MAGTEK®
SECURITY FROM THE INSIDE

MagTek Reader Management System (RMS)

Linux

Sample Code Manual

May 2026

Manual Part Number:
D998200733-100

REGISTERED TO ISO 9001:2015

Table 0.1 – Revisions

Rev Number	Date	Notes
100	May 11, 2026	Initial release.

SOFTWARE LICENSE AGREEMENT

IMPORTANT: YOU SHOULD CAREFULLY READ ALL THE TERMS, CONDITIONS AND RESTRICTIONS OF THIS LICENSE AGREEMENT BEFORE INSTALLING THE SOFTWARE PACKAGE. YOUR INSTALLATION OF THE SOFTWARE PACKAGE PRESUMES YOUR ACCEPTANCE OF THE TERMS, CONDITIONS, AND RESTRICTIONS CONTAINED IN THIS AGREEMENT. IF YOU DO NOT AGREE WITH THESE TERMS, CONDITIONS, AND RESTRICTIONS, PROMPTLY RETURN THE SOFTWARE PACKAGE AND ASSOCIATED DOCUMENTATION TO THE ADDRESS ON THE FRONT PAGE OF THIS DOCUMENT, ATTENTION: CUSTOMER SUPPORT.

TERMS, CONDITIONS, AND RESTRICTIONS

MagTek, Incorporated (the "Licensor") owns and has the right to distribute the described software and documentation, collectively referred to as the "Software."

LICENSE: Licensor grants you (the "Licensee") the right to use the Software in conjunction with MagTek products. LICENSEE MAY NOT COPY, MODIFY, OR TRANSFER THE SOFTWARE IN WHOLE OR IN PART EXCEPT AS EXPRESSLY PROVIDED IN THIS AGREEMENT. Licensee may not decompile, disassemble, or in any other manner attempt to reverse engineer the Software. Licensee shall not tamper with, bypass, or alter any security features of the software or attempt to do so.

TRANSFER: Licensee may not transfer the Software or license to the Software to another party without the prior written authorization of the Licensor. If Licensee transfers the Software without authorization, all rights granted under this Agreement are automatically terminated.

COPYRIGHT: The Software is copyrighted. Licensee may not copy the Software except for archival purposes or to load for execution purposes. All other copies of the Software are in violation of this Agreement.

TERM: This Agreement is in effect as long as Licensee continues the use of the Software. The Licensor also reserves the right to terminate this Agreement if Licensee fails to comply with any of the terms, conditions, or restrictions contained herein. Should Licensor terminate this Agreement due to Licensee's failure to comply, Licensee agrees to return the Software to Licensor. Receipt of returned Software by the Licensor shall mark the termination.

LIMITED WARRANTY: Licensor warrants to the Licensee that the disk(s) or other media on which the Software is recorded are free from defects in material or workmanship under normal use.

THE SOFTWARE IS PROVIDED AS IS. LICENSOR MAKES NO OTHER WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Because of the diversity of conditions and PC hardware under which the Software may be used, Licensor does not warrant that the Software will meet Licensee specifications or that the operation of the Software will be uninterrupted or free of errors.

IN NO EVENT WILL LICENSOR BE LIABLE FOR ANY DAMAGES, INCLUDING ANY LOST PROFITS, LOST SAVINGS, OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE, OR INABILITY TO USE, THE SOFTWARE. Licensee's sole remedy in the event of a defect in material or workmanship is expressly limited to replacement of the Software disk(s) if applicable.

GOVERNING LAW: If any provision of this Agreement is found to be unlawful, void, or unenforceable, that provision shall be removed from consideration under this Agreement and will not affect the enforceability of any of the remaining provisions. This Agreement shall be governed by the laws of the State of California and shall inure to the benefit of MagTek, Incorporated, its successors or assigns.

ACKNOWLEDGMENT: LICENSEE ACKNOWLEDGES THAT HE HAS READ THIS AGREEMENT, UNDERSTANDS ALL OF ITS TERMS, CONDITIONS, AND RESTRICTIONS, AND AGREES TO BE BOUND BY THEM. LICENSEE ALSO AGREES THAT THIS AGREEMENT SUPERSEDES ANY AND ALL VERBAL AND WRITTEN COMMUNICATIONS BETWEEN LICENSOR AND LICENSEE OR THEIR ASSIGNS RELATING TO THE SUBJECT MATTER OF THIS AGREEMENT.

