MAGENSA™
A MAGTEK COMPANY

Magensa Decrypt Service

Decrypt 2.0 Operations
Decrypt 2.0 Programming Manual

April 7, 2020

Document Number:
D998200346-20

REGISTERED TO ISO 9001:2015

Magensa, LLC I 1710 Apollo Court I Seal Beach, CA 90740 I Phone: (562) 546-6500 I Technical Support: (888) 624-8350
www.magensa.net

1 Revisions

Rev Number	Date	Notes
10-1	29 March 2019	Initial draft with DecryptCardSwipe operation
10-2	April 2019	As suggested modified input and output properties with the existing document.
10-3	April 2019	Updated the document with DecryptData operation.
10-4	23 April 2019	Updated the document based on below. Review comments provided GenerateMac operation
10-5	29 April 2019	Removed “Console Application Request and Response” section from all the operations
10-6	2 May 2019	Added “Status Codes and Messages” section in table of content.
10-7	07 July 2019	Modified Styles using Magtek theme and Style template
20	07 April 2020	Updated confidential information
20-1	07 April 2020	Updated with Magensa logo

2 Purpose of the Document

The purpose of this document is to provide description of Magensa Decrypt web service call operations.

3 Table of Contents

4 Introduction

Decrypt is one of the Magensa web services used for the POS (Point of Sale) transactions. At POS transactions high security is required as extremely sensitive information is handled.
In the decrypt service, we are going to deal with the below three operations.

- DecryptCardSwipe
- DecryptData
- GenerateMac

5 Decrypt 2.0 Operations

5.1 DecryptData

A command used to decrypt a block of data. This command supports any data encrypted by a MagTek reader including bulk data or individually encrypted fields such as tracks.

5.1.1 Input Properties

Property(*)	Value	Description
BillingLabel	<string>	A user selected value that can be included in Reports or Requests. Max length of 64 characters
CustomerTransactionID	<string>	A user selected value that can be included in Reports or Requests. Max length of 256 characters.
CustomerCode *	<string>	Customer code provided by Magensa at onboard time.
Password *	<string>	Password credential provided by Magensa at onboard time.
UserName *	<string>	User name credential provided by Magensa at onboard time.
Encrypted Data	<string>	Encrypted data block cryptogram in Hexadecimal format in multiples of 8 byte blocks (16 characters per block).
KSN *	<string>	Key Serial Number of the reader
KeyType *	<string>	Key type to be used to decrypt the data block cryptogram. This value shall be set to match the reader configuration. Enum values: `Pin` - Pin variant key `Data` - Data variant key

Note: * = Required

5.1.2 Output Properties

Property		Value	Property Description
CustomerTransactionID		<string>	A user selected value that can be included in Reports or Requests. Max length of 256 characters.
IsReplay		<string>	Boolean value informing that the KSN has been used in a prior transaction. Enum values: `true` – KSN has been used in a prior transaction. `false` – KSN has not been used prior to current transaction.
MagTranId		<string>	Transaction ID in GUID alpha numeric form.
DecryptedData		<string>	Decrypted data including any pad characters.

5.1.3 DecryptData Request

```
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:tem="http://tempuri.org/"
xmlns:dec="http://schemas.datacontract.org/2004/07/Decrypt.Core">
<soapenv:Header/>
<soapenv:Body>
<tem:DecryptData>
<!--Optional:-->
<tem:request>
<!--Optional:-->
<dec:BillingLabel></dec:BillingLabel>
<!--Optional:-->
<dec:CustomerTransactionID></dec:CustomerTransactionID>
<!--Optional:-->
<dec:Authentication>
<!--Optional:-->
<dec:CustomerCode>customercode</dec:CustomerCode>
<!--Optional:-->
<dec:Password>password</dec:Password>
<!--Optional:-->
<dec:Username>username</dec:Username>
</dec:Authentication>
<!--Optional:-->
<dec:EncryptedData>5F260E4080089DB1F2DAE45114E285C81C47B8395B33C547C23
1538C7447C3EBCAB430B57E491E332640EEDB3871B5F4A347DE69258B8B39E870A0BAE
3DF59E17050F77DB3E46FDDE46F4CF6DB0BA63961085FBDE67AA4359A727BB6250EA1A
9CFC51B609C83152DD63BF8989B0E9273713F6BFD80BE5526FB1E5B50ABEC706289726
3307607A714A2C1822A3DEC72987E0C4D44412ECFC38CD0424AD77CDAC01B288074D8A
36E528F79DF81DE739FA05AECD54A13518F4C290EA3DDFCCA6C6ACFF0012FC3939D02C
D13704B08D23CA00DBF7681A32B1ACB2822854BBDE9CE75D20B5E0D89968F502546F13
34B822E094C4AFE52ACA66E2662F0AD4B17314A64F28477E22D5F2B33</dec:Encrypt
edData>
<!--Optional:-->
<dec:KSN>9011400B487DBC000011</dec:KSN>
<!--Optional:-->
<dec:KeyType>Data</dec:KeyType>
</tem:request>
</tem:DecryptData>
</soapenv:Body>
</soapenv:Envelope>
```

