MUM

MULTOS Utility Manual

MAO-DOC-TEC-017 v2.10.0

Copyright

Trademarks

Published by

MAOSCO Limited
1st Floor,
GPS House,
215 Great Portland Street,
W1W 5PN,
London,
United Kingdom.

General Enquiries

Email: dev.support@multos.com
Web: http://www.multos.com

Document References

All references to other available documentation is followed by the document acronym in square [ ] brackets. Details of the content of these documents can be found on the MULTOS web site (http://www.multos.com).

Contents

1 Introduction

The MULTOS Utility application provides a single application that handles the different functions needed when working with MULTOS cards and devices. This release includes the following features:

- Loading and deleting of applications for developer cards
- Loading and deleting of applications for live cards
- Creating an MCD ID list for enablement data/MSM Control Data requests
- Enable cards using KMA supplied MSM Control Data
- Exchanging APDUs
- Running of scripts from the command line
- MULTOS 4.4 / 4.5 support
- Optional output of a trace file
- INI file for settings

Release 2.8 of the MULTOS Utility supports both MULTOS and MULTOS step/one cards.

2 Installation

2.1 System Requirements

- Windows PC (XP or later)
- PCSC based card reader
- .NET4 framework

2.2 Installation Process

1. Extract the files from the ZIP file and place in a folder of your choice
2. Modify the ini file as required (it can be used unchanged). It MUST be place in the same location as the executable.
3. If you wish to use the Global KMA WebServices interface for Developer Community Cards, run the setup.bat script (as administrator)

2.3 Card Reader Setup and Testing

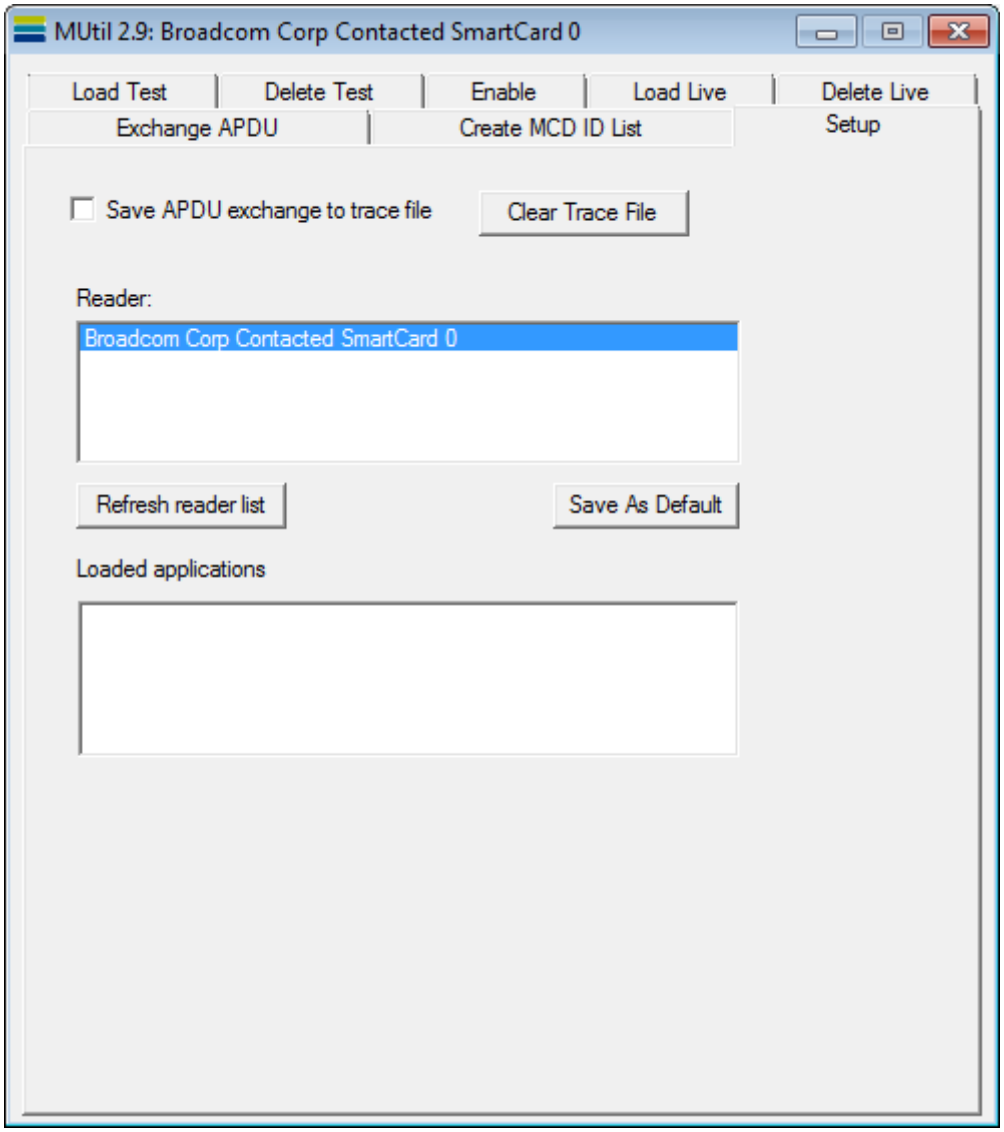
Once installed start MUTIL.EXE and go to the 'Setup' tab. See the following page for details of that screen.

To test that the selected reader is working:

1. Insert a card into the reader
2. Go to the 'Exchange APDU' screen
3. Click the green button
4. The card ATR should appear in the grey text box. Otherwise, an error message stating 'Card Not Found' will be displayed.

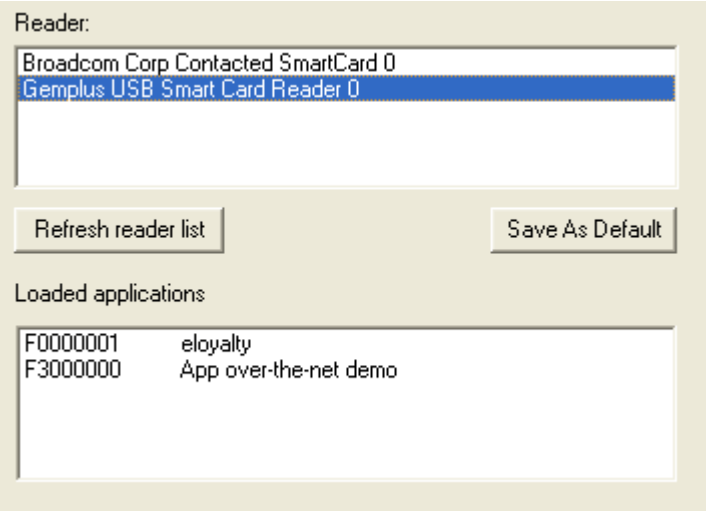
3 The MUTIL Dialogs

3.1 Setup Tab



The application is loaded with the Setup tab displayed by default.

Refresh reader list will rescan for connected PCSC readers. **Selecting a reader** will list any applications loaded on the card.



When checked, **Save APDU exchange to**

trace file will log all APDUs sent and replies received in the file specified by *LogPath* in MUtil.ini. If not specified, the log file will be *c:\temp\mutil_log.txt*.

The trace file contains lines like these:-

Send: 00a40800022f00
Recv: (9000) 32ms
Send: 00b201040002
Recv: 6111(9000) 15ms

The returned *Status Word* is shown in brackets to easily distinguish it from the rest of the returned data. The approximate time to execute the command is shown.

