where live cards are being tested. CPT 3000v3 supports all the requirements but they may be relaxed by users for whom high security is not an issue. Clicking this button will automatically set up the security settings to the minimum payment scheme requirements.

#### **Sort Scenario tables by Code.**

There are a number of selections in the scenario editor where a long list of options can be chosen, for instance country and currency codes. Normally these are arranged in alphabetical order of the name, checking this box re-orders them into numerical order of the code.

**Do Not Start Test When Card Inserted**

Normally the CAT 3000v3 will automatically begin a test whenever a card is inserted into the active card reader. However, sometimes it is convenient to delay the start of the test, so when this box is checked the CAT will wait for the "Start" button to be clicked before the test begins. The Start button will appear at the top right of the main screen adjacent to the card reader icon.

## File Paths Tab

The screenshot shows the 'Program Settings' dialog box with the 'File Paths' tab selected. The dialog has four tabs: 'General Settings', 'File Paths', 'DataBase & Security', and 'Login Settings'. The 'File Paths' tab contains three main sections: 1. 'Name of the folder into which imported scenarios are placed.' with a text box containing 'Imported Scenarios'. 2. 'Define Configuration Files' with a dropdown menu, an 'Apply' button, and a 'Browse' button. 3. 'Define Folder Paths' with a dropdown menu, an 'Apply' button, and a 'Browse' button. At the bottom of the dialog are three buttons: 'Save & Exit', 'Help', and 'Cancel'.

By default, all the configuration files and folders reside in the local base folder of your CAT installation. However, these paths can be modified to point to any file/folder in local or remote machine. Configuration files that can be edited are:

- User Data file: users.xml
- RSA Public key file: pubkeys.xml
- Scenario shortcut buttons definition file: shortcuts.xml

Folder paths that can be edited are:

- Scenario base
- Card Data storage
- Reference specification folder
- Livery images folder
- Shortcut button images folder
- Automatic daily report path

To edit any of the above path, please select the file/folder path using the drop down menu. Then browse for the required file/folder and click "Apply".

### **Scenario Base Directory**

This is the folder where the test scenarios are stored. By default this will be a local folder in the CPT folder system. However, in some situations, e.g. where a number of CPTs are in use on a single site and using a common set of scenarios, it may be convenient to store the scenarios somewhere else.

The scenario base directory can be anywhere that the PC's filing system can see, either on the same PC as the CAT software or at some remote location on a network.

It is permissible for a number of CAT/CPTs to share a scenario storage area.

### **Scenario Shortcut Buttons Definition File**

By default the layout of the scenario shortcut buttons and their containing tabs is held in the local file "shortcuts.xml", however, in situations where a number of CAT/CPTs are installed on a network it may be desirable to centralise the control of these buttons. In this case a new file path may be set up here.

### **Card Storage Directory**

The same comments above also apply to saved card storage, which can be local or remote as convenient. The word "Local" will appear by default to indicate the local "SavedCards" folder is in use.

Although it is possible for a number of CATs to share a saved cards folder the system was not designed to be used in this way and there is no protection against conflicts when two systems try to save data at the same time. But see Database Type, below.

### **User Data File and RSA Public Key Files**

Similarly, these two files may be local or remote and shared by a number of CATs across a network. These items are used to indicate the locations of the files to be used, which may be local or remote. Please note that whereas in the case of scenario and card storage a folder is defined, in the case of the user list and public key collection a file is specified.

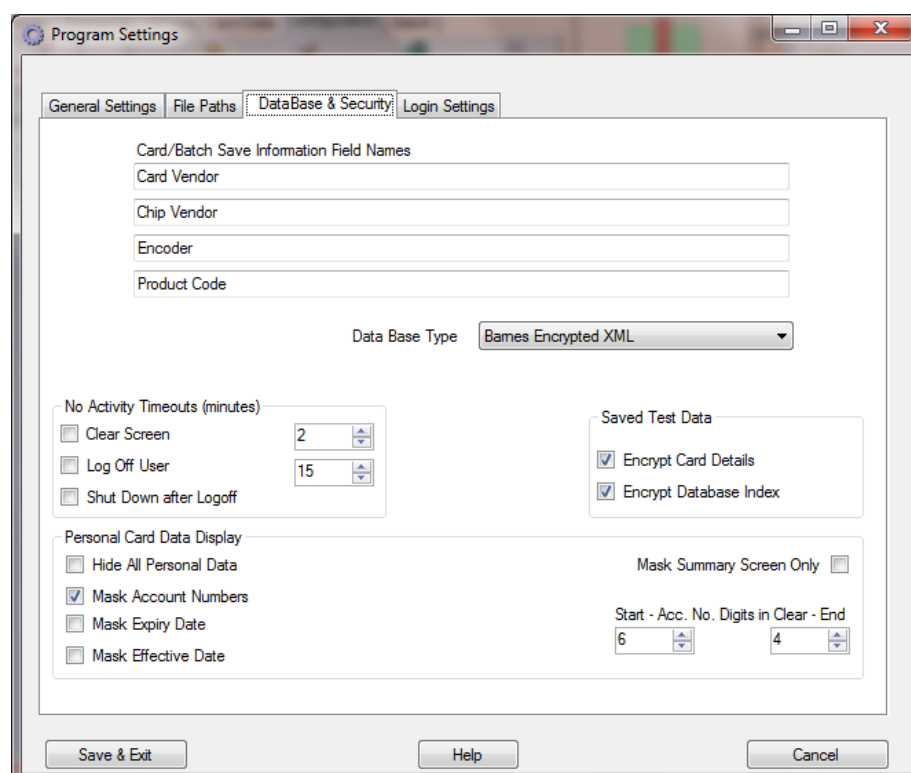
### **Specification Directory**

The directory in which the pdf copies of the card specifications are held can be defined here. By default a local folder named "specs" is set up, but where a number of units are networked it may be more convenient for them to share a common folder.

### **Destination for Automatic Daily Report Save.**

The Daily Report, which can be generated and exported manually at any time, can also be automatically saved each day. Entering a folder path in this field will cause the reports to be saved in that folder. Each time the system detects that the date has changed it will output a report covering the previous working day's activities. Leave the field blank to disable this feature.

## DataBase & Security Tab



This tab contains settings concerned with the saved card database and displayed data security.

