Magensa Web Service

Decrypt 2.0 Operations

Decrypt 2.0 Programming Manual

April 8, 2020

Manual Part Number:
D998200040-90

REGISTERED TO ISO 9001:2015

Table 0.1 – Revision

Rev Number	Date	By	Notes
10	January 2015	Donnie James	Initial Release
20	January 2015	Rebecca Robinson	Removed "keyname" from generate Mac. Remove error code 609.
30	April 2015	Andy Deignan	Added support for returning the HashedCardID in the CardID Field.
40	Nov 2015	Rebecca Robinson	Changed MagnePrint to MagneprintScore pg 8
50	July 2016	Rebecca Robinson	Added 2.0 label to references to Decrypt.
60	October 2016	Donnie James	Removed Decrypt v2.0 fields
70	October 2016	Donnie James	Added SOAPAction Header to sample request, the WSDL links, explanation of KeyType, and Track1 Track3 validation codes. Updated 3-Error to 3=No MagnePrint available Updated descriptions for input and output properties: BillingLabel, CustomerTransactionID, CustomerCode, Password, UserName, DeviceSN, MagTranID, DecryptedData MACedString. Removed the description of MagnePrintScore above 1.
80	June 2019	Rod Vesling	As suggested modified input and output properties with the existing document. Updated the document with DecryptData operation. Updated the document based on below. Review comments provided GenerateMac operation Removed "Console Application Request and Response" section from all the operations. Added "Status Codes and Messages" section in table of content.
90	April 2020	Rebecca Robinson	Removed username and password data

CONFIDENTIAL

NOTICE

Purpose of the document

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

Table of Contents

1 Introduction

Decrypt service is one of the Magensa web services which can be used for POS (Point of Sale) transactions. Because POS transactions include highly sensitive information, a high level of security is required at all times. With the Decrypt service, we are going to deal with the below three operations:

- DecryptCardSwipe
- DecryptData
- GenerateMac

2 DecryptCardSwipe Operation

Typically, the magnetic swipe card stores some data/information in the magnetic stripe. A device can read this data from the magnetic stripe when a magstripe card is swiped. These magnetic stripes contain three encrypted tracks of data.

Below are the Input and Out properties of the DecryptCardSwipe Service.

2.1 Input Properties

The DecryptCardSwipe operation request has the following 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 onboarding.
Password *	<string>	Password credential provided by Magensa at onboarding.
UserName *	<string>	User name credential provided by Magensa at onboarding.
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:

Property	Value	Property Description
		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

2.2 Output Properties

The DecryptCardSwipe operation response has the following Output properties:

Property	Value	Property Description
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.

Property	Value	Property Description
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.

2.3 SOAP Request and Response

Below is the SOAP request for the DecryptCardSwipe operation of our Decrypt service:

```
<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:DecryptCardSwipe>
      <!–Optional:–>
      <tem:request>
        <!–Optional:–>
        <dec:BillingLabel></dec:BillingLabel>
        <!–Optional:–>
        <dec:CustomerTransactionID></dec:CustomerTransactionID>
        <dec:Authentication>
          <!–Optional:–>
          <dec:CustomerCode>OSMAGTEK</dec:CustomerCode>
          <!–Optional:–>
          <dec:Password>password</dec:Password>
          <!–Optional:–>
          <dec:Username>username</dec:Username>
        </dec:Authentication>
        <dec:EncryptedCardSwipe>
          <!–Optional:–>
          <dec:DeviceSN>B487DBC022119AA</dec:DeviceSN>
          <dec:KSN>9011400B487DBC000009</dec:KSN>
          <!–Optional:–>
          <dec:KeyType>Pin</dec:KeyType>
          <!–Optional:–>
<dec:MagnePrint>6C38C9A21A9CAF317F5D4EC704FA93653B50C8C772FD5C349AD67376C7A7
4B9391CC08C4C9B1AAD5BF844CC948F0E8524CF8DAF13245C2AB</dec:MagnePrint>
          <!–Optional:–>
          <dec:MagnePrintStatus>61403000</dec:MagnePrintStatus>
          <!–Optional:–>
<dec:Track1>7B79AAA74CC47E47AFD321B3D64011B8988134E0A20BEE02765D1BE3C16C7317
A97317963D8573F7094AE2A3D912DF4383E6E877DB5F28D45378DA441BE05044264A4AB51
E4C6F75</dec:Track1>
          <!–Optional:–>
<dec:Track2>AFC797D9127D3646BBE2FE07070B08AF1FCB55A5C87619DC9646892695EF1A59
011D49E6298AEF26</dec:Track2>
          <!–Optional:–>
```

```
            <dec:Track3></dec:Track3>
          </dec:EncryptedCardSwipe>
        </tem:request>
      </tem:DecryptCardSwipe>
    </soapenv:Body>
</soapenv:Envelope>
```