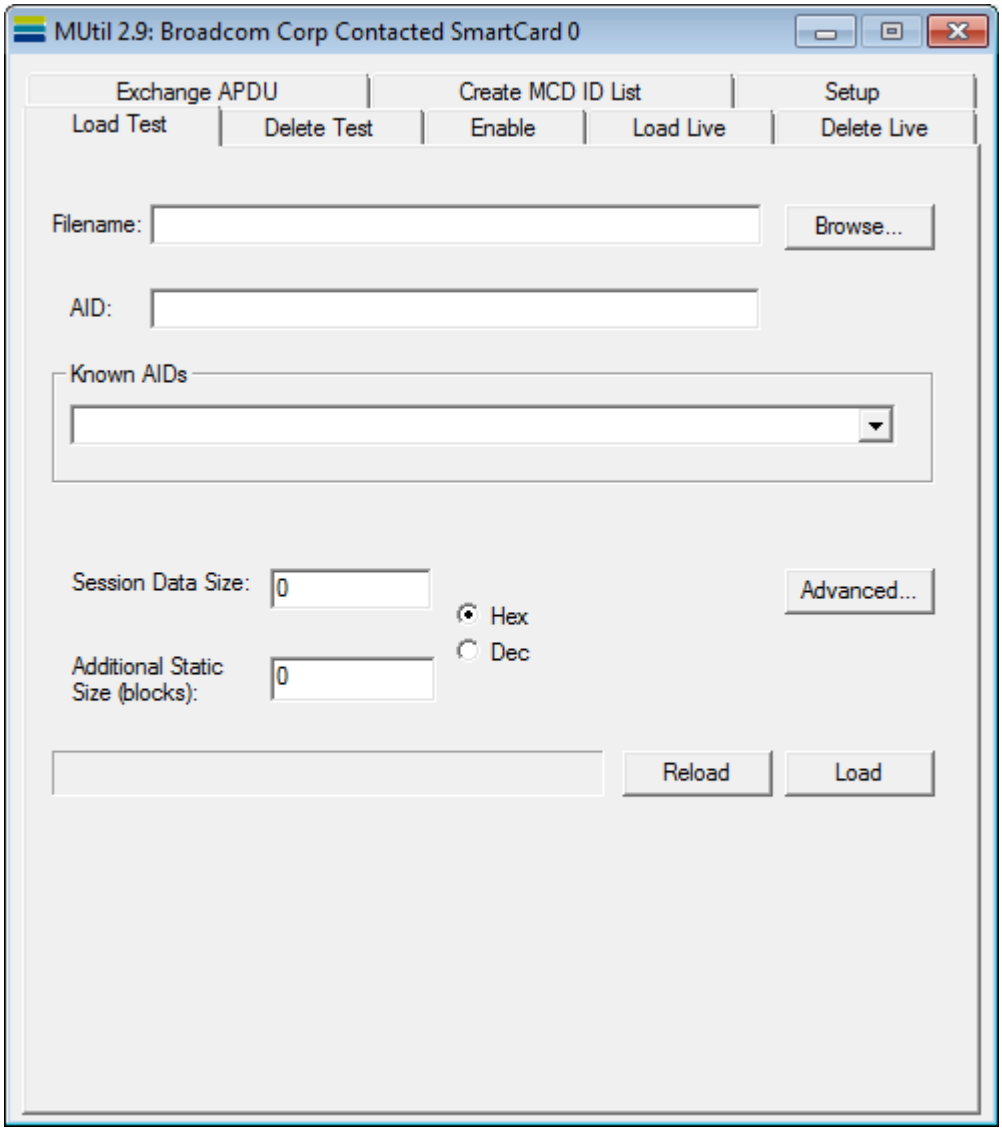
The trace file can be emptied by clicking the **Clear Trace File** button.

3.2 Load Test Tab

This tab is used to load an unprotected application onto a card that has been manufactured using test keys or onto live cards enabled under the Developer-Community Issuer Id (12000005). The latter requires an internet connection. The ALCs obtained are stored in the folder c:\temp and can be used later in the "Load Live" tab if required.

Information regarding the creation of ALU and the loading and deleting process is found in the "Guide to Generating Application Load Units" and the "Guide to Loading and Deleting Applications", both found at MULTOS website.

The main tab is used to provide the minimum information required to load an application:



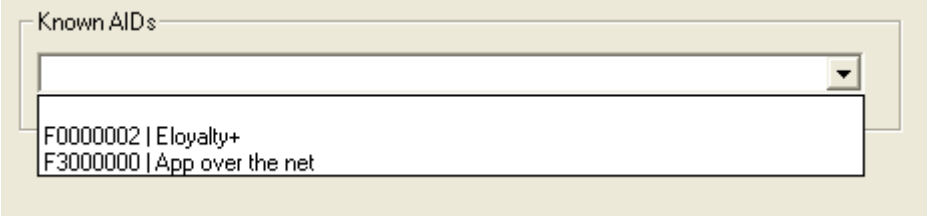
The browse button permits the selection of the file to load. The file formats and their file extensions supported are:

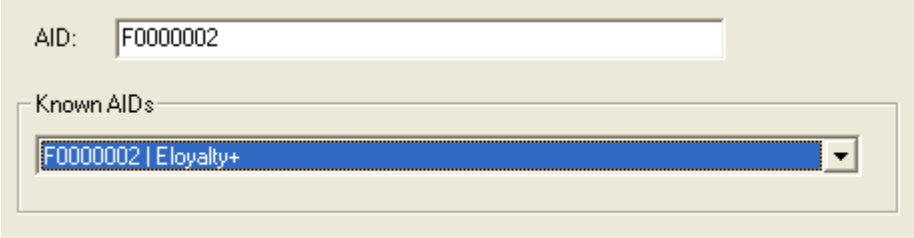
- AUR: application load unit response file
- ALU: application load unit
- INT, APP, AIF: file formats specific to development tools that are not in general circulation

The file path is displayed in the associated text box.

The **AID** text box should have the AID of the application being loaded. Note that the text entered must consist of valid hexadecimal values with no space between the characters.

Instead of typing this value, a value can be selected from the drop down box as shown below, populated from the [AID_LIST] section of MUtil.ini.





