

# SDK - MagneFlex Powder, Middleware, PIN PEDs Programmer's Manual (MagneFlex API)



February 2021

Manual Part Number:  
D998200118-70

REGISTERED TO ISO 9001:2015

Information in this publication is subject to change without notice and may contain technical inaccuracies or graphical discrepancies. Changes or improvements made to this product will be updated in the next publication release. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of MagTek, Inc.

MagTek® is a registered trademark of MagTek, Inc.

Bluetooth® is a registered trademark of Bluetooth SIG.

Microsoft® and Windows® are registered trademarks of Microsoft Corporation.

All other system names and product names are the property of their respective owners.

**Table 0.1 – Revisions**

Rev Number	Date	Notes
10	03/02/2016	Initial Release
20	03/22/2016	Renamed SendAPRCRequest to RequestSendAcquirerResponse. Added RequestOperationStatus.
30	07/15/2016	Added “Request” to page 7. Added “03= Read all tags operation” to RequestEMVTags. Deleted “Tones” and “FiedSeparator” from RequestManualSwipe. Added “AdditionalRequestData” to RequestSmartCard Updated Code in Appendix A.1, A.2, A.3.
40	10/02/2017	Changed the parameter Timeout to WaitTime in the RequestSendAcquirerResponse operation. Added details for the Reserved bytes of the RequestSmartCard operation.
50	11/02/2017	Added WaitTimeBeforeTransactionComplete to the RequestSendAcquirerResponse operation
60	05/09/2018	Added the CloseDevice and EndSession parameters to requests.
70	02/18/2021	Added the URI for BLE device connection type.

## 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.

## Table of Contents

<b>SOFTWARE LICENSE AGREEMENT .....</b>	<b>3</b>
<b>Table of Contents .....</b>	<b>5</b>
<b>1 Introduction .....</b>	<b>7</b>
<b>1.1 Nomenclature .....</b>	<b>7</b>
<b>1.2 About the MagTek Powder .....</b>	<b>7</b>
<b>1.3 SDK Contents.....</b>	<b>8</b>
<b>1.4 System Requirements.....</b>	<b>9</b>
<b>1.5 Interfaces for Operating Systems.....</b>	<b>9</b>
<b>2 How to Set Up the MagneFlex Powder .....</b>	<b>10</b>
<b>2.1 How to Connect MagneFlex Powder Service to a Host .....</b>	<b>10</b>
<b>2.2 How to Connect DynaPro Mini to a Windows Host via BLE .....</b>	<b>10</b>
<b>3 MagneFlex Powder Resources .....</b>	<b>14</b>
<b>3.1 CheckHealth .....</b>	<b>14</b>
<b>3.2 RequestCardSwipe .....</b>	<b>14</b>
<b>3.3 RequestEMVTags .....</b>	<b>15</b>
<b>3.4 RequestManualSwipe .....</b>	<b>17</b>
<b>3.5 RequestPIN .....</b>	<b>19</b>
<b>3.6 RequestSignature .....</b>	<b>21</b>
<b>3.7 RequestSmartCard .....</b>	<b>23</b>
<b>3.8 RequestSendAcquirerResponse .....</b>	<b>25</b>
<b>3.9 ReleaseDevice .....</b>	<b>27</b>
<b>3.10 RequestSendCommand .....</b>	<b>27</b>
<b>3.11 RequestOperationStatus.....</b>	<b>29</b>
<b>4 MagneFlex Powder Response Output Structures .....</b>	<b>30</b>
<b>4.1 CheckHealth Output .....</b>	<b>30</b>
<b>4.2 CardSwipe Output .....</b>	<b>30</b>
<b>4.3 ManualSwipe Output .....</b>	<b>31</b>
<b>4.4 PIN Output.....</b>	<b>33</b>
<b>4.5 Signature Output.....</b>	<b>33</b>
<b>4.6 Transaction Output SmartCard .....</b>	<b>34</b>
<b>4.7 Transaction Output ARPC .....</b>	<b>35</b>
<b>4.8 Data Output.....</b>	<b>36</b>
<b>4.9 OperationStatus Output .....</b>	<b>36</b>

## 0 - Table of Contents

---

Appendix A	TLV Data Format .....	37
A.1	ARQC Message Format .....	37
A.2	ARQC Response (from online processing) .....	37
A.3	Transaction Result Message – Batch Data Format.....	38

## 1 Introduction

This document provides instructions for software developers who want to create software solutions that include a IPAD, DynaPro, and DynaPro Mini connected to a Windows-based host via USB, BLE, or by Ethernet. It is part of a larger library of documents designed to assist IPAD, DynaPro, and DynaPro Mini implementers, which includes the following documents available from MagTek:

- *D99875585 DYNAPRO PROGRAMMER'S MANUAL ( COMMANDS )*
- *D99875629 DYNAPRO MINI PROGRAMMER'S MANUAL ( COMMANDS )*
- *D99875430 IPAD PROGRAMMER'S MANUAL (COMMANDS)*

### 1.1 Nomenclature

The general terms “device” and “host” are used in different, often incompatible ways in a multitude of specifications and contexts. For example “host” may have different meanings in the context of USB communication than it does in the context of networked financial transaction processing. In this document, “device” and “host” are used strictly as follows:

- **Device** refers to the MSR device (eg. Dynamag) that receives and responds to the command set specified in this document.
- **Host** refers to the piece of general-purpose electronic computing equipment the device is connected or paired to, which can send data to and receive data from the device. It also hosts the MagneFlex Powder.

The word “user” is also often used in different ways in different contexts. In this document, user generally refers to the cardholder.

### 1.2 About the MagTek Powder

The MagneFlex Powder provides a convenient HTTP command interface to a device connected to a host. An HTTP client (such as a web browser) makes JSON calls to the host that are mapped to the device’s low-level command set, as found in the Programmer’s Reference. The MagneFlex Powder can be launched on the host as either a Windows Service, or a through a standalone executable. Any HTTP client that can reach the host via a network can process commands to the device. Commands are processed as simple request/response pairs, as shown later in the document.

The API also includes a sample SOAPUI project that demonstrates how JSON calls to the MagneFlex Powder are formed and processed. In addition, source code for the standalone executable is provided, if the developer wishes to integrate the MagneFlex Powder directly into their own code.

The MagneFlex Powder is single-threaded. If the service is busy processing a command to the device, other calls will be rejected.