### Card/Batch Save Information Field names

When a card is saved in the database there are four free-format information fields available to the user. These fields may be used for selection and sorting when viewing and/or recalling saved data. The use of these fields is likely to vary from user to user, so the names of the fields can be set up here. Note, changing the names of the fields has absolutely no effect on the saved data, only on the visible title on the save and recall dialogs. The first three are also used to identify the three free format fields associated with each batch.

### Database Type

The CAT's standard stored card database is held in a number of encrypted XML files in the folder defined above. There is an independent file for each card test stored, and an index file which stores the card identities, group and date information, etc. This arrangement has been found to be suitable for the vast majority of users. However, in situations where a very large number of cards are stored there may be performance issues, so the facility has been provided to substitute any ODBC connected database engine for the indexing XML file.

In order to make use of this facility an XML file must be present which defines the ODBC connection string and a series of SQL commands which the CPT will use to manipulate the external database. This file is named "DBaseInfo.xml" and must reside in the saved card folder indicated above. The SQL statements in the file contain placeholder strings where the CAT software will substitute data used at run time. An example file is provided, please see Annex 1 for more detail.

**NB. Setting up database connections is a specialist task, please do not attempt it unless you feel it is necessary and you are sure you have the necessary skills.**

### **No Activity Timeouts**

For security reasons it may be undesirable to leave the CAT in a functional state, or with card details on the display, when unattended. The software can therefore be configured to clear the screen, log off the current user, and/or shut itself down, after a predetermined period of inactivity.

"Inactivity" is defined as a period of time during which no mouse movement or keyboard action occurs, and is defined in units of minutes. The first time-out clears all card data from the screen, the second logs off the current user, each of these is independently enabled using the check box adjacent to the time setting. The third check box, when checked, shuts the CAT software down after the log off timeout.

A warning message will appear on the screen twenty seconds before the timeout action occurs so that it can be aborted if the user is still present and wishes to keep the information visible. When logging off, if the user has walked away and left a login card in the machine there is an option available to disable that card, see below.

### **Mask Account Numbers in Reports**

When this box is checked, provided the test script in use supports the feature, the account number of any card tested will be displayed with some of its digits masked. Usually the first six and last four digits will be shown, the others being replaced by 'x' characters. This will apply to all screens and printouts, including stored results.

### **Hide Personal Data in Reports**

This check box takes the above masking a stage further and masks all personal data, i.e. the entire account number, the cardholder name and the expiry date.

### **Mask Summary Screen Only**

When either of the above masking options is active, checking this box restricts the masking to the summary screen only, the tree and the engineering log display all data. This function is intended for use in conjunction with a user permissions arrangement that only allows selected user grades to see the detailed card information.

### **Mask Expiry Date**

When this box is checked, and "Mask Account Numbers in Reports" is also checked, the expiry date is masked also. If "Mask Account Numbers in Reports" is not checked then this box is ignored.

### **Mask Effective Date**

When this box is checked, and "Mask Account Numbers in Reports" is also checked, the effective date is masked also. If "Mask Account Numbers in Reports" is not checked then this box is ignored.

### **Acc. No. Digits in Clear**

If the default account number masking of the first six and last four characters in clear is not acceptable, then any other combination may be entered here. The left box defines the number of clear characters at the start of the account number, and the right box the number of clear characters at the end.

**NB.** There is also a user permissions setting that overrides masking, so it is possible to designate a user grade for whom masking is never in force. This feature should be used with care.

## Log In Settings

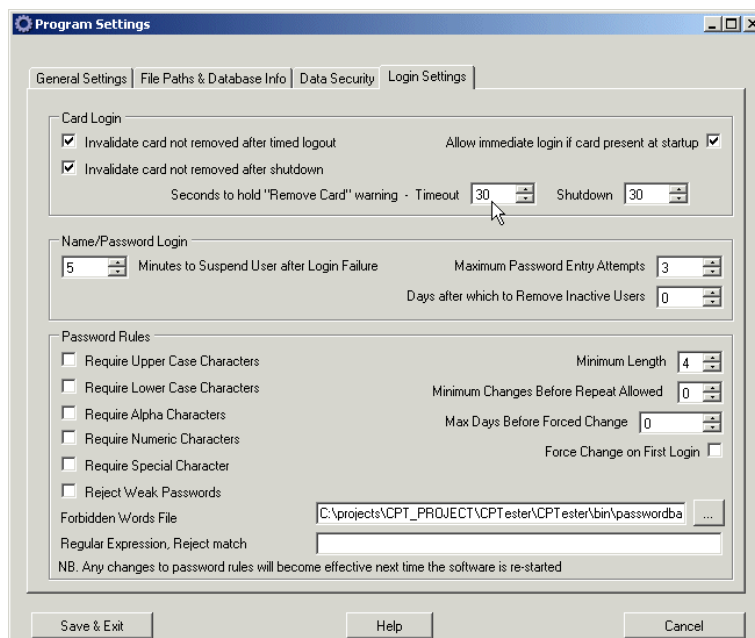
### Card Login

#### Invalidate card not removed after timed logout

If this box is checked then any login card left in the reader when a timed inactivity logout occurs will be invalidated. The card is not destroyed, but will have to be re-assigned to its user before it can be used again.

#### Invalidate card not removed after shutdown

If this box is checked then any login card left in the reader when the software has been shut down will be invalidated. The card is not destroyed, but will have to be re-assigned to its user before it can be used again



#### Allow immediate login if card present at startup

If the software finds a valid login card already present when it is started up it will normally wait for that card to be removed before allowing any user to log in. If this box is checked then the card will be used to log in normally.

#### Seconds to hold "Remove Card" warning.

Following a software shutdown, or a timed logout, if the login card is not removed a warning will be shown for the prescribed time, prompting the user to remove the card. Only after this time has elapsed will the card be invalidated if either of the "invalidate" check boxes are checked. Two times may be set, to cover the case of a timed logout and a software shutdown.

### Name/Password Login

#### Maximum Password Entry Attempts

The number here sets the maximum number of times a user may attempt password entry before the system shuts down.

#### Minutes to Suspend User after Login Failure.

Following the maximum number of password entry attempts without the correct password being seen, the user in question may be prevented from attempting another login for the number of minutes specified here. In the case of a genuinely forgotten password the system manager may delete and re-enrol the user to set a new password.

