MAGENSA™
SIMPLY STOPS FRAUD

Magensa Web Service

DecryptRSV201 Operation

Decrypts and Validates Card Data

September 5, 2014

Manual Part Number:
99810050-1.02

REGISTERED TO ISO 9001:2008

Table 0.1 - Revisions

Rev Number	Date	By	Notes
1.02	9/5/14	Rebecca Robinson	Combined Revisions with Document History (reducing document by one section). Reformatted. Updated Page 6 CustCode length. Page 6 updated HostID and HostPwd descriptions. Page 10 added error codes H067, H068.
A06	7/23/14	Jennifer Nguyen	Added "CustCode" fields to Section 2. Properties and Section 4. WSDL SOAP1.1 and SOAP1.2
1.01	February 21, 2013	Imran Jahanzeb	Initial Release
A05	3/31/10	Martin Cuadros	Updated the Value Descriptions of the "Score" Properties in Section 2. Replaced all Entries in Section 3, Table "Internal Errors" with just one Entry. Updated Section 3, Table "Other Errors" by removing "Y045" and adding "Y091" Score Value X.XX changed to X.XXX
A04	3/22/10	Martin Cuadros	Updated Section 3, Table "Other Codes" with codes returned during MP Validation
A03	3/8/10	Martin Cuadros	Clarified Value Description column of Input Property: OutputFormatCode '101' and '103', as well as Output Properties: "track1" and "track3"
A02	4/23/09	Martin Cuadros	Modified Note at the bottom of table in Section "2.2 Output Properties". Modified Value Descriptions of OutputFormatCode Property.

Purpose of the document

The purpose of this document is to provide a description of how to call the DecryptRSV201 operation of the Magensa web service.

Table of Contents

SECTION 1. Properties

1.1 Input Properties

Property (R/NR*)	Description	Value	Value Description
EncTrack1 (NR)	Encrypted Track 1 information returned by MagneSafe device when Card is swiped	<string>	[Encrypted Data]
		Null	There is no Track1 Data
EncTrack2 (R)	Encrypted Track 2 Information returned by MagneSafe device when Card is swiped	<string>	[Encrypted Data]
EncTrack3 (NR)	Encrypted Track 3 Information returned by MagneSafe device when Card is swiped	<string>	[Encrypted Data]
		Null	There is no Track 3 Data
EncMP (R)	Encrypted MagnePrint Information returned by MagneSafe device when Card is swiped	<string>	[Encrypted Data]
KSN (R)	20 character string returned by MagneSafe device when Card is swiped	<string>	
MPStatus (R)	MagnePrint Status of Card Swipe. This is an Alpha Numeric string, returned by MagneSafe device when Card is swiped.	<string>	
CardType (R)	Code which indicates what type of Card Data Format is been submitted	1	Encoding Format for Financial Transaction Cards (ISO 7811)

Continued on next page...

1.1 Input Properties (continued)

Property	Description	Value	Value Description
EncryptionBlockType (R)	Code which indicates what type of Encryption Block is used	1	MagneSafe V4/V5 compatible 2TDEA-CBC Encryption, IV=0 Block contains data only
		2	IPAD V1 compatible 2TDEA-CBC Encryption Block contains header + data (subject to change)
CustTranID (R)	An alphanumeric entry between 1 and 16 characters long	<[a-z][A-Z][0-9] >	This is a customer created ID to uniquely identify the transaction. The following 4 strings are examples of allowed values: TRAN87, None, MyTransaction, 37268
CustCode (NR)	Length = max 20 CHARS and the code does not enforced alpha capped	<[A-Z][0-9] >	The Magensa Customer Code for the originator of the transaction if the caller of the service is not to be billed directly.
HostID (R)	12 character Alpha Numeric ID Provided by Magensa for Web Service Authentication	<string>	
HostPwd (R)	14 character Password provided by Magensa for Web Service Authentication	<string>	
FutureInput (NR)	Reserved for future use	Null	Reserved for future use.
DeviceSN (NR)	Device Serial Number	<string>	Device Serial Number
		Null	No Device Serial Number available
RegisteredBy (R)	An alphanumeric entry between 1 and 20 characters long	<[a-z][A-Z][0-9] >	The company name of the caller of the web service
OutputFormatCode (R)	Code which indicates what kind of data is to be returned.	101	Return only decrypted track data: Track1, Track2, Track3 if provided
		102	Return only decrypted PAN
		103	Return the following decrypted data: PAN, Track1, Track2, Track3 if provided

Note: R/NR* = Required / Not Required

1.2 Output Properties

Hit Control + Click to Link to Contents

Property	Description	Value	Value Description
MagensaID	Magensa Transaction ID referencing performed Transaction	<40 char string>	Magensa Transaction ID referencing performed Transaction
		Null	Returned when an Error Occurs (See Status Codes in Section 2)
StatusMsg	Status Message	OK	Successful transaction
		<StatusMsg>	(See Status Codes in Section 2)
StatusCode	4 character alphanumeric code indicating status of transaction just performed	1000	Successful transaction
		<string>	(See Status Codes in Section 2)
Track1	Track1 decrypted data	Null	In the event of an error or no Track1 information present (See Status Codes in Section 2)
		N/A	Whenever the given output format code does not require track data to be returned
		<string>	Returned upon successful transaction whenever output format code asks for it
Track2	Track2 decrypted data	Null	In the event of an error or no Track2 information present (See Status Codes in Section 2)
		N/A	Whenever the given output format code does not require Track Data to be returned
		<string>	Returned upon successful transaction whenever output format code asks for it

