EMV Reference Guide

Public - Security Level 0

November 2021

REVISION HISTORY

Date	Version	Author(s)	Comments
5/4/16	2.0	C. Meaney	Added section AUTH_EMV_DATA, Appendix A: EMV_DATA, and Appendix B: AUTH_EMV_DATA
2/13/17	2.1	C. Meaney	Added tags 9F7C, C0, 9F6E to Appendix A: EMV_DATA Fields.
4/20/17	2.2	C. Meaney	Added tags 5F24, 8A, 9F39, 9F53 to Appendix A: EMV_DATA Fields. Removed tag 81. Sorted tags by hexadecimal order.
8/3/17	2.3	C. Meaney	Revised example 4-part keys.
6/1/18	2.4	M.Billips	Added MasterCard PAYMENT_INITIATION_CHANNEL (Contactless) and transaction samples

CONFIDENTIALITY STATEMENT

Contents

List of Tables

Submitting EMV Transactions

Identification of EMV-based authorizations requires the proper Card Entry Method [CARD_ENT_METH] to be submitted with each transaction.

NOTE: The tables that follow provide full definitions of the EPX EMV Codes.

When submitting EMV transactions with the Card Entry Method of "G - CHIP (EMV Contact)" or "R - Proximity VSDC or M/Chip data (EMV)", the EMV TLV data from the EMV kernel must be included in the [EMV_DATA] tag within the authorization request.

Response data from an EMV authorization request may include the tag [AUTH_EMV_DATA]. The data within this tag *must* be provided back to the EMV kernel.

The EMV TLV data to and from the EMV kernel must *not* be altered.

NOTE: EMV fallback transactions are presented as a standard swipe with the exception that the Chip Condition Code tag [CHIP_CONDITION_CODE] must be provided and set to the appropriate value.

Please review the EMV transaction samples in *Transaction Samples*, beginning on page *5*.

For detailed information about specific tags, please refer to the *EPX Data Dictionary*.

EPX EMV Codes

Card Entry Method

Table 1: Card Entry Method Values

CARD_ENT_METH	Description
G	CHIP (EMV Contact)
Q	Proximity / Contactless MSD (Track 1 or Track 2 allowed)
R	Proximity VSDC or M/Chip data (EMV) (Track 2 data is required)

Card Identification

Table 2: Card Identification Value

CARD_ID	Description
P	PIN (Online PIN)

End to End Encryption Identification

Table 3: End to End Encryption Identification Values

E2EE	Description
0	Use CARD_ENT_METH to Identify Format
1	MagTek V2 Format
2	3DES Format

TLV EMV Data

Table 4: TLV EMV Data Values

TLV_LIST	Description
EMV_DATA	Contains request data from the EMV kernel as a variable list of tags and their data in TLV format. For details about the EMV_DATA tag, refer to *Appendix A: EMV_DATA Fields*, page 22
AUTH_EMV_DATA	This response data must be provided back to the EMV kernel. Contains a variable list of tags and their data in TLV format. For more information, refer to *Appendix B: AUTH_EMV_DATA*, page 26.

Chip Condition Code

Table 5: Chip Condition Code Values

CHIP_CONDITION_CODE	Description
0	Not applicable to fallback transactions. For VSDC transactions must be '0'
1	Transaction was initiated from a magnetic stripe with a service code beginning with 2 or 6 and the last read at VSDC terminal was a successful chip read or was not a chip transaction.
2	Transaction was initiated at a chip-capable terminal from a magnetic stripe that contains service code 2 or 6, and the previous transaction initiated by that terminal was an unsuccessful chip read.

Reason Code (Reversal Requests)

Table 6: Reason Code Values

REASON_CODE	Description
0	User Cancel
1	Error Condition

MasterCard Contactless Transactions

The client application is required to send the PAYMENT_INITIATION_CHANNEL field with MasterCard Contactless transactions for both EMV and MSD methods. For more information about this field and its values, please reference the *EPX Data Dictionary*.

NOTE: The PAYMENT_INITIATION_CHANNEL field is mandatory for MasterCard only; this field is not required for any other network (Visa, Discover, and American Express).

Transaction Samples

About the Transaction samples

This chapter contains the following examples for both encrypted and unencrypted track data along with EMV, Contactless, and Non-EMV transaction methods:

Field Types

The samples that follow provide examples for each type of transaction. Within the examples, some fields are listed as mandatory (in **bold** text) and others as optional.

Note the following about mandatory and optional fields:

- Mandatory fields need to be submitted with the transaction request to ensure a successful response.
- Optional fields may be omitted.

Card Swipe Transaction with Encryption

This is an example of a Card Swipe transaction using E2E encryption type 3DES DUKPT (Data variant).

Request

```
<DETAIL CUST_NBR='1234' MERCH_NBR='1234567' DBA_NBR='1' TERMINAL_NBR='1'>
<AMOUNT>10.00</AMOUNT>
<BATCH_ID>1</BATCH_ID>
<TRAN_NBR>6</TRAN_NBR>
<TRAN_TYPE>CCR1</TRAN_TYPE>
<TRACK_DATA>004FFFF9876543210E0000DED4A250ABE6343390B4D1036B4D550EBC9EB81CA4BAC012
E7E7D2E654B6B83413D05A2F8C7EEB902</TRACK_DATA>
<CARD_ENT_METH>D</CARD_ENT_METH>
<E2EE>2</E2EE>
<INDUSTRY_TYPE>P</INDUSTRY_TYPE>
<CURRENCY_CODE>840</CURRENCY_CODE>
<MAC>MAC9876543210</MAC>
</DETAIL>
```

Response

```
<RESPONSE>
<FIELDS>
<FIELD KEY="MSG_VERSION">003</FIELD>
<FIELD KEY="CUST_NBR">1234</FIELD>
<FIELD KEY="MERCH_NBR">1234567 </FIELD>
<FIELD KEY="DBA_NBR">1</FIELD>
<FIELD KEY="TERMINAL_NBR">1</FIELD>
<FIELD KEY="TRAN_TYPE">CCR1</FIELD>
<FIELD KEY="BATCH_ID">1</FIELD>
<FIELD KEY="TRAN_NBR">6</FIELD>
<FIELD KEY="LOCAL_DATE">043015</FIELD>
<FIELD KEY="LOCAL_TIME">161506</FIELD>
<FIELD KEY="AUTH_GUID">09YD52FB08TX12WH015</FIELD>
<FIELD KEY="AUTH_RESP">00</FIELD>
<FIELD KEY="AUTH_CODE">000001</FIELD>
<FIELD KEY="AUTH_RESP_TEXT">APPROVAL</FIELD>
<FIELD KEY="AUTH_CARD_TYPE">M</FIELD>
<FIELD KEY="AUTH_TRAN_DATE_GMT">04/30/2015 04:15:06 PM</FIELD>
<FIELD KEY="AUTH_AMOUNT_REQUESTED">10.0000</FIELD>
<FIELD KEY="AUTH_AMOUNT">10.00</FIELD>
<FIELD KEY="AUTH_CURRENCY_CODE">840</FIELD>
<FIELD KEY="NETWORK_RESPONSE">00</FIELD>
<FIELD KEY="AUTH_CARD_COUNTRY_CODE">840</FIELD>
<FIELD KEY="AUTH_CARD_CURRENCY_CODE">840</FIELD>
<FIELD KEY="AUTH_CARD_B">MCC</FIELD>
<FIELD KEY="AUTH_CARD_A">MCW</FIELD>
<FIELD KEY="AUTH_CARD_C">MCW</FIELD>
<FIELD KEY="AUTH_MASKED_ACCOUNT_NBR">************0009</FIELD>
<FIELD KEY="AUTH_CARD_K">N</FIELD>
</FIELDS>
```

```
</RESPONSE>
```

Card Swipe Transaction without Encryption

This is an example of a Card Swipe transaction with no data encryption.