Below is the soap response for DecryptData operation of Decrypt service.
https://svc72.magensa.net/DecryptV3/Decrypt.svc?wsdl

5.1.4 DecryptData Response

```
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">
        <s:Body>
           <DecryptDataResponse xmlns="http://tempuri.org/">
             <DecryptDataResult
xmlns:a="http://schemas.datacontract.org/2004/07/Decrypt.Core"
xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
                 <a:CustomerTransactionId/>
                 <a:IsReplay>true</a:IsReplay>
                 <a:MagTranId>2c193b5c-de38-43d5-bc3b-
73f34b812ea2</a:MagTranId>
<a:DecryptedData>FC820102F28200FE820239008E120000000000000000420344034
1031E031F035F24031909305F25031711019F0607A00000000410109F0702FFC09F0D0
5BC50BC08009F0E0500000000009F0F05BC70BC98009F10120210600003220000000000
0000000000000FF9F2608B4E47438FF561F5B9F2701409F360200039505040000800009
B02E8009C01009F33032028C89F34031E03009F3704486F61809F4005720000B0015A0
8532561480001345 59F02060000000015009F03060000000000009F1A0208405713532
5614800013455D190920100100005410000F8A0230309F10120210600003220000000000
0000000000000FF50104465626974204D617374657243617264000</a:DecryptedDa
ta>
              </DecryptDataResult>
           </DecryptDataResponse>
        </s:Body>
     </s:Envelope>
```

5.2 GenerateMac

A command used to generate a MAC (Message Authentication Code) against a data block.

5.2.1 Input Properties

The GenerateMac operation request has below Input properties.

Property	Value	Description
BillingLabel	<string>	A user selected value that can be included in Reports or Requests. Max length of 64 characters.
CustomerTransactionID	<string>	A user selected value that can be included in Reports or Requests. Max length of 256 characters.
CustomerCode *	<string>	Customer code provided by Magensa at onboard time.
Password *	<string>	Password credential provided by Magensa at onboard time.
UserName *	<string>	User name credential provided by Magensa at onboard time.
DataToMAC*	<string>	Encrypted data block cryptogram in Hexadecimal format in multiples of 8 byte blocks (16 characters per block).
KSN *	<string>	Key Serial Number of the reader
KeyDerivationType*	<string>	Key type to be used to decrypt the data block cryptogram. This value shall be set to match the reader configuration. Enum values: `DUKPT` - **DUKPT method** `Fixed`- **Fix method**

Note: * = Required

5.2.2 Output Properties

Property	Value	Description
CustomerTransactionID	<string>	Customer transaction ID
IsReplay	<string>	Boolean value informing that the KSN has been used in a prior transaction. Enum values: `true` – KSN has been used in a prior transaction. `false` – KSN has not been used prior to current transaction.
MagTranId	<string>	Transaction ID in GUID alpha numeric form.
MACedString	<string>	MAC bytes (16 Hex characters)

GenerateMac is for generating a Message Authentication Code (MAC) against a data block. MAC is used to authenticate a message, to confirm that the message came from the authorized sender and has not been changed. Mac protects both data integrity and authenticity of the message.