# 1 - Introduction

---

## 1.3 SDK Contents

Executables:

File	Description
MTPPSCRA.WEBAPI.Host.exe	MagTek WEBAPI executable
MTPPSCRA.WEBAPI.HostService.exe	MagTek WEBAPI Windows service
MTPPSCRA.WEBAPI.Host.exe.config	MagTek WEBAPI executable configuration file
MTPPSCRA.WEBAPI.HostService.exe	MagTek WEBAPI Windows service configuration files

DLLs:

File	Description
MTDevice.DLL	MagTek PPSCRA Device constance library
MTLIB.DLL	MagTek PPSCRA interface library
MTPPSCRANET.DLL	MagTek PPSCRA library for .Net
MTPPSCRA.WEBAPI.DLL	MagTek PPSCRA library for WEB API
MTPPServiceNet.DLL	MagTek PPSCRA connection service library for .Net
MTEMVTLVParser.DLL	MagTek PPSCRA TLV EMV Parser
MTTLV.DLL	MagTek PPSCRA TLV library

Sample SOAPUI project:

File	Description
MTPPSCRA WEB API Sample-soapui-project.xml	Sample SOAPUI project file



# 1 - Introduction

---

## 1.4 System Requirements

Tested operating systems:

Windows 7  
Windows 8  
Windows 8.1  
Windows 10

Microsoft .Net Framework 4.5 installed. (The API installation process will install this if it does not already exist on the host.)

Tested development environments:

Windows 8.1 with Microsoft Visual Studio 2013

## 1.5 Interfaces for Operating Systems

The following table matches the device interface to operating system.

Device	Interface	Operating System
DynaPro	USB	Windows 7, Windows 8, 8.1 & Windows 10
	ETHERNET	Windows 7, Windows 8, 8.1 & Windows 10
DynaPro Mini	USB	Windows 7, Windows 8, 8.1 & Windows 10
	BLE	Windows 8, 8.1 & Windows 10
DynaPro Go	USB	Windows 7, Windows 8, 8.1 & Windows 10
	BLE	Windows 8, 8.1 & Windows 10
	802.11 Wireless	Windows 8, 8.1 & Windows 10
IPAD	USB	Windows 7, Windows 8, 8.1 & Windows 10

## 2 - How to Set Up the MagneFlex Powder

---

### 2 How to Set Up the MagneFlex Powder

#### 2.1 How to Connect MagneFlex Powder Service to a Host

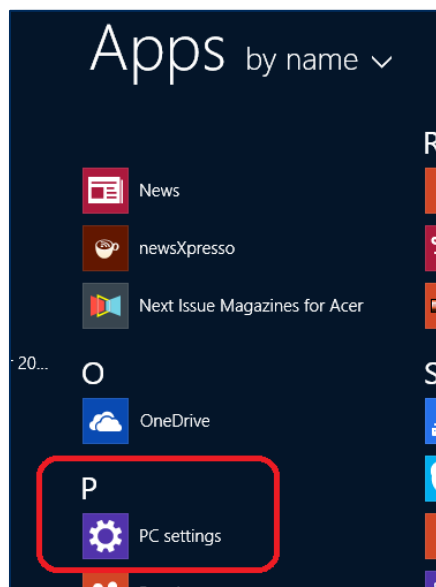
To use the MagneFlex Powder (MTPPSCRA.WEBAPI.HostService.exe)

- 1) Set the header ContentType to "application/json"
- 2) Build the JSON object for the MagneFlex Powder resource to be accessed.
- 3) Send HTTP request methods GET and POST (resource dependent) to the base address <http://localhost:9000/api/mtppscrahost/> with the resource endpoint concatenated.

#### 2.2 How to Connect DynaPro Mini to a Windows Host via BLE

To connect DynaPro Mini to a host with Windows 8.1 or higher and Bluetooth 4.0 hardware that supports BLE, follow these steps:

- 1) If you are using an external Bluetooth adapter, install any required drivers and connect it to the host.
- 2) On the host, install and configure the software you intend to use with DynaPro Mini:
  - a) Make sure the host software is configured to look for the device on the proper connection.
  - b) Make sure the host software knows which device(s) it should interface with.
  - c) Make sure the host software is configured to properly interpret incoming data from the device. This depends on whether the device is configured to transmit data in GATT format or streaming format emulating a keyboard.
- 3) Make sure the DynaPro Mini has an adequate charge
- 4) Unpair from any other host it is already paired with before continuing.
- 5) Enter app mode, scroll down to **Apps by name**, and launch the Windows **PC Settings** app.



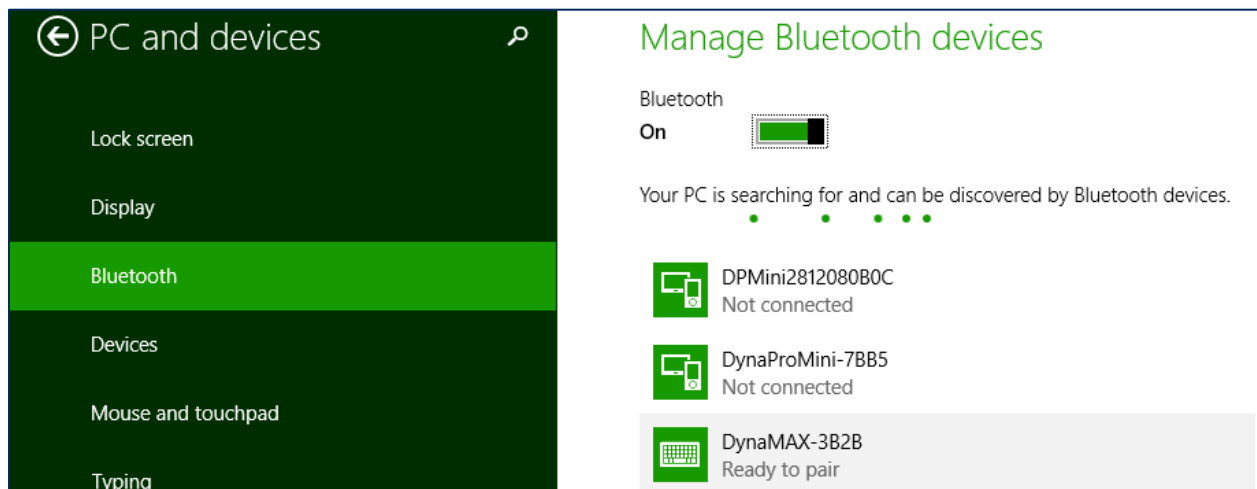
- 6) In the left side navigator, select **PC and devices** > **Bluetooth**.
- 7) Make sure Bluetooth is turned on and close the **PC and devices** app.
- 8) Launch the Windows **Manage Bluetooth Devices** app by following these steps:
  - a) Enter desktop mode by swiping in from the left side of the touchscreen.

## 2 - How to Set Up the MagneFlex Powder

- b) Touch the Bluetooth icon in the system tray and select **Add a Bluetooth Device** (see **Figure 2-1**).