Below is the soap response for the DecryptCardSwipe operation of the Decrypt service:

```
<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/>
        <a:IsReplay>false</a:IsReplay>
        <a:MagTranId>907c97c5-17d8-4c7d-9e41-b9bee62e7e37</a:MagTranId>
        <a:CardID/>
        <a:DecryptedCardSwipe>
<a:MagnePrint>020028F899DFC18E81B6173F0C673960CAD814F1788CB194FD368F7E048877
D53818DB7F4EC3ABC455486125F80D311F2D3E63E803390000</a:MagnePrint>
          <a:Track1>%B5325614800013455^CONTACTLESS/MAGTEK          D^1909201001000P
00669000000?</a:Track1>
          <a:Track2>;5325614800013455=190920100100669100000?</a:Track2>
          <a:Track3/>
        </a:DecryptedCardSwipe>
        <a:MagnePrintScore>3.0</a:MagnePrintScore>
      </DecryptCardSwipeResult>
    </DecryptCardSwipeResponse>
  </s:Body>
</s:Envelope>
```

3 DecryptData Operation

The DecryptData operation is used to decrypt the block of data that was encrypted by a MagTek reader.

Below are the Input and Out properties of the DecryptData Service.

3.1 Input Properties

The DecryptData operation request has the below 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.

Property	Value	Property Description
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

3.2 Output Properties

The DecryptData operation response has below output properties.

Property	Value	Property Description
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.

3.3 SOAP Request and Response

Below is the SOAP request for the DecryptData operation of the Decrypt service:

```
<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>OSMAGTEK</dec:CustomerCode>
          <!–Optional:–>
          <dec:Password>password</dec:Password>
          <!–Optional:–>
          <dec:Username>username</dec:Username>
        </dec:Authentication>
        <!–Optional:–>

<dec:EncryptedData>5F260E4080089DB1F2DAE45114E285C81C47B8395B33C547C231538C74
47C3EBCAB430B57E491E332640EEDB3871B5F4A347DE69258B8B39E870A0BAE3DF59E17050
F77DB3E46FDDE46F4CF6DB0BA63961085FBDE67AA4359A727BB6250EA1A9CFC51B609C8315
2DD63BF8989B0E9273713F6BFD80BE5526FB1E5B50ABEC7062897263307607A714A2C1822A
3DEC72987E0C4D44412ECFC38CD0424AD77CDAC01B288074D8A36E528F79DF81DE739FA05A
ECD54A13518F4C290EA3DDFCCA6C6ACFF0012FC3939D02CD13704B08D23CA00DBF7681A32B
1ACB2822854BBDE9CE75D20B5E0D89968F502546F1334B822E094C4AFE52ACA66E2662F0AD
4B17314A64F28477E22D5F2B33</dec:EncryptedData>
        <!–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 the DecryptCardSwipe operation of the Decrypt service:

```
        <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>FC820102F28200FE820239008E120000000000000000004203440341031E03
1F035F24031909305F25031711019F0607A00000000410109F0702FFC09F0D05BC50BC08009
F0E0500000000009F0F05BC70BC98009F10120210600003220000000000000000000000FF9F
2608B4E47438FF561F5B9F2701409F360200039505040000800 09B02E8009C01009F3303202
```

```
8C89F34031E03009F3704486F61809F4005720000B0015A0853256148000134559F0206000
0000015009F0306000000000009F1A02084057135325614800013455D1909201001000541
0000F8A0230309F1012021060000322000000000000000000000FF5010446562697420 4D6
173746572436172640000</a:DecryptedData>
                </DecryptDataResult>
              </DecryptDataResponse>
            </s:Body>
          </s:Envelope>
```

Magensa Web Service| Decrypt 2.0 Operations | Decrypt 2.0 Programming Manual

4 GenerateMac

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

4.1 Input Properties

The GenerateMac operation request has the 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

4.2 Output Properties

The GenerateMac operation response has the following 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).

Magensa Web Service| Decrypt 2.0 Operations | Decrypt 2.0 Programming Manual

4.3 SOAP Request and Response

Below is the SOAP request for the GenerateMac operation of Decrypt service:

```
<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:CustomerTransactionID>
        <dec:Authentication>
          <dec:CustomerCode>OSMAGTEK</dec:CustomerCode>
          <dec:Password>password</dec:Password>
          <dec:Username>username</dec:Username>
        </dec:Authentication>
```

```
        <dec:DataToMAC>3430313233343536373839303944393837000000000000000</dec:Dat
aToMAC>
        <dec:KSN>9010010B31ED13000001</dec:KSN>
        <dec:KeyDerivationType>DUKPT</dec:KeyDerivationType>
      </tem:request>
    </tem:GenerateMac>
  </soapenv:Body>
</soapenv:Envelope>
```

Below is the SOAP response for the GenerateMac operation of Decrypt service:

```
<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:CustomerTransactionId>
        <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 Status Codes and Messages

Status Codes and Messages returned by Magensa for Decrypt 2.0 Operations can be found below:

5.1 Internal Error

Code	StatusMsg	Notes
5000	Unknown Error	

5.2 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.

5.3 Other Errors

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