#### Days after which to Remove Inactive Users

If a user does not log in at all for this number of days then he or she will be automatically deleted. If the value is set to zero then automatic deletion will be disabled.

**Login using Windows User Name**

When this box is checked an extra button will appear on the login dialog. When this button is clicked the name of the current Windows user will be used to log in to the CAT 3000v3, no password will be required. For this process to work the name of the current Windows user must exist as a CAT 3000v3 user, if not then login will fail. Normal login using a name and password continues to operate as usual.

**NB.** This option by-passes all the normal login security arrangements, delegating them to the Windows login system. The no-activity timeouts for the CAT 3000v3 will need to be set up to ensure that the user is logged off at the same time that Windows times out.

**Password Rules**

System security may be compromised by the use of easily guessed or generally known passwords, this section enables a variety of checks to be put in place. These settings allow compliance with the latest payment scheme requirements for card personalisation bureaux.

**Minimum Length**

This allows a minimum password length to be set up. It is not possible to set less than four in this field.

**Minimum Changes Before Repeat Allowed.**

When setting a new password, the CPT can keep a history of that user's previous passwords, to ensure that they are not re-used, the number here determines the length of that history.

**Max Days Before Forced Change**

This entry allows a maximum password life to be enforced, so that a user will be forced to change their password after the defined period. When this is set up any user logging in after the set time period from their last password change will be presented with the change password dialog which must be completed before login can proceed.

**Force Change on First Login.**

When this check box is checked, new users will be forced to change their password the first time they login, this prevents the use of a password that may be known to the system manager or supervisor who enrolled the user.

**Require...**

Five check boxes labelled "Require something" will cause a new password to be rejected if at least one of the indicated type of character is not present. The box labelled "Require at least three of above" indicates that the password must contain at least one character from three of the four categories listed above it, i.e. upper case, lower case, numeric and special (punctuation).

**Reject Weak Passwords.**

This check box enables a number of additional rules to be enforced on new passwords. The test will reject any password consisting of a single upper case character followed by a series of lower case, and will reject any sequence of three or more characters either the same or consecutive values.

**Forbidden Words File**

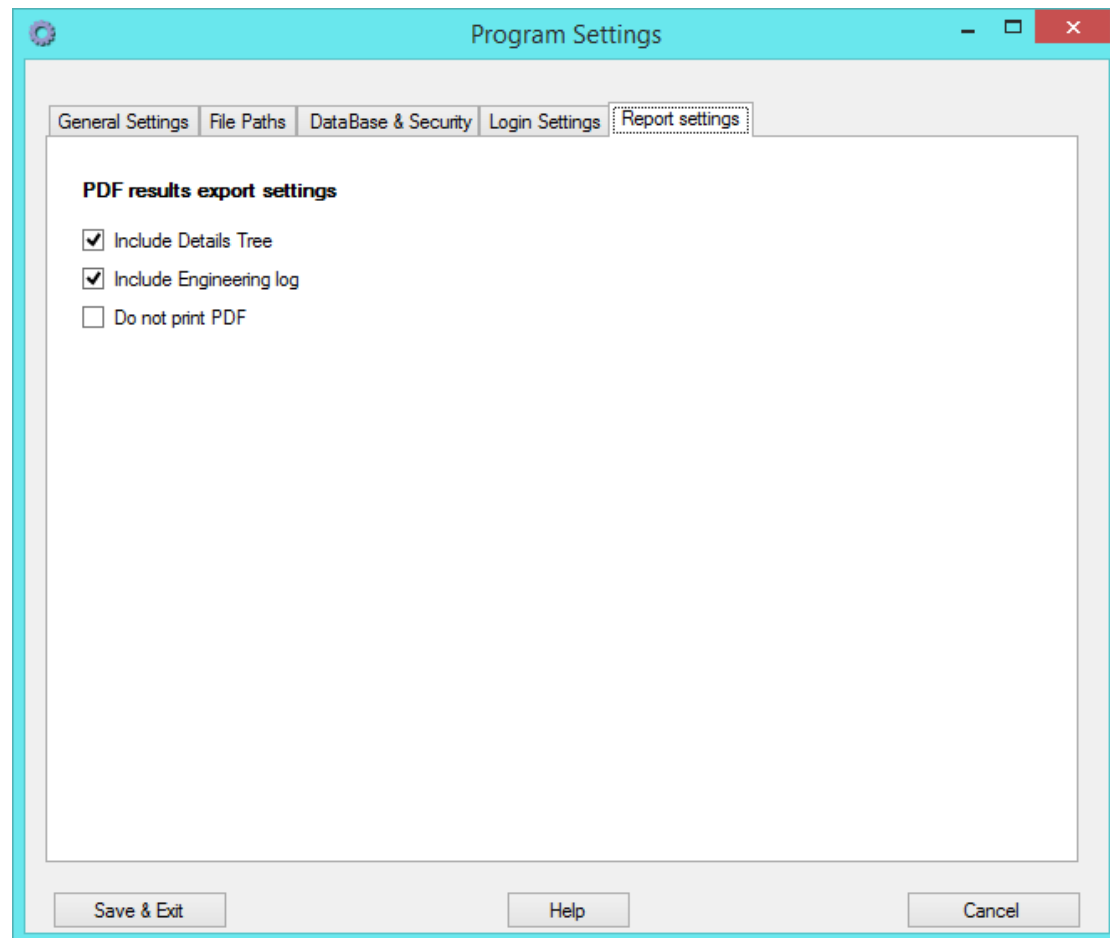
A text file may be defined containing a list of words which may not be used as passwords, this could be a dictionary, or a list of common names, or a combination of both. A sample list of English words and names is provided which may be used, edited or replaced to suit local conditions.

**Regular Expression, Reject match.**

Regular expressions are a standard method of defined text matching criteria. This entry allows additional password rejection criteria to be added. Before using this field the user is advised to learn about Regular Expression syntax, there is a wealth of material available in print and on the internet.

As an example, the expression "[A-Za-z]{2}[05][1-9][A-Za-z]{3}" will reject UK car numbers.

## Report Settings



Controls the data that will be exported in the PDF Report or whether or not the PDF report will be exported.

