



WF35 Magstripe Card Reader (MSR) Configuration

Contents

WF35 Magstripe Card Reader (MSR) Configuration	1
1.1 Introduction.....	2
1.2 Attaching MSR	3
1.3 Configure MSR by Configuration Utility	3
1.4 Configure MSR by WF35.....	5
1.5 MSR data encryption.....	6
1.6 MSR data encryption via RDP.....	7

1.1 Introduction

The Magstripe Card Reader (MSR) USB add-on module is designed from scratch for reliability, security, durability, affordability & software compatibility.

Unlike common CF/SD card based MSR solutions, Touch Dynamic's MSR has a far more reliable attachment mechanism which could withstand heavy duty and frequent swiping of credit cards / magstripe cards in busy hospitality environment. MSR can easily locks to PDA simply by a screw driver via MSR bottom hole.

For data security, the MSR has a unique encryption feature at MSR's hardware level. The encryption key can be configured by POS ISVs/SIs. This reduces the risk customer credit card data, originally stored in clear-text format, could be captured by unauthorized persons or trusted programs (e.g. notepad).

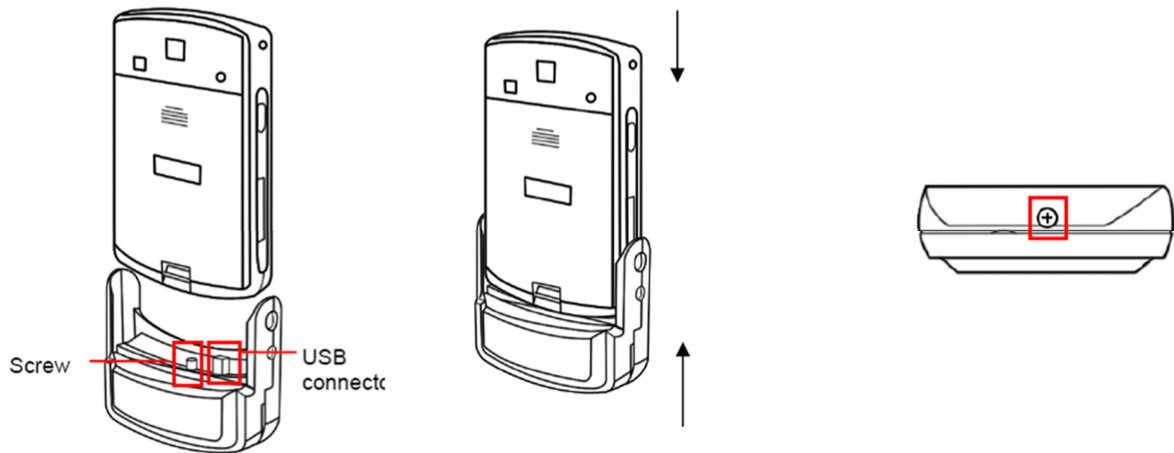
Since customers have no idea what program is actually running on the PDA, it simply cannot tell whether their cards data are processed securely within a trusted POS application or is stolen for mis-use. The encryption feature avoids potential mis-use of credit card data because only trusted POS applications, integrated with Touch Dynamic decryption SDK/API, could decrypt the card data within the application memory.

Touch Dynamic's MSR design is programming friendly. Since MSR emulates keyboard input, integrating with POS application is as easy as reading a text field. It doesn't require special programming interfaces like ActiveX, DLL & RS232. This also allows easy RDP application development.

Handheld based MSR is by nature a compact module and its rail length for card swipe is relatively shorter than conventional desktop one. Because of this, Touch Dynamic's MSR is carefully designed such that its magnetic head is positioned at the left, instead of at the middle. This will maximize the rail length and thus ensure high success read rate. There is an arrow on MSR to guide users to swipe a card from right to left.



1.2 Attaching MSR



- Place MSR at PDA bottom
- Connect MSR to PDA via USB socket
- Softly push the MSR towards PDA until it is good fit to the USB socket
- Fasten MSR with PDA via the screw at the MSR bottom

1.3 Configure MSR by Configuration Utility

Download the utility from [Touch Dynamic Web Site](#)