Request

```
<DETAIL CUST_NBR='1234' MERCH_NBR='1234567' DBA_NBR='1' TERMINAL_NBR='1'>
<AMOUNT>1.00</AMOUNT>
<BATCH_ID>1</BATCH_ID>
<TRAN_NBR>88</TRAN_NBR>
<TRAN_TYPE>CCR1</TRAN_TYPE>
<TRACK_DATA>500000******0009=251210100000000</TRACK_DATA>
<CARD_ENT_METH>D</CARD_ENT_METH>
<INDUSTRY_TYPE>P</INDUSTRY_TYPE>
<E2EE>0</E2EE>
<CURRENCY_CODE>840</CURRENCY_CODE>
<MAC>MAC9876543210</MAC>
</DETAIL>
```

Response

```
<RESPONSE>
<FIELDS>
<FIELD KEY="MSG_VERSION">003</FIELD>
<FIELD KEY="CUST_NBR">1234</FIELD>
<FIELD KEY="MERCH_NBR">1234567</FIELD>
<FIELD KEY="DBA_NBR">1</FIELD>
<FIELD KEY="TERMINAL_NBR">1</FIELD>
<FIELD KEY="TRAN_TYPE">CCR1</FIELD>
<FIELD KEY="BATCH_ID">1</FIELD>
<FIELD KEY="TRAN_NBR">88</FIELD>
<FIELD KEY="LOCAL_DATE">050815</FIELD>
<FIELD KEY="LOCAL_TIME">090824</FIELD>
<FIELD KEY="AUTH_GUID">09YD5MA3E9TR363A150</FIELD>
<FIELD KEY="AUTH_RESP">00</FIELD>
<FIELD KEY="AUTH_CODE">000008</FIELD>
<FIELD KEY="AUTH_RESP_TEXT">APPROVAL</FIELD>
<FIELD KEY="AUTH_CARD_TYPE">M</FIELD>
<FIELD KEY="AUTH_TRAN_DATE_GMT">05/08/2015 04:08:23 PM</FIELD>
<FIELD KEY="AUTH_AMOUNT_REQUESTED">1.0000</FIELD>
<FIELD KEY="AUTH_AMOUNT">1.00</FIELD>
<FIELD KEY="AUTH_CURRENCY_CODE">840</FIELD>
<FIELD KEY="NETWORK_RESPONSE">00</FIELD>
<FIELD KEY="AUTH_CARD_COUNTRY_CODE">840</FIELD>
<FIELD KEY="AUTH_CARD_CURRENCY_CODE">840</FIELD>
<FIELD KEY="AUTH_CARD_B">MCC</FIELD>
<FIELD KEY="AUTH_CARD_A">MCW</FIELD>
<FIELD KEY="AUTH_CARD_C">MCW</FIELD>
<FIELD KEY="AUTH_MASKED_ACCOUNT_NBR">************0009 </FIELD>
<FIELD KEY="AUTH_RTI_EST_CPD">010100</FIELD>
```

```
<FIELD KEY="AUTH_RTI_EST_FEE">0.0000</FIELD>
<FIELD KEY="AUTH_CARD_K">N</FIELD>
</FIELDS>
</RESPONSE>
```

Contact EMV with Encryption

This is an example of a Contact EMV transaction using E2E encryption type 3DES DUKPT (Data variant).

Request

```
<DETAIL CUST_NBR='1234' MERCH_NBR='1234567' DBA_NBR='1' TERMINAL_NBR='1'>
<AMOUNT>11.00</AMOUNT>
<TRAN_NBR>42</TRAN_NBR>
<BATCH_ID>1</BATCH_ID>
<TRAN_TYPE>CCR1</TRAN_TYPE>
<TRACK_DATA>004FFFF9876543210E0006ED082F094C48D501F5887C6A13B67277CAB3C10429A2CF58
E884C4DDD23B25061B3A2D63254105226</TRACK_DATA>
<EMV_DATA>9F34035E03009F26089D915F3C33FB90A89F2701809F100706010A03A0A0009F37045571
45629F3602006E950580C000800082021C009F3303E028C89F1A0208409F3501229F1E083730303932
3839329F03060000000000009A031806019C01009F02060000000011005F2A0208409F0902008D5F34
01019F4104000000079F0607A00000000310108407A0000000031010</EMV_DATA>
<CARD_ENT_METH>G</CARD_ENT_METH>
<E2EE>2</E2EE>
<INDUSTRY_TYPE>P</INDUSTRY_TYPE>
<CARD_ID>0</CARD_ID>
<MAC>MAC9876543210</MAC>
<CURRENCY_CODE>840</CURRENCY_CODE>
</DETAIL>
```

Response

```
<RESPONSE>
<FIELDS>
<FIELD KEY="MSG_VERSION">003</FIELD>
<FIELD KEY="CUST_NBR">1234</FIELD>
<FIELD KEY="MERCH_NBR">1234567</FIELD>
<FIELD KEY="DBA_NBR">1</FIELD>
<FIELD KEY="TERMINAL_NBR">1</FIELD>
<FIELD KEY="TRAN_TYPE">CCR1</FIELD>
<FIELD KEY="BATCH_ID">1</FIELD>
<FIELD KEY="TRAN_NBR">42</FIELD>
<FIELD KEY="LOCAL_DATE">060118</FIELD>
<FIELD KEY="LOCAL_TIME">101110</FIELD>
<FIELD KEY="AUTH_GUID">03RFVQ0HYP3274H5X43</FIELD>
<FIELD KEY="AUTH_RESP">00</FIELD>
<FIELD KEY="AUTH_CODE">000736</FIELD>
<FIELD KEY="AUTH_AVS"> </FIELD>
<FIELD KEY="AUTH_RESP_TEXT">APPROVAL 000736</FIELD>
<FIELD KEY="AUTH_CARD_TYPE">V</FIELD>
<FIELD KEY="AUTH_TRAN_DATE_GMT">06/01/2018 02:11:09 PM</FIELD>
```

```
<FIELD KEY="AUTH_AMOUNT_REQUESTED">11.00</FIELD>
<FIELD KEY="AUTH_AMOUNT">11.00</FIELD>
<FIELD KEY="AUTH_CURRENCY_CODE">840</FIELD>
<FIELD KEY="NETWORK_RESPONSE">00</FIELD>
<FIELD KEY="AUTH_CARD_COUNTRY_CODE">840</FIELD>
<FIELD KEY="AUTH_CARD_B">C</FIELD>
<FIELD KEY="AUTH_CARD_C">A</FIELD>
<FIELD KEY="AUTH_CARD_E">N</FIELD>
<FIELD KEY="AUTH_CARD_F">Y</FIELD>
<FIELD KEY="AUTH_CARD_G">Y</FIELD>
<FIELD KEY="AUTH_CARD_H">N</FIELD>
<FIELD KEY="AUTH_CARD_I">N</FIELD>
<FIELD KEY="AUTH_CARD_J">N</FIELD>
<FIELD KEY="AUTH_MASKED_ACCOUNT_NBR">************8282</FIELD>
<FIELD KEY="AUTH_CARD_L">C</FIELD>
</FIELDS>
</RESPONSE>
```

Contact EMV without Encryption

This is an example of a Contact EMV transaction with no data encryption.