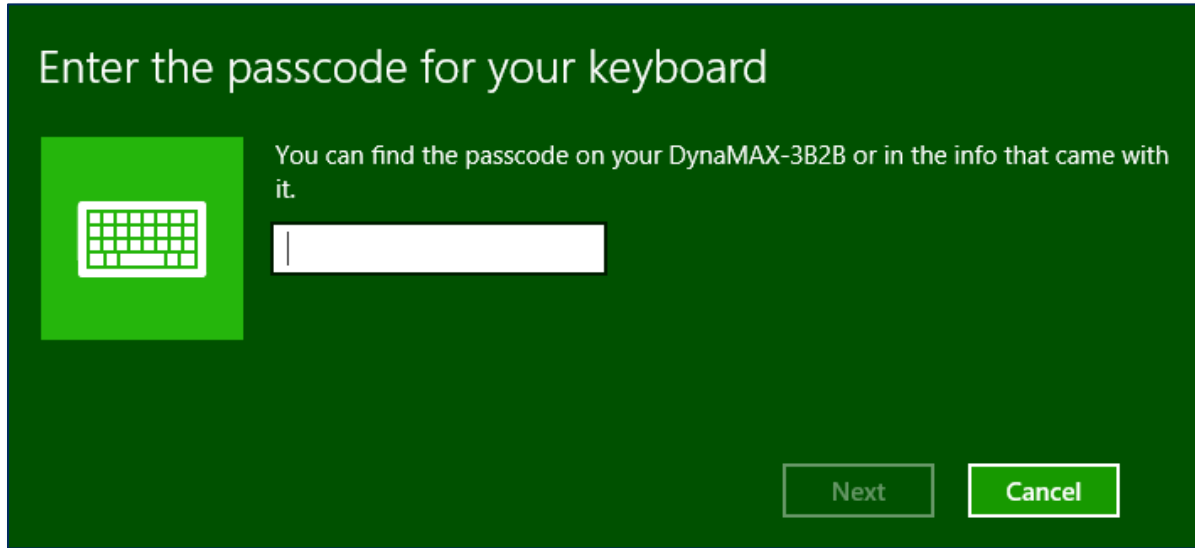
**Figure 2-1 - Launch Manage Bluetooth Devices App from Desktop Mode**



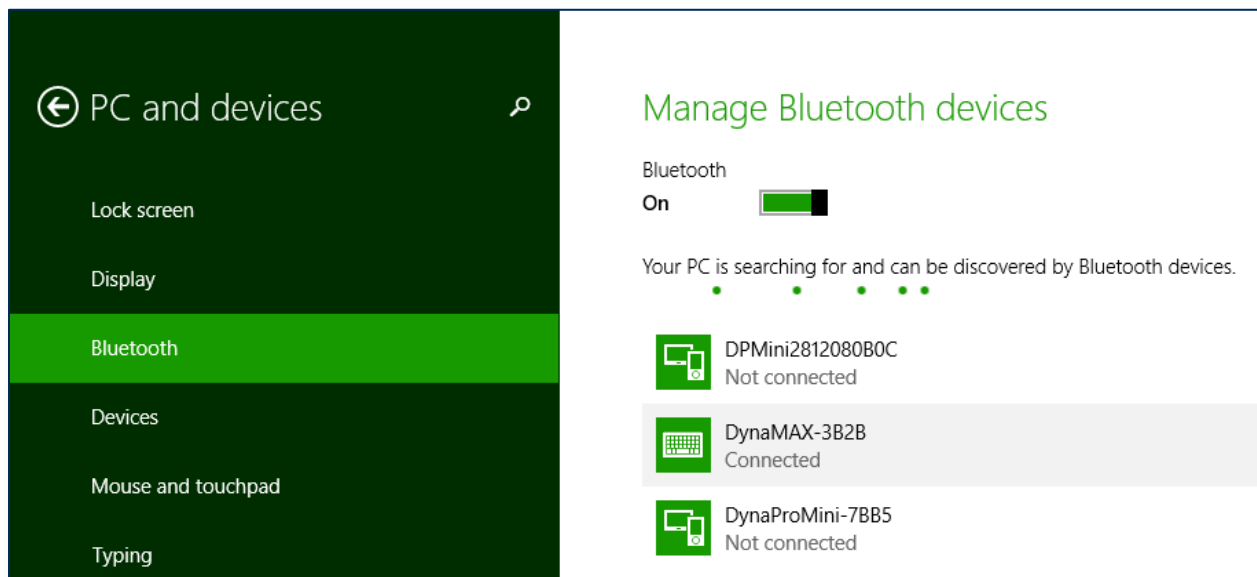
**Figure 2-2 – Windows 8 Manage Bluetooth Devices App**

- 9) Locate the serial number on the label on the bottom of the device. Note the final four digits.
- 10) Read through the list of pairable devices and locate the device called **DynaProMini-nnnn**, where nnnn is the last four digits of the device's serial number (if the device does not show in the list, power it off then power it back on). Below the device name you should see the text **Ready to pair**.
- 11) Select the device and press the **Pair** button. If the device is configured to run in KB mode, Windows will prompt you **Enter the passcode for your keyboard**.

## 2 - How to Set Up the MagneFlex Powder



- 12) Enter default passcode **000000** (or the device's actual password if it has been configured differently), then press the **Next** button. Windows will return you to the **Manage Bluetooth devices** page. After a short period of time, you will see the text **Connected** below the device you are pairing with. After a few seconds the device will disconnect, which is normal power-saving behavior.



- 13) Use the host software to test swiping a card. If you do not yet have host software and the device is configured to run in KB mode, open any text editor and swipe a card. The card contents should appear in the text editor.
- 14) The device consumes very little power when not transmitting card data, so it is not necessary to power off the device to conserve power. If the device appears as **Not connected** in the Windows list of Bluetooth devices, swiping a card should cause the device to reconnect briefly, transmit the card data, then disconnect.

## 2 - How to Set Up the MagneFlex Powder

---

15) Remember to change the default password. See the DynaPro Mini Programmer's Reference documents for details.

To unpair from the device:

- 1) Locate the device in the **Manage Bluetooth devices** window.  
Press the **Remove device** button.

## 3 - MagneFlex Powder Resources

---

### 3 MagneFlex Powder Resources

MagneFlex Powder can be hosted as a Windows service (MagTek PPSCRA WEBAPI Host service or executable (MTPPSCRA.WEBAPI.Host.exe).

#### 3.1 CheckHealth

Returns the operational status of the MagneFlex Powder.

Using Method GET:

```
api/mtppscrahost/CheckHealth
```

Return Value:

A string array containing API name and status.

#### 3.2 RequestCardSwipe

Triggers the device to prompt for a card swipe.