## User Control

All users of CAT 3000v3 must log on to the system before any functions will operate. When the system is shipped a single user is enrolled. The user name and password for this user are both "SYSTEM MANAGER". This standard user has full system manager permissions and should be used to enrol the necessary users for the system. For security reasons it is strongly recommended that this standard user be deleted as soon as the operational system manager grade user(s) have been enrolled.

There are eight available grades of user, as the system is shipped they are named System Manager, Manager, Engineer, Supervisor, Operator 1, Operator 2, Operator 3, and Operator 4. Apart from System Manager, which is fixed, these names may be changed to suit the individual operation of the end user.

NB. "System Manager" is the name of a user grade, "SYSTEM MANAGER" is the name of the default user shipped with new systems (who happens to hold the grade "System Manager"), please do not confuse the two.

A System Manager has full permission to do everything on the system and cannot be changed, the operational permission settings of all the other grades may be edited to suit the local situation using the permissions option on the user menu

To enrol a new user click the "Add New User" button, enter the user's name in the top box and select a user grade from the "User Level" drop down list. The password is then entered in the two boxes below the user level selection. The password is entered twice to confirm that no typing errors have occurred. When the data has been entered satisfactorily click the "Apply" button and the new user will be added to the list.

Once a user has been enrolled, if the login card option is enabled, a login card may be assigned to the user. To assign a login card simply select the user in the "users" list and click "Assign Card", then insert the card into the login reader and that card will be assigned to that user. NB. Because the login reader needs to be free to accept the new card, the manager or supervisor assigning the card must have logged on using the name and password method. . If it is desired that certain grades of operator must always use their card to log in, then the manager or supervisor can enter a password and simply not pass it on to the operator.

To unassign a login card simply select the user and click "Unassign Card", the login card does not need to be present for this operation.

To remove a user. The user must first be selected from the list of current users. Clicking on 'Delete User' will bring up a confirmation dialog which, on selecting OK, will permanently remove that user from the system.

If a user forgets their password then the only solution is to remove and re-enroll them, when a new password may be entered. Facilities available to each user grade are configured using the permissions dialog accessed from the user control menu.

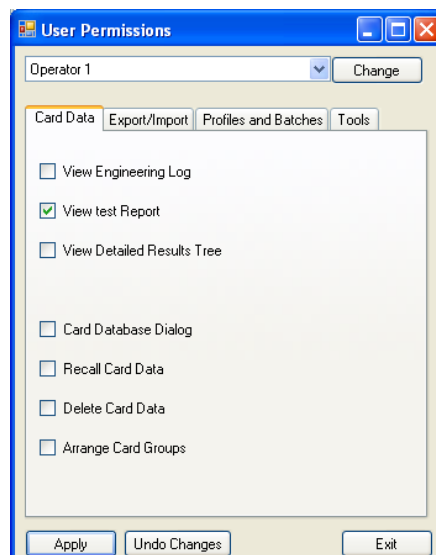
## User Permissions

The user permissions dialog consists of a drop down list with all the user grades selectable (except for System Manager, which cannot be edited) and a set of tabbed pages containing the settings options, most of these are check boxes, when the box is checked users of the selected grade have permission to perform the associated task, and vice versa.

NB. A change to a permission setting on this dialog affects all users of the selected grade immediately.

The "Change" button at the top of the dialog allows the visible name of the selected user grade to be changed. This change will not affect any of the permission settings or any of the enrolled users in that grade, only the name of the grade as displayed on the screen and in the usage log.

On the "Scenarios and Batches" tab there is a drop down list that allows a scenario access code to be associated with the selected user grade.



### Scenario Access Codes

The scenario access code for the user grade is set up on the Scenarios tab of the permissions dialog. Scenario Access Codes are described in the scenario Management section.

## Usage Log

All significant events in the operation of the CAT3000v3 are recorded in the usage log. This log is created automatically and can be inspected by a user with the necessary permissions.

Events logged are user login and logout, scenario recalls, cards tested, batches opened and closed, etc. A new log file is created for each day during which the system is operated, and all the events for that day are written to it. If the system is left on over midnight then a new file will be created for the first event of the new day. All times are recorded using local time from the PC's clock.

When the Usage Log option is chosen from the Management menu a list of available files is shown, identified by the date to which they refer. When one of these is chosen the information for that day is displayed. The data may be printed from this dialog or exported as a text file using the File/Export menu.

## The Daily Report

An extension of the usage log is the Daily Report. The Daily Report lists all the cards tested during the day it covers with their test result, time of test and the logged in operator who performed the test. Where cards were automatically saved the display includes a hyperlink to recover the test results for that card from the saved card database.

A Daily Report may be manually generated for any day for which there is a Usage Log available. Optionally the system can be configured to automatically save a Daily Report each day, see Program Settings.

## Backup and Restore

The file menu has two items, backup and restore, used for protecting the CAT's stored data. Each item has two sub menus, scenarios, and cards and batches.

These backup facilities are not intended to replace any existing company backup regime, any system administered by an IT professional will normally have procedures in place to back up the entire PC, in these cases the CAT software's local backup and restore functions will not be needed.

In networked systems, however, there is another possible use. If the data (i.e. scenarios, stored cards and batch data) is being held on a server it may be useful to keep a local copy to keep the system running in the case of a network failure. The backup is an exact copy of the in use file and directory structure, and can be used instead of the normal files simply by changing the path to the top level folder in Program Settings.

### Backup

After choosing the specific data type, scenarios or cards and batches, you will be presented with a folder browser dialog with which to choose the destination for the backed up data. The dialog allows a new folder to be created, but this is not essential, the backup process will create a new folder within the folder you choose so there is no danger of overwriting previously backed up data.

The automatically created folder will be named either "Scenarios" or "Cards and Batches" as appropriate with the current date appended, into this folder will be copied all the files and sub-folders appropriate to the data type being backed up.