Request

```
<DETAIL CUST_NBR='1234' MERCH_NBR='1234567' DBA_NBR='1' TERMINAL_NBR='1'>
<AMOUNT>11.00</AMOUNT>
<TRAN_NBR>43</TRAN_NBR>
<BATCH_ID>1</BATCH_ID>
<TRAN_TYPE>CCR1</TRAN_TYPE>
<TRACK_DATA>412000******8282=25082012060102842 84</TRACK_DATA>
<EMV_DATA>9F34035E03009F26087C3B38E966744E7F9F2701809F100706010A03A020009F3704C64B
F4849F3602006F950580C000800082021C009F3303E028C89F1A0208409F3501229F1E083730303932
3839329F03060000000000009A031806019C01009F02060000000011005F2A0208409F0902008D5F34
01019F4104000000089F0607A00000000310108407A0000000031010</EMV_DATA>
<CARD_ENT_METH>G</CARD_ENT_METH>
<E2EE>0</E2EE>
<INDUSTRY_TYPE>P</INDUSTRY_TYPE>
<CARD_ID>0</CARD_ID>
<MAC>MAC9876543210</MAC>
<CURRENCY_CODE>840</CURRENCY_CODE>
</DETAIL>
```

Response

```
<RESPONSE>
<FIELDS>
<FIELD KEY="MSG_VERSION">003</FIELD>
<FIELD KEY="CUST_NBR">1234</FIELD>
<FIELD KEY="MERCH_NBR">1234567</FIELD>
<FIELD KEY="DBA_NBR">1</FIELD>
<FIELD KEY="TERMINAL_NBR">1</FIELD>
<FIELD KEY="TRAN_TYPE">CCR1</FIELD>
```

```
<FIELD KEY="BATCH_ID">1</FIELD>
<FIELD KEY="TRAN_NBR">43</FIELD>
<FIELD KEY="LOCAL_DATE">060118</FIELD>
<FIELD KEY="LOCAL_TIME">103339</FIELD>
<FIELD KEY="AUTH_GUID">03RFVQ1QTF4FQGUVX5D</FIELD>
<FIELD KEY="AUTH_RESP">00</FIELD>
<FIELD KEY="AUTH_CODE">000746</FIELD>
<FIELD KEY="AUTH_AVS"> </FIELD>
<FIELD KEY="AUTH_RESP_TEXT">APPROVAL 000746</FIELD>
<FIELD KEY="AUTH_CARD_TYPE">V</FIELD>
<FIELD KEY="AUTH_TRAN_DATE_GMT">06/01/2018 02:33:38 PM</FIELD>
<FIELD KEY="AUTH_AMOUNT_REQUESTED">11.00</FIELD>
<FIELD KEY="AUTH_AMOUNT">11.00</FIELD>
<FIELD KEY="AUTH_CURRENCY_CODE">840</FIELD>
<FIELD KEY="NETWORK_RESPONSE">00</FIELD>
<FIELD KEY="AUTH_CARD_COUNTRY_CODE">840</FIELD>
<FIELD KEY="AUTH_CARD_B">C</FIELD>
<FIELD KEY="AUTH_CARD_C">A</FIELD>
<FIELD KEY="AUTH_CARD_E">N</FIELD>
<FIELD KEY="AUTH_CARD_F">Y</FIELD>
<FIELD KEY="AUTH_CARD_G">Y</FIELD>
<FIELD KEY="AUTH_CARD_H">N</FIELD>
<FIELD KEY="AUTH_CARD_I">N</FIELD>
<FIELD KEY="AUTH_CARD_J">N</FIELD>
<FIELD KEY="AUTH_MASKED_ACCOUNT_NBR">************8282</FIELD>
<FIELD KEY="AUTH_CARD_L">C</FIELD>
</FIELDS>
</RESPONSE>
```

Full Contact EMV with Encryption

This is an example of a Full Contact EMV Online PIN transaction using E2E encryption type 3DES DUKPT (Data variant).

Request

```
<DETAIL CUST_NBR='1234' MERCH_NBR='1234567' DBA_NBR='1' TERMINAL_NBR='1'>
<AMOUNT>10.00</AMOUNT>
<TRAN_NBR>9</TRAN_NBR>
<BATCH_ID>1</BATCH_ID>
<TRAN_TYPE>CCR1</TRAN_TYPE>
<TRACK_DATA>004FFFF9876543210E00006A91C1C1ED3A9559CEE546319B653311C8D9668D8C53C534
BD2849280956467A2AE0B9B7B2D441940</TRACK_DATA>
<EMV_DATA>9F34030200009F260828BF9D3AFCC8DD529F2701809F1008010103A0000000009F37044A
BAA8C49F3602008595054040040000820258009F3303E0F8C89F1A0208409F3501229F1E0832323135
333731309F03060000000000009A031504309C01009F02060000000010005F2A0208409F090200025F
3401009F4104000000039F0607A0000000041010</EMV_DATA>
<CARD_ENT_METH>G</CARD_ENT_METH>
<PIN_BLK>CC1D39F77DC96766FFFF9876543210E00001</PIN_BLK>
<E2EE>2</E2EE>
<CARD_ID>P</CARD_ID>
<INDUSTRY_TYPE>P</INDUSTRY_TYPE>
<MAC>MAC9876543210</MAC>
<CURRENCY_CODE>840</CURRENCY_CODE>
</DETAIL>
```