Using Method POST:

```
api/mtppscrahost/RequestCardSwipe (  
string DeviceID,  
int WaitTime,  
int DisplayMessage,  
int Tones,  
string FieldSeparator,  
boolean CloseDevice,  
boolean EndSession);
```

Parameter	Description
DeviceID	<p>URI of the device.</p> <p>For USB devices, Use an empty string to open the first device found. Otherwise use: USB://DEVICSERIALNUMBER Example, USB://99261829170E0810</p> <p>For Ethernet devices, use the form: IP://IPAddress:PORT Example, IP://10.57.10.180:26</p> <p>For 802.11 Wireless devices, use in the form: TLS12://TLSDEVICSERIALNUMBER TLS12TRUST://TLSDEVICSERIALNUMBER Example, TLS12://TLS99261829170E0810           TLS12TRUST://TLS99261829170E0810</p> <p>For BLE devices, use the form: BLEEMV://DEVICENAME Example, BLEEMV://DPG123456789A DEVICENAME is listed in the operating system Bluetooth settings.</p>

### 3 - MagneFlex Powder Resources

WaitTime	Time in seconds the device will wait for the action to be completed. (1 - 255)
DisplayMessage	Message to prompt the user with: 0 = Swipe Card / Idle alternating 1 = Swipe Card 2 = Please Swipe Card 3 = Please Swipe Card Again 4 = Chip Error, Use Mag Stripe
Tones	Tones to use: 0 = No sound 1 = One beep 2 = Two beeps
FieldSeparator	Delimiter to separate the output data.
CloseDevice	Flag which determines whether the connection to the device will be closed after the request is processed. Default value is "false". "false" = Do not close the device. "true" = Close device.
EndSession	Flag which determines whether an EndSession command is sent to the device after the request is processed. Default value is "false". When set to false, this flag may facilitate the display of a custom message after a request is processed. "false" = Do not end the session. "true" = End the session.

Return Value:

The Card Swipe output.

```
{"CardSwipeOutput": {}, "AdditionalOutputData": {}}
```

### 3.3 RequestEMVTags

Triggers the device to prompt for a card swipe.

Using Method POST:

```
api/mtpscrahost/RequestEMVTags (  
string DeviceID,  
int WaitTime,  
int TransactionType,  
int TagType,  
int TagOperation,  
int DataBase,  
string Data,  
enum RequestType,  
boolean CloseDevice,  
boolean EndSession);
```

### 3 - MagneFlex Powder Resources

Parameter	Description
DeviceID	<p>URI of the device.</p> <p>For USB devices, Use an empty string to open the first device found.            Otherwise use:            USB://DEVICSERIALNUMBER            Example, USB://99261829170E0810</p> <p>For Ethernet devices, use the form:            IP://IPAddress:PORT            Example, IP://10.57.10.180:26</p> <p>For 802.11 Wireless devices, use in the form:            TLS12://TLSDEVICSERIALNUMBER            TLS12TRUST://TLSDEVICSERIALNUMBER            Example, TLS12://TLS99261829170E0810                      TLS12TRUST://TLS99261829170E0810</p> <p>For BLE devices, use the form:            BLEEMV://DEVICENAME            Example, BLEEMV://DPG123456789A            DEVICENAME is listed in the operating system Bluetooth settings.</p>
WaitTime	Time in seconds the device will wait for the action to be completed. (1 - 255)
TransactionType	Transaction Type: 00 = Payment 01 = Cash 09 = Purchase with Cashback 20 = Refund
TagType	EMV tag to set or get: 00 = Reader tags 80 = Application tags Lower 7 bits indicate which application slot of operation.
TagOperation	Type of operation to be performed: 00 = Read single tag operation 03 = Read all tags operation 04 = Write operation FF = Set to factory defaults
DataBase	Database Selector: 00 = Contact L2 EMV Tags 01 = PayPass-MasterCard 02 = PayWave-VISA 03 = ExpressPay-AMEX 04 = Discover



### 3 - MagneFlex Powder Resources

Data	<p>TLV data block to send to the device. Data block must be formed as an F9 CBC-MAC container message. Reference the device manual for details.</p> <pre>AAAA /* 2-byte MSB message length excluding padding and CBC-MAC */ F9&lt;len&gt; /* container for MAC structure and generic data */ DFDF55 (MAC Encryption Type)&lt;len&gt;&lt;val&gt; DFDF25 (IFD Serial Number)&lt;len&gt;&lt;val&gt; FA&lt;len&gt; /* container for generic data */ &lt;tag&gt;&lt;len&gt;&lt;val&gt; ... &lt;tag&gt;&lt;len&gt;&lt;val&gt; &lt;Buffer if any to make blocks as multiple of 8 bytes&gt; &lt;CBC-MAC (4 bytes, use MAC variant of AMK)&gt;</pre>
RequestType	<p>"SET" for setting an EMV tag. "GET" for getting an EMV tag.</p>
CloseDevice	<p>Flag which determines whether the connection to the device will be closed after the request is processed. Default value is "false". "false" = Do not close the device. "true" = Close device.</p>
EndSession	<p>Flag which determines whether an EndSession command is sent to the device after the request is processed. Default value is "false". When set to false, this flag may facilitate the display of a custom message after a request is processed. "false" = Do not end the session. "true" = End the session.</p>

Return Value:  
The Card Swipe output.

```
{"CardSwipeOutput": {}, "AdditionalOutputData": {}}
```

#### 3.4 RequestManualSwipe

Triggers the device to begin a manual card data entry.

Using Method POST:

```
api/mtpscrahost/RequestManualSwipe (
string DeviceID,
int WaitTime,
int Options,
int Tones,
boolean CloseDevice,
boolean EndSession);
```

### 3 - MagneFlex Powder Resources

Parameter	Description
DeviceID	<p>URI of the device.</p> <p>For USB devices, Use an empty string to open the first device found. Otherwise use: USB://DEVICESTRIALNUMBER Example, USB://99261829170E0810</p> <p>For Ethernet devices, use the form: IP://IPAddress:PORT Example, IP://10.57.10.180:26</p> <p>For 802.11 Wireless devices, use in the form: TLS12://TLSDEVICESTRIALNUMBER TLS12TRUST://TLSDEVICESTRIALNUMBER Example, TLS12://TLS99261829170E0810                   TLS12TRUST://TLS99261829170E0810</p> <p>For BLE devices, use the form: BLEEMV://DEVICENAME Example, BLEEMV://DPG123456789A DEVICENAME is listed in the operating system Bluetooth settings.</p>
WaitTime	<p>Time in seconds the device will wait for the action to be completed. (1 - 255)</p>
Options	<p>This is an ORed combination of flags that changes the device's data entry request behavior as follows:</p> <p>Bits 0 and 1 0 = Acct,Date,CVC 1 = Acct,Date 2 = Acct,CVC 3 = Acct</p> <p>Bit 2 1=Use QwickCodes entry</p> <p>Bit 3 1=Use PAN in PIN block creation</p> <p>Bit 4 0=Use PAN min 9, max 19 1=Use PAN min 14, max 21</p> <p>Bits 5-7 are reserved and should be set to 0.</p>
Tones	<p>Tones to use: 0 = No sound 1 = One beep 2 = Two beeps</p>

### 3 - MagneFlex Powder Resources

---

Parameter	Description
CloseDevice	Flag which determines whether the connection to the device will be closed after the request is processed. Default value is “false”. “false” = Do no close the device. “true” = Close device.
EndSession	Flag which determines whether an EndSession command is sent to the device after the request is processed. Default value is “false”. When set to false, this flag may facilitate the display of a custom message after a request is processed. “false” = Do no end the session. “true” = End the session.

