MAGENSA™
SIMPLY STOPS FRAUD

Magensa Web Service

DecryptMICRv100 Operation

Decrypts MICR data

Sept 2014

Manual Part Number:

99810061-1.01

REGISTERED TO ISO 9001:2008

Copyright© 2011-2014

MagTek®, Inc.

Printed in the United States of America

Information in this document is subject to change without notice. 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.

MagnePrint® is a registered trademark of MagTek, Inc.

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	By	Notes
1.01	Sept 2014	R. Robinson	"Revisions" added to the Table of Contents. EncryptionBlockType determined. Updated text with “This is a customer created ID to uniquely identify the transaction. The following 4 strings are examples of allowed values: TRAN87, None, MyTransaction, 37268". Updated (See Status Codes in Section 2). Updated text with "Status Codes and Messages returned by Magensa for DecryptMICRV100 Operation". Removed Code/StatusMsg H023, H024 and H219, those are not supported by DecryptMICRV100 operation. Added error codes: H067 H067 CustCode has incorrect length - Input Validation and H068 H068 CustCode has incorrect format - Input validation.

NOTICE

The information contained herein is confidential and proprietary to:

Magensa LLC
1710 Apollo Court
Seal Beach, CA 90740
562-546-6500

Purpose of the document

The purpose of this document is to provide a description of how to call the DecryptMICRV100 operation of the Magensa web service.

Information in this document is subject to change without notice. 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 Magensa LLC.

Table of Contents

SECTION 1. Properties

1.1 Input Properties

Property (R/NR*)	Description	Value	Value Description
EncMICR (R)	Encrypted MICR information returned when Check is scanned	<String>	[Encrypted Data]
KSN (R)	20 character string returned device when check is scanned	<string>	
EncryptionBlockType (R)	Encryption block type indicates If the payload includes header.	1	Only 1 is supported at this time which is V4/V5 format without header.
CustTranID (R)	An Alpha Numeric 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
HostID (R)	12 character Alpha Numeric ID Provided by Magensa for Web Service Authentication	<12 character Alpha Numeric String>	
HostPwd (R)	14 character Password provided by Magensa for Web Service Authentication	<14 character string>	
FutureInput (NR)	Reserved for Future Use	Null	Reserved for Future Use.
CustCode (NR)	Customer Code	<20 character string>	
DeviceSN (NR)	Device Serial Number	<String>	Device Serial Number
		Null	No Device SN available

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 Alpha Numeric Code indicating Status of Transaction just performed	1000	Successful Transaction
		<Status Code>	(See Status Codes in Section 2)
MICR	Decrypted MICR	Null	In the event of an Error or no MICR Data
		<Decrypted Data>	Returned upon successful transaction whenever output format code asks for it
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.

SECTION 2. Status Codes and Messages

Status Codes and Messages returned by Magensa for DecryptMICRV100 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
H067	H067	CustCode has incorrect length - Input Validation
H068	H068	CustCode has incorrect format - Input validation
H186	H186	KSN has incorrect format – Input Validation
H187	H187	KSN has incorrect length – Input Validation
H200	H200	Invalid FutureInput – Input Validation
H211	H211	Invalid EncryptionBlockType – Input Validation
H251	H251	Invalid DeviceSN – Input Validation

Other errors

Code	StatusMsg	Notes
Y091	Invalid KSID	Occurs when the KSID found in the KSN provided is invalid.
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. 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.