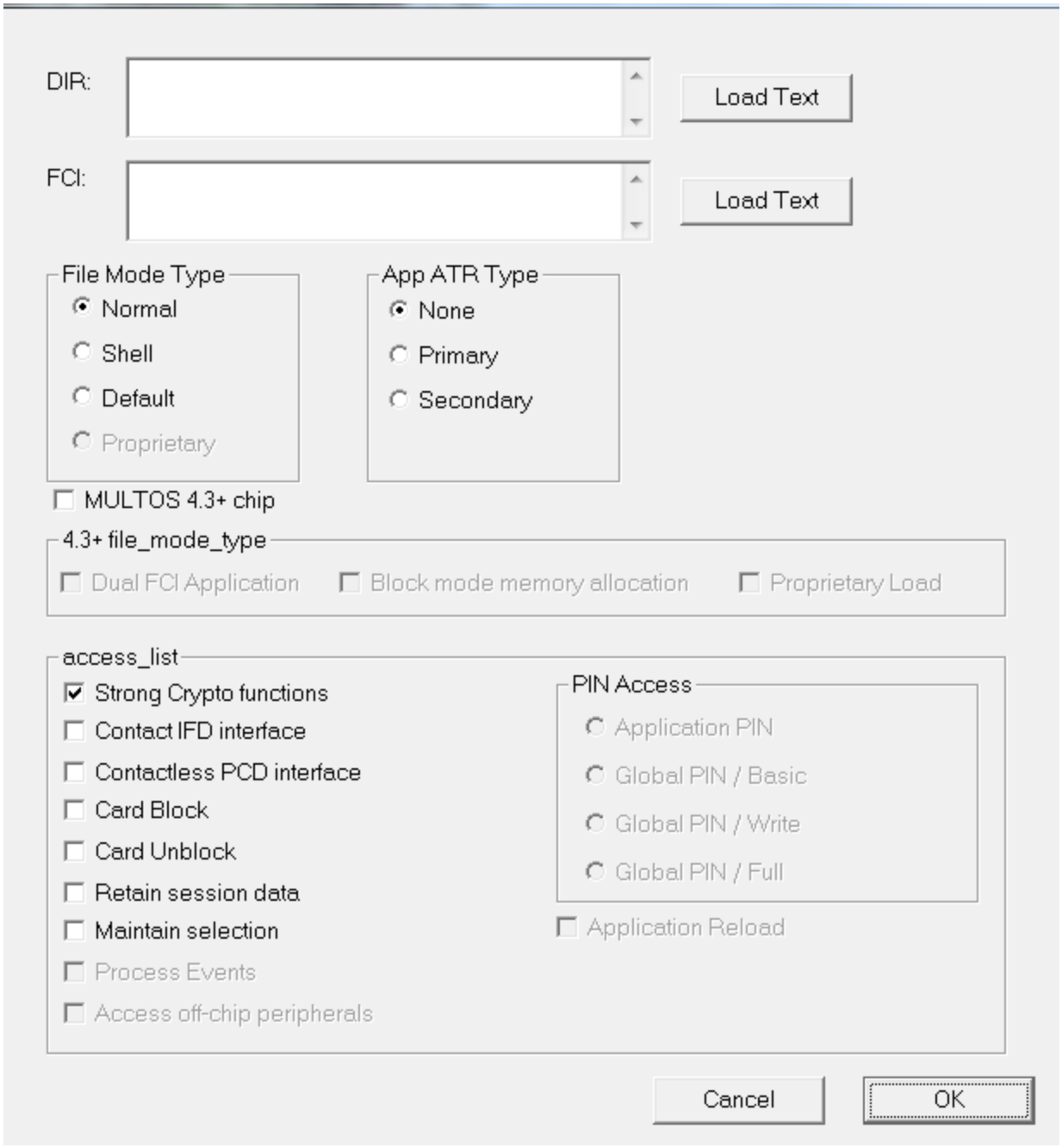
The **Session Data Size** text box holds a value indication the total number of session data used. Note that the value can be entered either as a decimal value or its hexadecimal equivalent. For example, if the session size is 22 decimal bytes, then the value 22 would be entered and the Dec radio button selected. If it were to be expressed as hexadecimal, the text box would read 16 and the Hex radio button option would be selected.

The **Additional Static** text box makes it possible to allocate further static memory to that contained in the ALU. This is in blocks of 255 bytes.

The **Load** button begins the loading process. The progress bar provides a visual interpretation of how the load is progressing. If a load fails, an error message will be displayed, which usually features the related MULTOS error code of the form 9D xx.

The **Reload** button performs a delete followed by a load.

The advanced screen contains additional information:



The MULTOS Utility will automatically create a directory file entry using the AID input. This can be added to or overwritten as the text box allows free text entry. Any value input should be a valid hexadecimal value.

The MULTOS Utility allows the creation of file control information as the text box allows free text entry. Any value input should be a valid hexadecimal value.

It is possible to create a text file that holds the directory file entry and another to hold the file control information. These can be written to the relevant text box using the load button.

The other fields are used to construct the Application Load Certificate:

The **File Mode Type** radio buttons are used to indicate if an application is a standard application, default or shell. If there are any doubts select standard. The application modes are explained in the "MULTOS Developer Guide". An additional option is available for later devices which allows for Proprietary application types.

The **App ATR Type** radio buttons are used to indicate if an application requests control of the ATR historical bytes and, if so, which ATR is to be used.
The **file_mode_type** checkboxes and **PIN Access** radio buttons are enabled by checking **MULTOS 4.3+** chip and give access to settings only available in MULTOS 4.3 and later:

- **Dual FCI Application:** application FCI data contains two FCI records
- **Block mode memory allocation**: The data lengths in the ALU are in 0xFF byte sized blocks
- **Proprietary Load**: enables any proprietary internal mechanism using during application loading that the card supports. Does not impact interoperability.
- **PIN Access**: these radio buttons control how the application being loaded is allowed to access the MULTOS global PIN.

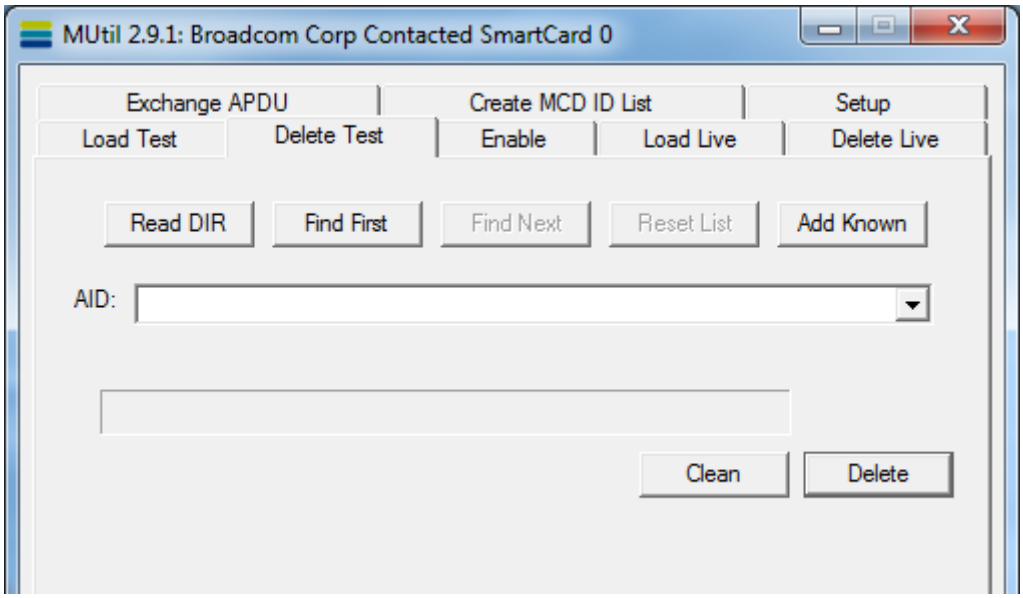
The remaining **access_list** checkboxes control the features that the application is allowed to access.

Note: If loading ALUs where the data size is in 0xFF byte blocks, you MUST specify this in the Advanced dialogue first before selecting the ALU file otherwise parsing of the ALU will fail.

3.3 Delete Test Tab

This tab is used to delete an application from a card that has been manufactured using test keys or onto live cards enabled under the Developer-Community Issuer Id (12000005). The latter requires an internet connection. The ADCs obtained are stored in the folder c:\temp and can be used later in the "Delete Live" tab if required.

Information regarding the loading and deleting process is found in the "Guide to Loading and Deleting Applications" found at MULTOS website.