Return Value:

The Card Manual output.

```
{"CardManualOutput": {}, "StatusCode":, "AdditionalOutputData":{}}
```

#### 3.5 RequestPIN

Prompts the user to enter a PIN by displaying one of five predetermined messages and playing a specified sound.

Using Method POST:

```
api/mtpscrahost/RequestPIN(  
string DeviceID,  
int WaitTime,  
int PinMode,  
int MaxPinLength,  
int MinPinLength,  
int Options,  
int Tones,  
string FieldSeparator,  
boolean CloseDevice,  
boolean EndSession);
```

### 3 - MagneFlex Powder Resources

Parameter	Description
DeviceID	<p>URI of the device.</p> <p>For USB devices, Use an empty string to open the first device found. Otherwise use: USB://DEVICESTRIALNUMBER Example, USB://99261829170E0810</p> <p>For Ethernet devices, use the form: IP://IPAddress:PORT Example, IP://10.57.10.180:26</p> <p>For 802.11 Wireless devices, use in the form: TLS12://TLSDEVICESTRIALNUMBER TLS12TRUST://TLSDEVICESTRIALNUMBER Example, TLS12://TLS99261829170E0810                   TLS12TRUST://TLS99261829170E0810</p> <p>For BLE devices, use the form: BLEEMV://DEVICENAME Example, BLEEMV://DPG123456789A DEVICENAME is listed in the operating system Bluetooth settings.</p>
WaitTime	Time in seconds the device will wait for the action to be completed. (1 - 255)
PinMode	<p>Message to display as a user prompt:</p> <p>0 = PINsgEnterPIN 1 = PINMsgEnterPINAmt 2 = PINMsgReenterPINAmt 3 = PINMsgReenterPIN 4 = PINMsgVerifyPIN</p>
MaxPinLength	Maximum PIN length. Must be less than 13.
MinPinLength	Minimum PIN length. Must be greater than 3.
Options	<p>PIN verification and format:</p> <p>0 = ISO0 Format, No verify PIN 1 = ISO3 Format, No verify PIN 2 = ISO0 Format, Verify PIN 3 = ISO3 Format, Verify PIN</p>
Tones	<p>Tones to use:</p> <p>0 = No sound 1 = One beep 2 = Two beeps</p>
FieldSeparator	Delimiter to separate the output data.

### 3 - MagneFlex Powder Resources

---

Parameter	Description
CloseDevice	Flag which determines whether the connection to the device will be closed after the request is processed. Default value is “false”. “false” = Do no close the device. “true” = Close device.
EndSession	Flag which determines whether an EndSession command is sent to the device after the request is processed. Default value is “false”. When set to false, this flag may facilitate the display of a custom message after a request is processed. “false” = Do no end the session. “true” = End the session.

Return Value:  
The PIN output.

```
{"PINOutput": {"PINData":,}, "AdditionalOutputData":{}}
```

### 3.6 RequestSignature

Prompts the user to sign.

Using Method POST:

```
api/mtpscrahost/RequestSignature (  
string DeviceID,  
int WaitTime,  
int Options,  
int Tones,  
boolean CloseDevice,  
boolean EndSession);
```

### 3 - MagneFlex Powder Resources

Parameter	Description
DeviceID	<p>URI of the device.</p> <p>For USB devices, Use an empty string to open the first device found. Otherwise use: USB://DEVICESTRIALNUMBER Example, USB://99261829170E0810</p> <p>For Ethernet devices, use the form: IP://IPAddress:PORT Example, IP://10.57.10.180:26</p> <p>For 802.11 Wireless devices, use in the form: TLS12://TLSDEVICESTRIALNUMBER TLS12TRUST://TLSDEVICESTRIALNUMBER Example, TLS12://TLS99261829170E0810           TLS12TRUST://TLS99261829170E0810</p> <p>For BLE devices, use the form: BLEEMV://DEVICENAME Example, BLEEMV://DPG123456789A DEVICENAME is listed in the operating system Bluetooth settings.</p>
WaitTime	Time in seconds the device will wait for the action to be completed. (1 - 255)
Options	Option to select the timeout behavior. 0 = Timeout will clear data 1 = Timeout with available data, signature can be retrieved if exists
Tones	Tones to use: 0 = No sound 1 = One beep 2 = Two beeps
CloseDevice	Flag which determines whether the connection to the device will be closed after the request is processed. Default value is "false". "false" = Do no close the device. "true" = Close device.
EndSession	Flag which determines whether an EndSession command is sent to the device after the request is processed. Default value is "false". When set to false, this flag may facilitate the display of a custom message after a request is processed. "false" = Do no end the session. "true" = End the session.

Return Value:  
The Signature output.

```
{ "SignatureOutput": {
  "SignatureOutputStatus": ,
```

### 3 - MagneFlex Powder Resources

```
"SignatureData":} ,  
"AdditionalOutputData":{}}
```

#### 3.7 RequestSmartCard

Begins an EMV transaction.

Using Method POST:

```
api/mtpscrahost/RequestSmartCard(  
string DeviceID,  
int CardType,  
int ConfirmationWaitTime,  
int PINEntryWaitTime,  
int Tones,  
int Options,  
int TransactionType,  
decimal Amount,  
decimal CashBack,  
int Reserved,  
array AdditionalRequestData,  
boolean CloseDevice,  
boolean EndSession);
```

Parameter	Description
DeviceID	<p>URI of the device.</p> <p>For USB devices, Use an empty string to open the first device found. Otherwise use: USB://DEVICESTRIALNUMBER Example, USB://99261829170E0810</p> <p>For Ethernet devices, use the form: IP://IPAddress:PORT Example, IP://10.57.10.180:26</p> <p>For 802.11 Wireless devices, use in the form: TLS12://TLSDEVICESTRIALNUMBER TLS12TRUST://TLSDEVICESTRIALNUMBER Example, TLS12://TLS99261829170E0810           TLS12TRUST://TLS99261829170E0810</p> <p>For BLE devices, use the form: BLEEMV://DEVICENAME Example, BLEEMV://DPG123456789A DEVICENAME is listed in the operating system Bluetooth settings.</p>