5.2.3 GenerateMac Request

```
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:tem="http://tempuri.org/" xmlns:dec="http://schemas.datacontract
.org/2004/07/Decrypt.Core">
<soapenv:Header/>
<soapenv:Body>
<tem:GenerateMac>
<tem:request>
<dec:BillingLabel>BillingLabel</dec:BillingLabel>
<dec:CustomerTransactionID>CustomerTransactionID</dec:CustomerTransact
ionID>
<dec:Authentication><dec:CustomerCode>customercode</dec:CustomerCode>
<dec:Password>password</dec:Password>
<dec:Username>username</dec:Username>
</dec:Authentication>
sedec:DataToMAC>34303132333435363738393039443938370000000000000</dec:
DataToMAC>
<dec:KSN>9010010B31ED13000001</dec:KSN>
<dec:KeyDerivationType>DUKPT</dec:KeyDerivationType>
</tem:request>
</tem:GenerateMac>
</soapenv:Body>
</soapenv:Envelope>
```

5.2.4 GenerateMac Response

```
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">
   <s:Body>
      <GenerateMacResponse xmlns="http://tempuri.org/">
         <GenerateMacResult
xmlns:a="http://schemas.datacontract.org/2004/07/Decrypt.Core"
xmlns:i="http://www.w3.org/2001/XMLSchema-instance">

<a:CustomerTransactionId>CustomerTransactionID</a:CustomerTransactionI
d>
            <a:IsReplay>true</a:IsReplay>
            <a:MagTranId>00350c72-23bf-4da6-9bb7-
b4804889f4df</a:MagTranId>
            <a:MACedString>2F19A27110AA871E</a:MACedString>
         </GenerateMacResult>
</GenerateMacResponse>
   </s:Body>
</s:Envelope>
```

5.3 DecryptCardSwipe

A command used to decrypt card swipes.

5.3.1 Input Properties

Property	Value	Property Description
BillingLabel	<string>	A user selected value that can be included in Reports or Requests. Max length of 64 characters.
CustomerTransactionID	<string>	A user selected value that can be included in Reports or Requests. Max length of 256 characters.
CustomerCode *	<string>	Customer code provided by Magensa at onboard time.
Password *	<string>	Password credential provided by Magensa at onboard time.
UserName *	<string>	User name credential provided by Magensa at onboard time.
DeviceSN	<string>	Device serial number of the reader
KSN *	<string>	Key serial number of the reader
KeyType *	<string>	Key type to be used to decrypt the data block cryptogram. This value shall be set to match the reader configuration. Enum values: `Pin` - Pin variant key `Data` - Data variant key
MagnePrint *	<string>	Copy the data exactly as it is transmitted from the reading device. If the transaction is hand keyed, fill this field with 112 zeros.
MagnePrintStatus *	<string>	Copy the data exactly as it is transmitted from the reading device. If the transaction is hand keyed, fill this field with 8 zeros.
Track1	<string>	Encrypted Track 1 data in Hexadecimal format in multiples of 8 byte blocks (16 characters per block).
Track2 *	<string>	Encrypted Track 2 data in Hexadecimal format in multiples of 8 byte blocks (16 characters per block).
Track3	<string>	Encrypted Track 3 data in Hexadecimal format in multiples of 8 byte blocks (16 characters per block).

Note: * = Required

5.3.2 Output Properties

Property	Value	Property Description
CustomerTransactionID	<string>	Customer transaction ID
IsReplay	<string>	Boolean value informing that the KSN has been used in a prior transaction. Enum values: `true` – KSN has been used in a prior transaction. `false` – KSN has not been used prior to current transaction.
MagTranId	<string>	Transaction ID in GUID alpha numeric form.
CardID	<string>	Hashed CardID.
MagnePrint	<string>	MagnePrint decrypted value.
Track1	<string>	Decrypted Track 1 data.
Track2	<string>	Decrypted Track 2 data.
Track3	<string>	Decrypted Track 3 data.
MagnePrintScore	<string>	MagnePrint Score. Valid scores are greater than or equal to -1 and less than or equal to 1. Any score above 1 is an error.

The Web Services Description Language URL for consuming this web service may be located at:
https://svc72.magensa.net/DecryptV3/Decrypt.svc?wsdl