### Restore

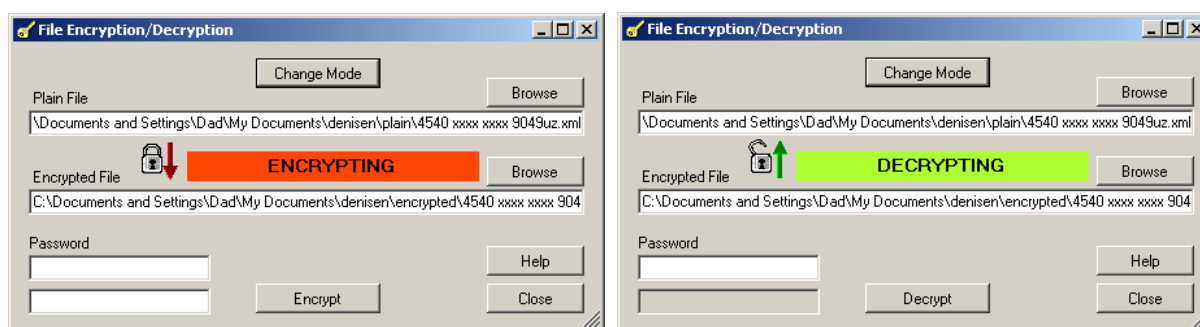
This is the reverse of the above. The folder browser allows you to identify the backed up data to be recovered, then that data will be copied to the standard scenario or card storage folders.

## File Encryption

It is in the nature of the CAT 3000v3 that much of the data handled by the system is confidential, and when transmitting this data from one location to another by electronic means it will be desirable, if not essential, to encrypt that data.

This feature, accessed from the "Utilities" ribbon, provides a convenient method of encrypting and decrypting files.

The dialog contains two file path entry boxes, one for the plain, or non-encrypted, file, the other for the encrypted file. The files may be anywhere in the PC's filing system, or any accessible location on the network. This facility can be used for any file; it is not restricted to CPT related files.



The browse button associated with each file path entry box allows the file name to be defined using a file open or save dialog as appropriate to the operating mode.

The operating mode is indicated by the panel in the centre of the dialog and is changed using the "Change Mode" button.

There are two password entry boxes, when encrypting both must be filled in with the same password to eliminate typing errors. Passwords must be at least four characters long, but longer passwords, up to a maximum of sixteen characters, will be more secure. In decryption mode only one password entry box is enabled.

The encrypted file includes a checksum which is verified on decryption, this allows the system to detect errors in the password entry or invalid files (i.e. files which were not encrypted by a CPT/CAT 3000v3 or which have been corrupted in transit).

NB. Only files which have been encrypted by a CPT/CAT 3000v3 can be decrypted by this facility, and files encrypted here can only be decrypted by a CPT/CAT 3000v3.

Some types of file may be encrypted and/or decrypted in the import/export functions available on the file menu, these facilities provide a shortcut the encryption engine used for this dialog. Encryption uses Triple DES in CBC mode, the key being derived from the password by a hashing algorithm.

## New Features and Enhancements

### Authorisation Codes

When the CAT 3000v3 is first installed it must receive an authorisation code from Barnes International. This code enables the software and sets the license period, but it also enables various optional features which may have been bought with the basic system.

If it is desired, at some later date, to enable one of these features that was not part of the original purchase then a new authorisation code will be issued by Barnes International. The new code is entered using the authorisation code entry dialog which is accessed from the "Administration" menu. This is the same dialog that was presented automatically when the system was first installed, and again when the license is about to expire.

When requesting a new code from Barnes it is important to quote the installation code presented on this dialog.

### Script Add-On and Update Packs

Some optional extras only consist of script files and scenario definitions, which need to be copied into the appropriate folders. Sometimes a feature will require a new authorisation code as well as extra files. These file add-on packs will be supplied in a format unique to Barnes International, compressed and encrypted, using the file extension ".bip". The file may be supplied in a variety of ways, depending on how it was purchased, e.g. it may be on the CD with the basic software installer, or it may be supplied later by e-mail or web download.

As well as new features these "bip" files will be used from time to time to supply updates to the existing software and script files.

To install one of these packs, select the package installer from the Administration menu and use the file open dialog to select the "bip" file to install. The process is then fully automatic; the new files will be extracted from the "bip" and copied to the appropriate folder(s). When updating the main software the CAT 3000v3 will be shut down so that the installer can be run, once the install process is complete the CAT 3000v3 may be started again in the normal way.

NB. Sometimes Windows™ security settings may cause some manual action to be required after the ".bip" file has been processed, when this occurs a message will appear in a dialog box or on the card image of the summary screen.

## Remote System Management

**NB. This Feature is an optional extra which will not be available on all systems, and even when installed, is subject to user permissions control.**

The Remote System Management option is intended for use in situations where a number of CAT3000v3 systems are installed in a networked system. In such an installation it is often useful to be able to manage the centralised resources from an office environment away from the operational testers.

scenarios, users, and public keys can all be maintained centrally from any system, by a user with the appropriate permissions, with or without the Remote System Management option.

Remote System Management bestows the following additional features on the machine where it is enabled.

- 1) Examination of the batch results on any of the other machines. \*\*
- 2) Examination of the saved cards on any of the other machines. \*\*
- 3) Examination of the usage log on any of the other machines.
- 4) Viewing the results from the most recent card tested on any of the other machines (regardless of whether that card was saved or not). \*\*
- 5) Re-processing the data from the most recent card tested on any of the other machines.

\*\* Please note that sensitive data masking will be according to the settings on the remote machine, not the local machine.

In order to do this the management machine must have read access to the folders where the remote machines are installed. It may be necessary to involve your network administrator to ensure this is so.

### Accessing a Remote System.

When the dialog opens a list of available remote systems is displayed. Select the desired system from the list and click the "Select Remote Unit" button. The dialog will close and the icon at the top right of the main screen will change to indicate that remote mode is selected. While this icon is shown, accessing the batch, saved card or usage log in the normal way will fetch the data from the selected remote system instead of from the local storage.

To select a different remote unit, open the dialog and select another one in the same way.

To revert to local operation click the "Local Operation" button on the dialog.

Local operation is also invoked automatically if a card is inserted into the local reader.

### Setting Up Remote Systems

Clicking the "Add New" button will open a Windows folder finder dialog. Use this to locate the network folder in which the desired remote CPT is installed, then click OK. A second folder dialog will then enable the definition of the folder where the remote system's saved cards are stored. By default this will be a folder named "SavedCards" under the main application folder, however, this might be different on some systems. When both folders have been defined the new system will be added to the list and can be accessed as described above.