### 3 - MagneFlex Powder Resources

Parameter	Description
CardType	Card type that can be used for the transaction: 1 = Magnetic stripe 2 = Contact smart card 3 = Magnetic stripe or contact smart card 4 = Contactless smart card (Not supported on DynaPro Mini) 5 = Contactless smart card + magnetic stripe 6 = Contactless smart card + contact smart card 7 = Magnetic stripe + contact smart card + contactless smart card.
ConfirmationWaitTime	Time the device will wait for the user to begin the transaction.
PINEntryWaitTime	Time the device will wait for the user to enter the PIN.
Tones	Tones to use: 0 = No sound 1 = One beep 2 = Two beeps
Options	Transaction options: 0 = Normal 1 = Bypass PIN 2 = Force Online 4 = Acquirer not available
TransactionType	Type of transaction to be used: 0x02 = Cash back 0x04 = Goods 0x08 = Services
Amount	The amount to be used and authorized in decimal format. 1.01 = 1 dollar and 1 cent
CashBack	The amount of cashback to be used and authorized in decimal format. 1.01 = 1 dollar and 1 cent
Reserved	Reserved for future use. These are the reserved bytes beginning at index 20 of the 0xA2 command. Reference device manual <b>D99875585</b> for more details. Example: 00000000000000000000000000000000084000 <b>01</b> 00 – QuickDip Mode 0000000000000000000000000000000008400000 <b>03</b> – PIN Verify 0000000000000000000000000000000008400000 <b>04</b> – PIN Set
AdditionalRequestData	Additional key/value pairs of data
CloseDevice	Flag which determines whether the connection to the device will be closed after the request is processed. Default value is “false”. “false” = Do no close the device. “true” = Close device.



### 3 - MagneFlex Powder Resources

---

Parameter	Description
EndSession	Flag which determines whether an EndSession command is sent to the device after the request is processed. Default value is “false”. When set to false, this flag may facilitate the display of a custom message after a request is processed. “false” = Do no end the session. “true” = End the session.

Return Value:

The Transaction output.

```
{"TransactionOutput": {}}
```

### 3.8 RequestSendAcquirerResponse

Sends the ARPC to the device.

Using Method POST:

```
api/mtppscrahost/RequestSendAcquirerResponse (  
string DeviceID,  
int WaitTime,  
int WaitTimeBeforeTransactionComplete,  
string IssuerAuthenticationData,  
string IssuerScriptTemplatel,  
string IssuerScriptTemplate2,  
int ApprovalStatus,  
string KSN,  
string DeviceSerialNumber,  
array AdditionalRequestData,  
boolean CloseDevice,  
boolean EndSession);
```

### 3 - MagneFlex Powder Resources

Parameter	Description
DeviceID	<p>URI of the device.</p> <p>For USB devices, Use an empty string to open the first device found. Otherwise use:            USB://DEVICSERIALNUMBER            Example, USB://99261829170E0810</p> <p>For Ethernet devices, use the form:            IP://IPAddress:PORT            Example, IP://10.57.10.180:26</p> <p>For 802.11 Wireless devices, use in the form:            TLS12://TLSDEVICSERIALNUMBER            TLS12TRUST://TLSDEVICSERIALNUMBER            Example, TLS12://TLS99261829170E0810                              TLS12TRUST://TLS99261829170E0810</p> <p>For BLE devices, use the form:            BLEEMV://DEVICENAME            Example, BLEEMV://DPG123456789A            DEVICENAME is listed in the operating system Bluetooth settings.</p>
WaitTime	Time in seconds the device will wait for the action to be completed. (1 - 255)
WaitTimeBeforeTransactionComplete	Time in seconds to wait after receiving the transaction response before the transaction is complete.
IssuerAuthenticationData	Issuer response to the transaction request in hexadecimal format. This field is for the data portion of the EVM Tag 91.
IssuerScriptTemplate1	Issuer Script to send to ICC in hexadecimal format. This field is for the data portion of the EVM Tag 71.
IssuerScriptTemplate2	Issuer Script to send to ICC in hexadecimal format. This field is for the data portion of the EVM Tag 72.
ApprovalStatus	Status from acquirer/issuer. This field represents the data portion of the EMV Tag 8A. Example: 0 – Approve 1 – Decline
KSN	Key serial number used for the transaction
DeviceSerialNumber	Device serial number
AdditionalRequestData	Additional key/value pairs of data

### 3 - MagneFlex Powder Resources

---

CloseDevice	Flag which determines whether the connection to the device will be closed after the request is processed. Default value is “false”. “false” = Do no close the device. “true” = Close device.
EndSession	Flag which determines whether an EndSession command is sent to the device after the request is processed. Default value is “false”. When set to false, this flag may facilitate the display of a custom message after a request is processed. “false” = Do no end the session. “true” = End the session.

Return Value:

The Transaction output

```
{"TransactionOutput": {}}
```

#### 3.9 ReleaseDevice

Closes the connection to the device.

Using Method POST:

```
api/mtpscrahost/ReleaseDevice();
```

Return Value:

None.

#### 3.10 RequestSendCommand

Sends a command to device and returns the raw response from device.

Using Method POST:

```
api/mtpscrahost/RquestSendCommand(  
string DeviceID,  
int WaitTime,  
string Data,  
enum RequestType,  
string WaitForReport,  
boolean CloseDevice,  
boolean EndSession);
```

### 3 - MagneFlex Powder Resources

Parameter	Description
DeviceID	<p>URI of the device.</p> <p>For USB devices, Use an empty string to open the first device found.            Otherwise use:            USB://DEVICESERIALNUMBER            Example, USB://99261829170E0810</p> <p>For Ethernet devices, use the form:            IP://IPAddress:PORT            Example, IP://10.57.10.180:26</p> <p>For 802.11 Wireless devices, use in the form:            TLS12://TLSDEVICESERIALNUMBER            TLS12TRUST://TLSDEVICESERIALNUMBER            Example, TLS12://TLS99261829170E0810                      TLS12TRUST://TLS99261829170E0810</p> <p>For BLE devices, use the form:            BLEEMV://DEVICENAME            Example, BLEEMV://DPG123456789A            DEVICENAME is listed in the operating system Bluetooth settings.</p>
WaitTime	Time in seconds the device will wait for the action to be completed. (1 - 255)
Data	Hex string for command. Reference device manual for details.
RequestType	<p>"SET" for commands where the ACK status is to be returned.            "GET" for commands where the data is to be returned.</p>
WaitForReport	<p>The report number to wait for before returning the response.</p> <p>Example:            Command 30 00 (Set KSN) will respond with an ACK (01) or with data in Get Mode (30).            WaitForReport = "01" will return the response for ACK report (01).            WaitForReport = "30" will return the data report (30).</p> <p>Reference device manual for report numbers corresponding to a command request.</p>
CloseDevice	<p>Flag which determines whether the connection to the device will be closed after the request is processed. Default value is "false".</p> <p>"false" = Do not close the device.            "true" = Close device.</p>

### 3 - MagneFlex Powder Resources

---

EndSession	Flag which determines whether an EndSession command is sent to the device after the request is processed. Default value is “false”. When set to false, this flag may facilitate the display of a custom message after a request is processed. “false” = Do not end the session. “true” = End the session.
------------	---

Return Value:

The Data output in Hex string format of device raw response for this command.

```
{
  "Data": ,
  "AdditionalOutputData": null
}
```

#### 3.11 RequestOperationStatus

Retrieves the operation status of the device.

