Shell Applications

MAO-DOC-HOW-003 v1.1

Contents

OPERATING CONFIGURATIONS 1
MULTOS Security Manager (MSM) Commands 1
Master File Commands 1
ONLY STANDARD APPLICATIONS LOADED 2
A DEFAULT APPLICATION IS PRESENT 3
A SHELL APPLICATION IS PRESENT 3
Possible Card Architecture 5
SHELL APPLICATIONS AND COMMAND HANDLING 6
Master File Commands 6
SELECT FILE Command 6
Selecting a Standard Application 7
Deselecting a Standard Application 7
Application Specific Commands 7
Get Response 7
OTHER THINGS TO CONSIDER 8
Status Word returned after selection 8
ATR Historical Characters 8
WRITING A SHELL APPLICATION 8

Operating Configurations

A MULTOS chip has three mutually exclusive operating configurations, which depend on the type of applications loaded. The possible configurations are:

- Only standard applications are loaded
- A default application is loaded with or without other standard applications
- A shell application is loaded with or without other standard applications

The configuration determines how MULTOS handles incoming APDU commands and when a shell application is present it has profound impact on application development.

MULTOS Security Manager (MSM) Commands

Before beginning the discussion of configurations it is useful to address the topic of MSM commands. These commands are the ones used to enable chips or load and delete applications and can only be handled by MULTOS. This applies no matter what operating mode is in use.

Master File Commands

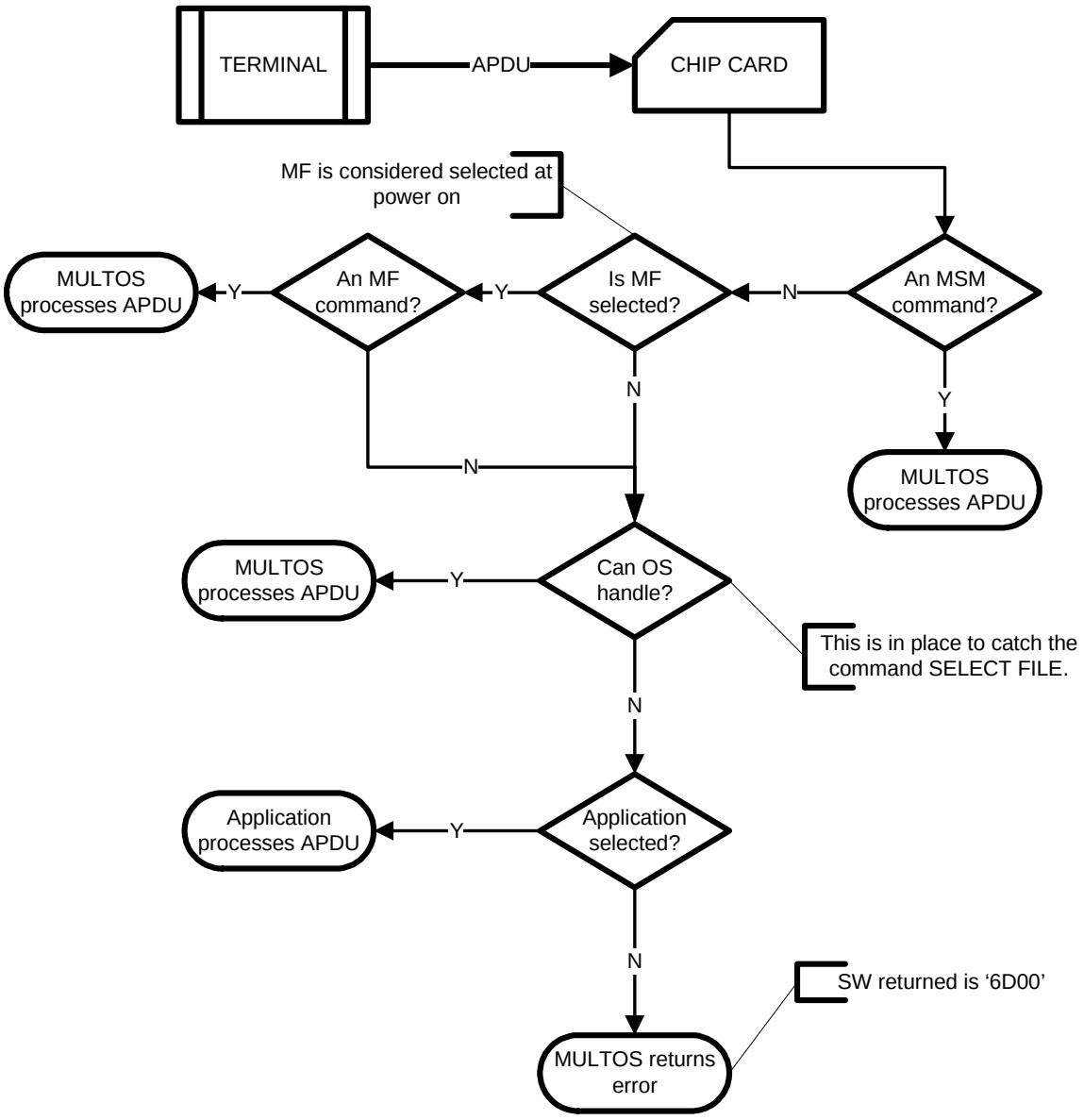
There are a series of commands that provide general card level information. In order for these to be processed correctly the Master File (MF) must be selected. The commands to which this applies are:

- CARD UNBLOCK
- GET CONFIGURATION DATA
- GET DATA
- GET MANUFACTURER DATA
- GET MULTOS DATA
- GET PURSE TYPE

For detailed information on these commands please see the "MULTOS Developers Reference Manual".

Only Standard Applications Loaded

A chip operating with only standard applications loaded corresponds to the common sense view of a multi-application chip card. That is, there is more than one application and one must be selected in order to perform the desired function.



When power is applied to the chip the Master File is implicitly selected. This means that both MSM and MF commands can be sent immediately.

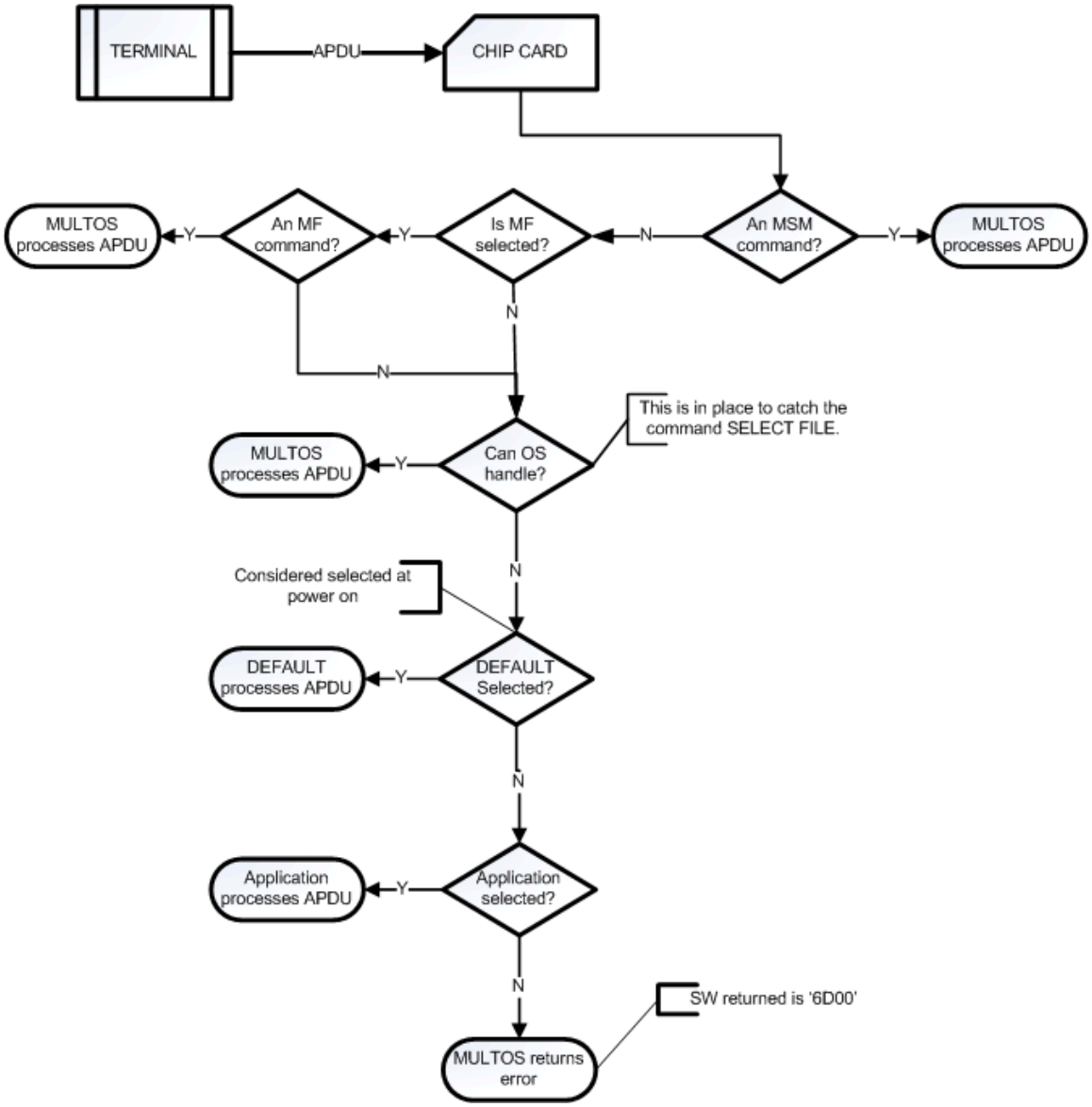
In order to choose an application the terminal sends the command SELECT FILE where the command data is the Application ID (AID) of the desired application. If the AID is found, the corresponding application will be selected. If the AID is not found, MULTOS will route it to the currently selected application, if any, or send an error if no application is selected.