The **Read DIR** button will read the directory file entries, if any, and, if formatted correctly will display each AID in the drop down box.

It is possible to load an application without a directory file entry or with an entry that does not contain the correct information. So, it would be possible to have an application loaded on a card, but be unable to delete because the full AID is not available. The button **Find First** sends a series of SELECT FILE commands and can ascertain the full AID of an application loaded. This can take some time as there are a possible 256 values for each byte and up to 16 bytes. The button **Find Next** can be used after **Find First**. This looks for further applications using the same method.

The **Add Known** button loads the list of known AIDs from the mutil.ini file. This is especially useful for cards containing a Shell application.

The buttons **Find First**, **Find Next, Add Known** and manual text entry populate the drop down box on the screen. There may be more than one entry, although only the current entry is shown. The **Reset List** button erases all list entries.

The AID displayed in the AID drop down box is the one that will be used to locate the application for deletion.

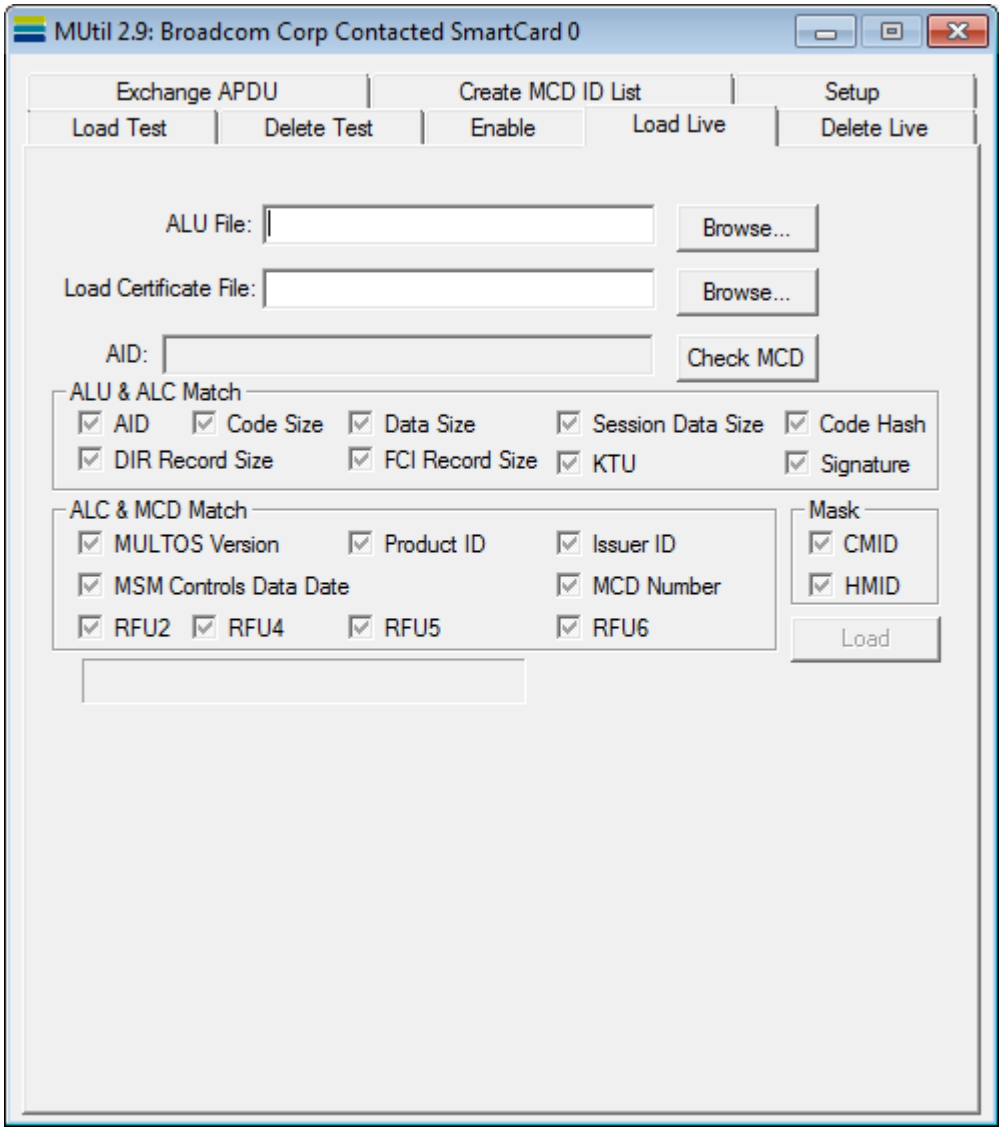
The **Delete** button begins the deleting process. The progress bar provides a visual interpretation of how the deletion is progressing. If a delete fails, an error message will be displayed, which usually features the related MULTOS error code of the form 9D xx.

The **Clean** button deletes all the applications listed in the directory file (DIR).

3.4 Load Live Tab

This tab is ambiguously named. It is used to load an application using a certificate, which can be done on developer cards or live cards. There are a series of checks done prior to commencing the load process. Note that if key checks indicate a mismatch, the MULTOS Utility will not permit the load process to start as it will fail.

Note: when loading of ALUs where the data size is in 255 byte blocks. In order for this to work, you MUST select the ALC file first.



3.4.1 Text Boxes and Buttons

For details on the matching check box display see the section How to interpret the matching check box display.

The Browse button permits the selection of the file to load. The file formats and their file extensions supported are:

- AUR: application load unit response file

- ALU: application load unit
- INT, APP, AIF: file formats specific to development tools that are not in general circulation

The application load certificates are also chosen using the corresponding browse button. The file formats and their file extensions supported are:

- ALR: application load certificate response file
- ALC: ALC data extracted from the ALR
- ALX: file containing multiple ALCs, used by step/one
- CER: file format not in general circulation

The greyed out AID text box displays the value found in the certificate.

The load button starts the loading process. The progress bar provides a visual interpretation of how the load is progressing. If the load fails, an error message will be displayed, which usually features the related MULTOS error code of the form 9D xx.

3.4.2 Load Checking

By clicking the Check MCD button the MCD, ALU and ALC are interrogated and the responses are compared with those held in the certificate.

When the application to be loaded and the application load certificate are chosen the MULTOS Utility checks that the different ALU and ALC components match. In this case the checking covers:

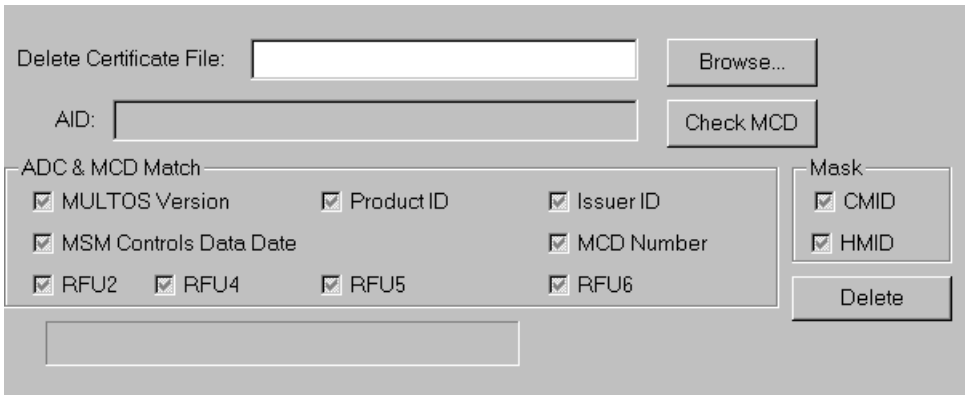
- AID: depending on the nature of the file to load, the AID may be specified. If it is, it is compared to that in the ALC.
- Sizes: the various component sizes declared in the ALC are compared to those found in the ALU.
- Code Hash: if a code hash is present in the ALC and if it is identified as a SHA-1 hash, the MULTOS Utility will calculate a hash as well and compare it to the one supplied. Otherwise, the presence is simply noted.
- Signature: if the ALU has an application signature this check ensures that the ALC indicates that a signature is present. It also ensures that the code, data, DIR and FCI sizes given in the ALC match exactly those found in the ALU.
- KTU: if the ALU has a KTU the checks ensures that the ALC indicates that one is present.