Using Method POST:

```
api/mtpscrahost/RquestOperationStatus();
```

Return Value:

The Operation status output.

```
{
  "OperationStatus": ,
  "DeviceID": null,
  "AdditionalOutputData": null
}
```

## 4 - MagneFlex Powder Response Output Structures

---

### 4 MagneFlex Powder Response Output Structures

The MagneFlex Powder returns the following outputs.

#### 4.1 CheckHealth Output

Returned after CheckHealth. A string array containing API name and status.

Example:

```
[  
  "MagTek PPSCRA WEB API",  
  "OK"  
]
```

#### 4.2 CardSwipe Output

Returned after a card swipe.

Example :

```
{  
  "CardSwipeOutput": {  
    "CardOperationStatus": 0,  
    "CardStatus": 0,  
    "CardType": 1,  
    "DataType": 34,  
    "EncryptedMagnePrint":  
"787E070A18ECF5087595FD4CDE53E550051E719BDCBCF29C7646D6B5AF90EEEEEA8871  
3ADE97F118095C8CF3C36426FAD860E1BF5C3465D21",  
    "EncryptedTrack1":  
"C5389DFDB735F9D9EF628E0FDC446FB9CCBE959DECD22655737B41CD249D6C67244  
6BF77A3738D09FBF8DD55A61906CB50C697994344DDFE657C3F8ED287BD4141788C400  
BAEFBA0E52BE1498AE186",  
    "EncryptedTrack2":  
"12BA7B8F7386EB4ED1EAD4467E621E26930A269FA733607B73AEE894F8F9B5A336706  
6B822881FE5",  
    "EncryptedTrack3":  
"12BA7B8F7386EB4ED1EAD4467E621E26F727B4225A3C8F73351BEF09B1ED74971CE9A  
1B4F84A1440109735A65864FAA2384D29912454DE6B37485C4060D8809AD7A00C24F2D  
78A340CEBDD00CE0AF419BAC7C9F89DD4415D45B578B962EE4126D6EB943ABC5D729B4  
5E7C09060B3E3AB",  
    "EncryptedMagnePrintLength": 56,  
    "EncryptedMagnePrintStatus": 0,  
    "EncryptedTrack1Length": 80,  
    "EncryptedTrack1Status": 0,  
    "EncryptedTrack2Length": 40,  
    "EncryptedTrack2Status": 0,  
    "EncryptedTrack3Length": 112,  
    "EncryptedTrack3Status": 0,  
    "MagStripeStatus": 0,  
    "PANDataLength": 32,  
    "Track1Length": 78,  
    "Track1Status": 0,  
  }  
}
```



## 4 - MagneFlex Powder Response Output Structures

```
    "DataType": 34,
    "EncryptedMagnePrint": "",
    "EncryptedTrack1":
"D5FCF8CAA7EB399A13D097C58D6D39123EA41CDCB45E3C3C4FAF1741984114DC5BD60
6E2AD201321C00E08A359B42D7CB4EA09B8853D11161E505BB7EF621CDD",
    "EncryptedTrack2":
"819EAA4AF1962A3BD08AEC151002BB03C42D731AAD37CC76DDD8BCDE0F93963BA9CED
1B157D630D4",
    "EncryptedTrack3": "",
    "EncryptedMagnePrintLength": 0,
    "EncryptedMagnePrintStatus": 1,
    "EncryptedTrack1Length": 64,
    "EncryptedTrack1Status": 0,
    "EncryptedTrack2Length": 40,
    "EncryptedTrack2Status": 0,
    "EncryptedTrack3Length": 0,
    "EncryptedTrack3Status": 1,
    "MagStripeStatus": 0,
    "PANDataLength": 32,
    "Track1Length": 57,
    "Track1Status": 0,
    "Track2Length": 39,
    "Track2Status": 0,
    "Track3Length": 0,
    "Track3Status": 1,
    "StatusCode": 0,
    "CardData":
"CardType=3|OperationStatus=0|CardStatus=0|DataType=34|Track1Status=0|
Track1Length=57|Track1=%M1111000004000001111^MANUAL
ENTRY/^22220000000000000000?|Track2Status=0|Track2Length=39|Track2=;11
11000004000001111=222200000000000000?|Track3Status=1|Track3Length=0|Tra
ck3=|EncTrack1Status=0|EncTrack1Length=64|EncTrack1=D5FCF8CAA7EB399A13
D097C58D6D39123EA41CDCB45E3C3C4FAF1741984114DC5BD606E2AD201321C00E08A3
59B42D7CB4EA09B8853D11161E505BB7EF621CDD|EncTrack2Status=0|EncTrack2Le
ngth=40|EncTrack2=819EAA4AF1962A3BD08AEC151002BB03C42D731AAD37CC76DDD8
BCDE0F93963BA9CED1B157D630D4|EncTrack3Status=1|EncTrack3Length=0|EncTr
ack3=|EncMPStatus=1|EncMPLength=0|EncMP=|MPSTS=00000000|MSStatus=0|KSN
=9500030000000120073E|SerialNumber=98D90C660E070F0E|PAN=819EAA4AF1962A
3BD08AEC151002BB03C42D731AAD37CC7673CBBC8B99470A82|CBCMAC=35F8A181",
    "CBCMAC": "35F8A181",
    "KSN": "9500030000000120073E",
    "MagnePrintStatus": "00000000",
    "PANData":
"819EAA4AF1962A3BD08AEC151002BB03C42D731AAD37CC7673CBBC8B99470A82",
    "MagTekSerialNumber": "98D90C660E070F0E",
    "Track1": "%M1111000004000001111^MANUAL
ENTRY/^22220000000000000000?",
    "Track2": ";1111000004000001111=222200000000000000?",
    "Track3": ""
  },
  "StatusCode": 0,
```



## 4 - MagneFlex Powder Response Output Structures

```
"AdditionalOutputData": null
}
```

### 4.4 PIN Output

Returned after a PIN request.

The PINData key contains a comma delimited value:

Field Name	Value
PIN KSN	PIN Key serial number
EPB	Encrypted PIN block
opStatus	Operation status

Example:

```
{
  "PINOutput": {"PINData": "9A006300000001200065,59D0274E9F58DD5F,0"},
  "AdditionalOutputData": null
}
```

### 4.5 Signature Output

Returned after a Signature request.