QUESTIONS REGARDING THIS AGREEMENT SHOULD BE ADDRESSED IN WRITING TO MAGTEK, INCORPORATED, ATTENTION: CUSTOMER SUPPORT, AT THE ADDRESS LISTED IN THIS DOCUMENT, OR E-MAILED TO SUPPORT@MAGTEK.COM.

DEMO SOFTWARE / SAMPLE CODE: Unless otherwise stated, all demo software and sample code are to be used by Licensee for demonstration purposes only and MAY NOT BE incorporated into any production or live environment. The PIN Pad sample implementation is for software PIN Pad test purposes only and is not PCI compliant. To meet PCI compliance in production or live environments, a third-party PCI compliant component (hardware or software-based) must be used.

Table of Contents

1 Overview

This document provides instructions to use the RMS Sample Code. Combining MagTek Linux SDK and web API calls to the Reader Management System (RMS) web service, the sample code assist in setting configurations, key injection, updating EMV Tags/CAPKs, and updating firmware for MagTek readers. The sample code is parsed into a collection of CLI apps (command line interface).

- Configuration app
- EMV Tags app
- Firmware app

For details on the RMS API see:
https://rmsv2.developer.magtek.com

1.1 Onboarding

This sample code is built with a public RMS Profile. MagTek will provide the necessary Profile configurations and authorization Web API Keys if requested.

1.2 Benefits

The MagTek Reader Management System (RMS) provides several key benefits for merchants and businesses, these include:

- **Centralized Management**: RMS allows for the remote management and configuration of MagTek readers across multiple locations from a single platform. Merchants can update firmware, keys, terminal settings, and CAPKs without manual intervention, reducing time, cost, and effort.
- **Enhanced Security**: RMS supports compliance with industry standards, such as PCI DSS, by ensuring secure payment card transactions and protecting sensitive customer data. It enables a secure process for keeping readers up to date with the latest firmware and configurations.
- **Efficient Updates**: RMS automates firmware updates and maintenance, allowing merchants to push updates remotely. This ensures all devices run the latest firmware, enhancing system reliability and reducing the need for manual updates.
- **System Reporting**: RMS offers reporting capabilities to track firmware versions and device settings, providing detailed insights by serial number for firmware, terminal, and CAPK updates in both production and test environments.
- **Scalability and Flexibility**: RMS is scalable to meet the needs of businesses, whether for a single store or multiple locations.
- **Cost Savings**: Automating reader management with RMS reduces the need for on-site visits, lowering maintenance costs and minimizing downtime. Centralized control streamlines administrative tasks, boosting operational efficiency.
- **Improved Customer Experience**: Efficiently managed payment readers reduce transaction errors and delays, improving customer satisfaction and loyalty, which positively impacts business reputation and revenue.

1.3 Requirements

The following packages are needed on the Linux host to build the sample code. Other dependencies are included in the makefile.

- make
- cmake
- g++

1.4 Building RMS Sample Code

1) Unzip the package.

2) Go to Sample folder:

```
$ cd Sample
```

3) Build the sample code using:

```
$ make
```

4) Various libraries and folders are generated. The two folders used for RMS Sample code are:

Folder	Description
/rms_mms	For DynaFlex readers: DynaFlex II PED, DynaFlex II Go, DynaProx, DynaFlex Pro, DynaFlex SCRA
/rms_scra	For V5 readers: mDynamo, tDynamo, Dynamag, Dynawave, iDynamo 6, eDynamo, DynaPad

5) Each sample code folder contains an account credential for access to RMS. This is by default configured for general public use. When accessing RMS for a custom profile, reassign the values as needed in the files:
/rms_mms/rms_account.json
/rms_scra/rms_account.json

```
{
   "rms_server": "https://svc1.magensa.net",
   "api_key": "MTPublic...",
   "profile_name": "MagTek_Production"
}
```

2 RMS MMS Sample Code

2.1 Configuration Update

1) Go to the folder: `rms_mms` and open a terminal.

2) Connect the reader to a USB port.