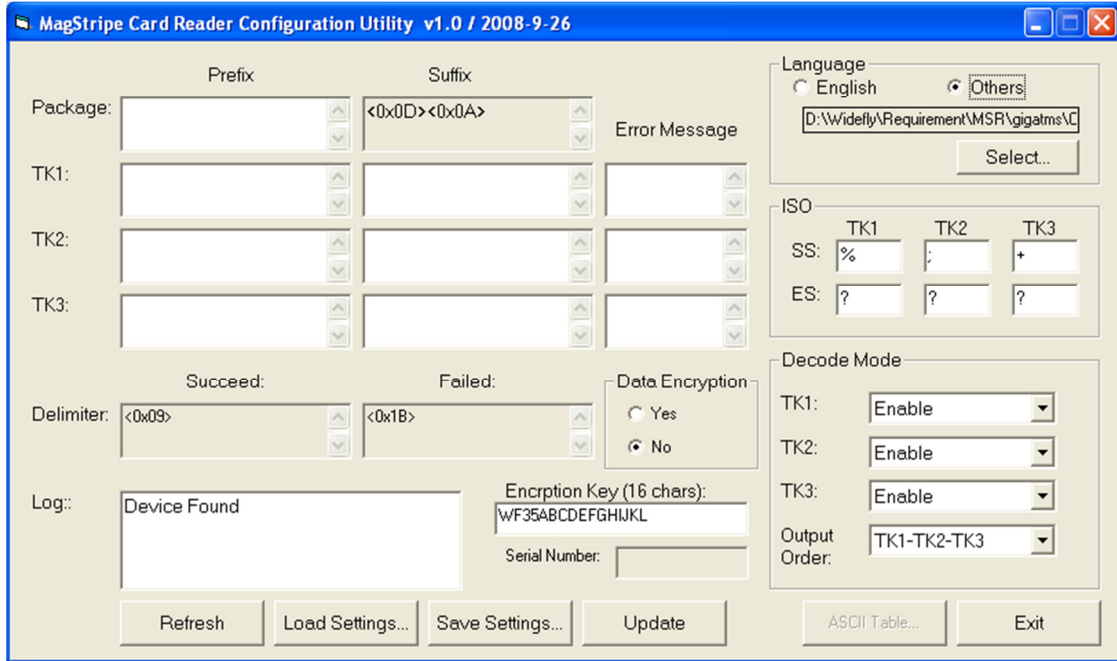
Custom USB cable (mini-USB cable + converter)



The custom cable connects to WF35 MSR & PC.

Full set of MSR functions could be modified by a Magstripe Card Reader Configuration Utility via a custom USB cable.

Run the configuration utility "hid_msr.exe". At bottom left, "Device Found" indicates WF35 MSR is found.



Configuration	Notes
TK[1/2/3] SS/ES	SS is start sentinel / ES is end sentinel According to ISO standard of magstripe card data: Track1 SS/ES: % / ? Track2 SS/ES: ; / ? Track3 SS/ES: + / ?
Decode Mode	Some tracks may be disabled Default track data order is TK1-TK2-TK3
TK[1/2/3] Prefix / Suffix	Additional prefix / suffix can be added to track 1/2/3
Package Prefix / Suffix	Additional Prefix / suffix characters can be added to beginning / ending of 3-track data For example, it is very common to add newline at package suffix. So, newline is the default suffix.
TK[1/2/3] Error Message	If there is error reading a track, specific error message could be defined. By default, it is empty. For example, you may define "ERR" as error message
Data Encryption	Yes or No. By default, data encryption is No.
Encryption Key	A 16-characters key. By default, the key is "WF35ABCDEF GHIJKL" You are recommended to change this key for production

	environment
Serial Number	MSR serial no (S/N). For MSR demo unit, S/N is empty.
Load / Save Settings	Settings can be saved / loaded via a text file. For default values, always use WF35.MAP. Otherwise, MSR data may be incorrectly translated.
Language	For correct mapping of characters (from MSR to PDA), it needs to use language file WF35.key.
Refresh	Refresh to re-connect MSR. Note that "refresh" does not retrieve settings from MSR internal memory, except encryption status (Yes/No).
Update	Write all MSR settings to the MSR internal memory
Delimiter	Reserved fields. Read only.

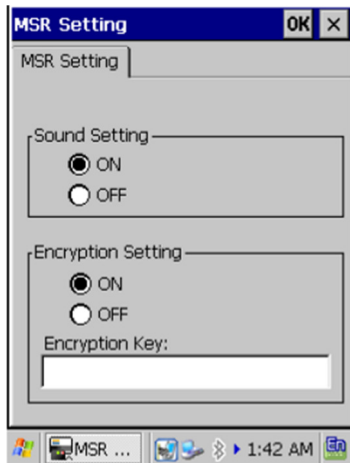
To update configuration of a MSR, always follows the steps below:

- "Load settings" : open WF35.map
- For language, press "Select" , use WF35.key (if you use English, MSR may translate characters incorrectly)
- Apply necessary configuration changes and press "Update" to update MSR device
- (It is suggested to save the configuration before update)

1.4 Configure MSR by WF35

A limited set of MSR functions could be configured via PDA.