Response

```
<RESPONSE>
<FIELDS>
<FIELD KEY="MSG_VERSION">003</FIELD>
<FIELD KEY="CUST_NBR">1234</FIELD>
<FIELD KEY="MERCH_NBR">1234567</FIELD>
<FIELD KEY="DBA_NBR">1</FIELD>
<FIELD KEY="TERMINAL_NBR">1</FIELD>
<FIELD KEY="TRAN_TYPE">CCR1</FIELD>
<FIELD KEY="BATCH_ID">1</FIELD>
<FIELD KEY="TRAN_NBR">9</FIELD>
<FIELD KEY="LOCAL_DATE">043015</FIELD>
<FIELD KEY="LOCAL_TIME">164508</FIELD>
<FIELD KEY="AUTH_GUID">09YD52H208YB6RN1019</FIELD>
<FIELD KEY="AUTH_RESP">00</FIELD>
<FIELD KEY="AUTH_CODE">000004</FIELD>
<FIELD KEY="AUTH_RESP_TEXT">APPROVAL</FIELD>
<FIELD KEY="AUTH_CARD_TYPE">M</FIELD>
<FIELD KEY="AUTH_TRAN_DATE_GMT">04/30/2015 04:45:08 PM</FIELD>
<FIELD KEY="AUTH_AMOUNT_REQUESTED">10.0000</FIELD>
<FIELD KEY="AUTH_AMOUNT">10.00</FIELD>
<FIELD KEY="AUTH_CURRENCY_CODE">840</FIELD>
<FIELD KEY="NETWORK_RESPONSE">00</FIELD>
<FIELD KEY="AUTH_CARD_COUNTRY_CODE">056</FIELD>
<FIELD KEY="AUTH_CARD_COUNTRY_NAME">BEL</FIELD>
```

```
<FIELD KEY="AUTH_CARD_CURRENCY_CODE">978</FIELD>
<FIELD KEY="AUTH_CARD_CURRENCY_NAME">EUR</FIELD>
<FIELD KEY="AUTH_CARD_B">MCC</FIELD>
<FIELD KEY="AUTH_CARD_A">MCS</FIELD>
<FIELD KEY="AUTH_CARD_C">MCS</FIELD>
<FIELD KEY="AUTH_SHA1">9C86E2255C0A2D34121F8E51A3ED35 C1D98FDEB9</FIELD>
<FIELD KEY="AUTH_MASKED_ACCOUNT_NBR">************1049 </FIELD>
<FIELD KEY="AUTH_CARD_K">N</FIELD>
<FIELD KEY="AUTH_CARD_L">C</FIELD>
<FIELD KEY="AUTH_EMV_DATA">910A9971B4D9826C69873031</FIELD>
</FIELDS>
</RESPONSE>
```

Full Contact EMV without Encryption

This is an example of a Full Contact EMV Online PIN transaction with no data encryption.

Request

```
<DETAIL CUST_NBR='1234' MERCH_NBR='1234567' DBA_NBR='1' TERMINAL_NBR='1'>
<AMOUNT>10.00</AMOUNT>
<TRAN_NBR>94</TRAN_NBR>
<BATCH_ID>1</BATCH_ID>
<TRAN_TYPE>CCR1</TRAN_TYPE>
<TRACK_DATA>541333******1049=1412201044780642</TRACK_DATA>
<EMV_DATA>9F34030200009F2608F74EBF6787FB9AD49F2701809F1008010103A0800000009F370488
23F32B9F3602008C9505404004000820258009F3303E0F8C89F1A0208409F3501229F1E0832323135
333731309F03060000000000009A031505089C01009F02060000000010005F2A0208409F090200025F
3401009F4104000000319F0607A0000000041010</EMV_DATA>
<CARD_ENT_METH>G</CARD_ENT_METH>
<PIN_BLK>F034E99B9C8C72B1FFFF9876543210E0001C</PIN_BLK>
<CARD_ID>P</CARD_ID>
<INDUSTRY_TYPE>P</INDUSTRY_TYPE>
<E2EE>0</E2EE>
<MAC>MAC9876543210</MAC>
<CURRENCY_CODE>840</CURRENCY_CODE>
</DETAIL>
```

Response

```
<RESPONSE>
<FIELDS>
<FIELD KEY="MSG_VERSION">003</FIELD>
<FIELD KEY="CUST_NBR">1234</FIELD>
<FIELD KEY="MERCH_NBR">1234567</FIELD>
<FIELD KEY="DBA_NBR">1</FIELD>
<FIELD KEY="TERMINAL_NBR">1</FIELD>
<FIELD KEY="TRAN_TYPE">CCR1</FIELD>
<FIELD KEY="BATCH_ID">1</FIELD>
<FIELD KEY="TRAN_NBR">94</FIELD>
<FIELD KEY="LOCAL_DATE">050815</FIELD>
<FIELD KEY="LOCAL_TIME">094008</FIELD>
```

```
<FIELD KEY="AUTH_GUID">09YD5MBTXAYUPG7R155</FIELD>
<FIELD KEY="AUTH_RESP">00</FIELD>
<FIELD KEY="AUTH_CODE">000012</FIELD>
<FIELD KEY="AUTH_RESP_TEXT">APPROVAL</FIELD>
<FIELD KEY="AUTH_CARD_TYPE">M</FIELD>
<FIELD KEY="AUTH_TRAN_DATE_GMT">05/08/2015 04:40:08 PM</FIELD>
<FIELD KEY="AUTH_AMOUNT_REQUESTED">10.0000</FIELD>
<FIELD KEY="AUTH_AMOUNT">10.00</FIELD>
<FIELD KEY="AUTH_CURRENCY_CODE">840</FIELD>
<FIELD KEY="NETWORK_RESPONSE">00</FIELD>
<FIELD KEY="AUTH_CARD_COUNTRY_CODE">056</FIELD>
<FIELD KEY="AUTH_CARD_COUNTRY_NAME">BEL</FIELD>
<FIELD KEY="AUTH_CARD_CURRENCY_CODE">978</FIELD>
<FIELD KEY="AUTH_CARD_CURRENCY_NAME">EUR</FIELD>
<FIELD KEY="AUTH_CARD_B">MCC</FIELD>
<FIELD KEY="AUTH_CARD_A">MCS</FIELD>
<FIELD KEY="AUTH_CARD_C">MCS</FIELD>
<FIELD KEY="AUTH_SHA1">9C86E2255C0A2D34121F8E51A3ED 35C1D98FDEB9
</FIELD>
<FIELD KEY="AUTH_MASKED_ACCOUNT_NBR">************1049</FIELD>
<FIELD KEY="AUTH_CARD_K">N</FIELD>
<FIELD KEY="AUTH_CARD_L">C</FIELD>
<FIELD KEY="AUTH_EMV_DATA">910A9971B4D9826C69873031</FIELD>
</FIELDS>
</RESPONSE>
```

Contactless EMV with Encryption

This is an example of a Contactless EMV transaction using E2E encryption type 3DES DUKPT (Data Variant) using a MasterCard.

IMPORTANT!

The PAYMENT_INITIATION_CHANNEL tag is included with this transaction sample identifies it as a MasterCard transaction. This tag is not required for any other card brand (Visa, Discover, and American Express) and should be omitted from transaction requests for these other card brands.

Request

```
<DETAIL cust_nbr='1234' merch_nbr='1234567' dba_nbr='1' terminal_nbr='1'>
<AMOUNT>10.00</AMOUNT>
<TRAN_NBR>2</TRAN_NBR>
<BATCH_ID>123</BATCH_ID>
<TRAN_TYPE>CCR1</TRAN_TYPE>
<TRACK_DATA>004FFFF9876543210E00006A91C1C1ED3A9559CEE546319B653311C8D9668D8C53C534
BD2849280956467A2AE0B9B7B2D441940</TRACK_DATA>
<EMV_DATA>9F34030200009F260828BF9D3AFCC8DD529F2701809F1008010103A0000000009F37044A
BAA8C49F3602008595054040040000820258009F3303E0F8C89F1A0208409F3501229F1E0832323135
333731309F03060000000000009A031504309C01009F02060000000010005F2A0208409F090200025F
3401009F4104000000039F0607A0000000041010</EMV_DATA>
<CARD_ENT_METH>R</CARD_ENT_METH>
<E2EE>2</E2EE>
<INDUSTRY_TYPE>P</INDUSTRY_TYPE>
<PAYMENT_INITIATION_CHANNEL>22</PAYMENT_INITIATION_CHANNEL>
<MAC>MAC9876543210</MAC>
<CURRENCY_CODE>840</CURRENCY_CODE?
</DETAIL>
```

