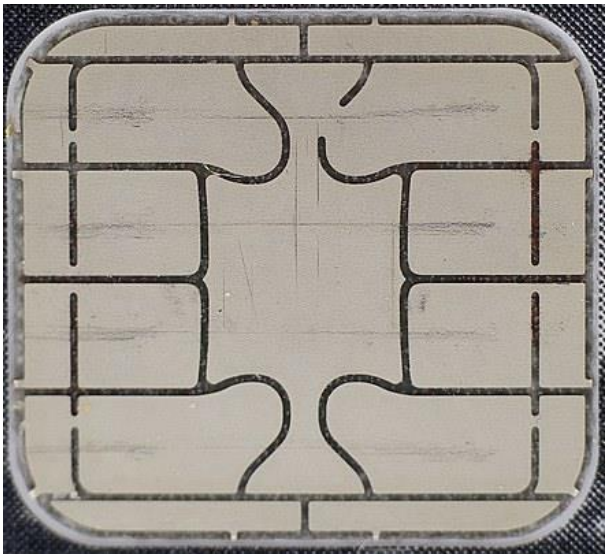


# Decoding EMV data

## Reading EMV records

| Code | Value |
|---|---|
| CLA | '00' |
| INS | 'B2' |
| P1 | Record number |
| P2 | Reference control parameter (see Table 39) |
| Lc | Not present |
| Data | Not present |
| Le | '00' |

| b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | Meaning |
|---|---|---|---|---|---|---|---|---|
| x | x | x | x | x | | | | SFI |
| | | | | | 1 | 0 | 0 | P1 is a record number |

*1 - READ RECORD Command* [EMV 4.3, Book 1, 11.2]

## TLV format

TLV items consist of a tag (1 or more bytes, up to three is common), a length (1 or more bytes, up to two is common), and a value.

## Decoding the tag field

| b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | Meaning |
|---|---|---|---|---|---|---|---|---|
| 0 | 0 | | | | | | | Universal class |
| 0 | 1 | | | | | | | Application class |
| 1 | 0 | | | | | | | Context-specific class |
| 1 | 1 | | | | | | | Private class |
| | | 0 | | | | | | Primitive data object |
| | | 1 | | | | | | Constructed data object |
| | | | 1 | 1 | 1 | 1 | 1 | See subsequent bytes |
| | | | Any other value <31 | | | | | Tag number |

*2 - Tag field structure (first byte)* [EMV 4.3, Book 3, Annex B]

| b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | Meaning |
|---|---|---|---|---|---|---|---|---|
| 1 | | | | | | | | Another byte follows |
| 0 | | | | | | | | Last tag byte |
| | Any value > 0 | | | | | | | (Part of) tag number |

*3 - Tag field structure (subsequent bytes)* [EMV 4.3, Book 3, Annex B]

## Decoding the length field

"When bit **b8** of the most significant byte of the length field is set to 0, the length field consists of only one byte. Bits **b7** to **b1** code the number of bytes of the value field. The length field is within the range 1 to 127. When bit **b8** of the most significant byte of the length field is set to 1, the subsequent bits **b7** to **b1 of** the most significant byte code the number of subsequent bytes in the length field. The subsequent bytes code an integer representing the number of bytes in the value field. Two bytes are necessary to express up to 255 bytes in the value field." *[EMV 4.3, Book 3, Annex B]*

# EMV Tag dictionary

| Name | Description | Source | Format | Template | Tag | Length |
|---|---|---|---|---|---|---|
| Authorisation Code | Value generated by the authorisation authority for an approved transaction | Issuer | As defined by the Payment Systems | — | '89' | 6 |
| Authorisation Response Code | Code that defines the disposition of a message | Issuer/ Terminal | an 2 | — | '8A' | 2 |
| Authorisation Response Cryptogram (ARPC) | Cryptogram generated by the issuer and used by the card to verify that the response came from the issuer. | Issuer | b | — | — | 4 or 8 |
| Bank Identifier Code (BIC) | Uniquely identifies a bank as defined in ISO 9362. | ICC | var. | 'BF0C' or '73' | '5F54' | 8 or 11 |
| Card Risk Management Data Object List 1 (CDOL1) | List of data objects (tag and length) to be passed to the ICC in the first GENERATE AC command | ICC | b | '70' or '77' | '8C' | var. up to 252 |
| Card Risk Management Data Object List 2 (CDOL2) | List of data objects (tag and length) to be passed to the ICC in the second GENERATE AC command | ICC | b | '70' or '77' | '8D' | var. up to 252 |

*4 - Data Elements Dictionary* [EMV 4.3, Book 3, Annex A1]