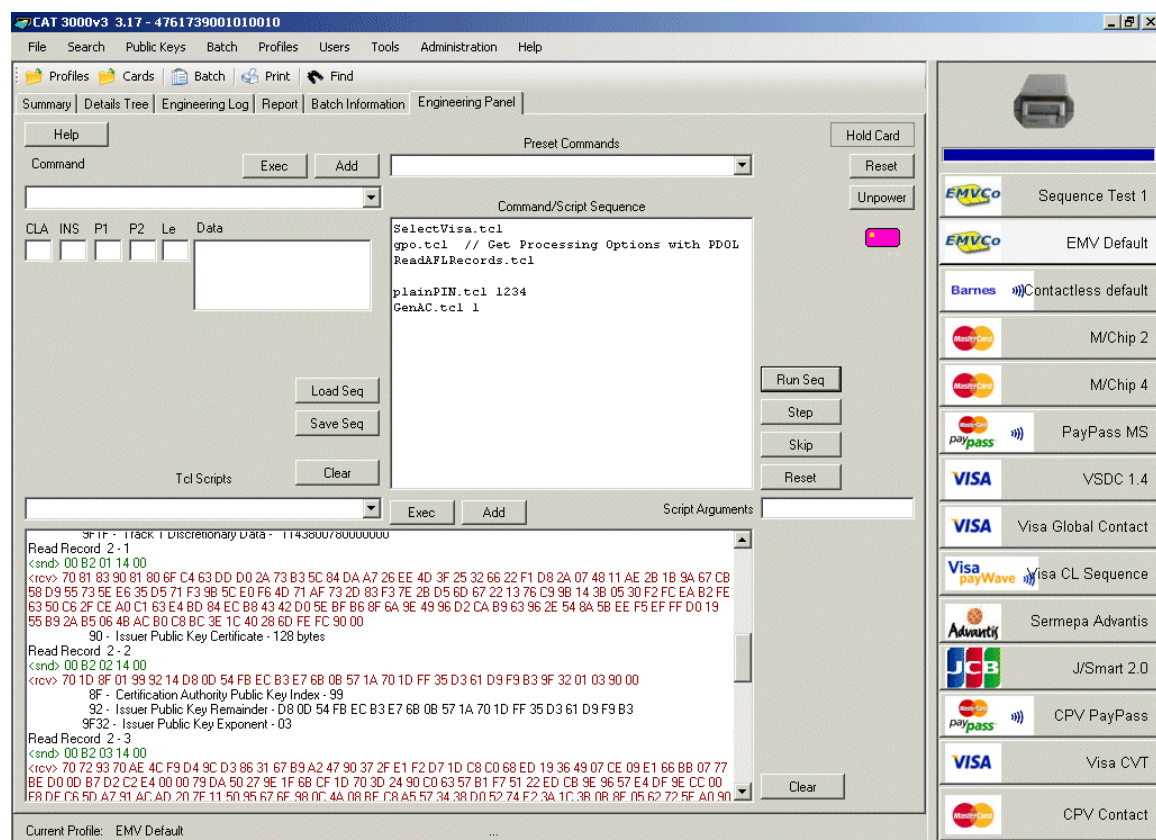
To Remove a system from the list, select it and click "Remove".

## Card Data Re-Processing

When a remote system is active for viewing the card save database dialog will have an extra button labeled "Load Last Log". When this button is clicked the data from the last card tested on the remote system will be imported into the local system and processed through the data first analyser of the currently selected scenario. In this instance the sensitive data will be masked according to the settings on the local machine.

## Engineering Panel

The Engineering Panel is designed for use by card engineers to carry out detailed diagnostics and evaluation of card performance. It is only to users with Tcl script editing authorisation.



## Hold Card

In the top right corner of the screen is the "Hold Card" button, this activates or deactivates the "Hold Card" mode. When the CAT is in "Hold Card mode" putting a card into the reader will not run the selected profile, all card interaction is then controlled from the Engineering Panel.

Hold Card mode remains in force until explicitly deactivated, even if the screen is changed. This makes it possible to refer to other results screens (e.g. the Engineer's Log) without losing the sequence of events from the Engineering Panel.

### Commands, Scripts and Sequences

These are three methods of interacting with the card.

- A **command** is an individual APDU with any necessary data.
- A **script** is a Tcl script located in the "EngPanel" folder under the main scripts folder.
- A **sequence** is any combination of commands and/or scripts strung together to be run either in a single hit or one at a time.

**Commands** are entered in hexadecimal using either the edit box (top left) or the individual byte windows (labelled CLA INS etc) just beneath it. These two entry areas track each other, so that any change made in one will automatically appear in the other. The hexadecimal entry box also features a drop down list that saves the last twenty commands sent to the card or added to a sequence.

Commands can also be chosen from the drop down list of "Preset Commands". The commands in this list can be complete commands ready to send to the card, or partial commands which require manual completion. The list can be customised by the user, using the file "engcmds.txt", which is also in the "EngPanel" folder under the main scripts folder. Each line of the file represents one item in the list. There are two fields, the first is the label that appears in the list and the second is the hexadecimal to be loaded into the command entry window. The two fields are separated by the "pipe" character "|".

**Scripts** are individual, usually quite short, Tcl scripts resident in the "EngPanel" folder under the main scripts folder. These scripts are drawn from the standard EMV test scripts, but are much simplified and are separated into individual functions, mostly they send a single APDU to the card and analyse the response. These are intended to be used in much the same way as commands but allow the generation of APDU/data streams that require the use of data from previous operations on the card and/or complex calculations such as MAC generation etc. Scripts can also place comments in the results window, in much the same way as the standard test scripts place comments in the Engineer's Log.

Commands and scripts may be invoked individually using the "Exec" button adjacent to their respective entry windows, or may be added to the sequence using their respective "Add" buttons.

A **Sequence** is a number of commands and/or scripts strung together. The individual items may be invoked as a continuous stream using the "Run" button, or individually using the "Step" button. The "Reset" button sets the sequence counter back to zero and highlights the first line of the sequence, as each step is executed the next line will be highlighted. The highlighted line is the next item to be implemented. The "Skip" button advances to the next line in the sequence without executing the currently highlighted line.