After an application is selected all commands, except MSM commands, are sent to it until it is deselected. An application is ready to receive commands until either a successful SELECT FILE command is handled by MULTOS or power has been removed from the device.

A Default Application is Present

In some cases the intended use of a chip card is made easier by having an application immediately available to receive commands. That is, there is no need to use SELECT FILE because the application is present and ready to go.

Note that in this configuration the default application must be the first application loaded.



To some extent this command handling flow does not differ greatly from the standard only one. However, after power on the default application is implicitly selected, which means that any command except an MSM one will go directly to it. If a Master File command is required immediately after power on, then the Master File must be explicitly selected before the command is sent.

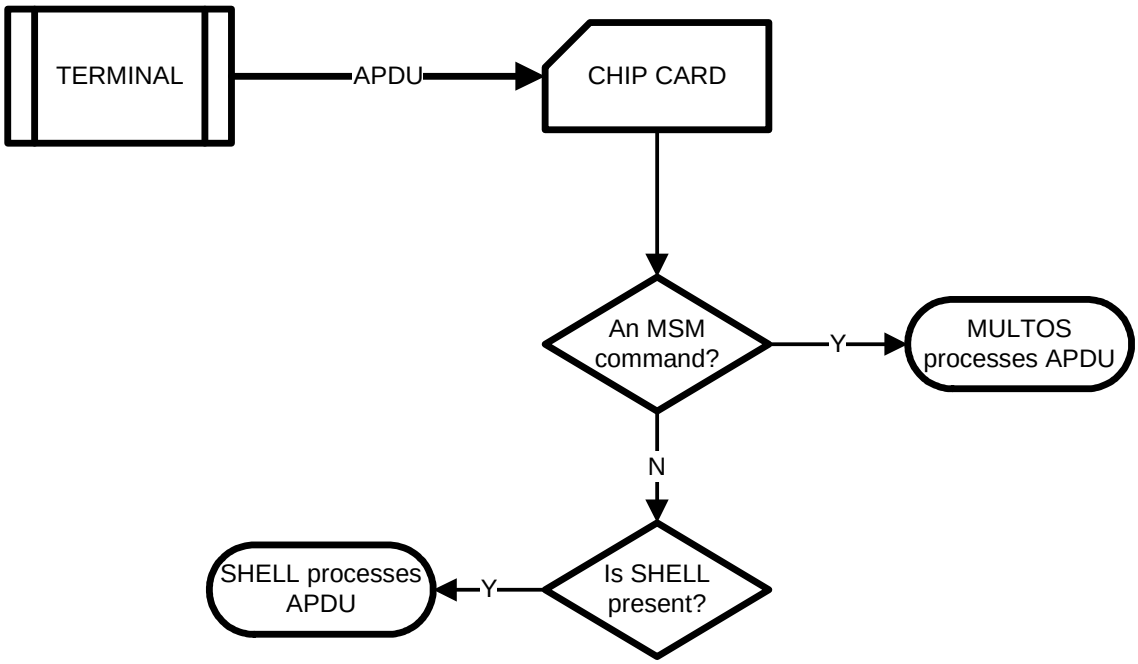
If another application or file is selected using SELECT FILE, then the command flow is exactly the same as that for standard only configurations. The deselection criteria remain the same as well.

