MCH100 Magnetic Card Reader
USB Interface-Keyboard

Setting AP
Simple User Guide
For DUKPT Key Loading

UIC Document No.: TM099-S Revision C
November 03, 2014

Simple User Guide for DUKPT Key Loading

The following steps illustrate how to make the output encryption function work after the user received a brand new MCH100 from the supplier. MCH100 won't output the payment card data in encrypted form until the initial DUKPT key has been loaded. The initial DUKPT key can be loaded in either clear text or ANSI TR-31 format. However, once the initial DUKPT key is loaded via ANSI TR-31 format, MCH100 is not allowed to accept clear text format for the DUKPT key loading.

From the viewpoint of product life cycle, MCH100 will go through several phases in relation to key management. The phase number will be increased automatically according to the conditions on key loading operation, but doesn't have to move sequentially one increment at a time.

Phase	Key Loading Key	DUKPT Key	Security	Remark
Phase 0	Empty	Initial DUKPT key can be loaded or reset to empty for MFG testing purpose.	Card data can be encrypted or unencrypted according to the existence of DUKPT key.	Phase 0 can be seen only in the factory.
Phase 1	factory default*	Initial DUKPT key has **not** been loaded.	No authentication is required for initial DUKPT key loading; Card data is **not** encrypted.	The initial DUKPT key loading needs to be performed in clear text because the Key Loading Key has not been updated yet.
Phase 2	factory default*	Initial DUKPT key has been loaded.	No authentication is required for initial DUKPT key loading; Card data is encrypted**.	The initial DUKPT key updating needs to be performed in clear text because the Key Loading Key has not been updated yet.
Phase 3	updated (different than the factory default)	Initial DUKPT key has **not** been loaded	No authentication is required for initial DUKPT key loading; Card data is **not** encrypted.	The initial DUKPT key loading can be performed in clear text or in ANSI TR-31 format.

Phase 4	updated (different than the factory default)	Initial DUKPT key has been loaded only via clear text format (not via ANSI TR-31 format).	No authentication is required for initial DUKPT key loading; Card data is encrypted**.	The initial DUKPT key loading can be performed in clear text or in ANSI TR-31 format.
Phase 5	updated (different than the factory default)	Initial DUKPT key has been loaded via ANSI TR-31 format.	Authentication is needed for initial DUKPT key loading; Card data is encrypted**.	The initial DUKPT key loading needs to be performed in ANSI TR-31 format.
Phase 6 (Terminated)	factory default	Key generation reaches to the end	No more card reading operation will be performed.	The reader reached the end of its lifetime.
	updated (different than the factory default)			

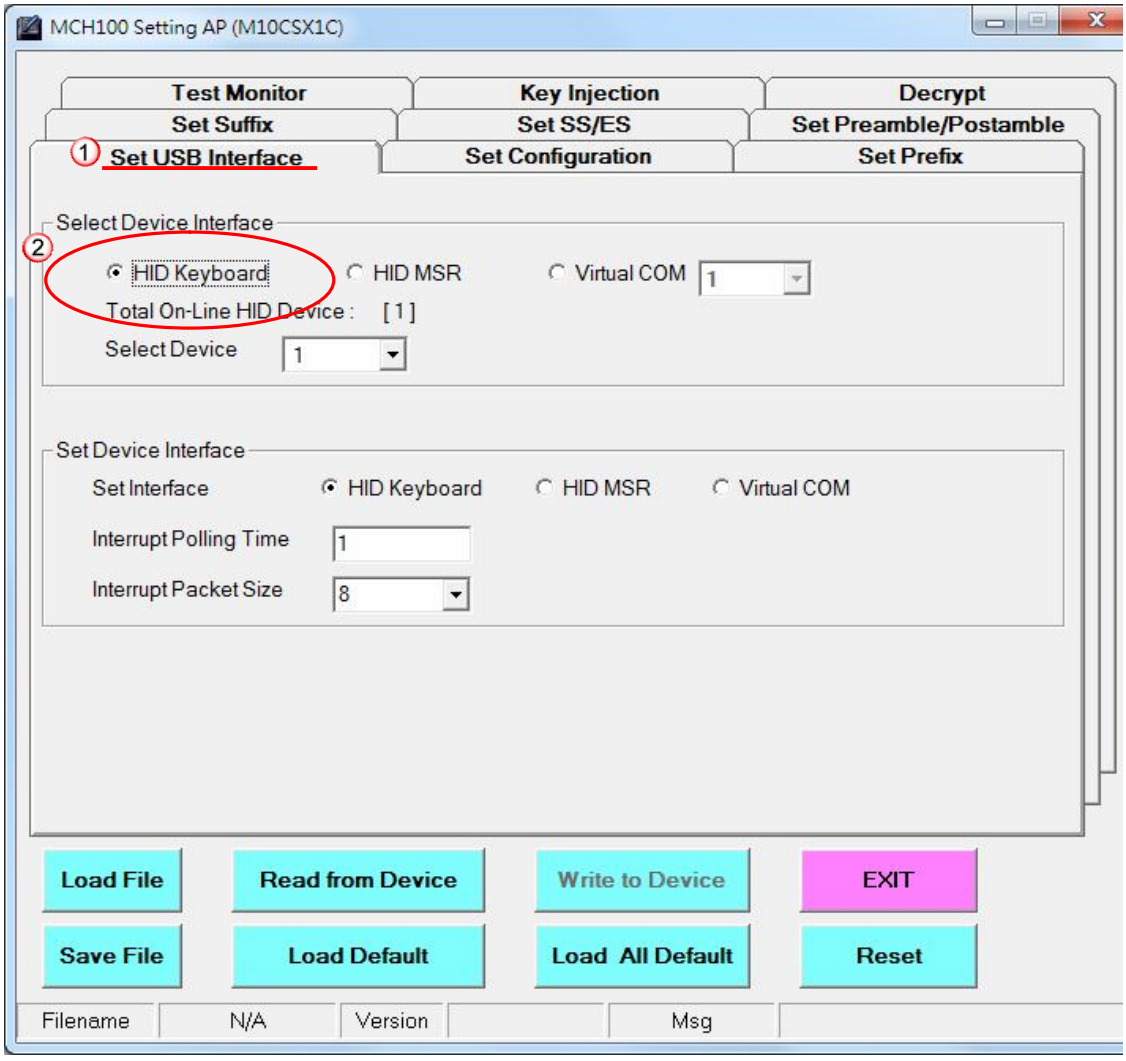
* Before the Key Loading Key is loaded, the initial DUKPT key loading is not allowed to be performed in ANSI TR-31 format.

** Only the payment card data that can pass the Luhn check (also known as the mod 10 check) will be encrypted. For non-payment cards, which are unable to pass Luhn check, the card data won't be encrypted.

➢ Load DUKPT Key in clear text format

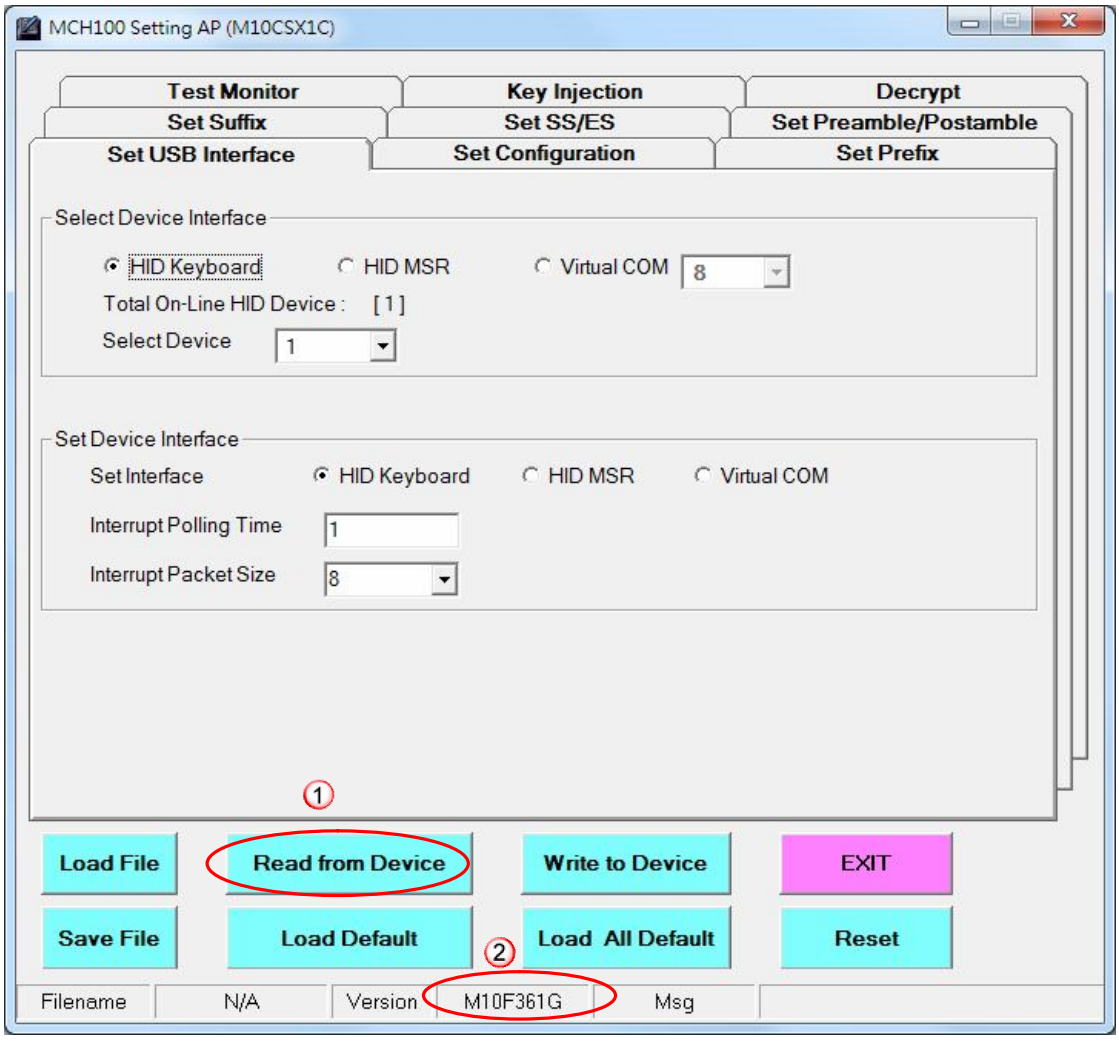
The initial DUKPT key can be loaded into MCH100 in clear text format only when no initial DUKPT key has been loaded via ANSI TR-31 format. Once the initial DUKPT key is loaded via ANSI TR-31 format, MCH100 is not allowed to accept clear text format for the DUKPT key loading operation.