Continued on next page…

1.2 Output Properties (continued)

Hit **Control + Click** to Link to Contents

Property	Description	Value	Value Description
Track3	Track3 decrypted data	Null	In the event of an error or no Track3 information present (See Status Codes in Section 2)
		N/A	Whenever the given output format code does not require Track Data to be returned
		<string>	Returned upon successful transaction whenever output format code asks for it
PAN	Decrypted PAN	Null	In the event of an Error or no PAN in the Track Data (See Status Codes in Section 2)
		N/A	Whenever the given output format code does not require PAN to be returned
		<string>	Returned upon successful transaction whenever output format code asks for it
Score	Score obtained against a previously Registered MagnePrint Reference	Null	In the event of certain Errors (See Status Codes in Section 2)
		N/A	Returned when not enough Information is available to determine a score value
		X.XXX	Decimal value indicating the Score obtained when the Transaction MagnePrint provided was Scored against the Designated Reference MagnePrint based on prior information supplied.
FutureOutput	Reserved for future use	Null	Reserved for future use

NOTICE

Notes:

- If available, decrypted data will be returned even in the presence of errors.
- It is very important to be consistent in supplying or omitting input property EncTrack1 when using authentication related operations. Information present in Track1 is used to create/retrieve authentication information at Registration/Scoring time respectively.

SECTION 2. Status Codes and Messages

Status Codes and Messages returned by Magensa for DecryptRSV201 Operation

*Hit **Control + Click** to Link to Contents*

Internal errors (e.g. Updating the Database, Decrypting the information, accessing config files, etc)

Code	StatusMsg	Notes
IXXX	Service is unavailable code:X	Internal Error - Where: 001 => XXX => 999

Input Validation errors

Code	StatusMsg	Notes
H001	H001	HostID has incorrect length - Input Validation
H002	H002	HostID has incorrect format - Input validation
H003	H003	HostPwd has incorrect length - Input Validation
H004	H004	HostPwd has incorrect format - Input validation
H009	H009	CustTranID has incorrect length - Input Validation
H010	H010	CustTranID has incorrect format - Input validation
H023	H023	RegisteredBy has incorrect length – Input Validation
H024	H024	RegisteredBy has incorrect format - Input validation
H176	H176	EncTrack1 has incorrect format – Input Validation
H177	H177	EncTrack1 has incorrect length – Input Validation
H178	H178	EncTrack2 has incorrect format – Input Validation
H179	H179	EncTrack2 has incorrect length – Input Validation
H180	H180	EncTrack3 has incorrect format – Input Validation
H181	H181	EncTrack3 has incorrect length – Input Validation
H182	H182	EncMP has incorrect format – Input Validation
H183	H183	EncMP has incorrect length – Input Validation
H186	H186	KSN has incorrect format – Input Validation
H187	H187	KSN has incorrect length – Input Validation
H188	H188	MPStatus has incorrect format – Input Validation
H189	H189	MPStatus has incorrect length – Input Validation
H200	H200	Invalid FutureInput – Input Validation

Continued on next page…

SECTION 2. Status Codes and Messages (continued)

Status Codes and Messages returned by Magensa for DecryptRSV201 Operation

*Hit **Control** + **Click** to Link to Contents*

Input Validation errors

Code	StatusMsg	Notes
H206	H206	Invalid CardType – Input Validation
H211	H211	Invalid EncryptionBlockType – Input Validation
H219	H219	Invalid OutputFormatCode – Input Validation
H251	H251	Invalid DeviceSN – Input Validation
H067	H067	CustCode has incorrect length - Input Validation
H068	H068	CustCode has incorrect format - Input validation

Other errors

Code	StatusMsg	Notes
Y001	No PAN Found in Track2 Data	
Y091	Invalid KSID	Occurs when the KSID found in the KSN provided is invalid.
Y093	Invalid MagnePrint	Error obtained while Scoring Transaction MagnePrint against a Reference MagnePrint made up of Zeroes.
Y094	Invalid MagnePrint	"Negative 2 - Invalid Transaction CRC / PAN" Obtained when Scoring Transaction MagnePrint against a Reference MagnePrint Made up of Zeroes.
Y095	Error Scoring Card.	Occurs whenever an error occurs while Scoring card
Y096	Y096	This occurs whenever the Card has an inactive MagnePrint Reference.
Y097	Y097	This occurs when the DUKPT KSN and Counter is replayed.
Y098	Problem Decrypting Data	This occurs if there is a problem while decrypting the Data.
Y099	Error validating Credentials	Error Validating (HostID and HostPwd) against assigned DB or Operation.