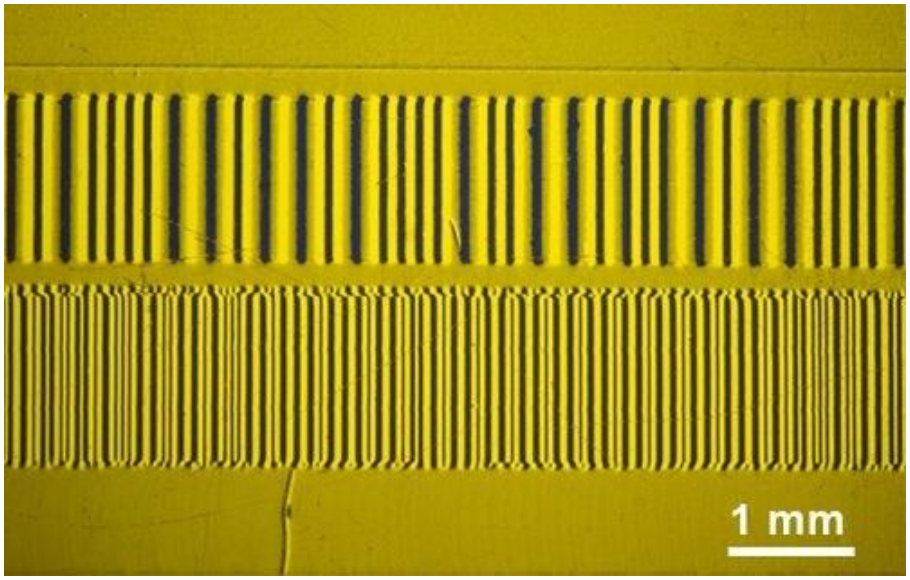
| Name | Description | Source | Format | Template | Tag | Length |
|---|---|---|---|---|---|---|
| Amount, Authorised (Numeric) | Authorised amount of the transaction (excluding adjustments) | Terminal | n 12 | — | '9F02' | 6 |
| Amount, Other (Binary) | Secondary amount associated with the transaction representing a cashback amount | Terminal | b | — | '9F04' | 4 |
| Amount, Other (Numeric) | Secondary amount associated with the transaction representing a cashback amount | Terminal | n 12 | — | '9F03' | 6 |
| Amount, Reference Currency | Authorised amount expressed in the reference currency | Terminal | b | — | '9F3A' | 4 |
| Application Cryptogram | Cryptogram returned by the ICC in response of the GENERATE AC command | ICC | b | '77' or '80' | '9F26' | 8 |
| Application Currency Code | Indicates the currency in which the account is managed according to ISO 4217 | ICC | n 3 | '70' or '77' | '9F42' | 2 |
| Application Currency Exponent | Indicates the implied position of the decimal point from the right of the amount represented according to ISO 4217 | ICC | n 1 | '70' or '77' | '9F44' | 1 |
| Application Discretionary Data | Issuer or payment system specified data relating to the application | ICC | b | '70' or '77' | '9F05' | 1-32 |
| Application Effective Date | Date from which the application may be used | ICC | n 6 YYMMDD | '70' or '77' | '5F25' | 3 |

*5 - Data Elements Dictionary* [EMV 4.3, Book 3, Annex A1]

| Name | Description | Source | Format | Template | Tag | Length |
|---|---|---|---|---|---|---|
| Card Status Update (CSU) | Contains data sent to the ICC to indicate whether the issuer approves or declines the transaction, and to initiate actions specified by the issuer. Transmitted to the card in Issuer Authentication Data. | Issuer | b | — | — | 4 |
| Cardholder Name | Indicates cardholder name according to ISO 7813 | ICC | ans 2-26 | '70' or '77' | '5F20' | 2-26 |
| Cardholder Name Extended | Indicates the whole cardholder name when greater than 26 characters using the same coding convention as in ISO 7813 | ICC | ans 27-45 | '70' or '77' | '9F0B' | 27-45 |
| Cardholder Verification Method (CVM) List | Identifies a method of verification of the cardholder supported by the application | ICC | b | '70' or '77' | '8E' | 10-252 |
| Cardholder Verification Method (CVM) Results | Indicates the results of the last CVM performed | Terminal | b | — | '9F34' | 3 |
| Certification Authority Public Key Check Sum | A check value calculated on the concatenation of all parts of the Certification Authority Public Key (RID, Certification Authority Public Key Index, Certification Authority Public Key Modulus, Certification Authority Public Key Exponent) using SHA-1 | Terminal | b | — | — | 20 |

*6 - Data Elements Dictionary* [EMV 4.3, Book 3, Annex A1]

# Magnetic stripe format




## Track 1 magnetic stripe format

- **Start sentinel** — one character (generally '%')
- **Format code="B"** — one character (alpha only)
- **Primary account number** (PAN) — up to 19 characters. Usually, but not always, matches the credit card number printed on the front of the card.
- **Field Separator** — one character (generally '^')
- **Name** — 2 to 26 characters, surnames separated by space if necessary, Surname separator: /
- **Field Separator** — one character (generally '^')
- **Expiration date** — four characters in the form YYMM.
- **Service code** — three characters
- **Discretionary data** — may include Pin Verification Key Indicator (PVKI, 1 character), PIN Verification Value (PVV, 4 characters), Card Verification Value or Card Verification Code (CVV or CVC, 3 characters)
- **End sentinel** — one character (generally '?')
- **Longitudinal redundancy check** (LRC) — it is one character and a validity character calculated from other data on the track.