	Action
Step 1	1. Open "Set USB Interface" panel. 2. Select device interface: HID Keyboard.



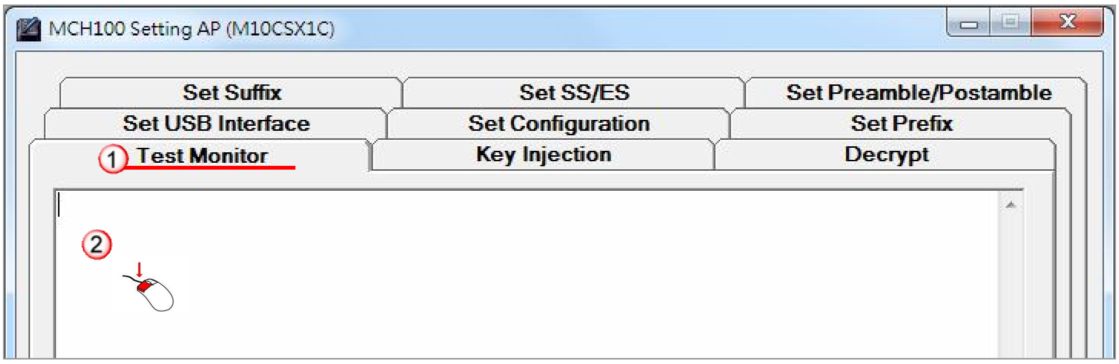
Step 2

1. Click the “Read from Device” button.
2. If successful, the F/W version will be displayed on the bottom middle of the screen.

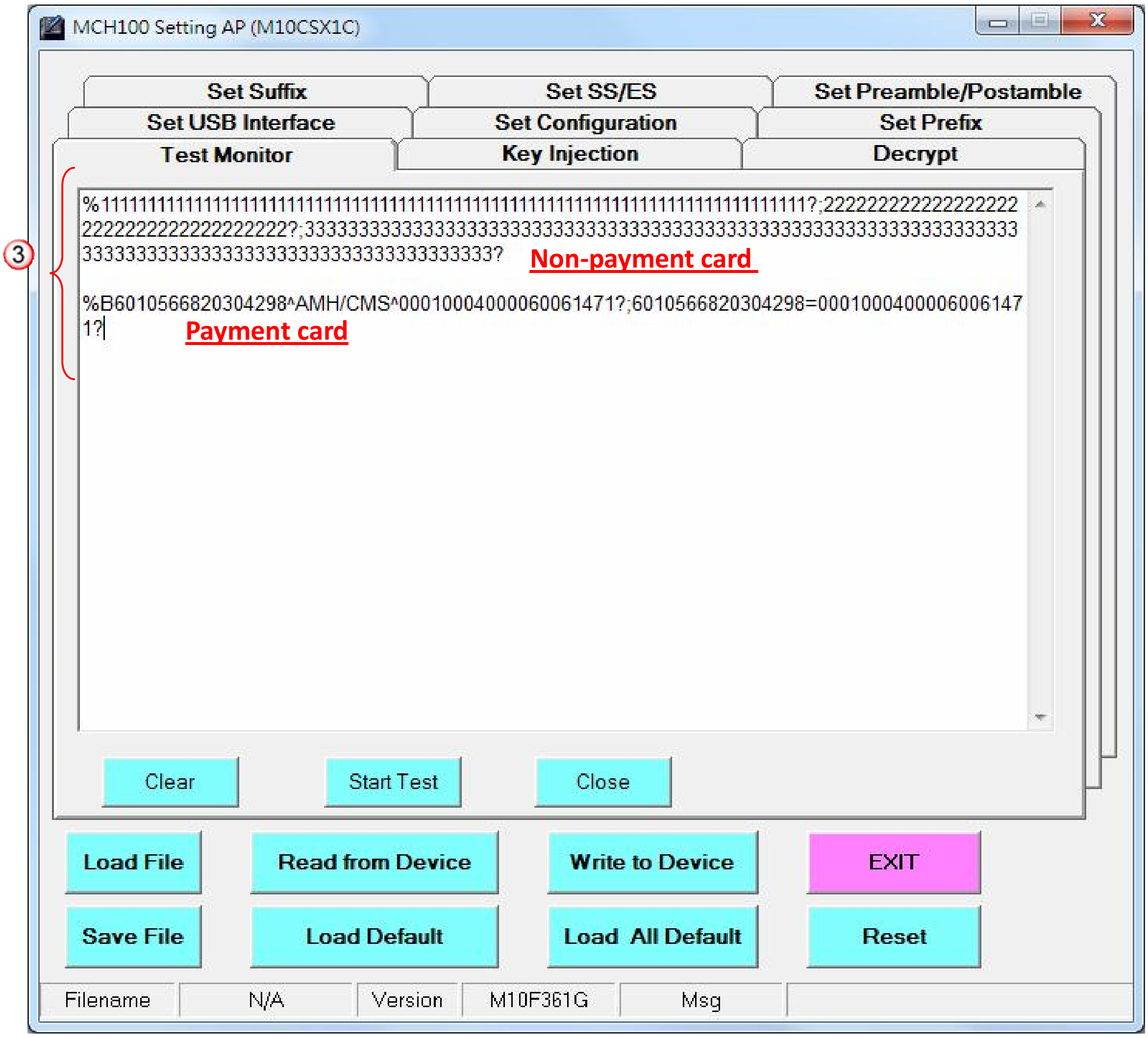


Step 3 Before the "Initial DUKPT Key" is loaded, the reader won't encrypt the card data. The user can follow the following steps to get the card data:

1. Open "Test Monitor" panel.
2. Click mouse button on display area. Let the cursor stays on the screen.

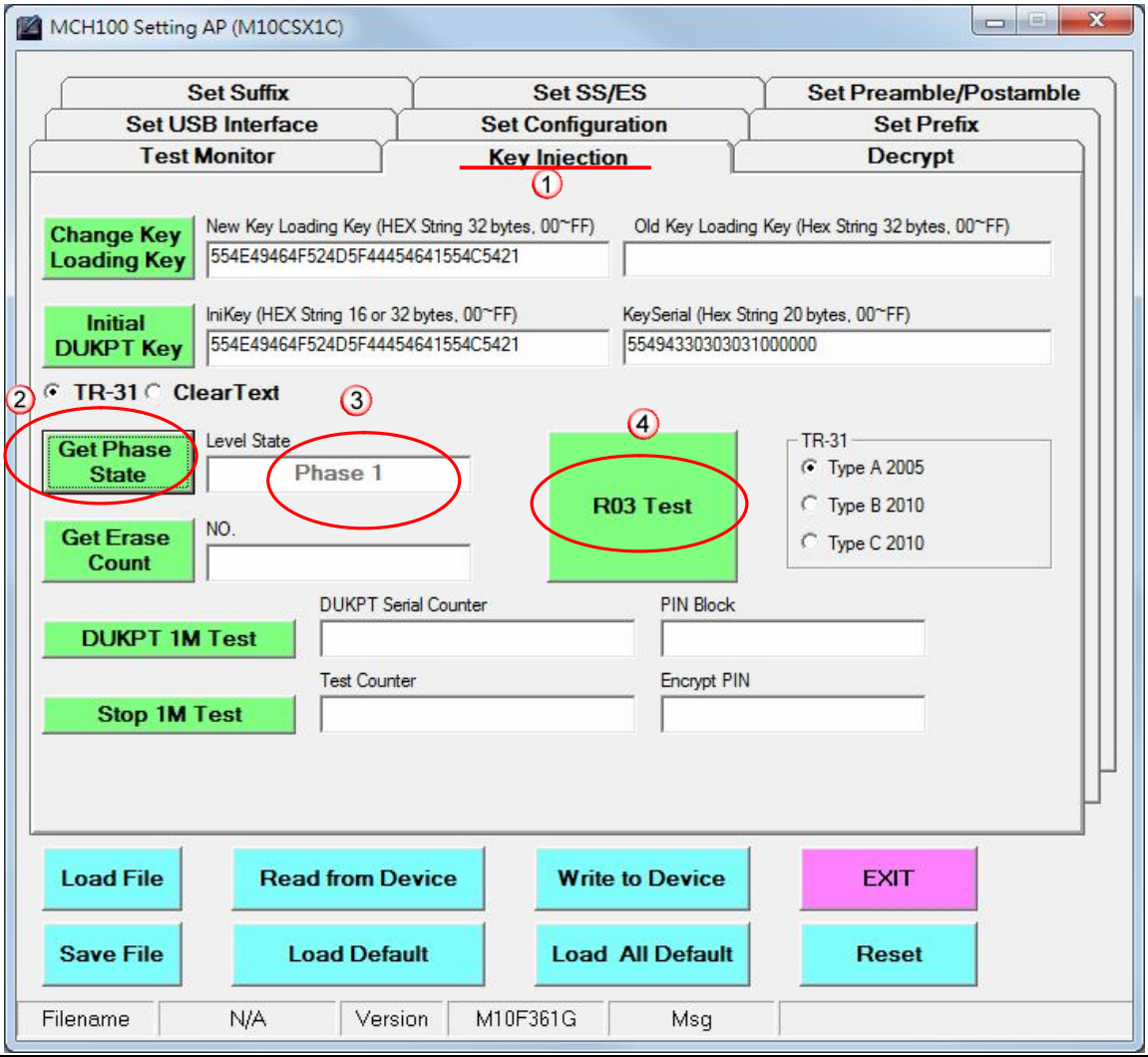


3. Swipe a card and the card data will be shown on the screen.



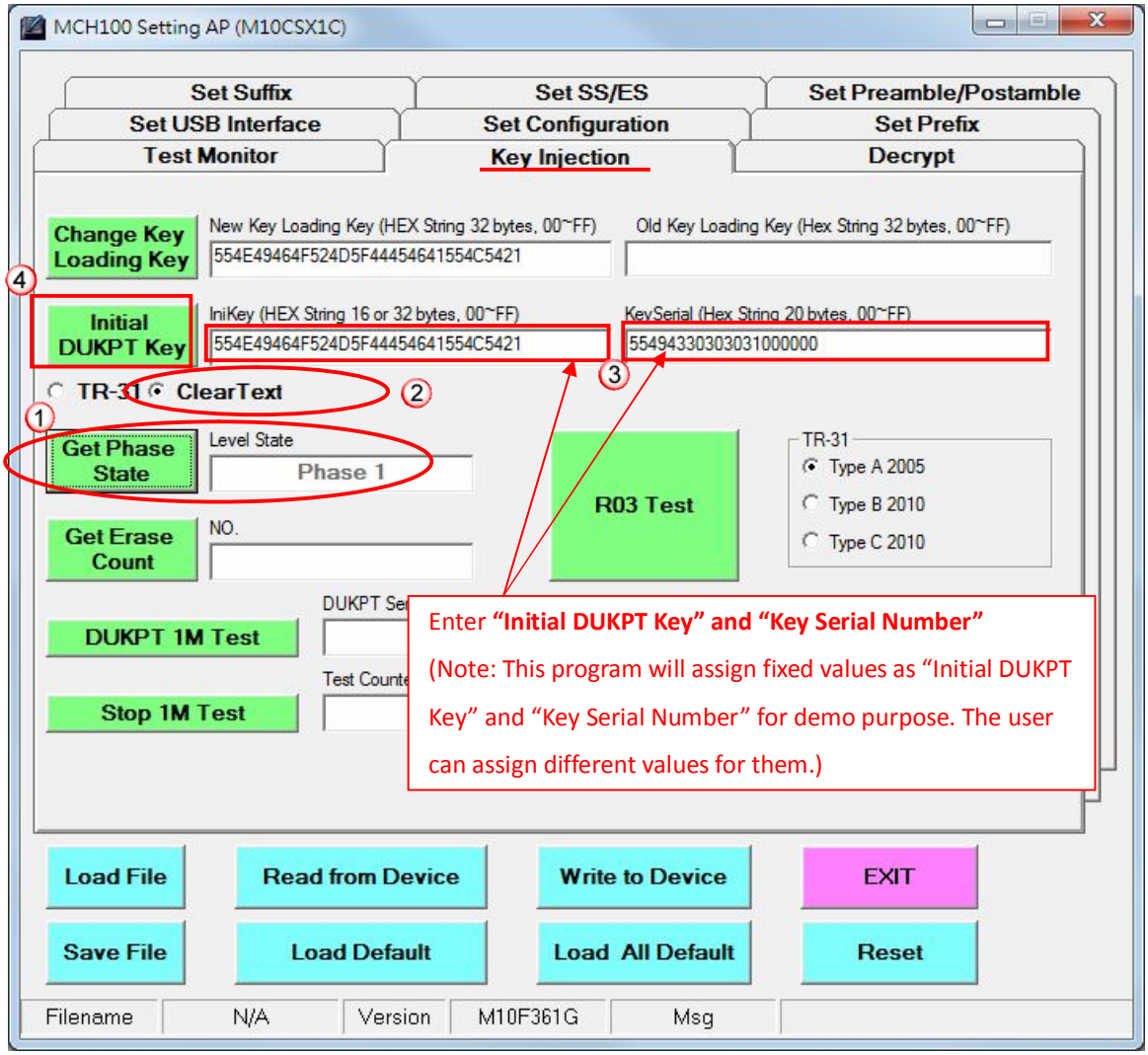
Step 4 Check phase state:

1. Open “Key Injection” panel.
2. Click “Get Phase State” button.
3. For a brand-new MCH100, clicking “Get Phase State” button will get “Phase 1” message. Skip the following operation if “Phase 1” message is displayed after clicking “Get Phase State” button.
4. If “Phase 0” shows up, click “R03 Test” button to move forward to “Phase 1”. (Don’t forget to click “Get Phase State” button to get the updated message.)
   (Note: If MCH100 is not running in “Phase 0”, clicking “R03 Test” button will pop up a small screen showing “Key Initial Fail” message.)



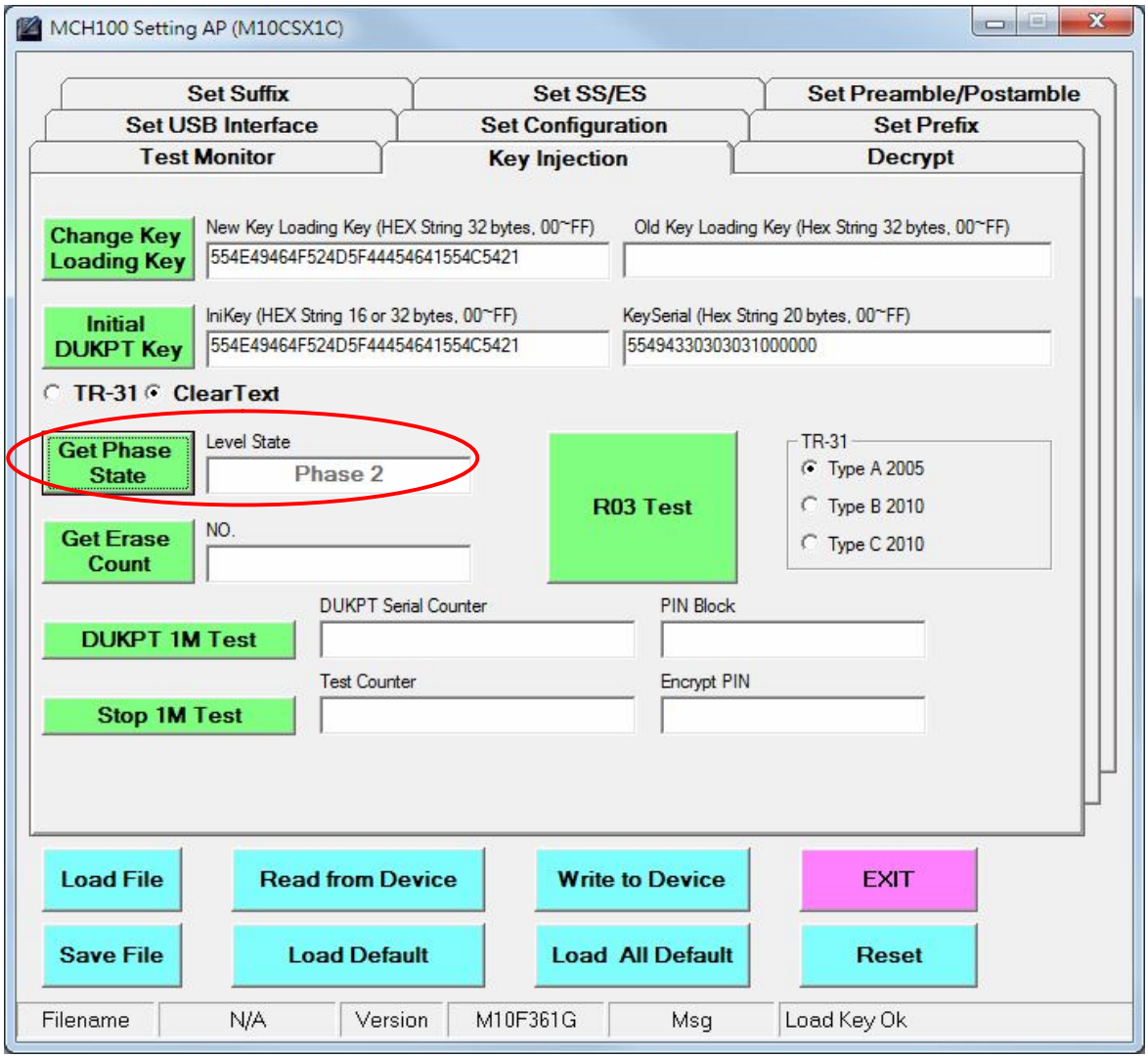
Step 5 Load "Initial DUKPT Key" and "Key Serial Number" in clear text.

1. Click "Get Phase State" button, and you will get "Phase 1".
2. Click "Clear Text" button.
3. Enter "Initial DUKPT Key" and "Key Serial Number". (Note: This program will assign fixed values as "Initial DUKPT Key" and "Key Serial Number" for demo purpose. The user can assign different values for them.)
4. Click "Initial DUKPT Key" button.