3) Enter command below. Enter password if prompted. This is for device port access.

```
$ sudo ./rms_mms_config_update
```

4) A list of available configurations is returned. List depends on the firmware ID and RMS Profile.
   Example:

```
Device Serial Number:B568DAF
Main Firmware ID:1000009714-AB3-PCI
Response Code:200
ResultCode: 0
Result: Success
Configurations Available: 3
1: Mask4Zero4
2: SCDEEnableNameExpirationDateServiceCode
3: Mask8Asterisk4_DynaFlex
Enter '1'...'3' to update configuration.
To force update configuration, enter '*' before the number
('*1'...'*3').
Enter '0' to exit:
```

5) At the prompt, select a configuration by entering its number listed to its left.
   A sequence of commands are downloaded from RMS and sent to the reader. Status of the configuration is shown as updated or failed and the end of the sequence.

```
Selected Configuration 1
Updating Configuration...
Configuration: Mask4Zero4
CommandsToDevice (1)
  Name: LeadingUnmaskedCharacters
  Command:
SENDCOMMAND,AA0081040110D111841BD11181072B06010401F609850101890BE109E2
07E205E103C30104
CommandsToDevice (2)
  Name: PANMaskedCharacter
.
.
.
Configuration Mask4Zero4 has been updated.
```

6) Whenever a configuration reports `is up to date`, it may be redone by entering *N, where N is the configuration. Example: *1

2.2 EMV Tags/CAPKs Update

1) Go to the folder: `rms_mms` and open a terminal.

2) Connect the reader to a USB port.

3) Enter command below. Enter password if prompted. This is for device port access.

```
$ sudo ./rms_mms_emvtags_capks_update
```

4) The sample code downloads the sequence of commands to update the EMV Tags and CAPKs available for the reader.

   Example:

```
Response Code:200
ResultCode: 0
Result: Success
Updating Configuration: TERMINAL
Setting ARQC Tag List
Sending command
[AA0081040100D111847DD11181072B06010401F609850101896DE16BE169E167E165C
.
.
.
Configuration TERMINAL has been updated.
```

5) Whenever a configuration result is: `Configuration is up to date`

   it may be redone by adding `-f` to force the update.

```
$ sudo ./rms_mms_emvtags_capks_update -f
```

2.3 Firmware Update

1) Go to the folder: `rms_mms` and open a terminal.

2) Connect the reader to a USB port.

3) Enter command below. Enter password if prompted. This is for device port access.

```
$ sudo ./rms_mms_firmware_update
```

4) The parameters for the firmware update is as follows.

```
rms_mms_firmware_update TYPE
  TYPE (type of firmware): MAIN|BOOT1|BLE|WLAN
```

5) Example for updating MAIN firmware.

```
$ sudo ./rms_mms_firmware_update MAIN
```

6) If an update is available, the change note for the update is shown. Below that, a confirmation to update is shown. Enter `y` to update.

```
Firmware update is available.
New Firmware: FIRMWARE, DYNAFLEX II GO MAIN APP PCI (COMMON KERNEL),
Version AB3
.
.
.
Do you want to update the MAIN firmware? (y/N)
```

7) A sequence of commands are downloaded from RMS and sent to the reader. Status of the update is shown as finished or failed and the end of the sequence.

```
Updating MAIN firmware...
Beginning DYNAFLEX II GO MAIN APP PCI (COMMON KERNEL)
Updating firmware...
  [1%]
.
.
.
  [100%]
  result (0)
Firmware update done.
Saving Firmware Image - Please Wait...
Wait for 30000 ms...
Done waiting.
Detecting device...
Detecting Device: GetDeviceList
Detecting Device: GetDeviceList > 0
Detecting Device: Found USB Device
Device detected.
Finished DYNAFLEX II GO MAIN APP PCI (COMMON KERNEL)
```

3 RMS SCRA Sample Code

3.1 Configuration Update

1) Go to the folder: `rms_scra` and open a terminal.

2) Connect the reader to a USB port.

3) Enter command below. Enter password if prompted. This is for device port access.

```
$ sudo ./rms_scra_config_update
```

4) A list of available configurations is returned. List depends on the firmware ID and RMS Profile. Example:

```
Device Serial Number:000F42353641394334313032343234414l
Main Firmware ID:000D31303030303039323734613032
Response Code:200
ResultCode: 0
Result: Success
Configurations Available: 5
1: DataVariant
2: Mask6Zero4
3: EMVNotificationsBoth
4: Mask8Zero2Mod10
5: Mask8Asterisk4
Enter '1'...'5' to update configuration.
To force update configuration, enter '*' before the number
('*1'...'*5').
Enter '0' to exit:
```

5) At the prompt, select a configuration by entering its number listed to its left.