Response

```
<RESPONSE>
<FIELDS>
<FIELD KEY="MSG_VERSION">003</FIELD>
<FIELD KEY="CUST_NBR">1234</FIELD>
<FIELD KEY="MERCH_NBR">1234567</FIELD>
<FIELD KEY="DBA_NBR">1</FIELD>
<FIELD KEY="TERMINAL_NBR">1</FIELD>
<FIELD KEY="TRAN_TYPE">CCR1</FIELD>
<FIELD KEY="BATCH_ID">123</FIELD>
<FIELD KEY="TRAN_NBR">2</FIELD>
<FIELD KEY="LOCAL_DATE">053118</FIELD>
<FIELD KEY="LOCAL_TIME">115307</FIELD>
<FIELD KEY="AUTH_GUID">09KFVNJVN7H2961GW74</FIELD>
<FIELD KEY="AUTH_RESP">00</FIELD>
<FIELD KEY="AUTH_CODE">001911</FIELD>
<FIELD KEY="AUTH_RESP_TEXT">APPROVAL</FIELD>
<FIELD KEY="AUTH_CARD_TYPE">M</FIELD>
<FIELD KEY="AUTH_TRAN_DATE_GMT">05/31/2018 03:53:06 PM</FIELD>
<FIELD KEY="AUTH_AMOUNT_REQUESTED">10.00</FIELD>
<FIELD KEY="AUTH_AMOUNT">10.00</FIELD>
<FIELD KEY="AUTH_CURRENCY_CODE">840</FIELD>
<FIELD KEY="NETWORK_RESPONSE">00</FIELD>
<FIELD KEY="AUTH_CARD_COUNTRY_CODE">056</FIELD>
<FIELD KEY="AUTH_CARD_COUNTRY_NAME">BEL</FIELD>
<FIELD KEY="AUTH_CARD_CURRENCY_CODE">978</FIELD>
<FIELD KEY="AUTH_CARD_CURRENCY_NAME">EUR</FIELD>
<FIELD KEY="AUTH_CARD_B">MCC</FIELD>
<FIELD KEY="AUTH_CARD_A">MCS</FIELD>
<FIELD KEY="AUTH_CARD_C">MCS</FIELD>
<FIELD KEY="AUTH_MASKED_ACCOUNT_NBR">************1049</FIELD>
<FIELD KEY="AUTH_CARD_K">N</FIELD>
<FIELD KEY="AUTH_CARD_L">C</FIELD>
</FIELDS>
```

```
</RESPONSE>
```

Contactless EMV without encryption

This is an example of a Contactless EMV transaction with no data encryption using a MasterCard.

IMPORTANT!

The PAYMENT_INITIATION_CHANNEL tag is included with this transaction sample identifies it as a MasterCard transaction. This tag is not required for any other card brand (Visa, Discover, and American Express) and should be omitted from transaction requests for these other card brands.

Request

```
<DETAIL CUST_NBR='1234' MERCH_NBR='1234567' DBA_NBR='1' TERMINAL_NBR='1'>
<AMOUNT>10.00</AMOUNT>
<TRAN_NBR>95</TRAN_NBR>
<BATCH_ID>1</BATCH_ID>
<TRAN_TYPE>CCR1</TRAN_TYPE>
<TRACK_DATA>541333******1031=1412201014590756</TRACK_DATA>
<EMV_DATA>9F34031E00009F2608796662AC9E9D7C289F2701809F1008010103A0080000009F37042F
D436019F3602006A9505404000000820258009F3303E0F8C89F1A0208409F3501229F1E0832323135
333731309F0306000000000000009A031505089C01009F02060000000010005F2A0208409F090200025F
3401009F4104000000329F0607A0000000041010</EMV_DATA>
<CARD_ENT_METH>R</CARD_ENT_METH>
<PAYMENT_INITIATION_CHANNEL>22</PAYMENT_INITIATION_CHANNEL>
<INDUSTRY_TYPE>P</INDUSTRY_TYPE>
<E2EE>2</E2EE>
<MAC>MAC9876543210</MAC>
<CARD_ID>0</CARD_ID>
<CURRENCY_CODE>840</CURRENCY_CODE>
</DETAIL>
```

Response

```
<RESPONSE>
<FIELDS>
<FIELD KEY="MSG_VERSION">003</FIELD>
<FIELD KEY="CUST_NBR">1234</FIELD>
<FIELD KEY="MERCH_NBR">1234567</FIELD>
<FIELD KEY="DBA_NBR">1</FIELD>
<FIELD KEY="TERMINAL_NBR">1</FIELD>
<FIELD KEY="TRAN_TYPE">CCR1</FIELD>
<FIELD KEY="BATCH_ID">1</FIELD>
<FIELD KEY="TRAN_NBR">95</FIELD>
<FIELD KEY="LOCAL_DATE">050815</FIELD>
<FIELD KEY="LOCAL_TIME">094531</FIELD>
```

```
<FIELD KEY="AUTH_GUID">09YD5MW7DD8TTLJE156</FIELD>
<FIELD KEY="AUTH_RESP">00</FIELD>
<FIELD KEY="AUTH_CODE">000013</FIELD>
<FIELD KEY="AUTH_RESP_TEXT">APPROVAL</FIELD>
<FIELD KEY="AUTH_CARD_TYPE">M</FIELD>
<FIELD KEY="AUTH_TRAN_DATE_GMT">05/08/2015 04:45:31 PM</FIELD>
<FIELD KEY="AUTH_AMOUNT_REQUESTED">10.0000</FIELD>
<FIELD KEY="AUTH_AMOUNT">10.00</FIELD>
<FIELD KEY="AUTH_CURRENCY_CODE">840</FIELD>
<FIELD KEY="NETWORK_RESPONSE">00</FIELD>
<FIELD KEY="AUTH_CARD_COUNTRY_CODE">056</FIELD>
<FIELD KEY="AUTH_CARD_COUNTRY_NAME">BEL</FIELD>
<FIELD KEY="AUTH_CARD_CURRENCY_CODE">978</FIELD>
<FIELD KEY="AUTH_CARD_CURRENCY_NAME">EUR</FIELD>
<FIELD KEY="AUTH_CARD_B">MCC</FIELD>
<FIELD KEY="AUTH_CARD_A">MCS</FIELD>
<FIELD KEY="AUTH_CARD_C">MCS</FIELD>
<FIELD KEY="AUTH_SHA1">F489736651A030067F74EE7E329AB 77E85830639</FIELD>
<FIELD KEY="AUTH_MASKED_ACCOUNT_NBR">************1031 </FIELD>
<FIELD KEY="AUTH_CARD_K">N</FIELD>
<FIELD KEY="AUTH_CARD_L">C</FIELD>
<FIELD KEY="AUTH_EMV_DATA">910A9971B4D9826C69873031</FIELD>
</FIELDS>
</RESPONSE>
```

Contactless MSD with Encryption

This is an example of a Contactless MSD transaction using E2E encryption type 3DES DUKPT (Data variant) using a MasterCard.