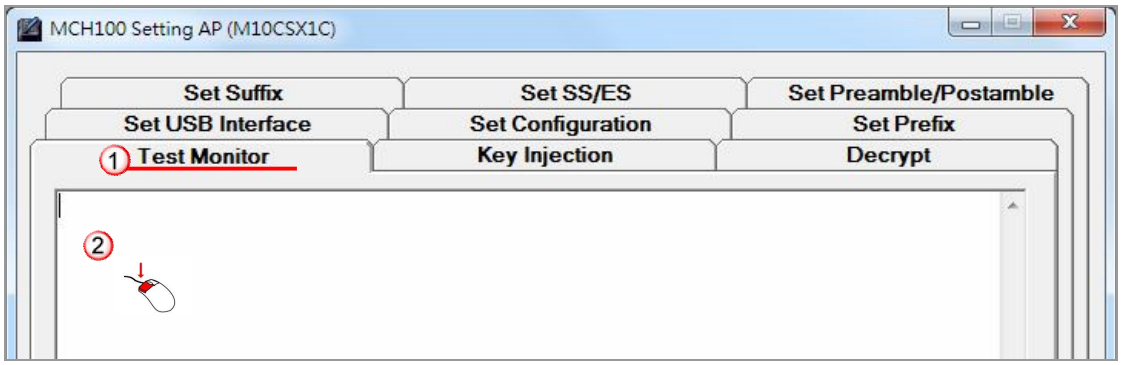
5. If changing key successfully, "Load Key OK" will show up at the bottom right of the screen.

6. Click “Get Phase State” button, and you will get “Phase 2”.

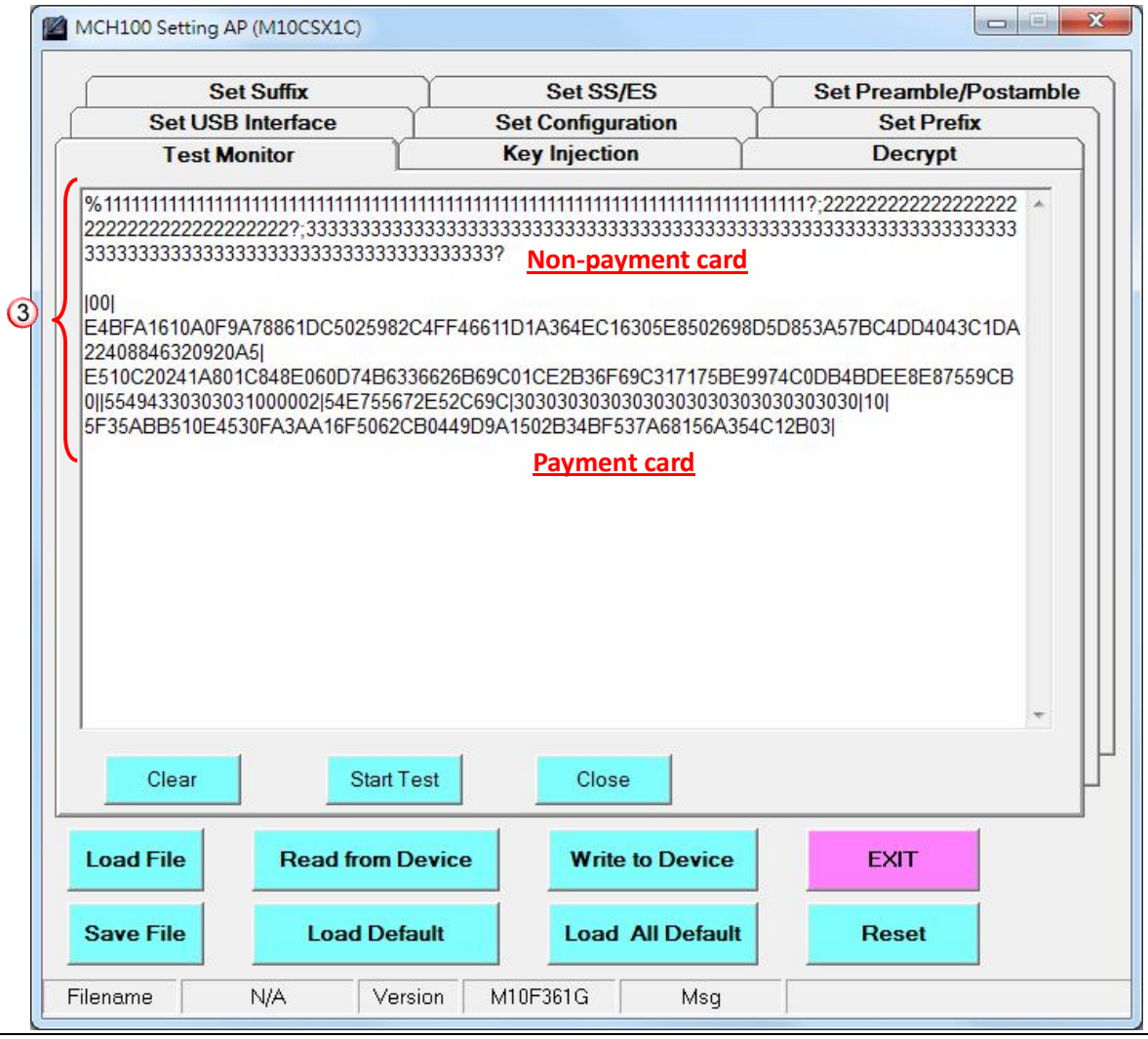


Step 6 After the Initial DUKPT Key has been loaded, the reader is able to encrypt the card data. The reader will automatically encrypt the payment card data that can pass the Luhn check (also known as the mod 10 check). For non-payment card, which are unable to pass Luhn check, the card data won't be encrypted. Follow the following steps to get the card data:

1. Open "Test Monitor" panel.
2. Click mouse button on display area. Let the cursor stays on the screen.



3. Swipe a card and the card data will be shown on the screen.

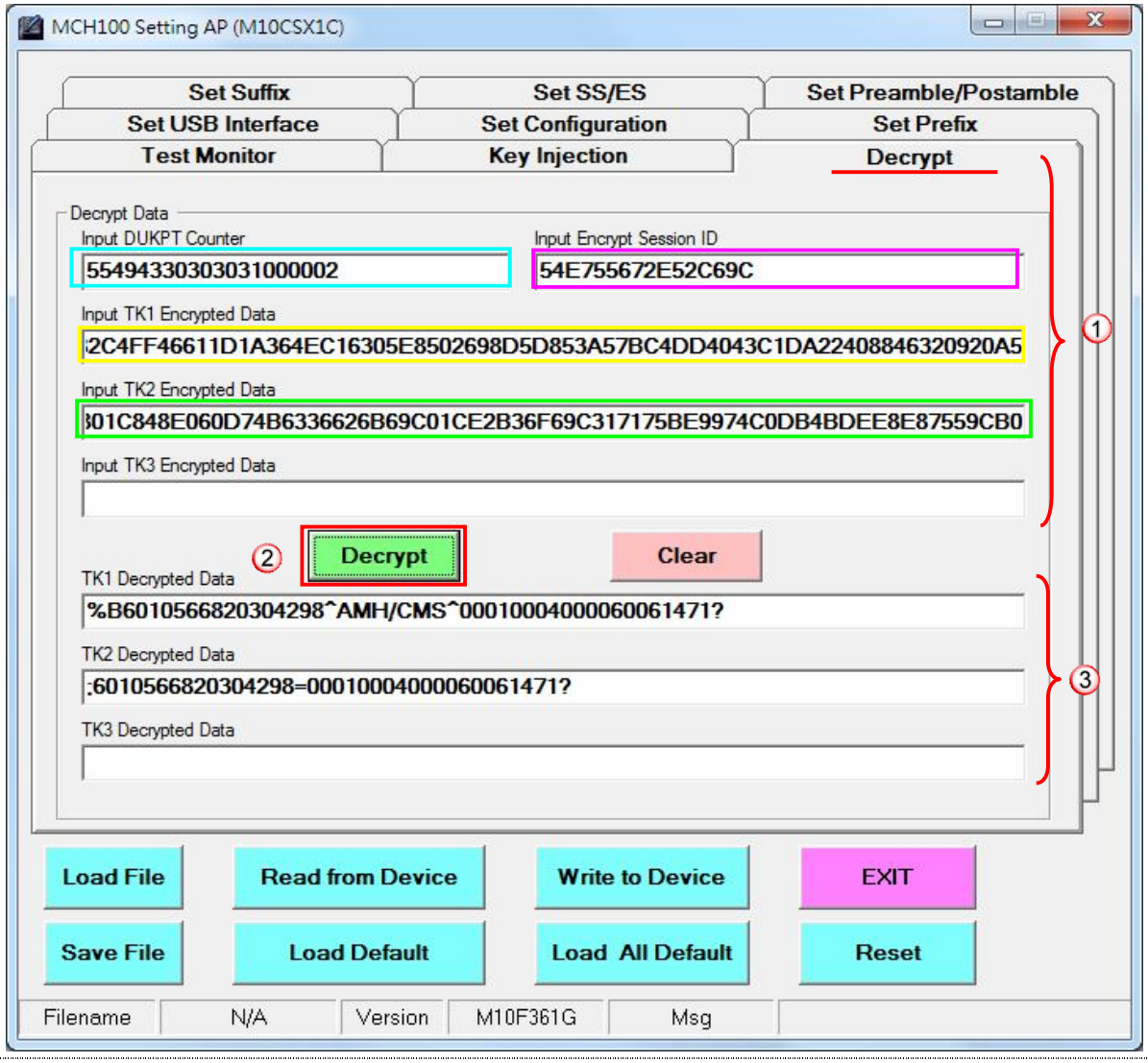


Step 7

1. Copy the encrypted output data from “Test Monitor” screen and paste them to corresponding fields on “Decrypt” panel.
2. Press “Decrypt” button to show the result of decrypted card data.
3. The decrypted data are then shown on the corresponding fields.