The ALC and MCD matching checks cover MULTOS Version, Product ID, Issuer ID, MSM Controls Data Date and the various RFU fields. All must match exactly.

Finally the mask match display shows if the Certification Method ID and Hash Method ID of the MCD is the same as that given in the ALC. A mismatch here will not stop the process, but may indicate that the certificate would not work on the MCD.

3.5 Delete Live Tab

This tab is ambiguously named. It is used to delete an application using a certificate, which can be done on developer cards or live cards. There are a series of checks done prior to commencing the delete process. Note that if key checks indicate a mismatch, the MULTOS Utility will not permit the process to start as it will fail.



For details on the matching check box display see the section How to interpret the matching check box display.

The Browse button permits the selection of the application delete certificate. The file formats and their file extensions supported are:

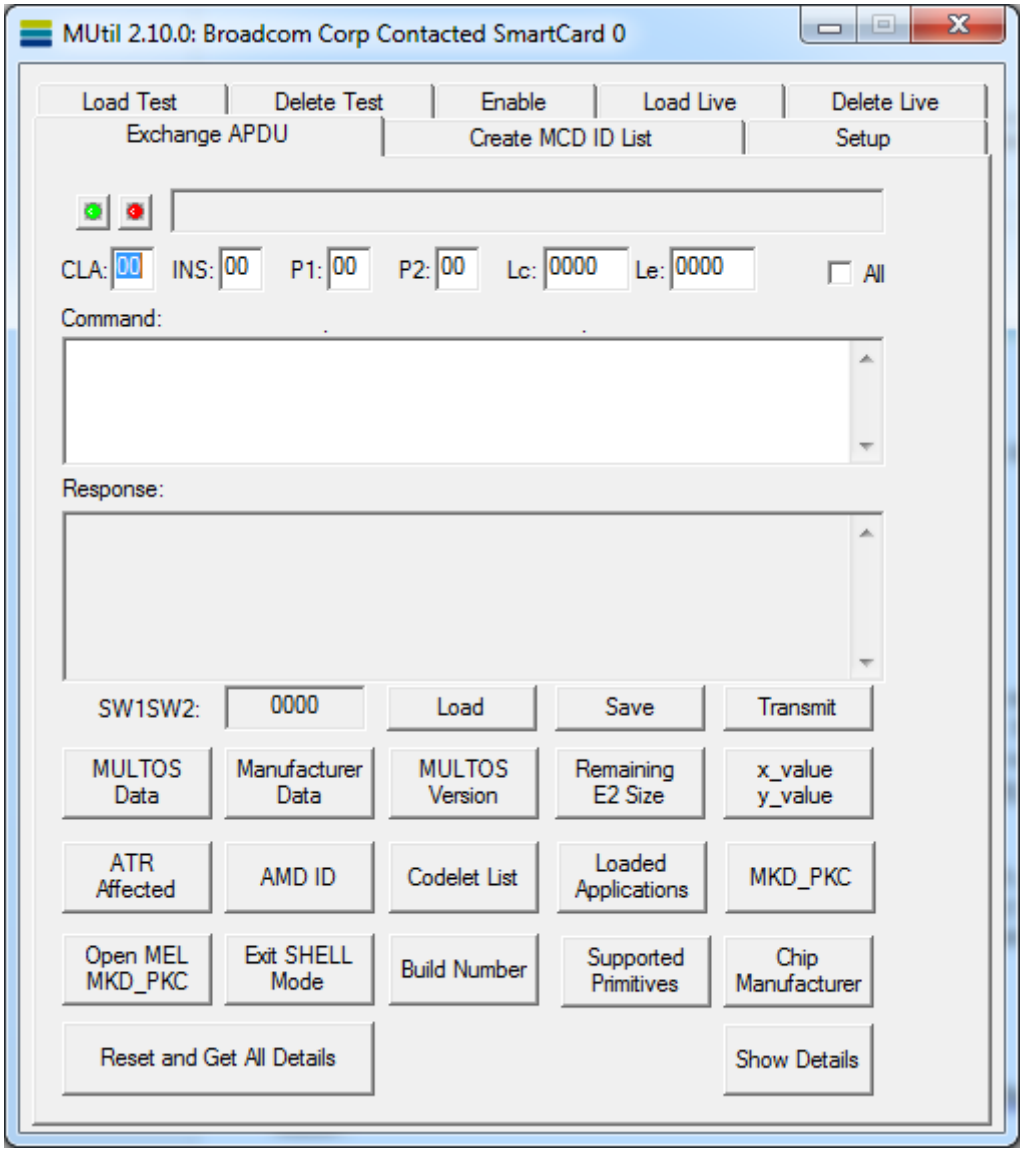
- ADR: application delete certificate response file
- ADC: ADC data extracted from the ADR
- ADX: file containing multiple ADCs, used by step/one
- CER: file format not in general circulation

After clicking the button MCD Check the result of the checks are displayed here. The checks cover MULTOS Version, Product ID, Issuer ID, MSM Controls Data Date and the various RFU fields. All must match exactly.

Finally the mask match display shows if the Certification Method ID and Hash Method ID of the MCD is the same as that given in the ADC. A mismatch here will not stop the process, but may indicate that the certificate would not work on the MCD.

3.6 Exchange APDU Tab

It is possible to use the application to communicate to applications loaded on a card using the Exchange APDU tab.



3.6.1 Power Buttons

The button with the green dot is used to power on the card in the reader. It is good practice to first power on the card and then send the desired command. However, the application will do this automatically when the transmit button is clicked. If the power on was successful, the ATR will be displayed in the grey ATR Display text box. Note that double clicking the green power button, once the card is powered on, will do a warm reset.

The button with the red dot is used to power off the card. The ATR will be removed from the ATR Display. It is good practice to power off the card before removing it from the reader. In fact, the application will not send any commands to the card if it has been removed and replaced without explicitly clicking the power off button.

3.6.2 ATR Display

The grey box above the APDU entry boxes displays the Answer to Reset returned by the card in the reader.

3.6.3 APDU Entry Boxes

Underneath the ATR display there are input boxes for an APDU. Simply input the CLA, INS, P1, P2, Lc and Le required. Please note that check box labelled "All" is meant to be checked when the application should return all data irrespective of the data size. See the section How to Communicate with an Application for more information.

3.6.4 Exchange APDU Buttons and Status Word Display

There are three buttons available. They are:

- Load: allows a saved command to be loaded
- Save: allows an APDU command including CLA, INS, P1, P2, Le, Lc and any command data to be saved to disk
- Transmit: sends the displayed command APDU to the card.

To the left of the APDU buttons is a grey text box labelled SW1SW2. The status word returned by the chip is displayed here. Please note that if a communication error occurs the text box may display the first two bytes of a communication sub-system error.