Note: The support of contactless MSD is only required for American Express for the L3 certification. Most brands have phased out contactless MSD and only contactless EMV is available out in the field.

IMPORTANT!

The PAYMENT_INITIATION_CHANNEL tag is included with this transaction sample identifies it as a MasterCard transaction. This tag is not required for any other card brand (Visa, Discover, and American Express) and should be omitted from transaction requests for these other card brands.

Request

```
<DETAIL CUST_NBR='1234' MERCH_NBR='1234567' DBA_NBR='1' TERMINAL_NBR='1'>
<AMOUNT>10.00</AMOUNT>
<TRAN_NBR>9</TRAN_NBR>
<BATCH_ID>1</BATCH_ID>
<TRAN_TYPE>CCR1</TRAN_TYPE>
```

```
<TRACK_DATA>004FFFF9876543210E00006A91C1C1ED3A9559CEE546319B653311C8D9668D8C53C534
BD2849280956467A2AE0B9B7B2D441940</TRACK_DATA>
<CARD_ENT_METH>Q</CARD_ENT_METH>
<E2EE>2</E2EE>
<INDUSTRY_TYPE>P</INDUSTRY_TYPE>
<PAYMENT_INITIATION_CHANNEL>21</PAYMENT_INITIATION_CHANNEL>
<MAC>MAC9876543210</MAC>
<CARD_ID>0</CARD_ID>
<CURRENCY_CODE>840</CURRENCY_CODE>
</DETAIL>
```

Response

```
<RESPONSE>
<FIELDS>
<FIELD KEY="MSG_VERSION">003</FIELD>
<FIELD KEY="CUST_NBR">1234</FIELD>
<FIELD KEY="MERCH_NBR">1234567</FIELD>
<FIELD KEY="DBA_NBR">1</FIELD>
<FIELD KEY="TERMINAL_NBR">1</FIELD>
<FIELD KEY="TRAN_TYPE">CCR1</FIELD>
<FIELD KEY="BATCH_ID">1</FIELD>
<FIELD KEY="TRAN_NBR">9</FIELD>
<FIELD KEY="LOCAL_DATE">043015</FIELD>
<FIELD KEY="LOCAL_TIME">164508</FIELD>
<FIELD KEY="AUTH_GUID">09YD52H208YB6RN1019</FIELD>
<FIELD KEY="AUTH_RESP">00</FIELD>
<FIELD KEY="AUTH_CODE">000004</FIELD>
<FIELD KEY="AUTH_RESP_TEXT">APPROVAL</FIELD>
<FIELD KEY="AUTH_CARD_TYPE">M</FIELD>
<FIELD KEY="AUTH_TRAN_DATE_GMT">04/30/2015 04:45:08 PM</FIELD>
<FIELD KEY="AUTH_AMOUNT_REQUESTED">10.0000</FIELD>
<FIELD KEY="AUTH_AMOUNT">10.00</FIELD>
<FIELD KEY="AUTH_CURRENCY_CODE">840</FIELD>
<FIELD KEY="NETWORK_RESPONSE">00</FIELD>
<FIELD KEY="AUTH_CARD_COUNTRY_CODE">056</FIELD>
<FIELD KEY="AUTH_CARD_COUNTRY_NAME">BEL</FIELD>
<FIELD KEY="AUTH_CARD_CURRENCY_CODE">978</FIELD>
<FIELD KEY="AUTH_CARD_CURRENCY_NAME">EUR</FIELD>
<FIELD KEY="AUTH_CARD_B">MCC</FIELD>
<FIELD KEY="AUTH_CARD_A">MCS</FIELD>
<FIELD KEY="AUTH_CARD_C">MCS</FIELD>
<FIELD KEY="AUTH_SHA1">9C86E2255C0A2D34121F8E51A3 ED35C1D98FDEB9</FIELD>
<FIELD KEY="AUTH_MASKED_ACCOUNT_NBR">************1049 </FIELD>
<FIELD KEY="AUTH_CARD_K">N</FIELD>
<FIELD KEY="AUTH_CARD_L">C</FIELD>
</FIELDS>
</RESPONSE>
```

Contactless MSD without Encryption

This is an example of a Contactless MSD transaction with no data encryption using a MasterCard.

Note: The support of contactless MSD is only required for American Express for the L3 certification. Most brands have phased out contactless MSD and only contactless EMV is available out in the field.

IMPORTANT!

The PAYMENT_INITIATION_CHANNEL tag is included with this transaction sample identifies it as a MasterCard transaction. This tag is not required for any other card brand (Visa, Discover, and American Express) and should be omitted from transaction requests for these other card brands.

Request

```
<DETAIL CUST_NBR='1234' MERCH_NBR='1234567' DBA_NBR='1' TERMINAL_NBR='1'>
<AMOUNT>1.00</AMOUNT>
<TRAN_NBR>88</TRAN_NBR>
<BATCH_ID>1</BATCH_ID>
<TRAN_TYPE>CCR1</TRAN_TYPE>
<TRACK_DATA>500000******0009=251210100000000</TRACK_DATA>
<CARD_ENT_METH>Q</CARD_ENT_METH>
<INDUSTRY_TYPE>P</INDUSTRY_TYPE>
<PAYMENT_INITIATION_CHANNEL>21</PAYMENT_INITIATION_CHANNEL>
<E2EE>0</E2EE>
<MAC>MAC9876543210</MAC>
<CARD_ID>0</CARD_ID>
<CURRENCY_CODE>840</CURRENCY_CODE>
</DETAIL>
```

Response

```
<FIELDS>
<FIELD KEY="MSG_VERSION">003</FIELD>
<FIELD KEY="CUST_NBR">1234</FIELD>
<FIELD KEY="MERCH_NBR">1234567</FIELD>
<FIELD KEY="DBA_NBR">1</FIELD>
<FIELD KEY="TERMINAL_NBR">1</FIELD>
<FIELD KEY="TRAN_TYPE">CCR1</FIELD>
<FIELD KEY="BATCH_ID">1</FIELD>
<FIELD KEY="TRAN_NBR">88</FIELD>
<FIELD KEY="LOCAL_DATE">050815</FIELD>
<FIELD KEY="LOCAL_TIME">090824</FIELD>
<FIELD KEY="AUTH_GUID">09YD5MA3E9TR363A150</FIELD>
<FIELD KEY="AUTH_RESP">00</FIELD>
<FIELD KEY="AUTH_CODE">000008</FIELD>
```

```
<FIELD KEY="AUTH_RESP_TEXT">APPROVAL</FIELD>
<FIELD KEY="AUTH_CARD_TYPE">M</FIELD>
<FIELD KEY="AUTH_TRAN_DATE_GMT">05/08/2015 04:08:23 PM</FIELD>
<FIELD KEY="AUTH_AMOUNT_REQUESTED">1.0000</FIELD>
<FIELD KEY="AUTH_AMOUNT">1.00</FIELD>
<FIELD KEY="AUTH_CURRENCY_CODE">840</FIELD>
<FIELD KEY="NETWORK_RESPONSE">00</FIELD>
<FIELD KEY="AUTH_CARD_COUNTRY_CODE">840</FIELD>
<FIELD KEY="AUTH_CARD_CURRENCY_CODE">840</FIELD>
<FIELD KEY="AUTH_CARD_B">MCC</FIELD>
<FIELD KEY="AUTH_CARD_A">MCW</FIELD>
<FIELD KEY="AUTH_CARD_C">MCW</FIELD>
<FIELD KEY="AUTH_SHA1">D4A779E26312D3EAADC54B2AF2353A97E28095B5 </FIELD>
<FIELD KEY="AUTH_MASKED_ACCOUNT_NBR">************0009 </FIELD>
<FIELD KEY="AUTH_RTI_EST_CPD">010100</FIELD>
<FIELD KEY="AUTH_RTI_EST_FEE">0.0000</FIELD>
<FIELD KEY="AUTH_CARD_K">N</FIELD>
</FIELDS>
</RESPONSE>
```

EMV Fallback with Encryption

This is an example of an EMV Fallback transaction using E2E encryption type 3DES DUKPT (Data variant).

