Enablement

MAO-DOC-TEC-101 v1.4

Contents

Enablement Data

The purpose of this article is to put enablement into context, explain what takes place during enablement and finally discuss how to transmit enablement data to the card.

Note: Enablement Data is often referred to as MSM Controls Data or MSM CD.

Understanding Enablement

When a MULTOS chip is manufactured it does not belong to an issuer and as a consequence is not configured to process application loading and deleting. The chip has a unique ID, its MULTOS Carrier Device (MCD) ID, and a set of chip specific symmetric transport keys. The chip is said to be in protected state.

When an issuer purchases MULTOS chips and wishes to deploy them, the first thing to do is to enable them. This binds the chip irrevocably to the issuer and allows the issuer only to load and delete applications.

What's in Enablement Data?

The main elements of enablement data are:

- Issuer ID
- MCD Number
- Product ID
- Communications settings
- MULTOS Public Key Certificate MKD_PK_C
- MULTOS Private Key MKD_SK

The Issuer ID is one of the most important data elements updated during enablement. This issuer unique value is embedded and signed in every request to the KMA. During loads and deletes it is one of the first elements checked. If the certificate does not contain the same value, the load or delete will not take place.

Prior to enablement the chip is identified by the MCD ID, but after it is the MCD Number that is used. This is important as it plays a role in confidential loads.

The Product ID allows issuers to segregate their card base as they see fit. This value can also be used to target certificates at particular products. For example, a gold card program cardholder may have access to a special, say, loyalty application. If all gold cards have the same product ID (or share a range of ID), then a load certificate can be created that would only allow those chips to load the application.

For a contact interface the communication settings are held in the Answer-To-Reset (ATR) value. Here the chip announces its preferred transport protocol(s), communications speed and other information. Once set at enablement this can not be changed at all during the lifetime of the chip.

Another important change that takes place at enablement is the replacing of the symmetric transport keys by an asymmetric key pair. The chip's public key is made available in a certified format and that key is used during confidential loads.
[loading of asym keys for load/delete, transport keys still present but never used again]

There are many other things that are included in MSM Controls Data, but they affect low level activities and are not generally visible.

Enablement Data is encrypted

As mentioned earlier each card has its own unique set of symmetric transport keys. The key values are derived from the chip's MCD ID. When enablement data for a chip is generated the KMA system derives the MCD specific keys and encrypts all the data. Only the target MCD can decrypt it and use it.

How to obtain Enablement Data

Enablement data must be requested online from the MULTOS Key Management Authority (KMA) using StepXpress (https://www.stepxpress.com/).

A list of MCD IDs for which the issuer wants MSM Controls Data is submitted. The list is checked for internal duplication (that is, two listings of the same MCD ID in the list). If there are no duplicates, the list is processed and MSM Controls Data is made available for download to the issuer.

How to enable a card

The process of card enablement is based on the use of the command SET MSM CONTROLS. However, prior to using some preparatory work needs to be performed. The steps to perform are:

- Optionally, check if the chip is already enabled using the GET MULTOS DATA command – see below (only use where there is the possibility of this having happened).
- Read the MSM Controls Data file header and locate the length of an individual MSM CD record
- Read the MCD ID from the target MULTOS chip
- Locate the corresponding MSM CD record, which is indexed by MCD ID
- Extract the MSM CD record
- Prepare SET MSM CONTROLS command(s)

The amount of MSM CD in a record will be longer than the maximum command data permitted in a single APDU. Therefore, the enablement data must be broken into APDU command size chunks so that it can be transmitted to the card.

The command SET MSM CONTROLS always uses the same CLA, INS, P1 and P2 value. This means that there is no explicit start, block order or end sequence visible to the chip at APDU level. This has two consequences, which are:

- The total length of the enablement data as indicated in the MSM CD file header must be included as the first two bytes of the very first SET MSM CONTROLS command. Note that the length value is used as-is and does not count its self as part of the total length.
- The enablement data must be sent in order; i.e., block 1 must be the start of the data and block 2 must be the data that immediately follows in the MSM CD file.

When the commands are prepared they are transmitted to the MCD. Note that command preparation may be done on the fly. So, the enablement equipment may generate one command after another in real time. If any command reports an error condition, the enablement process is stopped.

GET MULTOS DATA Command

The command APDU is as described in the table below.

Field	Value	Comment
CLA	'80'	Always same value
INS	'00'	Always same value
P1	'00'	Always same value
P2	'00'	Always same value
Lc	-	Not present
Command Data	-	Not present
Le	7F	Always same value

This command always returns the status word '90 00'.

The data returned is

Field	**Size (bytes)**
MULTOS Version Number	2
IC Manufacturer ID	1
Implementer ID	1
MCD ID	6
Product ID	1
Issuer ID	4
MSM Controls Data Date	1
MCD Number	8
RFU	80
Maximum Dynamic Size	2
Maximum Public Size	2
Maximum DIR File Record Size	2
Maximum FCI Record Size	2
Maximum ATR Historical Byte Record Size	2
Maximum ATR File Record Size	2
MULTOS Public Key Certificate Length	2
Security Level*	1
Certification Method ID	2
Application Signature Method ID	2
Encipherment Descriptor	2
Hash Method ID	2

*The value of **Security Level** is '5A' when the card is enabled. Any other value means that the card is not yet enabled.

SET MSM CONTROLS Command

The command APDU is as described in the table below.

Field	Value	Comment
CLA	'BE'	Always same value
INS	'10'	Always same value

P1	'00'	Always same value
P2	'00'	Always same value
Lc	xx	Length of data
Command Data		Enablement data of size Lc
Le	-	Not present

As with any command if it is successful the returned status word will be '90 00'. There are several error conditions that may arise.

'9D40' Invalid MSM Controls Ciphertext

If this error is given in response to the very first command, the chip does not accept the total length of MSM CD, as indicated in the first two bytes of the command data, as valid. The reasons this would arise is that the length is:

- Less than a platform defined minimum
- Greater than a platform defined maximum
- Not an integer multiple of eight (8)

After the first command it is the catch all error for failed enablement. There are several reasons why this error would arise. The most likely are too much data has been transmitted or the cryptographic verification has failed.

To verify if too much data has been sent check the first two bytes of the first command sent as these indicate the total length of the enablement data that should have been transmitted. If the actual amount sent is greater, then too much has been sent. To fix this simply change the total, length bytes to the correct value and begin the enablement commands transmission again.

Note that if insufficient data is sent no error is signalled. The chip will continue to wait for more data until a reader time out occurs.

The cause of failed cryptographic verification is more difficult to diagnose. Check that the data transmitted corresponds to the MCD to which it was transmitted. If so, check that the data transmitted is exactly what was in the file. In some cases an APDU level log is not enough to catch the problem and a lower level log may be required.

'9D41' MSM Controls Already Set

A MULTOS chip can generally only be enabled once*. If after a successful enablement the command is sent, the chip will reject it and send this status word. Note that once a chip is enabled it can not be disabled nor can the data set be changed.

* As of MULTOS 4.5 it is possible for MULTOS devices (where supported) to initially be enabled using step/one methods and later be re-enabled using full MULTOS methods.

Related Materials

The document entitled "MULTOS KMA File Interface Formats (External)" provides field level descriptions of the MSM CD request and response files.

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