Sequences can be saved and reloaded using the "Save Seq" and "Load Seq" buttons adjacent to the sequence window.

In addition to using the "Add" buttons for scripts and commands, the sequence window can be edited directly. When doing this it is important to ensure that only one command or script is placed on each line. Comments and blank lines may be used to improve the readability of a sequence, these will be ignored by the system. Comments must always begin with the double forward slash sequence, "//", as used in C++, C# etc. The comment delimiter, "//", must be placed either as the first character on a line or following a command or a script name, the comment then occupies the rest of the line.

## Card Operations

When a card is placed in the reader an icon will appear indicating that it is present, the icon is coloured blue to indicate the card is not yet powered. At any time that the card is unpowered the "Eject" button may be used to remove it. Clicking the "Start" Button powers up the card, the icon turns magenta and the card's ATR will appear in the results window.

The "Start" button is now a "Reset" button, which may be used to give the card a warm reset, and the "Eject" button becomes the "Stop" button, which de-powers the card.

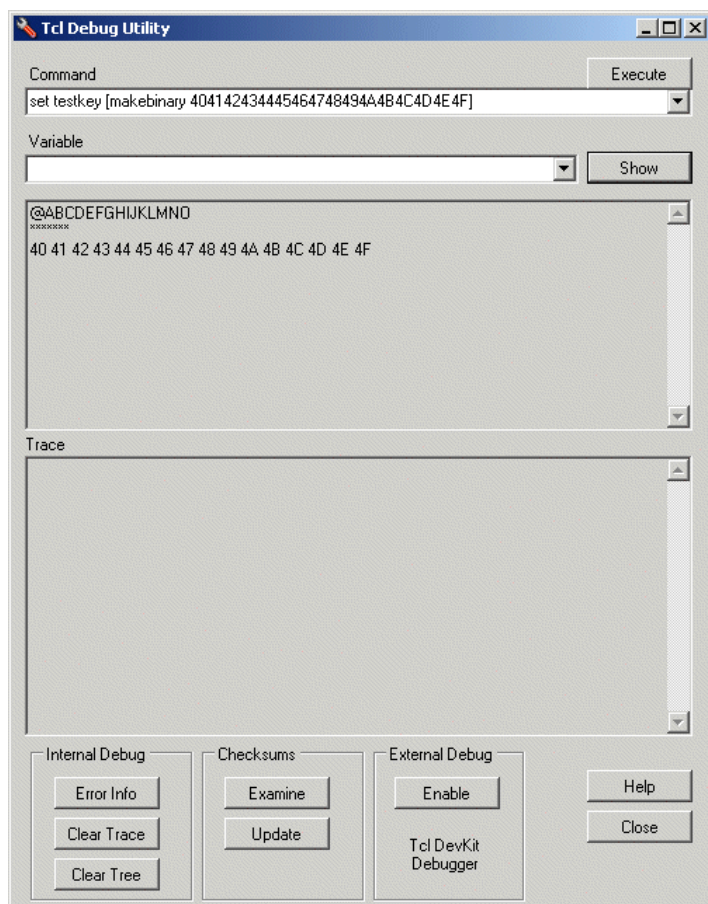
While the card is powered commands, scripts and sequences may be used to interact with it.

## Profiles

While the CAT is in "Hold Card" mode, if any profile is selected, either using the shortcut buttons or the profile management menu, the Tcl script from the first stage of the profile will be executed immediately (Normally these scripts are not executed until a card test is performed). This means that the Tcl variables defining that terminal simulation are set up and may be used by Engineering Panel scripts to construct commands requiring data defined by the PDOL, CDOL's etc.

This profile selection can also be used to change the reader which is in use.

## Tcl Debug Utility



The Tcl Debug utility provides the script programmer with a window into the Tcl interpreter. It is intended for use in debugging Tcl scripts, but for the initiated, can also be used to examine card data.

It is not a full development environment, and does not include a source level debugger, for those facilities Barnes recommends the Tcl DevKit Debugger from ActiveState.

The debug utility allows individual Tcl commands to be executed, variables to be inspected, and debug trace comments from a script to be displayed. It also allows the script checksums to be updated following a change.

For Tcl language reference please consult the ActiveState Tcl reference help file installed with the CAT 3000v3, the book

shipped with the CAT 3000v3, or one of the many excellent publications and tutorials available online and in computer bookshops.

For Tcl language extensions used in the CAT 3000v3, see the Tcl extensions manual, this is also reproduced as a help file accessible from the help menu.

### **Command Window**

Any valid Tcl command may be executed by entering it into this window and clicking the "Execute" button. The return value from the command will be displayed in the response window below the variable window. Scripts may be executed directly from here using the "source" Tcl command.

The window includes a drop down list of the last twenty commands executed, these can be recalled to either be repeated or edited.

### **Variable Window**

This allows any global variable to be inspected. Enter the variable name and click the "Show" button, the variable's current value will be displayed in the window below in both direct and hexadecimal dump formats. If the variable is an array and no index is given then the indices for that array will be listed.

The window includes a drop down list of the last twenty variable names inspected, these can be recalled to either be repeated or edited.

### **Trace Window**

One of the extension commands provided by CAT 3000v3 is "CPTDebug". Information passed to this command is displayed in the "Trace" window whenever the script is run with the Tcl Debug Utility active. If this dialog is not active then the command is ignored. This window is also used to display interpreter error information (see below)

### **Internal Debug**

The "Error Info" button displays the contents of the interpreter's error info variable in the trace window. This variable is loaded with useful information whenever a Tcl error is thrown, and the data it contains is used to write the error report file in the log folder. Using this button is usually quicker and easier than accessing the error log file.

The "Clear Trace" button clears the trace window, "CPTDebug" messages are always added to the end of the current contents, there is no automatic clearing.

The "Clear Tree" button clears the tree results display, this is useful when debugging tree building scripts.

### **Checksums**

All Tcl scripts have a checksum written into a comment as the last line of the file. In a CPT, or when the logged on user of a CAT does not have developer authorisation, then any script with an invalid checksum will cause an error to be thrown.

Checksums come in two varieties.