Request

```
<DETAIL CUST_NBR='1234' MERCH_NBR='1234567' DBA_NBR='1' TERMINAL_NBR='1'>
<AMOUNT>10.00</AMOUNT>
<BATCH_ID>1</BATCH_ID>
<TRAN_NBR>12</TRAN_NBR>
<TRAN_TYPE>CCR1</TRAN_TYPE>
<TRACK_DATA>004FFFF9876543210E00009A0D85CC20880302E11AACA32111B0668818B76D88D2AD1A
EE05FD4DFC9C015700FBDC4B5C52F6B0F</TRACK_DATA>
<E2EE>2</E2EE>
<CARD_ENT_METH>D</CARD_ENT_METH>
<INDUSTRY_TYPE>P</INDUSTRY_TYPE>
<CHIP_CONDITION_CODE>2</CHIP_CONDITION_CODE>
<MAC>MAC9876543210</MAC>
<CURRENCY_CODE>840</CURRENCY_CODE>
</DETAIL>
```

Response

```
<RESPONSE>
<FIELDS>
<FIELD KEY="MSG_VERSION">003</FIELD>
<FIELD KEY="CUST_NBR">1234</FIELD>
<FIELD KEY="MERCH_NBR">1234567</FIELD>
<FIELD KEY="DBA_NBR">1</FIELD>
<FIELD KEY="TERMINAL_NBR">1</FIELD>
<FIELD KEY="TRAN_TYPE">CCR1</FIELD>
```

```
<FIELD KEY="BATCH_ID">1</FIELD>
<FIELD KEY="TRAN_NBR">12</FIELD>
<FIELD KEY="LOCAL_DATE">043015</FIELD>
<FIELD KEY="LOCAL_TIME">170641</FIELD>
<FIELD KEY="AUTH_GUID">09YD52X9EA1YGJN001D</FIELD>
<FIELD KEY="AUTH_RESP">00</FIELD>
<FIELD KEY="AUTH_CODE">000001</FIELD>
<FIELD KEY="AUTH_RESP_TEXT">APPROVAL</FIELD>
<FIELD KEY="AUTH_CARD_TYPE">M</FIELD>
<FIELD KEY="AUTH_TRAN_DATE_GMT">04/30/2015 05:06:40 PM</FIELD>
<FIELD KEY="AUTH_AMOUNT_REQUESTED">10.0000</FIELD>
<FIELD KEY="AUTH_AMOUNT">10.00</FIELD>
<FIELD KEY="AUTH_CURRENCY_CODE">840</FIELD>
<FIELD KEY="NETWORK_RESPONSE">00</FIELD>
<FIELD KEY="AUTH_CARD_COUNTRY_CODE">056</FIELD>
<FIELD KEY="AUTH_CARD_COUNTRY_NAME">BEL</FIELD>
<FIELD KEY="AUTH_CARD_CURRENCY_CODE">978</FIELD>
<FIELD KEY="AUTH_CARD_CURRENCY_NAME">EUR</FIELD>
<FIELD KEY="AUTH_CARD_B">MCC</FIELD>
<FIELD KEY="AUTH_CARD_A">MCS</FIELD>
<FIELD KEY="AUTH_CARD_C">MCS</FIELD>
<FIELD KEY="AUTH_SHA1">A7FB5834A8B8E5338342FB2114EC3FB479A30CC7</FIELD>
<FIELD KEY="AUTH_MASKED_ACCOUNT_NBR">************1189</FIELD>
<FIELD KEY="AUTH_CARD_K">N</FIELD>
<FIELD KEY="AUTH_CARD_L">C</FIELD>
</FIELDS>
</RESPONSE>
```

EMV Fallback without Encryption

This is an example of an EMV Fallback transaction with no data encryption.

Request

```
<DETAIL CUST_NBR='1234' MERCH_NBR='1234567' DBA_NBR='1' TERMINAL_NBR='1'>
<AMOUNT>5.00</AMOUNT>
<BATCH_ID>1</BATCH_ID>
<TRAN_NBR>96</TRAN_NBR>
<TRAN_TYPE>CCR1</TRAN_TYPE>
<TRACK_DATA>541333******1189=1412201067910618</TRACK_DATA>
<CARD_ENT_METH>D</CARD_ENT_METH>
<INDUSTRY_TYPE>P</INDUSTRY_TYPE>
<CHIP_CONDITION_CODE>2</CHIP_CONDITION_CODE>
<E2EE>0</E2EE>
<CURRENCY_CODE>840</CURRENCY_CODE>
<MAC>MAC9876543210</MAC>
</DETAIL>
```

Response

```
<RESPONSE>
<FIELDS>
```

```
<FIELD KEY="MSG_VERSION">003</FIELD>
<FIELD KEY="CUST_NBR">1234</FIELD>
<FIELD KEY="MERCH_NBR">1234567</FIELD>
<FIELD KEY="DBA_NBR">1</FIELD>
<FIELD KEY="TERMINAL_NBR">1</FIELD>
<FIELD KEY="TRAN_TYPE">CCR1</FIELD>
<FIELD KEY="BATCH_ID">1</FIELD>
<FIELD KEY="TRAN_NBR">96</FIELD>
<FIELD KEY="LOCAL_DATE">050815</FIELD>
<FIELD KEY="LOCAL_TIME">095744</FIELD>
<FIELD KEY="AUTH_GUID">09YD5MWTP96R608Q157</FIELD>
<FIELD KEY="AUTH_RESP">00</FIELD>
<FIELD KEY="AUTH_CODE">000014</FIELD>
<FIELD KEY="AUTH_RESP_TEXT">APPROVAL</FIELD>
<FIELD KEY="AUTH_CARD_TYPE">M</FIELD>
<FIELD KEY="AUTH_TRAN_DATE_GMT">05/08/2015 04:57:44 PM </FIELD>
<FIELD KEY="AUTH_AMOUNT_REQUESTED">5.0000</FIELD>
<FIELD KEY="AUTH_AMOUNT">5.00</FIELD>
<FIELD KEY="AUTH_CURRENCY_CODE">840</FIELD>
<FIELD KEY="NETWORK_RESPONSE">00</FIELD>
<FIELD KEY="AUTH_CARD_COUNTRY_CODE">056</FIELD>
<FIELD KEY="AUTH_CARD_COUNTRY_NAME">BEL</FIELD>
<FIELD KEY="AUTH_CARD_CURRENCY_CODE">978</FIELD>
<FIELD KEY="AUTH_CARD_CURRENCY_NAME">EUR</FIELD>
<FIELD KEY="AUTH_CARD_B">MCC</FIELD>
<FIELD KEY="AUTH_CARD_A">MCS</FIELD>
<FIELD KEY="AUTH_CARD_C">MCS</FIELD>
<FIELD KEY="AUTH_SHA1">A7FB5834A8B8E5338342FB2114EC3 FB479A30CC7
</FIELD>
<FIELD KEY="AUTH_MASKED_ACCOUNT_NBR">************1189 </FIELD>
<FIELD KEY="AUTH_CARD_K">N</FIELD>
<FIELD KEY="AUTH_CARD_L">C</FIELD>
</FIELDS>
</RESPONSE>
```

Appendix A: EMV_DATA Fields

EMV_DATA

The EMV_Data tag contains the request data from the EMV kernel as a variable list of tags and their data in TLV format.