SECTION 3. WSDL

DecryptRSV201

Decrypt Card Information using Magensa.

Test

The test form is only available for requests from the local machine.

SOAP 1.1

The following is a sample SOAP 1.1 request and response. The **placeholders** shown need to be replaced with actual values.

```
POST /WSMagensa/Service.asmx HTTP/1.1
Host: ns.magensa.net
Content-Type: text/xml; charset=utf-8
Content-Length: length
SOAPAction: "http://www.magensa.net/DecryptRSV201"

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <DecryptRSV201 xmlns="http://www.magensa.net/">
      <DecryptRSV201_Input>
        <EncTrack1>string</EncTrack1>
        <EncTrack2>string</EncTrack2>
        <EncTrack3>string</EncTrack3>
        <EncMP>string</EncMP>
        <KSN>string</KSN>
        <DeviceSN>string</DeviceSN>
        <MPStatus>string</MPStatus>
        <CustTranID>string</CustTranID>
        <CustCode> string</CustCode>
        <HostID>string</HostID>
        <HostPwd>string</HostPwd>
        <OutputFormatCode>string</OutputFormatCode>
        <CardType>string</CardType>
        <EncryptionBlockType>string</EncryptionBlockType>
        <RegisteredBy>string</RegisteredBy>
        <FutureInput>string</FutureInput>
      </DecryptRSV201_Input>
    </DecryptRSV201>
  </soap:Body>
</soap:Envelope>
HTTP/1.1 200 OK
Content-Type: text/xml; charset=utf-8
Content-Length: length

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <DecryptRSV201Response xmlns="http://www.magensa.net/">
      <DecryptRSV201Result>
        <MagensaID>string</MagensaID>
        <StatusMsg>string</StatusMsg>
        <StatusCode>string</StatusCode>
        <Track1>string</Track1>
```

```
        <Track2>string</Track2>
        <Track3>string</Track3>
        <PAN>string</PAN>
        <Score>string</Score>
        <FutureOutput>string</FutureOutput>
      </DecryptRSV201Result>
    </DecryptRSV201Response>
  </soap:Body>
</soap:Envelope>
```

SOAP 1.2

The following is a sample SOAP 1.2 request and response. The **placeholders** shown need to be replaced with actual values.

```
POST /WSMagensa/Service.asmx HTTP/1.1
Host: ns.magensa.net
Content-Type: application/soap+xml; charset=utf-8
Content-Length: length

<?xml version="1.0" encoding="utf-8"?>
<soap12:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap12="http://www.w3.org/2003/05/soap-envelope">
  <soap12:Body>
    <DecryptRSV201 xmlns="http://www.magensa.net/">
      <DecryptRSV201_Input>
        <EncTrack1>string</EncTrack1>
        <EncTrack2>string</EncTrack2>
        <EncTrack3>string</EncTrack3>
        <EncMP>string</EncMP>
        <KSN>string</KSN>
        <DeviceSN>string</DeviceSN>
        <MPStatus>string</MPStatus>
        <CustTranID>string</CustTranID>
        <CustCode>string</CustCode>
        <HostID>string</HostID>
        <HostPwd>string</HostPwd>
        <OutputFormatCode>string</OutputFormatCode>
        <CardType>string</CardType>
        <EncryptionBlockType>string</EncryptionBlockType>
        <RegisteredBy>string</RegisteredBy>
        <FutureInput>string</FutureInput>
      </DecryptRSV201_Input>
    </DecryptRSV201>
  </soap12:Body>
</soap12:Envelope>
HTTP/1.1 200 OK
Content-Type: application/soap+xml; charset=utf-8
Content-Length: length

<?xml version="1.0" encoding="utf-8"?>
<soap12:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap12="http://www.w3.org/2003/05/soap-envelope">
  <soap12:Body>
    <DecryptRSV201Response xmlns="http://www.magensa.net/">
      <DecryptRSV201Result>
```

```
        <MagensaID>string</MagensaID>
        <StatusMsg>string</StatusMsg>
        <StatusCode>string</StatusCode>
        <Track1>string</Track1>
        <Track2>string</Track2>
        <Track3>string</Track3>
        <PAN>string</PAN>
        <Score>string</Score>
        <FutureOutput>string</FutureOutput>
      </DecryptRSV201Result>
    </DecryptRSV201Response>
  </soap12:Body>
</soap12:Envelope>
```

SECTION 4. Glossary

Word	Definition
DUKPTKSN Counter	**Derived Unique Key Per Transaction (DUKPT)** is a key management scheme in which for every transaction, a unique key is used which is derived from a fixed key. Therefore, if a derived key is compromised, future and past transaction data is still protected since the next or prior keys cannot be determined easily. **Derived Unique Key Per Transaction (DUKPT) Key Serial Number (KSN) Counter** This 10 byte field contains the DUKPT Key Serial Number used for encryption. This eighty bit field includes the Initial Key Serial Number in the leftmost 59 bits and a value for the Encryption Counter in the rightmost 21 bits.