In this case, the payment card data are as follows:

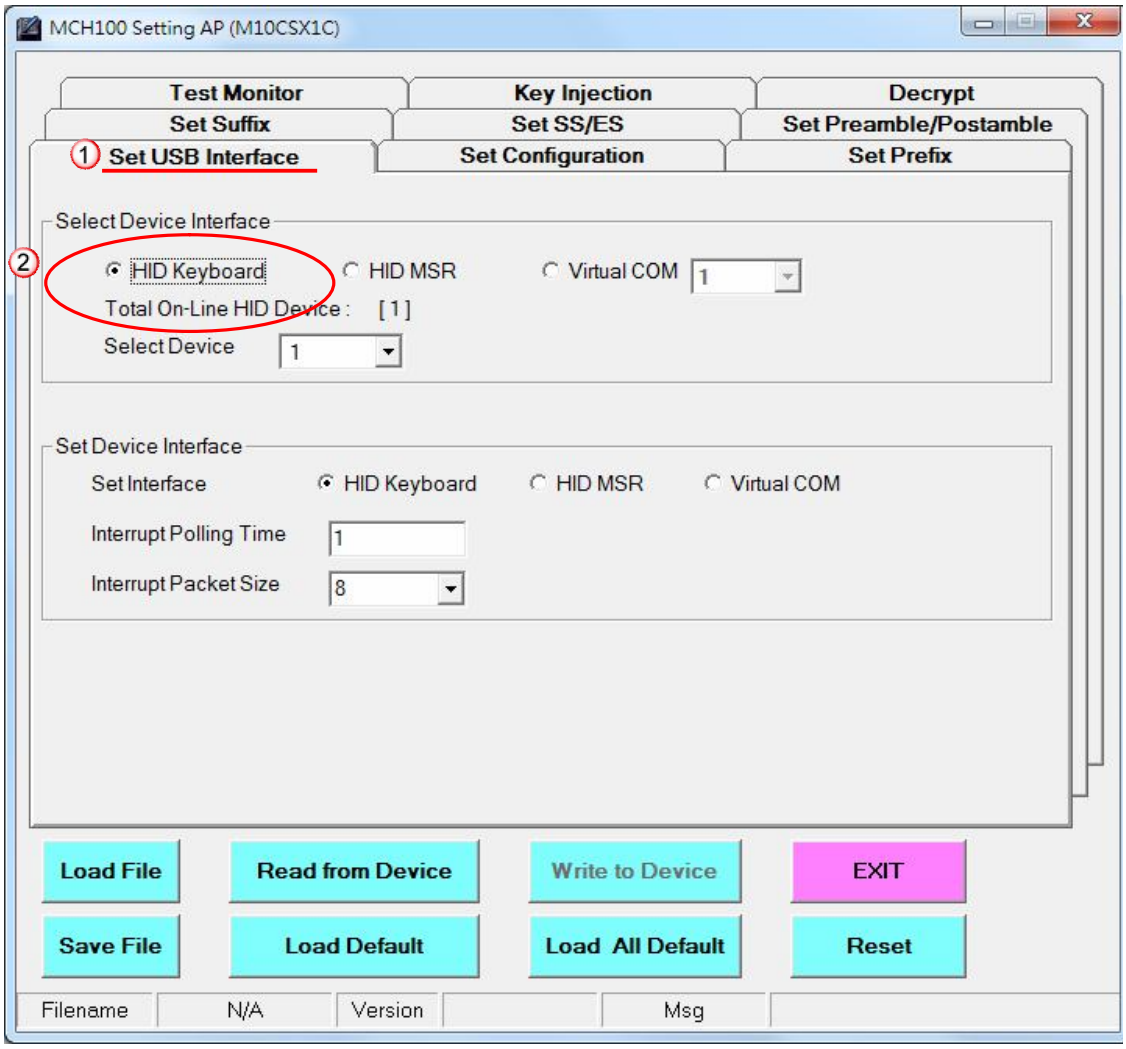
|00|
E4BFA1610A0F9A78861DC5025982C4FF46611D1A364EC16305E8502698D5D853A57BC4DD4043C1DA
ED0B14244399FEE77597949A0325903C4CB1630CD3B3F532|
E510C20241A801C848E060D74B6336626B69C01CE2B36F69C317175BE9974C0DB4BDEE8E87559CB
0||5549433030303100000 2|54E755672E52C69C|30303030303030303030303030303030|10|
5F35ABB510E4530FA3AA16F5062CB0449D9A1502B34BF537A68156A354C12B03|



➢ Load DUKPT Key in TR-31 format

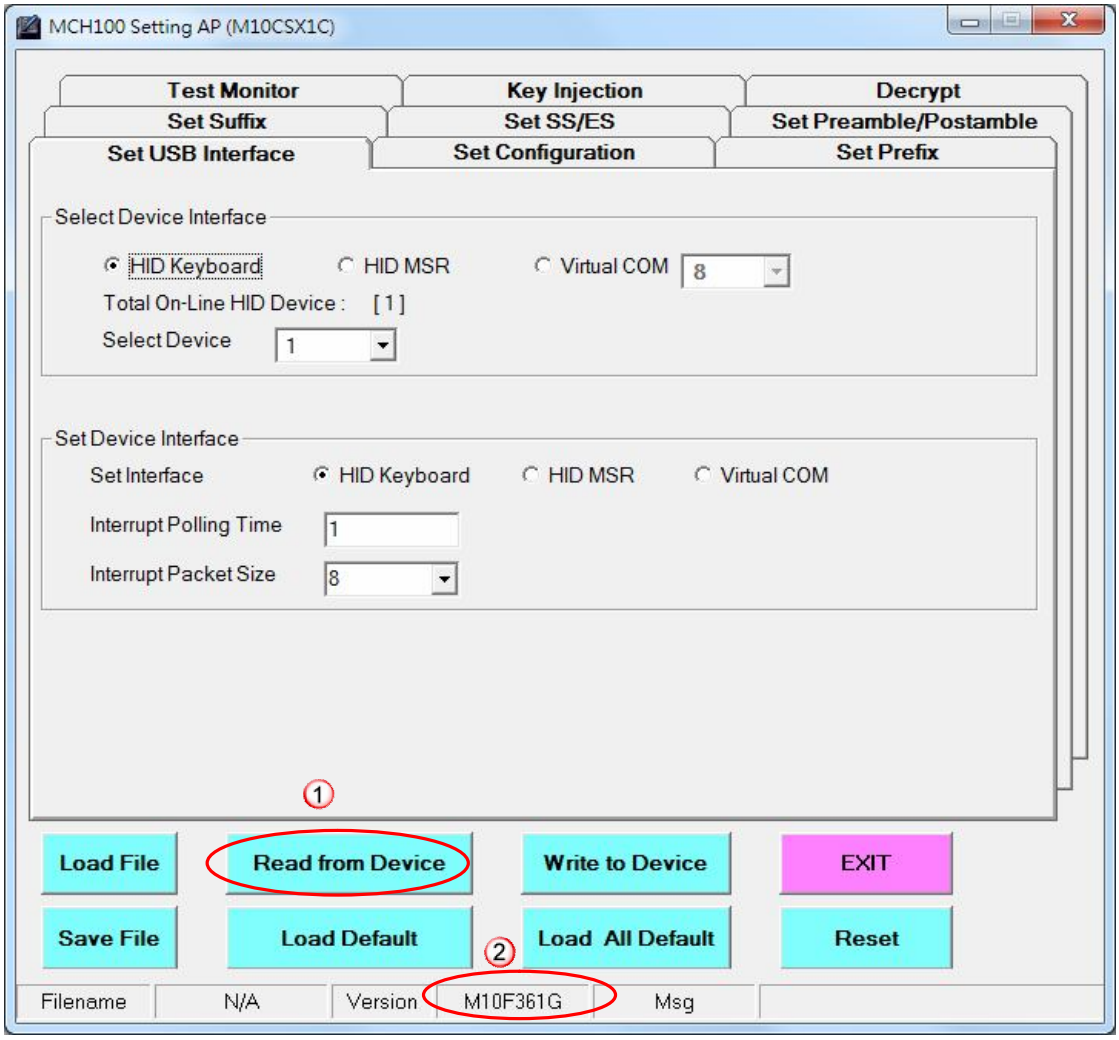
To load the key in TR-31 format, the factory default “Key Loading Key” has to be changed to a new one (different than the factory default). The following steps illustrate how to load the initial DUKPT key in ANSI TR-31 format.

	Action
Step 1	1. Open “Set USB Interface” panel. 2. Select device interface: HID Keyboard.



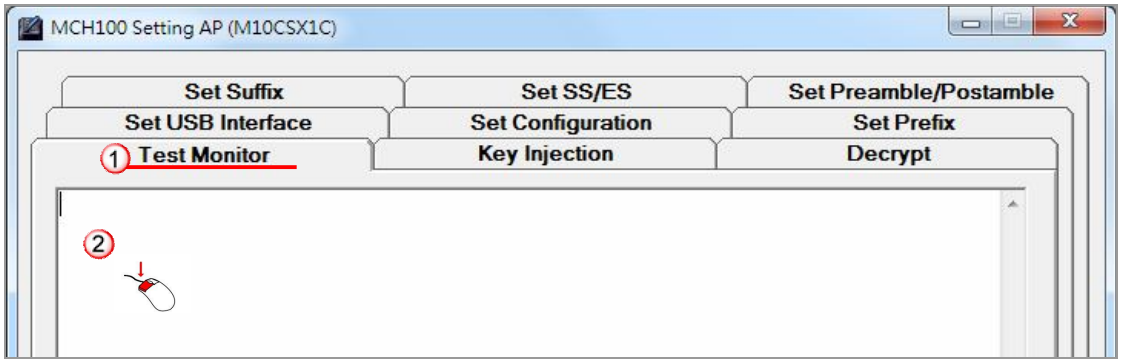
Step 2

1. Click the “Read from Device” button.
2. If successful, the F/W version will be displayed on the bottom middle of the screen.