- Variable Type: Alphanumeric
- Max Length: 510

Example:

```
<EMV_DATA>9F34030200009F260828BF9D3AFCC8DD529F2701809F1008010103A0000000009F37044A
BAA8C49F3602008595054040040000820258009F3303E0F8C89F1A0208409F3501229F1E0832323135
333731309F03060000000000009A031504309C01009F02060000000010005F2A0208409F090200025F
3401009F4104000000039F0607A0000000041010</EMV_DATA>
```

Allowed / Maximum EMV Fields

The maximum length for the EMV_DATA tag is 510 bytes.

NOTE: *Table 7* provides all EMV fields that EPX will accept. Not every transaction will contain all of these fields. If the field is present in the EMV data and is referenced in the table, include it in the EMV_DATA tag in any order. **Do not** include a field that is **not** present in this table.

Table 7: EMV_DATA Fields

Field	Max Length (byte)	Field Name	Field Description
71	Variable	Issuer Script Template 1	Contains proprietary issuer data for transmission to the ICC before the second GENERATE AC command. *Tag data is normally in the response from the issuer. (Usually not included in the EMV data from the card, however EPX will allow this in the door if by chance it is)
72	Variable	Issuer Script Template 2	Contains proprietary issuer data for transmission to the ICC after the second GENERATE AC command Tag data is normally in the response from the issuer. (Usually not included in the EMV data from the card, however EPX will allow this in the door if by chance it is)
82	8	Application Interchange Profile	Indicates the capabilities of the card to support specific functions in the application
84	20	Dedicated File (DF) Name	Identifies the name of the DF as described in ISO/IEC 7816-4

Field	Max Length (byte)	Field Name	Field Description
8A	2	Authorization Response Code (ARC)	Data element generated by the Issuer Host System or the Reader indicating the disposition of the transaction.
91	20	Issuer Authentication Data	
95	14	Terminal Verification Results	Status of the different functions as seen from the terminal
9A	10	Transaction Date	Local date that the transaction was authorized
9C	6	Transaction Type	Indicates the type of financial transaction, represented by the first two digits of ISO 8583:1987 Processing Code
C0	Var	Secondary PIN Block	Visa specific, Secondary PIN Block
5F24	6	Application Expiration Date	Date after which the card application expires. (*YYMMDD*)
5F2A	10	Transaction Currency Code	Indicates the currency code of the transaction according to ISO 4217
5F34	8	Application Primary Account Number (PAN) Sequence Number	Identifies and differentiates cards with the same PAN
9F02	18	Amount, Authorized (Numeric)	Authorized amount of the transaction (excluding adjustments)
9F03	18	Amount, Other (Numeric)	Secondary amount associated with the transaction representing a cashback amount
9F06	38	Application Identifier (AID) – terminal	Identifies the application as described in ISO/IEC 7816-5
9F07	10	Application Usage Control (AUC)	Indicates issuer's specified restrictions on the geographic usage and services allowed for the card application.
9F09	10	Application Version Number	Version number assigned by the payment system for the application
9F10	70	Issuer Application Data	Contains proprietary application data for transmission to the issuer in an online transaction

Field	Max Length (byte)	Field Name	Field Description
9F1A	10	Terminal Country Code	Indicates the country of the terminal, represented according to ISO 3166
9F1E	22	Interface Device (IFD) Serial Number	Unique and permanent serial number assigned to the IFD by the manufacturer
9F26	22	Application Cryptogram	Cryptogram returned by the ICC in response of the GENERATE AC command
9F27	8	Cryptogram Information Data	Indicates the type of cryptogram and the actions to be performed by the terminal
9F33	12	Terminal Capabilities	Indicates the card data input, CVM, and security capabilities of the terminal
9F34	12	Cardholder Verification Method (CVM) Results	Indicates the results of the last CVM performed
9F35	8	Terminal Type	Indicates the environment of the terminal, its communications capability, and its operational control
9F36	10	Application Transaction Counter (ATC)	Counter maintained by the application in the ICC (incrementing the ATC is managed by the ICC)
9F37	14	Unpredictable Number	Value to provide variability and uniqueness to the generation of a cryptogram
9F39	2	Point-of-Service (POS) Entry Mode	Indicates the method by which the PAN was entered, according to the first two digits of the ISO POS Entry Mode
9F41	14	Transaction Sequence Counter	Counter maintained by the terminal that is incremented by one for each transaction
9F53	2	Transaction Category	MasterCard specific, Transaction Category Code 9F53
9F5B		Issuer Script Results	Indicates the results of Issuer Script processing. When the reader/terminal transmits this data element to the acquirer, in this version of Kernel 3, it is acceptable that only byte 1 is transmitted, although it is preferable for all five bytes to be transmitted.
9F6E	4	Form Factor Indicator (qVSDC)	Indicates the form factor of the consumer payment device and the type of contactless interface over which the transaction was conducted. This information is made available to the issuer host.

Field	Max Length (byte)	Field Name	Field Description
9F7C	32	Customer Exclusive Data (CED)	Contains data for transmission to the issuer. Note: This tag is contained in U.S. contactless transactions and contains issuer proprietary information in TLV format. The tag is personalized on the card or device. If present in an interregional transaction, the tag is treated as supplemental data.

Appendix B: AUTH_EMV_DATA Fields

AUTH_EMV_DATA

The AUTH_EMV_DATA tag is provided in the response and the data must be provided back to the EMV kernel. The tag currently can contain up to 3 EMV tags from the issuer: Tags 91, 71, and 72. Data will be returned within this tag in the response nearly always.

- Tag 91—Issuer Authentication Data will be present 99.9% of the time.
- Tag 71—Issuer Script Template 1 will be present .01% of the time
- Tag 72—Issuer Script Template 1 will be present .01% of the time

Issuer scripts 0x71 and 0x72 can be very large, up to 128 bytes each, which is presented in HEX ASCII (so 256 characters each).

NOTE: Our UAP / Demo environment does not return this tag as we are unable to replicate this in Demo mode.

- Variable Type: Alphanumeric
- Max Length: variable

Example:

```
<FIELD KEY="AUTH_EMV_DATA">910AD1020739E23C7D443035</FIELD>
```