*[Wikipedia (Magnetic stripe card), 17 June 2020, 23:48 UTC]*

## Track 2 magnetic stripe format

- **Start sentinel** — one character (generally ';')
- **Primary account number** (PAN) — up to 19 characters. Usually, but not always, matches the credit card number printed on the front of the card.

- **Separator** — one char (generally '=')
- **Expiration date** — four characters in the form YYMM.
- **Service code** — three digits. The first digit specifies the interchange rules, the second specifies authorization processing and the third specifies the range of services
- **Discretionary data** — as in track one
- **End sentinel** — one character (generally '?')
- **Longitudinal redundancy check** (LRC) — it is one character and a validity character calculated from other data on the track. Most reader devices do not return this value when the card is swiped to the presentation layer, and use it only to verify the input internally to the reader.

*[Wikipedia (Magnetic stripe card), 17 June 2020, 23:48 UTC]*

## Service code

**First digit**

- 1: International interchange OK
- 2: International interchange, use IC (chip) where feasible
- 5: National interchange only except under bilateral agreement
- 6: National interchange only except under bilateral agreement, use IC (chip) where feasible
- 7: No interchange except under bilateral agreement (closed loop)
- 9: Test

**Second digit**

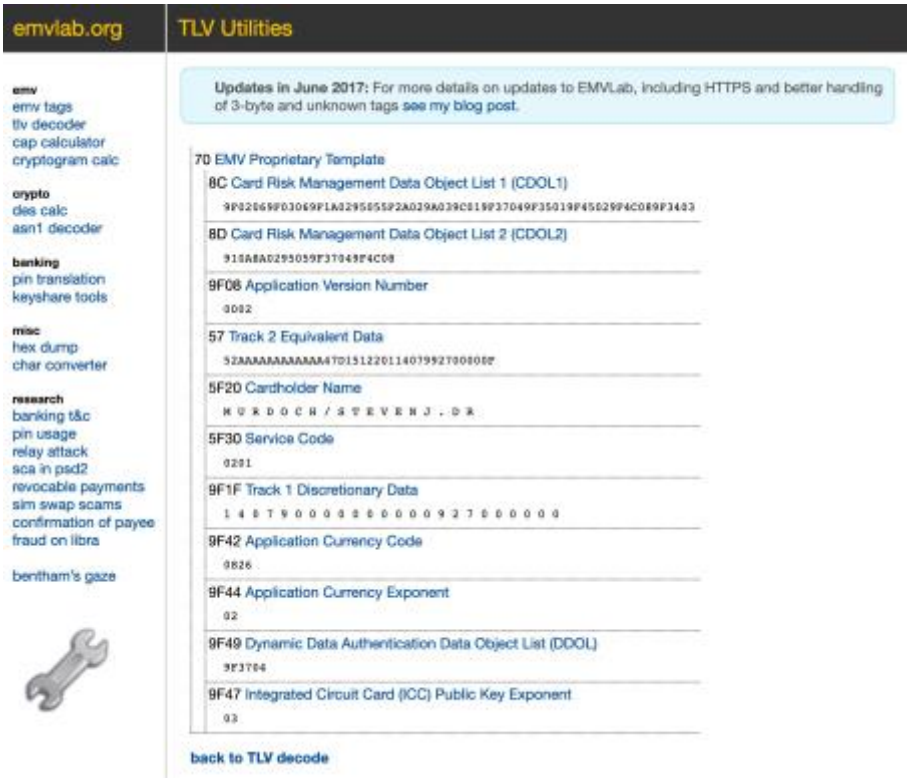
- 0: Normal
- 2: Contact issuer via online means
- 4: Contact issuer via online means except under bilateral agreement

**Third digit**

- 0: No restrictions, PIN required
- 1: No restrictions
- 2: Goods and services only (no cash)
- 3: ATM only, PIN required
- 4: Cash only
- 5: Goods and services only (no cash), PIN required
- 6: No restrictions, use PIN where feasible
- 7: Goods and services only (no cash), use PIN where feasible

*[Wikipedia (Magnetic stripe card), 17 June 2020, 23:48 UTC]*

## EMV Lab TLV decoder




*7 - Example of using EMVLab TLV decoder*

I created the EMV Lab TLV decoder as an easy way to decode TLV data. It knows about many (but not all) EMV tags.

## Acknowledgements

Images from Wikimedia Commons: EMV contact pads, magnetic strip card.