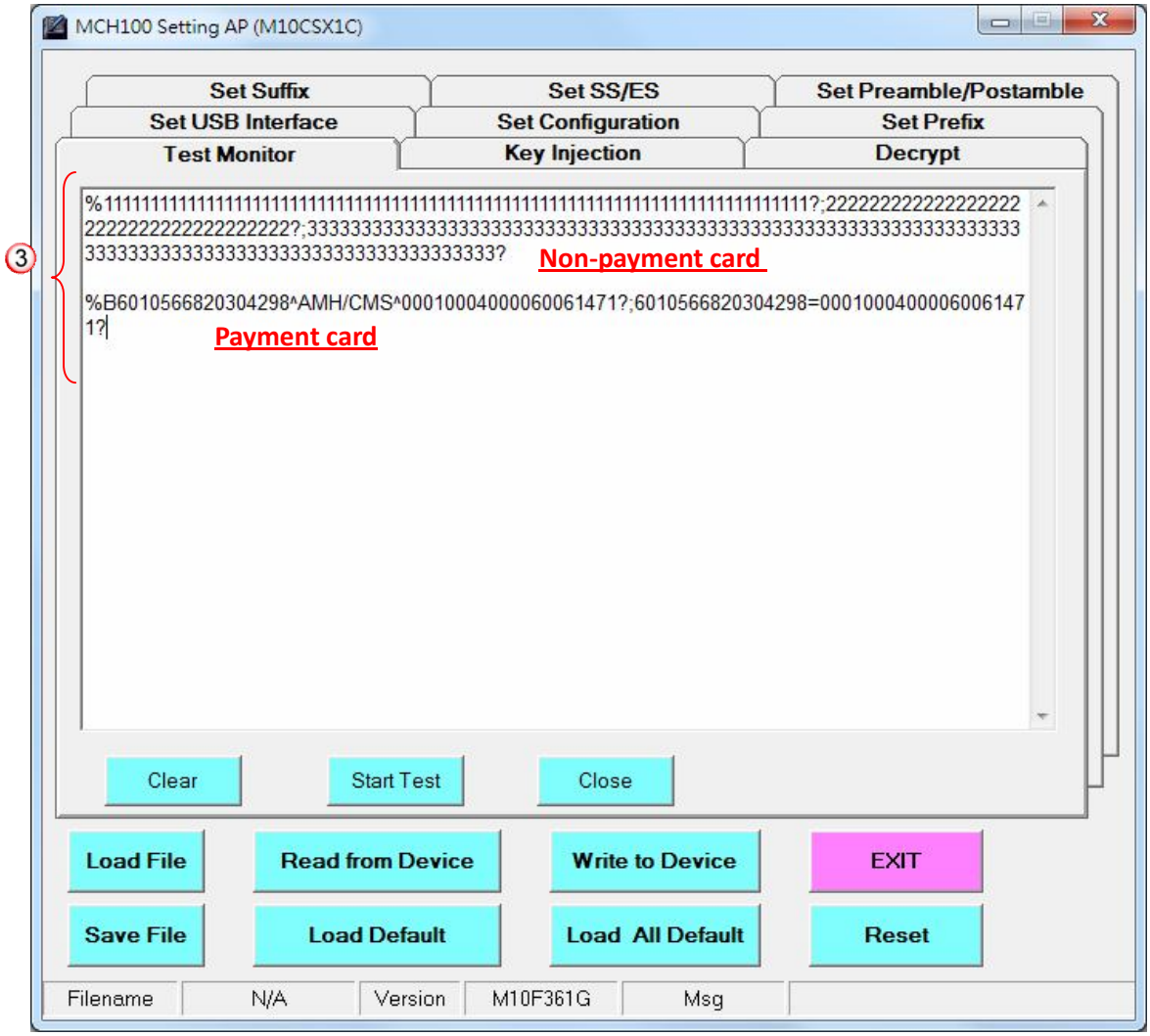


Step 3 Before the "Initial DUKPT Key" is loaded, the reader won't encrypt the card data. The user can follow the following steps to get the card data:

1. Open "Test Monitor" panel.
2. Click mouse button on display area. Let the cursor stays on the screen.

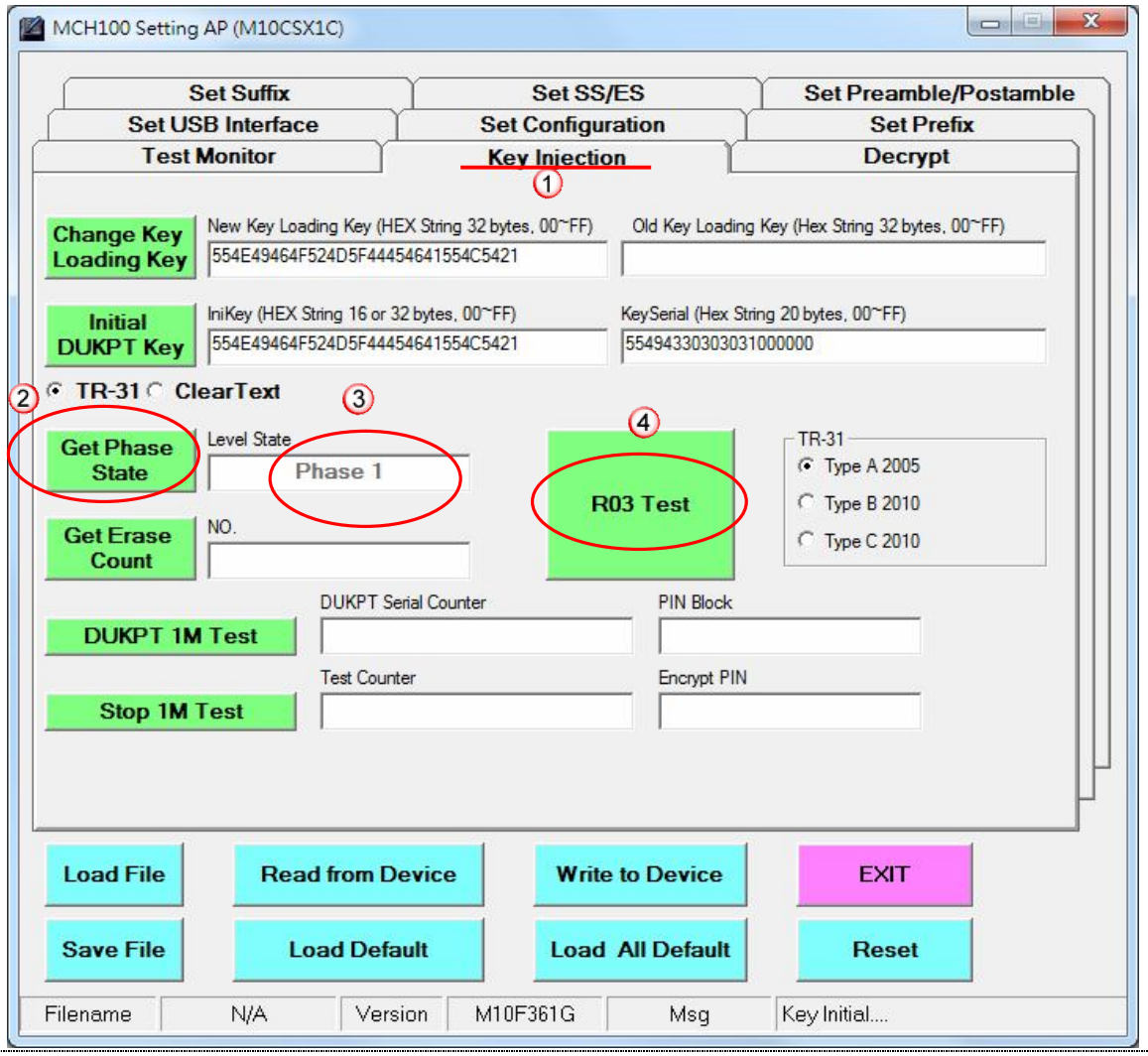


3. Swipe a card and the card data will be shown on the screen.



Step 4 Check phase state:

1. Open “Key Injection” panel.
2. Click “Get Phase State” button.
3. For a brand-new MCH100, clicking “Get Phase State” button will get “Phase 1” message. Skip the following operation if “Phase 1” message is displayed after clicking “Get Phase State” button.
4. If “Phase 0” shows up, click “R03 Test” button to move forward to “Phase 1”. (Don’t forget to click “Get Phase State” button to get the updated message.)
   (Note: If MCH100 is not running in “Phase 0”, clicking “R03 Test” button will pop up a small screen showing “Key Initial Fail” message.)