Example:

```
{
  "SignatureOutput": {
    "SignatureOperationStatus": 0,
    "SignatureData":
"FF0UXBvcFVsVWhVZFlgWVxZWFlUWVbdTF1EYThhNGEwYShhJGecZRR1EGUMZQR1AGT8ZP
hk9GjwaOxo6GjkbORs6GzscPBw9HD4dPx1BhkMfRh9HIEggSSBKIU0iTiJPI1AjUiRTJFQ
lVCVVJlUnVShVKFQoUylSKVEpUCpPKk4qTCTKK0gsRixELEEtPy09LTwtOi44LjcuNi41L
jQuMy40LjUuNi43LzgvOS86LzvwPS9AMEEwQzBFMEgxSjFLMU0yTzJRM1Q0VjRXNFg1WDV
ZN1k3WDhXOVU5VDpTOlI7UTxOPU09TD5JQEdBRUFEQ0JEQRART9GPkc9SDxIO0k6SjhLO
Es3TDdMnk01TjROM04yTjNNM0w0SzVKNko3SThIOUg6RztGPEU/REBDQUJDQkRARz9JPks
8TjxPO1E6UTlSOVP//0Y1RjZGN0c3RzhHOuc6SDtIPEg9ST5JQE1BSkNLRUtGTEhMSk5NT
k9QU1BTUlDWFNZVFtVXVZeV19YX1hg//9PTk5OTk1NTUxMS0xKTEdKRkpESUNJQUhASD5
HPUc7Rz1GNkY1Rv//bDFrMGowaTBoMGcwZjBkMGMwYjFhMWAYXjNdNFw1WzZaN1o4WT1ZO
lg8Vz1XP1Y/VkBVQ1VEVUZUR1RjVEpUTFROVE9VUVVTV1RXVdWWFdzV1pYW1lcwV5ZX1l
hWWJZZFh1WGZXZ1doVmpValVsVG1Tb1JvUnBRcVFyUHJPdE90TnVODk12THdMd0t3SndJd
0h3R3dGd0V3RHdDd0J3QXdAdkBlQHRac0ByQHFAcEBvQG5BbUFsQWtBa0JqQmlCaUNoQ2d
DZkR1RGREZEVjRWJFYkZhrmBGX0dfrv//fC18LnwvfS5+Ln8ugC2CLYMthC2FLIYsiCyJL
IoriyuMK44rjyuRK5MrlCuULJUs1iz//4otiy2LLIsriiqKKYqiSjJK4ksiS2JLokviTC
IM4g2iDeIO4g+iECIQYhDiEaJSiLLiUyJTYpOik+LUP//nCyDLZ0unS+dMJ0xnTKdNJ01n
TadN505nTuePJ49nkCeQZ5EnkWeRp5HnkiesZ9K//+fLqAuoS6iLaMtpC2lLaUspiyoK6k
rqiuRkqwrSquKa8q//+gP6A+oD2hPaE8ojyJ06Q7pTunOqg6qjqrOaw5rTmuOa86sDqxO
///n0z//59MoEygS6FLoUqiSqNKpEmmSKdIqEepR6tGrEatRq9FsUX//8EswSvBKsErwCv
ALMATwC7AL78wvzK/M780vza/Ob86vzy/Pb8/v0K/Rb9Hv0i/Sb9KwEv//788wDzBPmI7w
zrEOsQ5xTnGOMg3yTbKNcs0zDTNM88y0THSMNMv1C/VLtYu//DPsM9xD3EPsU+xj/HP8h
AyUHLQsxDzkTPRdBf0kfTSNVK1krXTNHN2U7aUP/"
```

SDK - MagneFlex Powder, Middleware, | PIN PEDs | Programmer's Manual (MagneFlex API)







### Appendix A TLV Data Format

#### A.1 ARQC Message Format

This section gives the format of the ARQC Message delivered in the ARQC Message notification. It is a TLV object with the following contents:

```
F9<len>/* container for MAC structure and generic data */
  DFDF54 (MAC KSN)<len><val>
  DFDF55 (MAC Encryption Type)<len><val>
  DFDF25 (IFD Serial Number)<len><val>
  FA<len>/* container for generic data */
    70<len>/*container for ARQC */
      DFDF53<len><value>/*fallback indicator */
      5F20<len><value>/*cardholder name */
      5F30<len><value>/*service code */
      DFDF4D<len><value>/* Mask T2 ICC Data */
      DFDF52<len><value>/* card type */
      F8<len>/*container tag for encryption */
        DFDF59(Encrypted Data Primitive)<len><Encrypted Data val (Decrypt
data to read tags)>
        DFDF56(Encrypted Transaction Data KSN)<len><val>
        DFDF57(Encrypted Transaction Data Encryption Type)<val>
        DFDF58(# of bytes of padding in DFDF59)<len><val>
(Buffer if any to be a multiple of 8 bytes)
CBC-MAC (4 bytes, always set to zeroes)
```

#### A.2 ARQC Response (from online processing)

This section gives the format of the data for the Online Processing Result / Acquirer Response message. This request is sent to the reader in response to an ARQC Message notification from the reader. It is a TLV object with the following contents:

```
F9<len>/* container for MAC structure and generic data */
  DFDF54 (MAC KSN)<len><val>
  DFDF55 (Mac Encryption Type)<len><val>
  DFDF25 (IFD Serial Number)<len><val>
  FA<len>/* Container for generic data */
    70<len>/* Container for ARQC */
      8A<len> approval
(ARQC padding, if any, to be a multiple of 8 bytes)
CBC-MAC (4 bytes, use MAC variant of MSR DUKPT key that was used in ARQC request, from
message length up to and including ARQC padding, if any)
```

### A.3 Transaction Result Message – Batch Data Format

This section gives the format of the data the device uses to do completion processing

```
FE<len> /* container for generic data */
  DFDF25(IFD Serial Number)<len><val>
  FA<len> /* container for generic data */
    F0<len> /* Transaction Results */
      F1<len> /* container for Status Data */
      ... /* Status Data tags */

      F2<len> /* container for Batch Data */
      ... /* Batch Data tags defined in DFDF17 */
      ... /* Note: Sensitive Data cannot be defined in DFDF17 */

      F3<len> /* container for Reversal Data, if any */
      ... /* Reversal Data tags defined in DFDF05 */
      ... /* Note: Sensitive Data cannot be defined in DFDF05 */

      F7<len> /* container for Merchant Data */
      ... /* < Merchant Data tags */

      F8<len> /* container tag for encrypted data */
      DFDF56(Encrypted Transaction Data KSN)<len><val>
      DFDF57(Encrypted Transaction Data Encryption Type)<val>

      FA<len> /* container for generic data */
      DF30(Encrypted Tag 56 TLV, T1 Data)<len><val>
      DF31(Encrypted Tag 57 TLV, T2 Data)<len><val>
      DF32(Encrypted Tag 5A TLV, PAN)<len><val>
      DF35(Encrypted Tag 9F1F TLV, T1 DD)<len><val>
      DF36(Encrypted Tag 9F20 TLV, T2, DD)<len><val>
      DF37(Encrypted Tag 9F61 TLV, T2 CVC3)<len><val>
      DF38(Encrypted Tag 9F62 TLV, T1, PCVC3)<len><val>
      DF39(Encrypted Tag DF812A TLV, T1 DD)<len><val>
      DF3A(Encrypted Tag DF812B TLV), T2 DD<len><val>
      DF3B(Encrypted Tag DFDF4A TLV, T2 ISO Format)<len><val>
```