3.6.5 Command and Response Data

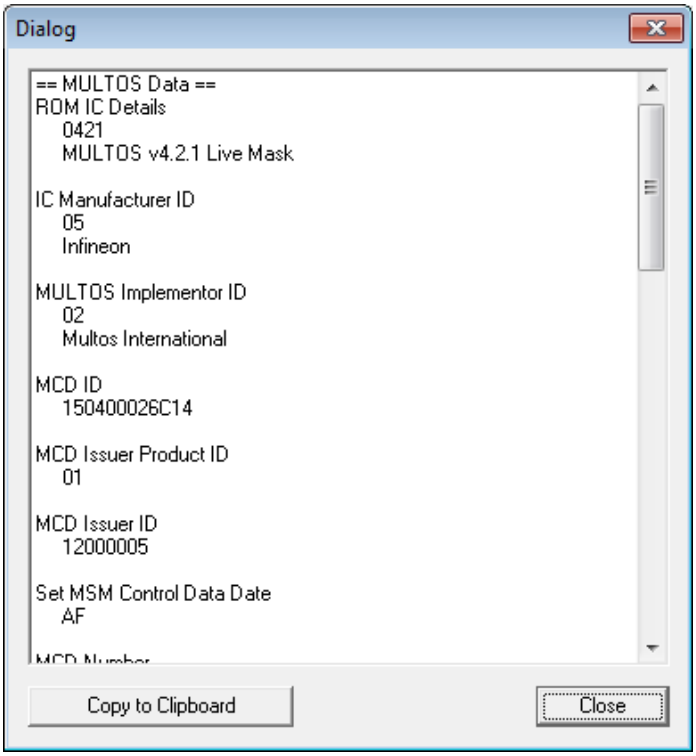
The Command Data text box is used to hold any data that is to be sent to the card. While the Response Data text box displays the data returned by the card. Please note that all data is displayed in as hexadecimal values.

3.6.6 Get Data Buttons

The buttons at the bottom of Exchange Data tab send the commands "Get MULTOS Data", "Get Manufacturer Data" and "Get Configuration Data". The Show Details button interprets the returned data and looks up text descriptions for various items from the Mutil.ini file.

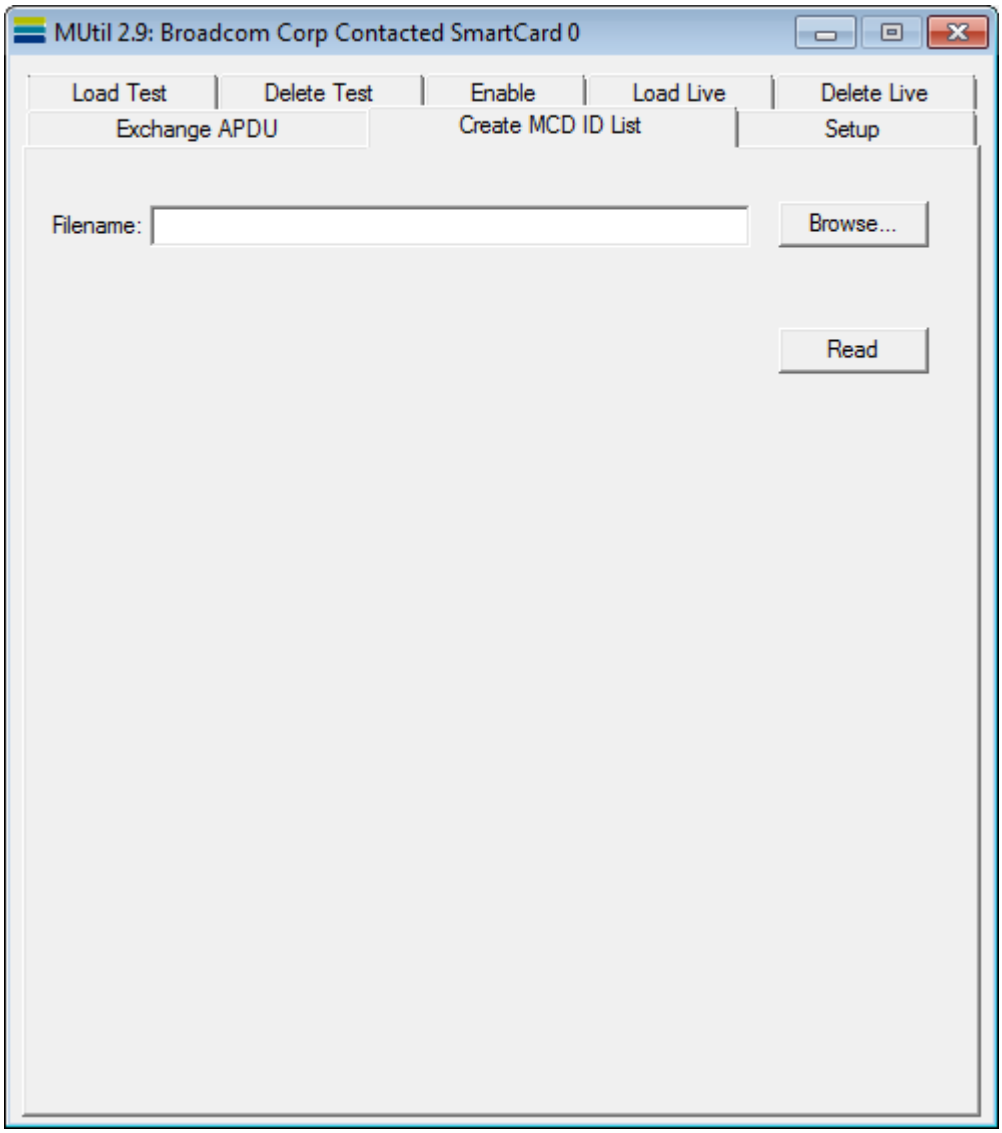
Copy to Clipboard allows for these details to be copied and used elsewhere.

The "Reset and Get All Details" button automatically gets all the card data and displays it on one go.



3.7 Create MCD ID List Tab

An MCD ID list is required to request enablement data. See the section How to Create an MCD ID List for further information. The tab appears as:



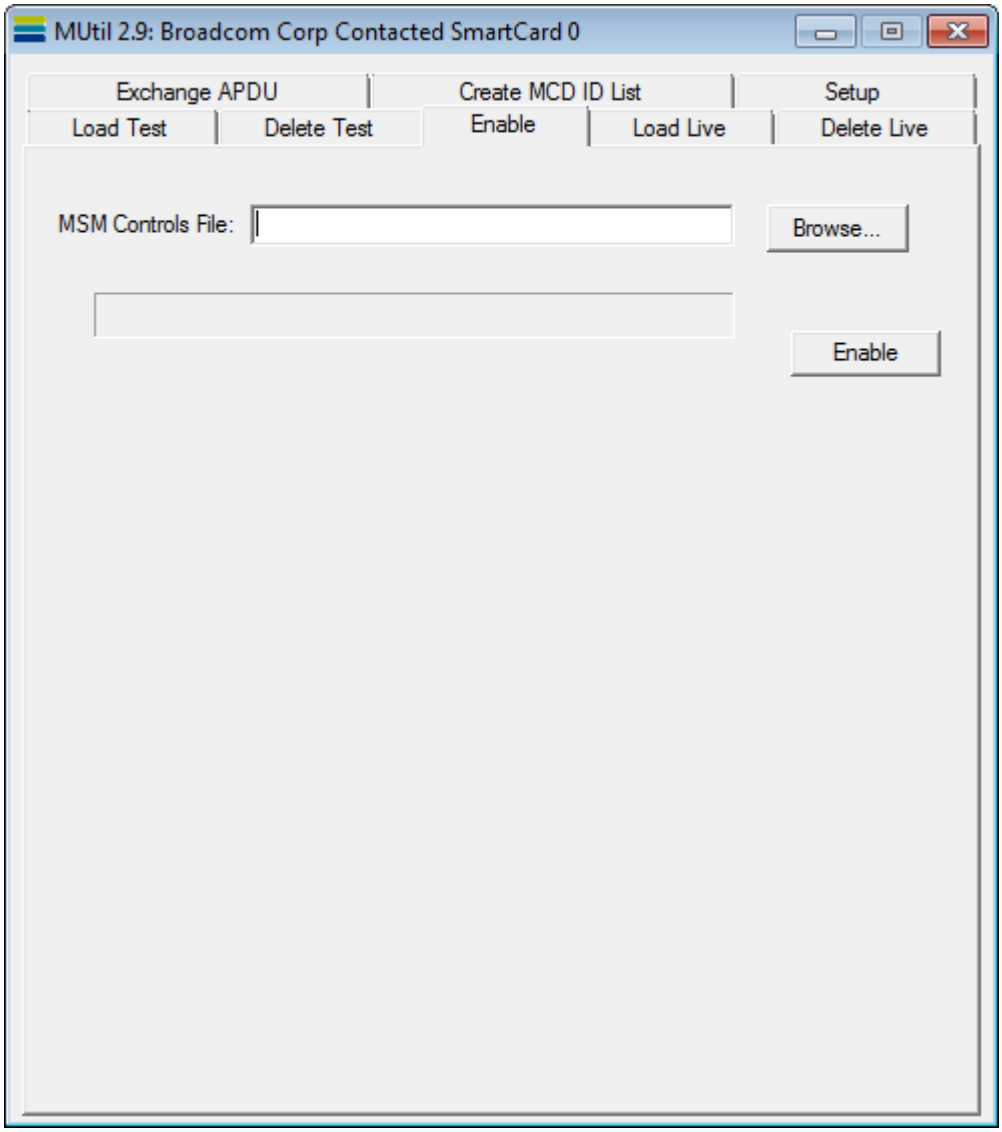
The buttons available are:

MCD ID List **Browse**: This button is used to select the directory and file to which MCD ID will be appended.

MCD ID List **Read**: When clicked the MULTOS Utility sends the command "Get Manufacturer Data" to the chip. The 1-byte IC Type, the 1-byte IC Type and 6-byte MCD will be extracted from the data returned and appended to the file displayed in the browse text box.

3.8 Enable Tab

Provided that one has the required MSM Controls Data, the application can be used to enable cards. See the section How to Enable Cards for more information.



The buttons available are:

Browse: This button is used to select the directory and file where the MSM Control Data response file is held.

Enable: When clicked the MULTOS Utility searches the MSM CD response file given in the browse text box for an entry corresponding to the card in the card reader. The enablement data, if found, is transmitted to the card.

4 Scripting

4.1 Command Line

Scripting is supported as a command line feature.

The command line is

mutil <scriptname> <tracefile name> [-rdr<n>]

E.g.

mutil testscript.txt testresults.txt –rdr1

The reader number (-rdr) is zero based and refers to the order of the readers displayed in the Setup tab of MUtil. If the –rdr switch is omitted, the default is 0 (the top reader in the list).

If the script fails, it returns a value of 1, otherwise 0.

4.2 Syntax

The script syntax is as follows:

- **Comments**: Lines starting with a semi-colon are comments and get copied into the trace file.

- **Commands** start with a dot followed by two letters (not case sensitive). The commands supported are as follows:-
  - .EX <apdu>
    Exchange APDU
  - .ON
    Power on
  - .XX
    Power off
  - .LL <alu file>,<alc file>
    Load Live
  - .LT <alu file>,<AID>,<session data size>,[<file_mode_type|<access_list>]
    Load Test
  - .DL <adc file>
    Delete Live
  - .DT <AID>
    Delete Test
  - .EN <msm file>
    Enable a card using an msm in the provided file.
  - .CS <script file>
    Call a sub-script
  - .FR <freeze cert file>
    Freeze a step/one card (supports .afc, .afr and .afx file extensions)
  - .ID [bin | hex]
    Outputs the mcd-id (as per the "Create MCD ID List" tab) in either binary or hex form.

Status words: For the .EX command, you can optionally specify the value of the status word you expect by putting it in brackets, e.g. (616C). Wildcards are accepted e.g. (61??). If the actual status word returned doesn't match that expected the script exits at that point.

Expected response data: For the .EX command, you can optionally specify the expected response data in the () as well as the expected status word. ?? can be used to allow any value. Failure to match causes the script to exit.

Continuation markers: A '\' character at the end of a line acts as a continuation marker allowing long commands to be spread over several lines.

Please note: Long APDU data (Lc > 255 bytes) is not currently supported in the scripting engine.

4.3 Example script

```
;Load unprotected ALU - <ALU>,<AID>,<SD Size in hex>,[<file_mode_type>|<access_list>]
.LT eloyaltyplus.alu,F0000002,02

;Power on
.ON

;Select application
.EX 00 A4 04 00 04 \
 F0000002 (9000)

;Read points
.EX 7051000002 (0010 9000)

;Power off
.XX

; Unload ALU
.DT F0000002

;TEST COMPLETED
```

5 How To Guide

5.1 How to Load an Application onto a Developer Card

The MULTOS Utility is able to generate load certificates on the fly for any cards manufactured with test keys. This is what is done when using the "Load Test" facility.
To load an application onto a developer card:

- Insert card in card reader
- Go to the tab Load Test
- Use the browse button to locate the file to load
- Input the AID, where each character represents a valid hexadecimal value and where there are no spaces between the characters
- Input the size of session data used by the application in either decimal or hexadecimal representation

At this point there is enough information to load the application. There are, however, other options available when the advanced button is clicked. If required, any of the following can be done:

- Create a directory entry or add to the automatically generated DIR entry or import directory entry from a text file
- Create File Control Information (FCI) or import FCI from a text file
- Select File Mode Type
- Select Application ATR Type; i.e., which ATR historical bytes the application wishes to control
- Set file_mode_type bits and access_list bits.

Once all the information is entered, click the load button.

The progress bar will display the progress of the load. If successful, a message will confirm the load. If it fails, a message box will appear indicating the MULTOS error given by the chip.

5.2 How to Delete an Application from a Developer Card

The MULTOS Utility is able to generate delete certificates on the fly for any cards manufactured with test keys. This is what is done when using the "Delete Test" facility.
To delete an application onto a developer card:

- Insert card in reader
- Go to the Delete Test tab
- Input AID:
    - Directly into drop down text box, if known, or
    - Assuming there is a correctly formatted directory entry use the button Read DIR to get the AID, or
    - Use the Find First button or Find Next button as appropriate
- Click delete button

The progress bar will display the progress of the delete. If successful, a message will confirm the delete. If it fails, a message box will appear indicating the MULTOS error given by the chip.