5.3.3 DecryptCardSwipe Request

```
<?xml version="1.0" encoding="UTF-8"?>
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:dec="http://schemas.datacontract.org/2004/07/Decrypt.Core"
xmlns:tem="http://tempuri.org/">
   <soapenv:Header />
   <soapenv:Body>
      <tem:DecryptCardSwipe>
         <!--Optional:-->
         <tem:request>
            <!--Optional:-->
            <dec:BillingLabel>0</dec:BillingLabel>
            <!--Optional:-->
            <dec:CustomerTransactionID>0</dec:CustomerTransactionID>
            <dec:Authentication>
               <!--Optional:-->
               <dec:CustomerCode>customercode</dec:CustomerCode>
               <!--Optional:-->
               <dec:Password>password</dec:Password>
               <!--Optional:-->
               <dec:Username>username</dec:Username>
            </dec:Authentication>
           <dec:EncryptedCardSwipe>
               <!--Optional:-->
               <dec:DeviceSN>B487DA9022119AA</dec:DeviceSN>
               <dec:KSN>9011400B487DA9000007</dec:KSN>
               <!--Optional:-->
               <dec:KeyType>Pin</dec:KeyType>
               <!--Optional:-->
               <dec:MagnePrint>A4C4870970E452710FCBFD6D3388ECC2121D4B2
8A0282DEA7523A5E9470B6B731D28AE31A7C828B89E684A7413006EA5AB0BC4B51F74E
BAC</dec:MagnePrint>
               <!--Optional:-->
               <dec:MagnePrintStatus>61401400</dec:MagnePrintStatus>
               <!--Optional:-->
               <dec:Track1>54EE1021145099EC55772C6C00B0D3CE6BCE1B0266E
6483FD76F80243AE91286596AD0761840B731EC9A2168BB6943B3BE5FE7E605EF73212
2DC852E14DEF760BB40CBFE2F4B91AB</dec:Track1>
               <!--Optional:-->
               <dec:Track2>B156DB6D856FA0592C0C3029745053F9C1701836FB3
5B87E091BEE77E9446E97B86DD0D1CD5597D8</dec:Track2>
               <!--Optional:-->
               <dec:Track3 />
            </dec:EncryptedCardSwipe>
         </tem:request>
      </tem:DecryptCardSwipe>
   </soapenv:Body>
</soapenv:Envelope>
```

5.3.4 DecryptCardSwipe Response

```
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/">
<s:Body>
<DecryptCardSwipeResponse xmlns="http://tempuri.org/">
<DecryptCardSwipeResult
xmlns:a="http://schemas.datacontract.org/2004/07/Decrypt.Core"
xmlns:i="http://www.w3.org/2001/XMLSchema-instance">
<a:CustomerTransactionId>0</a:CustomerTransactionId>
<a:IsReplay>true</a:IsReplay>
<a:MagTranId>7fe9fb87-9220-4aa0-b5cb-5a003829132f</a:MagTranId>
<a:CardID>uISJfty0btbZIRbjfwLWjMrdOl0Es+r4LjGqZh45U1E=</a:CardID>
<a:DecryptedCardSwipe>
<a:MagnePrint>020020882CDC25063DA83890AB3E736FC7879F510AEBFD6F150B4D87
D8B94E9BCDE760932E0CED36C0702909E6D03808DF16D0026ACE0000</a:MagnePrint
><a:Track1>%B5325614800013455^CONTACTLESS/MAGTEK D^1909201001000P
00669000000?</a:Track1>
        <a:Track2>;5325614800013455=19092010010066910000?</a:Track2>
<a:Track3/>
</a:DecryptedCardSwipe><a:MagnePrintScore>0.7584068</a:MagnePrintScore
></DecryptCardSwipeResult>
</DecryptCardSwipeResponse>
</s:Body>
</s:Envelope>
```

6 Status Codes and Messages

Status Codes and Messages returned by Magensa for Decrypt 2.0 Operations.

Internal errors

Code	StatusMsg	Notes
5000	Unknown Error	

Input Validation Errors

Code	StatusMsg	Notes
601	EncryptedData is required	
602	KSN is required	
603	CustomerCode is required	
604	Username is required	
605	Password is required	
606	EncryptedData is not valid	Either the value was not HEX, not multiple of 16 characters, or the value was too long.
607	KSN is not valid	Either the value was not HEX, or the value was too long.
608	DataToMac is required	
610	Track2 is required	
611	MagnePrint is required	
612	Track2 is not valid	Either the value was not HEX, not multiple of 16 characters, or the value was too long.
613	MagnePrint is not valid	Either the value was not HEX, not multiple of 16 characters, or the value was too long.
614	MagnePrint Status is required	
615	CustomerTransactionID is not valid	Occurs if the length is more than 256 characters.
616	BillingLabel is not valid	Occurs if the length is more than 64 characters.
655	Track1 is not valid	Either the value was not HEX, not multiple of 16 characters, or the value was too long.
656	Track3 is not valid	Either the value was not HEX, not multiple of 16 characters, or the value was too long.
657	DataToMAC is not valid	Either the value was not HEX, not multiple of 16 characters, or the value was too long.

Other Errors

Code	StatusMsg	Notes
701	Access Denied	
702	Device Not Allowed	
706	KSID Access Denied	