Global checksums can only be generated by Barnes International and will work on any CPT or CAT, these are used on the scripts shipped as standard with new systems, or on updates. It is possible to lock global checksums to the system's authorisation code so that scripts shipped as options will not work on systems not licensed for those options, also some options generate scripts on the fly, for these scripts a dynamic variant is used.

CAT generated checksums are locked to the serial number of the CAT on which they are generated and will only work on CATs or CPTs licensed to the same organisation. The serial number of a CAT or CPT is in two parts, the first part identifies the organisation and the second part the individual installation. When one organisation buys a number of systems then they will all have the same first part, and this is the identifier used to generate the checksum.

The two buttons in this section allow the checksums to be examined and updated. The "Examine" button will check all the Tcl files in the scripts folder and report the status ("OK" or "Bad") and if "OK" the type of checksum. The information is written to the trace window.

The "Update" button will write a new "CAT" checksum to any script that has a "Bad" checksum, the scripts which have been updated, and their new checksum values, are reported in the trace window.

**External Debug**

When the "Enable" button is activated, the interpreter will connect to a Tcl DevKit Debugger running in remote debug mode. Scripts invoked by the CAT in normal operation will then be run via the debugger giving full source level debug facilities.

For more information on the Tcl DevKit Debugger please visit [tcl.activestate.com](http://tcl.activestate.com).

## ***Annex A – External Database Connection***

In situations where the CAT's internal card storage facilities are not suitable, a means has been provided to hold the data in an external ODBC connected database instead. Use of this facility requires the provision of a suitable database by the user, and while Barnes' engineers will make every effort to support the user in this task, such databases will inevitably be outside the control of Barnes International Ltd.

NB. The actual storage of the individual card files is not affected by this database change, the database only contains the file name of the encrypted card data store, not the saved data itself.

The CAT will need to be able to access and manipulate the information in the database as if it were in the Barnes encrypted XML files, so an interface must be provided to allow this to happen. This is achieved by defining a number of SQL commands with "placeholder" strings into which the CAT will place information at run time. These SQL strings are defined in an XML file, "DBaseInfo.xml", which must reside in the same folder the CPT's card store.

An example DBaseInfo.xml file is provided for reference purposes, along with an example database in an Access file. In this example each card group is implemented as a table, with an additional table listing the group names. Each entry in a group table represents a saved card file, the fields being the card identity, the four "info" fields, the time stamp and the name of the file containing the test data.

Please note that all information is exchanged over this interface in plain text, any encryption required must be implemented within the database. The actual card data file, however, is always encrypted, this is unaffected by the method used to index and identify it.

The entries in the example XML file are shown below,

### **<DBInfo>**

The ODBC connection string, modify this as required

```
<connection>Driver={Microsoft Access Driver
(*.mdb)};Dbq=C:\Barnes\CPT
3000v3\SavedCards\cptcards.mdb;Uid=Admin;Pwd=;</connection>
```

Each of the following entries may contain one or more individual SQL statements which will be executed in sequence, please note, however, that where data is being retrieved only the information returned by the last statement will be received by the CAT.

```
<!--Get a card file name using the card id, group and date-->
<SQLGetPath>
<command>SELECT File FROM [##GROUP##] WHERE CardId = '##CARDID##' AND
When = '##DATE##'</command>
</SQLGetPath>
```

Placeholder strings are surrounded by "##" and their names should be self-explanatory. In the above the words "File", "CardId" and "When" are the names of the fields in the group table which hold the file name, the card identity and the time stamp respectively.

```
<!--Get a list of groups-->
<SQLGroups>
<command>SELECT Groups FROM GroupList</command>
</SQLGroups>
```

```
<!--Save a card-->
<SQLSave>
<command>INSERT INTO [##GROUP##] (CardId, Info1, Info2, Info3, Info4,
When, File) VALUES ('##CARDID##', '##INFO1##', '##INFO2##',
'##INFO3##', '##INFO4##', '##DATE##', '##FILE##') </command>
</SQLSave>

<!--Amend a card record-->
<SQLAmend>
<command>UPDATE [##GROUP##] SET CardId='##CARDID##',
Info1='##INFO1##', Info2='##INFO2##', Info3='##INFO3##',
Info4='##INFO4##' WHERE CardId = '##ID##' AND When =
'##DATE##' </command>
</SQLAmend>

<!--Get a list of cards from a group, the column order must be
cardid, date, info1 - info4-->
<SQLList>
<command>SELECT CardId, When, Info1, Info2, Info3, Info4 FROM
[##GROUP##] </command>
</SQLList>

<!--Get a list of card file names from a group-->
<!-- Used to define the files to be deleted when a group is deleted-->
>
<SQLFiles>
<command>SELECT File FROM [##GROUP##] </command>
</SQLFiles>

<!--Get the number of cards in a group-->
<SQLCount>
<command>SELECT COUNT * from [##GROUP##] </command>
</SQLCount>

<!--Delete a group, with all its card records-->
<SQLDeleteGroup>
<command>DELETE FROM GroupList WHERE Groups = '##GROUP##' </command>
<command>DROP TABLE [##GROUP##] </command>
</SQLDeleteGroup>

<!--Create a new group-->
<SQLCreateGroup>
<command>INSERT INTO GroupList (Groups) VALUES ('##GROUP##')
</command>
<command>CREATE TABLE [##GROUP##] (CardId char(50), Info1 char(50),
Info2 char(50), Info3 char(50), Info4 char(50), When char(50), File
char(50) ) </command>
</SQLCreateGroup>

<!--Delete a single card record-->
<SQLDeleteCard>
<command>DELETE FROM [##GROUP##] WHERE When = '##DATE##' </command>
</SQLDeleteCard>

<!--Delete all the cards in a group before a given date-->
```

**<SQLPurge>**

```
<command>DELETE FROM [##GROUP##] WHERE When &lt; '##DATE##'
```

```
</command>
```

**</SQLPurge>**

In the above note the use of the “&lt;” syntax to represent the “<” character, this required because “<” is a special character in XML.

```
<!--Get a list of card files saved before a given date from a group-->
```

```
<!--Used immediately before SQLPurge to identify the card files to be deleted-->
```

**<SQLOldFiles>**

```
<command>SELECT file FROM [##GROUP##] WHERE When &lt;
```

```
'##DATE##'</command>
```

**</SQLOldFiles>****</DBInfo>**