Configure MSR setting at **Start > Settings > Control Panel > MSR**



Sound Setting

- ON: When MSR is plugged to the PDA, system will play the MSR plug-in tone and the taskbar displays a MSR tray icon. Similarly, when the MSR is removed, system will play a sound and hide the taskbar MSR icon.

Encryption Setting

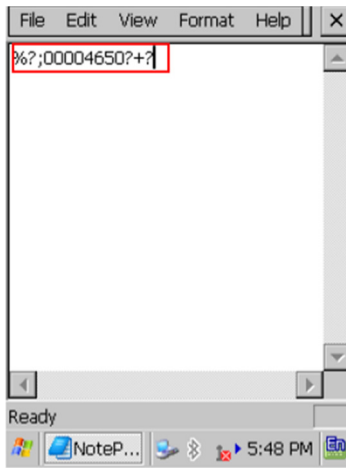
- ON: When read card data, the data will be shown as encrypted scrambled message
- Encryption key: This is to set the encryption key into the MSR

Note:

- The encryption input field is only for writing a new encryption key to MSR hardware. It doesn't display existing encryption key of the attached MSR for security purpose
- Default MSR encryption key is **WF35ABCDEFGHIJKL**. In production environment, this key should be changed for better security

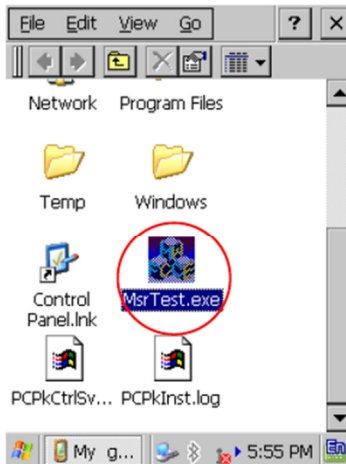
1.5 MSR data encryption

Data encryption is a unique feature to protect clear-text credit card (Magstripe card) data from being copied easily by notepad or any untrusted applications.



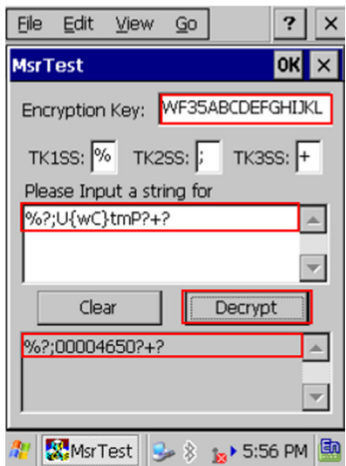
Clear-text data without encryption

- By default MSR encryption is off.
- Swiping of a magstripe card will generate clear-text keyboard input that could be captured by Notepad



Download MSR Test Utility

- Download the utility from [Touch Dynamic website](#)
- MSR test utility demonstrates how decryption mechanism could be incorporated to the POS application. Thus, only trusted application could decrypt the card data within program memory



MSR Test Utility

- Run MsrTest.exe
- Default encryption key is **WF35ABCDEF GHIJKL**
- Tap the input focus on text box and swipe a card
- Data is encrypted like a scrambled message
- Press "Decrypt" to decrypt the original data

1.6 MSR data encryption via RDP

Application running via RDP is indeed server-side application. Touch Dynamic's MSR works perfectly with server-side RDP POS application as well as local PDA application.

Since MSR would generate characters like "@#\$%~", default RDP configuration may translate such characters incorrectly or it would activate "sticky key" feature of Windows XP/Server. To avoid this, one line of RDP file has to be modified. See below:



When RDP works with MSR, it needs to modify the RDP profile file. Change the value of "KeyboardHookMode:i:0" to "0".

To demonstrate MSR via RDP, follow the screenshots below:



First of all, create a RDP file via "Remote Desktop Connection". You could save the password & username to facilitate "Auto logon RDP"

Open the RDP file by notepad (Start > Programs > notepad).

Modify one line:

"KeyboardHookMode:i:0". By default, this value is "1". Value "0" ensures no improper translation of characters from keyboard input generated by the MSR.



- Copy the files to server. Connect PDA to server via RDP.
- Run "Msr Test.exe" at server side. First, locate focus on "Input a string" box and swipe a credit card at WF35.
- Press "Decrypt" to retrieve original card data

For the source code of this demo utility, please refer to file "MsrTest-source WIN32.zip" in the folder.

The POS app could integrate with this decryption library (DLL) so that credit card data could be processed securely within application.