A Shell Application is Present

In some cases technical or business requirements are such that the command handling offered by MULTOS is not adequate. For example, an existing terminal base may be expecting a single

application card or may not use SELECT FILE to activate applications. In these cases a shell application, which is developed in the same way as any other, is appropriate. I

Note that in this configuration the shell application must be the first application loaded.

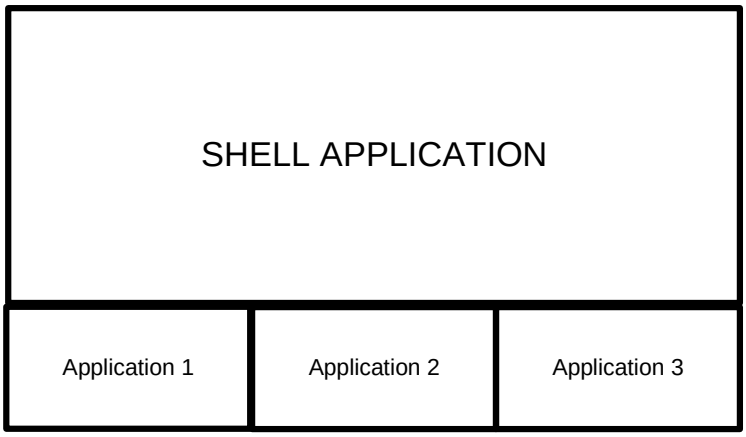


As can be seen from the diagram the incoming APDU is not handled by MULTOS except in the case of an MSM command. Every other command is sent to the shell, which means the shell must be programmed to handle any command it receives.

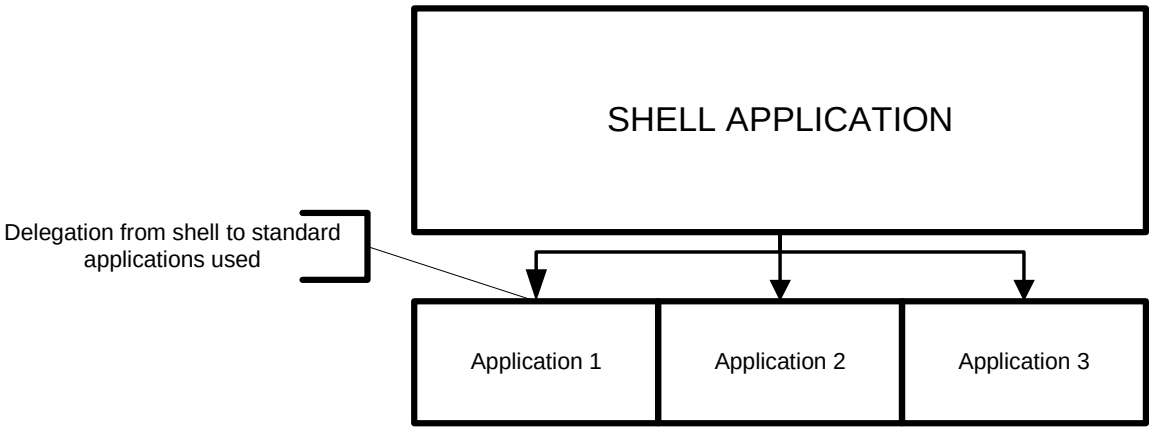
In this case, the shell application is implicitly selected at power on and can not be deselected.

Possible Card Architecture

The presence of a shell application does not preclude the presence of other standard applications. It does preclude the presence of a default application. There are two possible card architectures that an issuer could use.



Application functionality
embedded in Shell



Application functionality in
separate standard applications

The first approach embeds all application functionality in the shell application itself. This means that the shell is a self-contained application that can perform multiple functions.

The second approach is to have the shell application present along with a number of standard applications. If a command arrives that is meant for a standard application, the shell can make use of delegation to pass the command to it.

Of course, a hybrid approach where some standard applications are present and some application functionality embedded in the shell is also possible.

