EMV transaction processing is a series of commands and responses between the **EMV terminal** (Point of Sale, ATM) and the **EMV card** (chip card). The data exchanged is often in **Tag-Length-Value (TLV)** format.

Let's break down the typical contact EMV transaction flow, step by step, highlighting key actions and relevant EMV tags.

**Understanding TLV Format:** EMV data is structured using TLV.

- **Tag:** A unique identifier (1 or 2 bytes, sometimes more) that indicates the type of data (e.g., 9F02 for Amount, Authorised).
- **Length:** The length (in bytes) of the Value field. Can be 1 or more bytes.
- **Value:** The actual data.

---

**EMV Transaction Flow: Step-by-Step with Key Tags**

**Phase 1: Transaction Initiation & Application Selection**

1. **Card Insertion/Tap & Power-Up:**
    - **Action:** The card is inserted into the terminal's chip reader, or a contactless card is tapped. The terminal provides power to the chip.
    - **Card Response:** The card responds with an **Answer To Reset (ATR)**. The ATR contains fundamental information about the card's capabilities and communication protocols. While not a TLV tag, it's the very first data exchange.
    - **Key EMV Tags (Not present yet, but context for subsequent steps):** The terminal begins initializing its internal state, including **Terminal Verification Results (TVR - Tag '95')** and **Transaction Status Information (TSI - Tag '9F18')** to all zeros, which will be updated throughout the transaction.
2. **Application Selection:**
    - **Action:** The terminal and card determine which payment application (e.g., Visa, Mastercard, RuPay) will be used for the transaction. This can happen in a few ways:
        - **List of AID (Application Identifier):** The card sends a list of AIDs it supports.
        - **Terminal's Preferred AIDs:** The terminal has its own list of preferred AIDs.

        - **Priority Rules:** They negotiate based on priority.
    - **Terminal Command:** SELECT command.
    - **Card Data Provided (Examples):**
        - **4F (Application Identifier - AID):** Identifies the payment application on the card (e.g., A0000000031010 for Visa Credit/Debit).
        - **50 (Application Label):** Human-readable name of the application (e.g., "VISA CREDIT").
        - **87 (Application Priority Indicator):** Specifies the priority of the application on the card.
        - **9F12 (Application Preferred Name):** Another human-readable name, potentially prioritized.
        - **9F04 (Application Version Number):** Version of the application on the card.
    - **Card Response:** The card confirms the selected application.

**Phase 2: Transaction Processing & Data Acquisition**

3. **Initiate Application Processing (Get Processing Options):**
    - **Action:** The terminal requests essential processing data from the selected application on the card.
    - **Terminal Command:** GET PROCESSING OPTIONS (GPO). This command includes the **PDOL (Processing Options Data Object List - Tag '9F38')**. The PDOL tells the card *what data* the terminal needs for the transaction (e.g., Amount, Transaction Currency Code, Unpredictable Number).
    - **Terminal Provided Data (Examples within GPO/PDOL):**
        - **9F02 (Amount, Authorised):** The transaction amount.
        - **9F03 (Amount, Other):** Cashback amount, if any.
        - **5F2A (Transaction Currency Code):** e.g., 0978 for EUR.
        - **9A (Transaction Date):** Date of the transaction.
        - **9C (Transaction Type):** e.g., 00 for purchase.
        - **9F37 (Unpredictable Number):** A random number generated by the terminal for the current transaction, crucial for cryptogram generation.

        - **9F33 (Terminal Capabilities):** Indicates the terminal's capabilities (e.g., supports online PIN, signature, DDA).
        - **9F40 (Additional Terminal Capabilities):** More detailed terminal capabilities.
    - **Card Response:** The card responds with:
        - **82 (Application Interchange Profile - AIP):** Indicates the capabilities of the application on the card (e.g., supports SDA, DDA, CVMs, online/offline processing).
        - **94 (Application File Locator - AFL):** A list of files/records on the card that contain application data, telling the terminal *where* to read the data.

4. **Read Application Data:**
    - **Action:** The terminal reads the necessary data from the card's files/records, as indicated by the AFL. This is done using READ RECORD commands.
    - **Card Data Provided (Examples):**
        - **5A (Application Primary Account Number - PAN):** The card number.
        - **5F24 (Application Expiration Date):** Card expiry date.
        - **5F34 (Application PAN Sequence Number):** Differentiates cards with the same PAN (e.g., if a card is reissued).
        - **5F20 (Cardholder Name):** Name on the card.
        - **8C (Card Risk Management Data Object List 1 - CDOL1):** List of data elements the *card* needs from the *terminal* to generate the ARQC.
        - **8D (Card Risk Management Data Object List 2 - CDOL2):** List of data elements the *card* needs from the *issuer* (in the authorization response) to generate the ARPC.
        - **8E (Cardholder Verification Method List - CVM List):** Prioritized list of CVMs supported by the card.
        - **9F17 (Personal PIN Unblock Code):** For PIN management.
        - **9F2D (Issuer Script Template 1):** For issuer script commands.