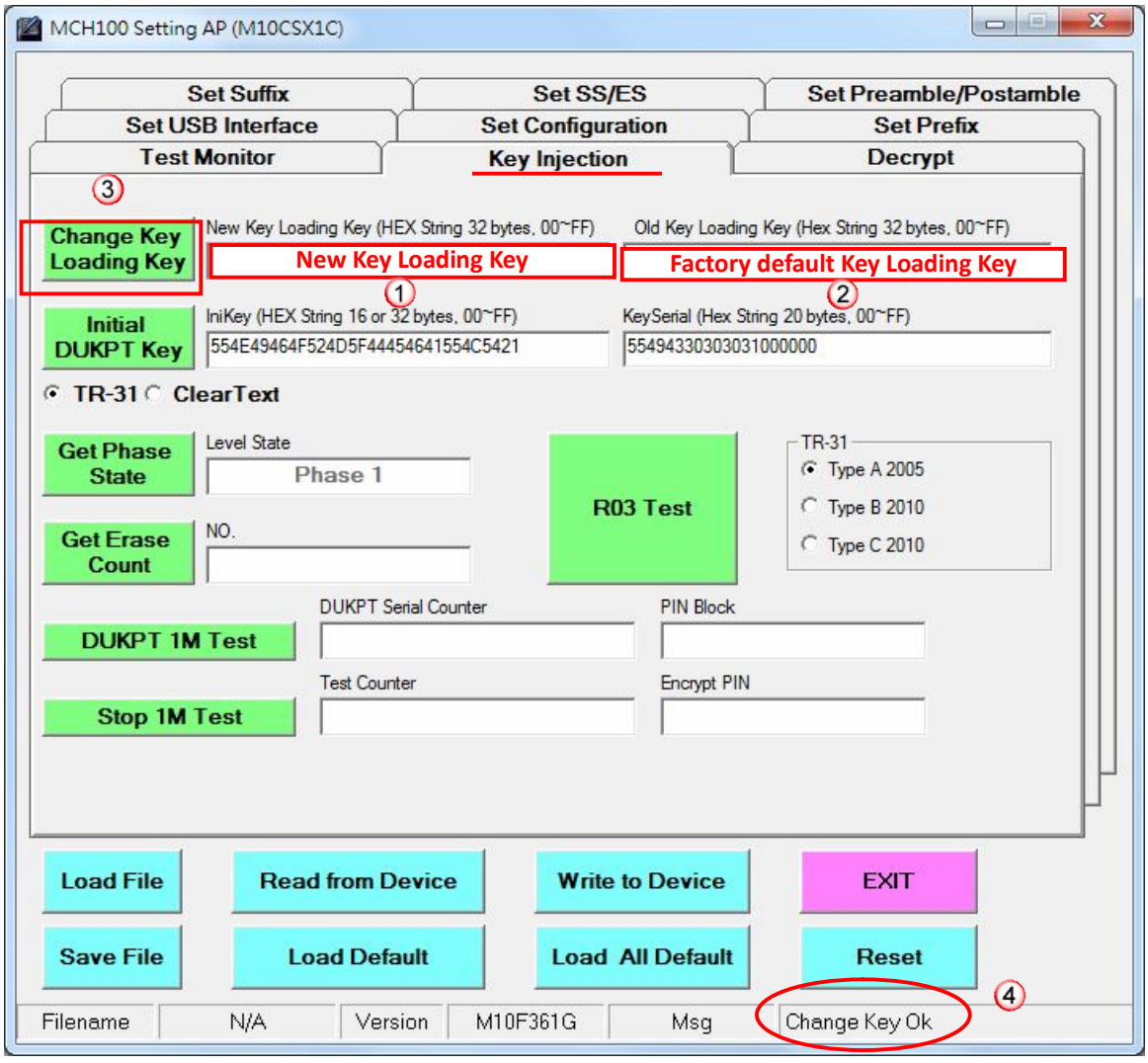


Step 5 Replace the factory default "Key Loading Key" with a new one:

In order to enable the Remote Key Update capability, after receiving the reader from the supplier, the user has to replace the factory default "Key Loading Key" with a new one via a secure computer in a secure environment, and keep the new "Key Loading Key" in a secure place to protect it from unauthorised access. The user can follow the following procedure to change the "Key Loading Key":

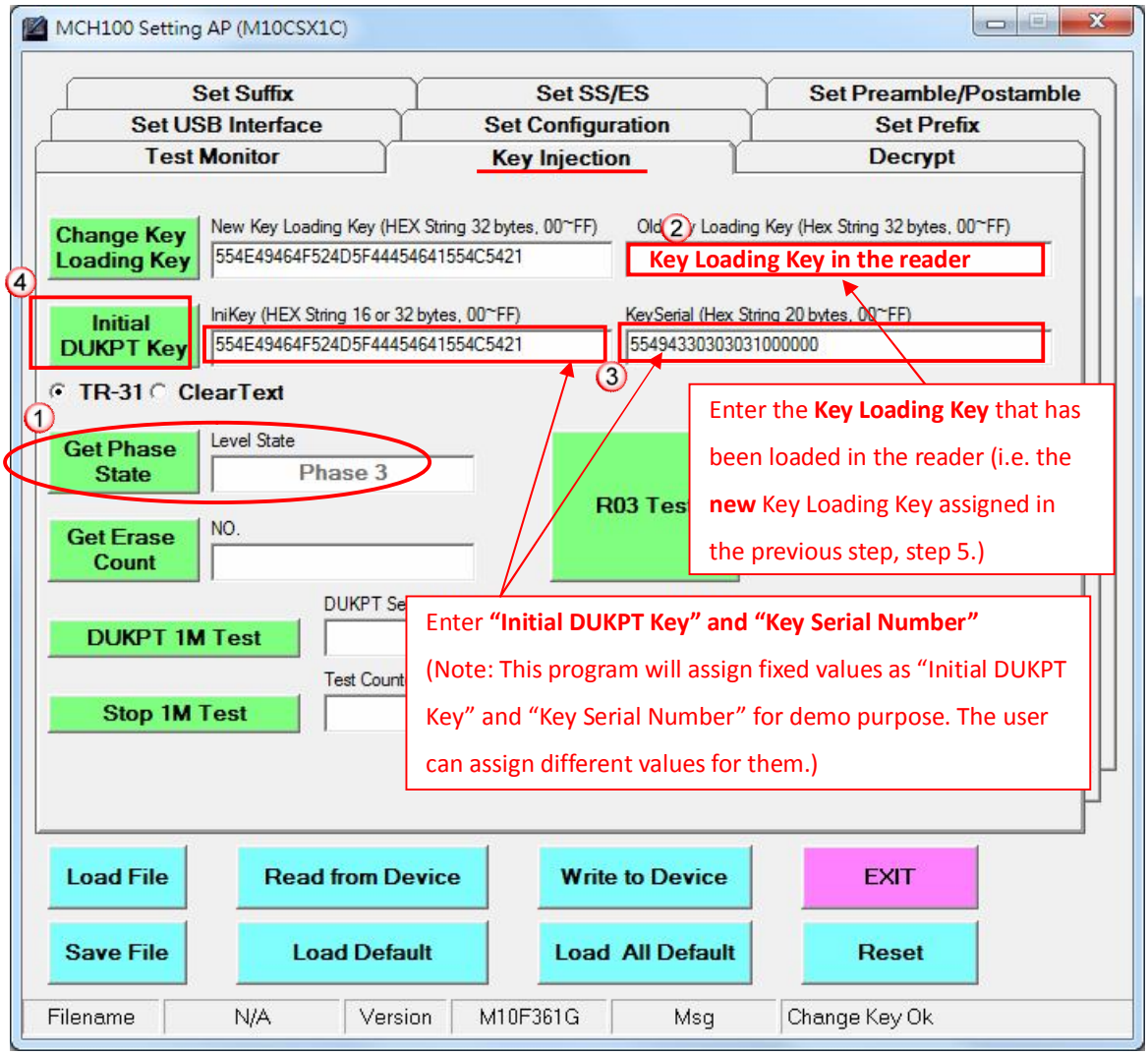
1. A fixed key value has been assigned by MCH100 Setting AP as a new key for demo purpose. Do remember the key value if you change it. Without the correct key (Key Loading Key), the user is unable to update both Keying Loading Key and initial DUKPT key.
2. Input the factory default Key Loading Key. (Please contact UIC sales to obtain the factory default "Key Loading Key".)
3. Click "Change Key Loading Key" button.
4. If successful, "Chang Key OK" message will show up at the bottom right of the screen.

After this step, the user needs the new Key Loading Key to load initial DUKPT key and Key Serial number. The user also needs the new "Key Loading Key" to change it to another one when needed.

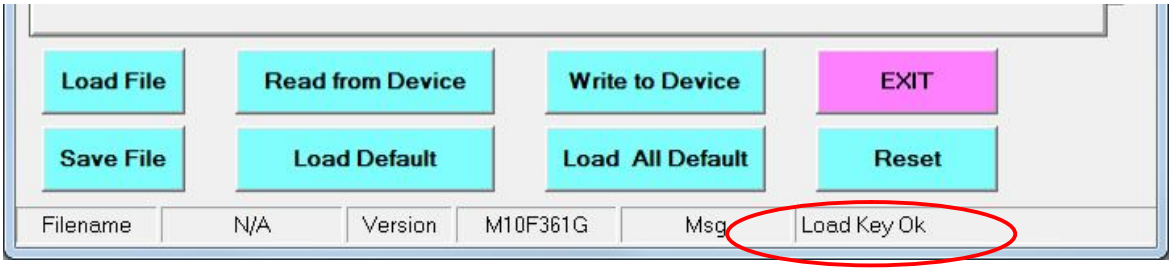


Step 6 Load "Initial DUKPT Key" and "Key Serial Number".