Shell Applications and Command Handling

As mentioned previously all incoming commands (with the usual exception of MSM commands) are received by the shell application. This must then be able to handle a series of commands.

Master File Commands

When a shell application is present all the Master File commands must be handled by it. To make this easier MULTOS provides primitives that the application can use to extract and return the data required.

Note, however, that CARD UNBLOCK and GET CONFIGURATION DATA do not have primitive support. This means that a chip with a shell application present will not be able to support those commands.

SELECT FILE Command

The command SELECT FILE permits a terminal to select an application, the Directory (DIR) or the Answer-To-Reset (ATR) files. In addition, the command SELECT FILE can be used by applications to access an internal file structure. The command always has a CLA byte of '00' and an INS byte of 'A4'. The P1 value determines how a file will be selected while the P2 value indicates if File Control Information (FCI) should be returned.

When no shell application is present MULTOS inspects every command and only passes the ones it can not handle to the selected application, if any. In some cases replicating this behavior exactly presents complex, low level difficulties. The use of a shell application is a serious step that replaces the operating system's command handling with a bespoke application. Unless it is absolutely necessary incurring additional difficulties is not advised.

To ensure the simplicity of operation, it is suggested that a shell application not support the selection of DIR or ATR files. In practice, this means that the shell application can consider SELECT FILE commands with a P1 value of '00', '02' or '08' as being application specific commands.

In addition, where there are standard applications also present on the chip it is suggested that any SELECT FILE command that has P1 P2 parameter values of '04 00', '04 02' or '04 0C' be reserved for application selection.

Note: The difficulties revolve around the use of CheckCase primitive at the shell level particularly when delegation is used. See the delegation how-to for a fuller discussion of this topic.

Note: If support for reading the Directory is included then the command READ RECORD must also be supported. Similarly reading the ATR is supported, then so must the command READ BINARY.

Selecting a Standard Application

In the case where standard applications are present and when a SELECT FILE command is identified as indicating the possible selection of a standard application, the shell application must handle the command. The steps involved are:

1. Determine if the selected application is present
2. If present, determine if File Control Information (FCI) should be returned
3. If present, return success indication and FCI, if any
4. If not present, send command to selected application
5. If not present and no other application is selected, return an error message

To determine if the application is present the shell application should read each record in the Directory (DIR) file until it either finds a record with the matching AID or reads all records without finding a match. If a match is found, the corresponding record number should be noted as it is used to locate the application's FCI.

Note: The above handling assumes that each standard application has a DIR entry that contains the AID.

Deselecting a Standard Application

If an application has been selected and the shell successfully handles SELECT FILE that selects another application, the first application's session has ended. Normally the operating system will clear that application's session data, but when a shell is present it must see that this is done.

MULTOS provides the primitive "Reset Session Data", which is available only to a shell application. When called the primitive erases the session data of all active standard applications.

Application Specific Commands

After an application is selected all commands, except SELECT FILE and any other command the shell is programmed to handle, must be sent to the selected application.

Get Response

During the normal course of operation MULTOS will attend to the low level communications handling. Occasionally, the terminal may send an unexpected GET RESPONSE command, which the operating system will pass to the shell. In this case, the command should be routed to the selected application or, if no application is selected, an error should be returned.

Other Things to Consider

From an OS point of view command handling is the most important role that the shell plays. There are some other areas where the presence of a shell application has an effect.

Status Word returned after selection

MULTOS provides a primitive called "Set Select SW", which allows an application to set the status word returned upon selection. Normally the SW is '9000'. However, an application may wish, for example, to indicate to a terminal that it is blocked by returning a specific status word. A shell application does not have access to this information and will simply indicate successful selection.

If a particular SW must be returned, the standard application (the delegate application) would need to ensure that it is done. One method would be to inform the shell of the expected SW and have the shell handle future selects appropriately. Another method would be for the standard application to include a persistent state variable so that if the application state was blocked, it would return the correct status word and not perform any disallowed processing.

ATR Historical Characters

A MULTOS card supports two types of ATR. They are:

- Primary ATR which is returned upon a cold reset
- Secondary ATR which is returned upon a warm reset

MULTOS provides default values for the historical bytes, but an ATR's historical bytes can be controlled by an application. However, when a shell is present it controls the historical bytes of all ATR.

Writing a Shell Application

A shell application exists and executes within the MULTOS virtual machine. This means that a shell application can be developed just like any other application.

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