A sequence of commands are downloaded from RMS and sent to the reader. Status of the configuration is shown as updated or failed and the end of the sequence.

```
Selected Configuration 1
Configuration: DataVariant
Sending command [0900]
Response: 000A9011880B56A9C4000001
Sending command [1900]
.
.
.
Done Changing to DataVariant
Configuration DataVariant has been updated.
```

6) Whenever a configuration reports `is up to date`, it may be redone by entering *N, where N is the configuration. Example: *1

3.2 EMV Tags/CAPKs Update

1) Go to the folder: `rms_scra` and open a terminal.

2) Connect the reader to a USB port.

3) Enter command below. Enter password if prompted. This is for device port access.

```
$ sudo ./rms_scra_emvtags_capks_update
```

4) The sample code downloads the sequence of commands to update the EMV Tags and CAPKs available for the reader.

   Example:

```
Device Response: 000D313030303030399323734613032
Main Firmware ID:000D313030303030399323734613032
Device Response:
001F42353641353131313032323234414100901450 0B56A5110000005344C35C6F
UIK:001F42353641353131313032323234414100901450 0B56A5110000005344C35C6F
Get Terminal Config (0) Extended Command: 03060008010000FA03DFDF26
Extended Response:
000000180016FA820012DFDF260E4D414754454B2044454641554C54
Result Code: 0000
Value: 4D414754454B2044454641554C54
Value String: MAGTEK DEFAULT
DB Name: MAGTEKDEFAULT
Get Terminal Config (1) Extended Command: 03060008010001FA03DFDF26
Extended Response: 03950000
Get Terminal Config (2) Extended Command: 03060008010002FA03DFDF26
Extended Response: 03950000
Get Terminal Config (3) Extended Command: 03060008010003FA03DFDF26
Extended Response: 03950000
Get Terminal Config (4) Extended Command: 03060008010004FA03DFDF26
Extended Response: 03950000
.
.
.
Done Loading MagTek Default Contact Tags and CAPK
Configuration MAGTEKDEFAULT has been updated.
```

5) Whenever a configuration result is: `Configuration is up to date`
   it may be redone by adding `-f` to force the update.

```
$ sudo ./rms_mms_emvtags_capks_update -f
```

3.3 Firmware Update

1) Go to the folder: `rms_scra` and open a terminal.

2) Connect the reader to a USB port.

3) Enter command below. Enter password if prompted. This is for device port access.

```
$ sudo ./rms_scra_firmware_update
```

4) The parameters for the firmware update is as follows.

```
rms_scra_firmware_update TYPE
  TYPE (type of firmware): MAIN|BLE
```

5) Example for updating MAIN firmware.

```
$ sudo ./rms_scra_firmware_update MAIN
```

6) If an update is available, the change note for the update is shown. Below that, a confirmation to update is shown. Enter `y` to update.

```
Firmware update is available.
New Firmware: Main_1000009274 version A02 firmware
.
.
.
Do you want to update the MAIN firmware? (y/N)
```

7) A sequence of commands are downloaded from RMS and sent to the reader. Status of the update is shown as finished or failed and the end of the sequence.

```
Updating MAIN firmware...
Beginning mDynamo firmware Main 1000009274 version A02 firmware
Updating firmware...
.
.
.
Sending command
[94255A00044A6000000000FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFF]
Response: 0000
Sending command [95015A]
Response: 0000
Sending command [0200]
Response: 0000
Wait for 15000 ms...
Done waiting.
Detecting device...
.
.
.
Device detected.
```

```
Sending command [970100]
Response: 0000
Finished mDynamo Firmware-1000009274-A02 Update
MAIN Firmware update completed.
```

8) Whenever a firmware result is: `Firmware is up to date`
   it may be redone by adding `-f` to force the update.

```
$ sudo ./rms_scra_firmware_update MAIN -f
```

Appendix A Glossary of Terms

- API – Application Programming Interface
- EMV –Europay, MasterCard® and Visa®
- KSN - Key Serial Number
- MUT - MagTek Update Token
- SDK – Software Developer's Kit
- SN - Serial Number
- UIK - Unique Identifier Key
- Force update – Supplying Version:0 in the web API call. Otherwise RMS determines of update.