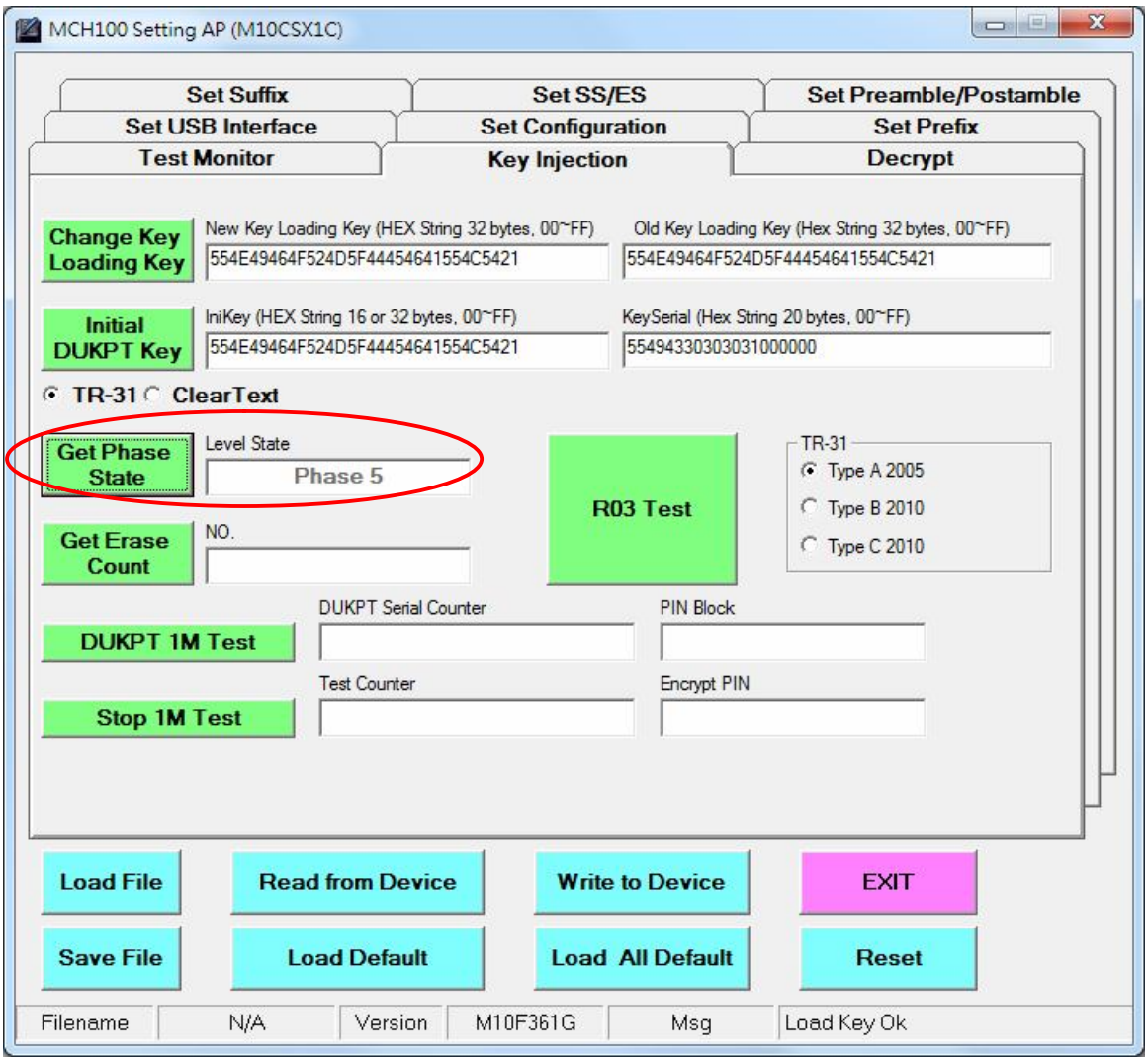
1. Click "Get Phase State" button, and you will get "Phase 3".
2. Enter the Key Loading Key that has been loaded in the reader (i.e. the new Key Loading Key assigned in the previous step, **Step 5**, in which the program assigns 554E49464F524D5F44454641554C5421 for it.)
3. Enter "Initial DUKPT Key" and "Key Serial Number". (Note: This program will assign fixed values as "Initial DUKPT Key" and "Key Serial Number" for demo purpose. The user can assign different values for them.)
4. Click "Initial DUKPT Key" button.



5. If changing key successfully, "Load Key OK" will show up at the bottom right of the screen.

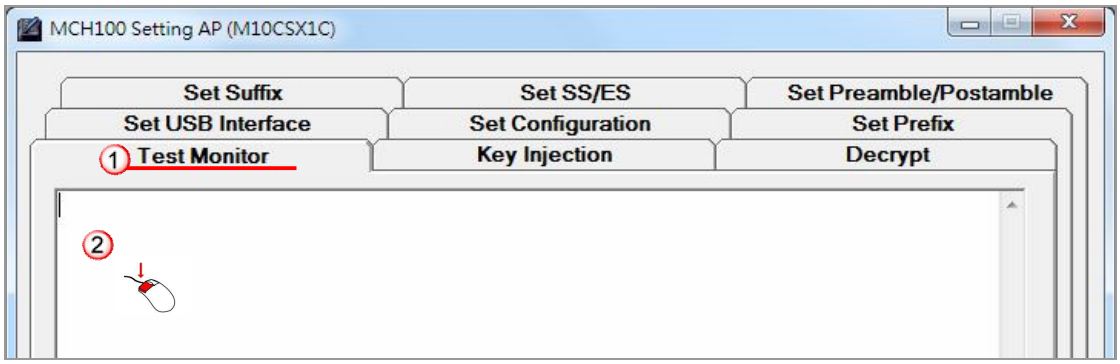


6. Click “Get Phase State” button, and you will get “Phase 5”.

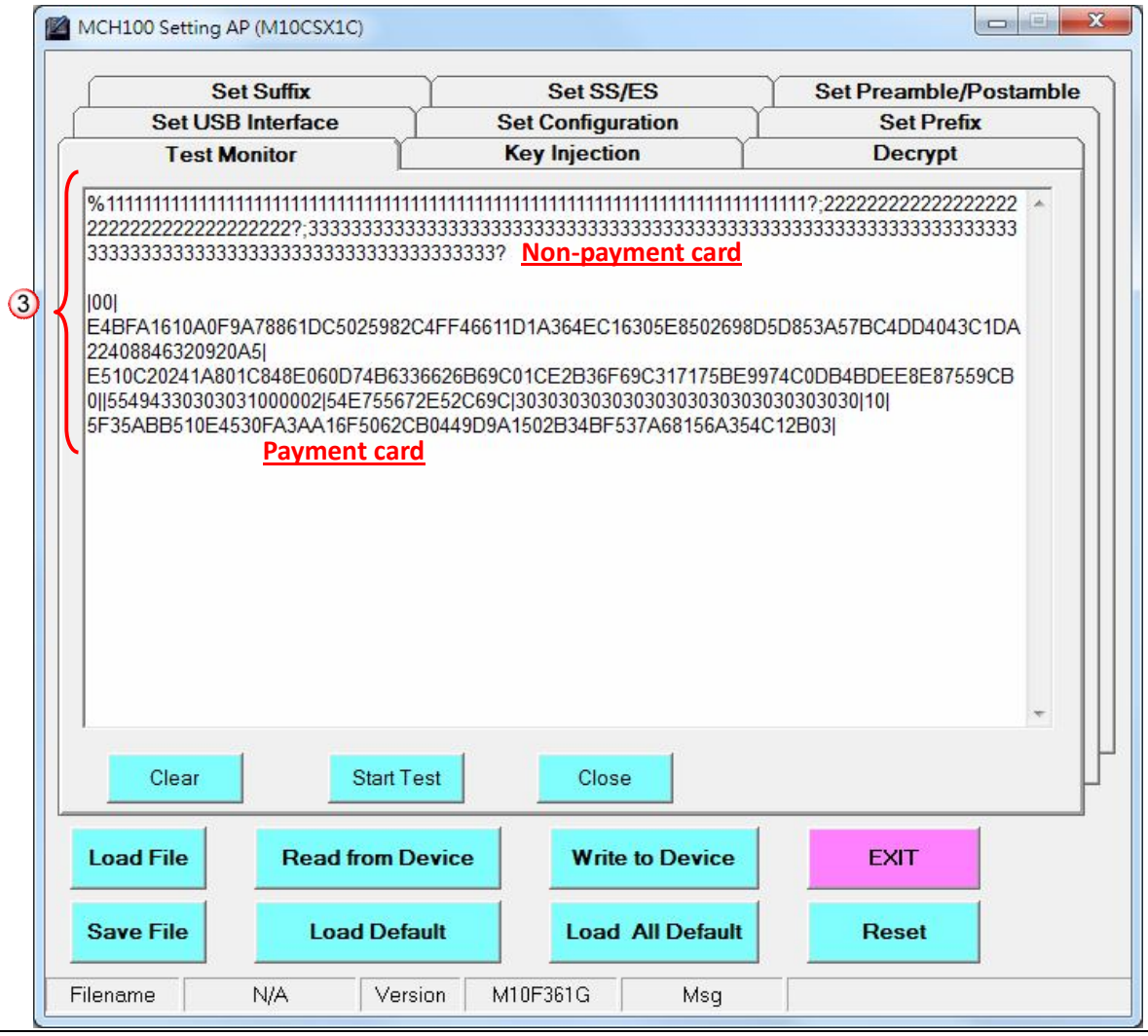


Step 7 After the Initial DUKPT Key has been loaded, the reader is able to encrypt the card data. The reader will automatically encrypt the payment card data that can pass the Luhn check (also known as the mod 10 check). For non-payment card, which are unable to pass Luhn check, the card data won't be encrypted. Follow the following steps to get the card data:

1. Open "Test Monitor" panel.
2. Click mouse button on display area. Let the cursor stays on the screen.



3. Swipe a card and the card data will be shown on the screen.



Step 8

1. Copy the encrypted output data from "Test Monitor" screen and paste them to corresponding fields on "Decrypt" panel.
2. Press "Decrypt" button to show the result of decrypted card data.
3. The decrypted data are then shown on the corresponding fields.

In this case, the payment card data are as follows:

|00|
E4BFA1610A0F9A78861DC5025982C4FF46611D1A364EC16305E8502698D5D853A57BC4DD4043C1DA
ED0B14244399FEE77597949A0325903C4CB1630CD3B3F532|
E510C20241A801C848E060D74B6336626B69C01CE2B36F69C317175BE9974C0DB4BDEE8E87559CB
0||5549433030303100002|54E755672E52C69C|30303030303030303030303030303030|10|
5F35ABB510E4530FA3AA16F5062CB0449D9A1502B34BF537A68156A354C12B03|