5.3 How to Load an Application using an ALC

This method of loading an application mirrors the live loading process in that both an ALU and an ALC are supplied as separate files. To load an application using an ALC:

- Insert card in card reader
- Go to Load Live tab.
- Use the browse buttons to locate the file to be loaded and the certificate file
- The AID from the certificate will be displayed in AID text box
- The results of ALU & ALC Match will be displayed in that area. See the section How to interpret the matching check box display for more information.
- Click the Check MCD button to have the MULTOS Utility compare the MCD values with those in the ALC. The results will be displayed in the corresponding area. See the section How to interpret the matching check box display for more information.
- If the matching results are satisfactory, click the load button.

If the load succeeds a message box will appear indicating success. If it fails, a message box will appear giving the reason and MULTOS error given.

5.4 How to Delete an Application using an ADC

This method of deleting an application mirrors the live deletion process in that an ADC is supplied as a separate file. To delete an application using a certificate:

- Insert card in reader
- Go to Delete Live tab
- Use the browse button to find the delete certificate
- The AID in the certificate will be displayed in the AID text box
- Click the Check MCD button
- The results will be displayed. See how to interpret the responses.
- If the matching results are satisfactory, click the delete button

If the delete succeeds a message box will appear indicating success. If it fails, a message box will appear giving the reason and MULTOS error given.

5.5 How to use Developer Community Cards

Developer Community Cards are simply live cards that have been enabled with Issuer ID 12000005 on the Global KMA. It is possible to use them in two ways:-

- By manually ordering ALCs and ADCs using StepXpress and using the “Load Live” and “Delete Live” tabs of MUtil or
- By letting MUtil automatically obtain ALCs and ADCs via the web services interface of StepXpress using the “Load Test” and “Delete Test” tabs of MUtil. For this to work you must complete the [STEPXPRESS] section of MUtil.ini as follows:-

```
[STEPXPRESS]
User=Developer0XX
Pwd=mypassword
Token=BBBBBBBB-AAAA-ZZZZ-YYYY-XXXXXXXXXXXX
IssuerId=12000005
```

To obtain the Token value please e-mail services@stepnexus.com

5.6 How to Communicate with an Application

Once an application has been loaded, the Exchange APDU tab can be used to send commands to it. For the following example, let the application ID of the standard mode application be F0001234 and let there be a command GetTotal that has a CLA of 90, and INS of 10, P1 and P2 are both 00 and the Le is 02.

The steps to run the command are:

- Insert card in reader
- Go to Exchange APDU tab
- Click the power on button and the ATR should then be displayed
- Select the application
- Input the SELECT FILE command with a CLA of 00, an INS of A4, P1 would be 04, P2 would be 0C, Lc would be 04, Le would be 0 and the command data would be F0001234. If the select command is successful, the SW should be 9000.
- Click the transmit button
- Input the GetTotal command as given above and click the transmit button. If the command executes successfully, 2 bytes of response data should be returned and the SW would be 9000. If it fails, an application defined SW should be returned.

Once an application is successfully selected any number of commands may be sent to it. See the "MULTOS Developers Guide" for further information about what constitutes an application session.

5.7 How to interpret the matching check box display

Both the Load Live tab and the Delete Live tab use check boxes to display the results after value matching has been done. There are four possible states:

☑ + disabled text: NOT PRESENT. This indicates that the value is not present in one set of the data to be compared and, therefore, no matching can be done.
☑ + enabled text: IMPERFECT MATCH. This means that the values compared do not match, but there is a low likelihood of a load failure.
☑ : MATCH. The values match exactly.
☐: MISMATCH. The values compared do not match. This may result in the MULTOS Utility not allowing a load or delete to take place.

5.8 How to Create an MCD ID List

An MCD ID list is needed in order to request enablement data. To successfully generate an MCD ID list:

- Use the browse button to create an empty *.mid file. The file extension is automatically appended to the file name.
- Insert a MULTOS card in the card reader and click the read button. The application will then extract the IC Manufacturer byte, the IC Type byte and the 6-byte MCD ID and append the resulting 8-byte value to the *.mid file.
- Remove previous, insert next card and click the read button.

It is worth noting that the 8 bytes read from the card will simply be appended to the file. There is no check in place to ensure that a duplicate entry is not made.

5.9 How to Enable Cards

When MSM CD has been received it is possible to use the MULTOS Utility to enable cards. To do so:

- Use the browse button to locate the *.msm file
- Insert card into card reader
- Click the enable button. If there is an entry for that card in the supplied MSM CD file, it will be used to enable the card. If not, an error message stating "MSM Controls Data Record not found in file" will be displayed.

5.10 How to use a MULTOS Trust Anchor Device

MULTOS Trust Anchor devices (e.g. Multos International M5 products) may be used via their serial interface. When operating in this "Command Mode" the devices interact exactly as a T=1 smartcard would operate. To make these devices appear in the list of Readers on the Setup tab you need to add an entry to the MUtil.ini file as follows:-

```
[SERIAL_READERS]
;<COMx>,<baud>
COM3:9600
```

Note: The fastest speed supported is 57600.

6 Glossary

Term	Definition
AID	An AID is the Application Identifier, which is used to select the application once it has been loaded onto the card
ALU	An ALU is an application load unit. This file holds the different application components in a known file format.
APDU	APDU stands for application protocol data unit. When a command is sent to an application it is done using an APDU. In general, the command consists of mandatory class (CLA), instruction (INS), parameter 1 (P1) and parameter 2 (P2) bytes. If data is being sent to the application, then there would be a length of command data (Lc) byte and the command data. If the application should send a response, then the length of expected (Le) data byte would be present. For further information see ISO/IEC 7816-4.
Application Delete Certificate	An application delete certificate, or an ADC, is required to delete an application. It contains details about the application that are cryptographically signed.
Application Load Certificate	An application load certificate, or an ALC, is required to load an application. It contains details about the application that are cryptographically signed.
ATR	An ATR is a bit string returned by a chip when it is reset. It consists of interface characters that specify the communication parameters supported by the chip and historical characters that may be manipulated by MULTOS applications.
Enablement	When a card is first manufactured it exists in a protected state. The card does not belong to any MULTOS issuer and the card will only process enablement commands. So, enablement is, in general, the process where a card is bound to a single MULTOS issuer and the chip is made ready for use.
KTU	A key transformation unit is a component of a confidential ALU. It is used to hold details about how other parts of the ALU have been enciphered. For more information see the "Guide to Generating Application Load Units".
MCD	MCD is an abbreviation for MULTOS Carrier Device. It is meant to be a generic term for any device that implements the MULTOS operating system..
MCD ID	An MCD ID is a 6-byte value that, prior to enablement, uniquely identifies a MULTOS chip.
MKD PK C	After a card is enabled it has its own unique RSA key pair. The public component is referred to as MKD PK. In order to ensure that any functions that require this key are using a good value the MKD PK is supplied in a certified format. This certified format is the MKD PK C, which is also known as the card public key certificate.
MSM Control Data	MSM Control Data is sometimes referred to as MSM CD or enablement data. This is the data that is used to enable a MULTOS card.
Status Word	When an application processes an incoming APDU it may return data, but will always return a Status Word. This is a 2-byte value that indicates the success or failure of the processing. In some cases the most significant byte is referred to as SW1 and the least significant byte as SW2. It may also be referred to generally as an SW. For further information about possible SW values see ISO/IEC 7816-4. Note that if there is a communications failure, the SW display will show the error given by the communications layer. In the special case where it reads "0000" that means a communications timeout has occurred and may indicate an abnormal end to the smart card program.

----- End of Document -----