        - **9F42 (Application Currency Code):** Currency in which the application's internal amounts are maintained.
        - **9F44 (Application Currency Exponent):** Exponent for the application's currency.
        - **9F46 (ICC Public Key Certificate):** Part of the card's cryptographic key material for ODA.
        - **9F47 (ICC Public Key Exponent):** Part of the card's cryptographic key material for ODA.
        - **9F48 (ICC Dynamic Data):** Used in DDA/CDA.
        - **BF0C (File Control Information - FCI):** Contains details about the files.

**Phase 3: Security Checks & Decision Making (Offline/Online)**

5. **Offline Data Authentication (ODA):**
    - **Action:** The terminal verifies the authenticity of the card and its data *offline* using cryptographic techniques.
    - **Types:**
        - **SDA (Static Data Authentication):** Terminal verifies a digital signature over static card data.
            - **Tags used:** 9F4A (Signed Data), 9F32 (Issuer Public Key Exponent), 9F46 (ICC Public Key Certificate), 9F47 (ICC Public Key Exponent), 8F (Certification Authority Public Key Index - CA PKI), 90 (Issuer Public Key Certificate).
        - **DDA (Dynamic Data Authentication):** Terminal requests the card to generate a digital signature over dynamic data (including 9F37 Unpredictable Number).
            - **Tags used:** In addition to SDA tags, involves 9F4B (Signed Dynamic Application Data).
        - **CDA (Combined DDA/Application Cryptogram Generation):** Most secure. The card generates a digital signature over transaction data *and* the cryptogram data.
            - **Tags used:** Similar to DDA, but the signature covers the ARQC/TC data.

  - **Outcome:** Updates bits in **95 (Terminal Verification Results - TVR)**. For example, a bit might be set if ODA fails.

6. **Cardholder Verification Method (CVM) Selection:**
   - **Action:** The terminal and card agree on how to verify the cardholder (PIN, signature, no CVM).
   - **Terminal Data:** 9F33 (Terminal Capabilities), 9F35 (Terminal Type).
   - **Card Data:** 8E (Cardholder Verification Method List - CVM List), 9F34 (Cardholder Verification Method (CVM) Results).
   - **Process:** The terminal iterates through the prioritized 8E CVM List from the card, comparing it with its own 9F33 capabilities and transaction conditions (e.g., amount thresholds). The first matching CVM is selected.
   - **Outcome:** The chosen CVM is performed (e.g., PIN entry). The result is recorded in 9F34 (CVM Results).

7. **Terminal Risk Management:**
   - **Action:** The terminal performs its own risk checks based on configuration.
   - **Terminal Configured Data (Examples):**
     - **9F01 (Acquirer Identifier):** Identifies the acquirer.
     - **9F0D (Issuer Action Code - Denial - IAC-Denial):** Card-issuer specified rules for declining offline.
     - **9F0E (Issuer Action Code - Online - IAC-Online):** Card-issuer specified rules for going online.
     - **9F0F (Issuer Action Code - Default - IAC-Default):** Card-issuer specified default rules.
     - **9F1D (Terminal Risk Management Data):** Various risk parameters.
     - **9F4C (ICC Dynamic Number):** Used for DDA.
   - **Outcome:** Updates bits in 95 (TVR). For example, a bit set if the transaction exceeds a floor limit.

8. **Card Action Analysis (First GENERATE AC Command):**
   - **Action:** Based on all the preceding steps (ODA results, CVM results, terminal risk, card risk management rules), the card decides whether the

transaction can be approved offline, declined offline, or needs to go online for authorization.

- **Terminal Command:** GENERATE AC (Application Cryptogram) with a Command Payload that contains data requested by the card in **8C (CDOL1)**. This includes crucial transaction data.
- **Terminal Data Provided (Examples, as part of the GENERATE AC command payload):**
    - 9F02 (Amount, Authorised)
    - 9F03 (Amount, Other)
    - 9F1A (Terminal Country Code)
    - 95 (Terminal Verification Results - TVR) - *Current state of TVR*
    - 5F2A (Transaction Currency Code)
    - 9A (Transaction Date)
    - 9C (Transaction Type)
    - 9F37 (Unpredictable Number)
    - 82 (Application Interchange Profile - AIP)
    - 9F36 (Application Transaction Counter - ATC) - *Current value of ATC*
    - 9F10 (Issuer Application Data - IAD) - *Contains proprietary data from the issuer, important for ARQC verification*.
- **Card Response:** The card generates and returns one of three cryptograms:
    - **9F26 (Application Cryptogram - ARQC/TC/AAC):** This is the core cryptogram. The *type* of cryptogram is indicated by the cryptogram's structure and the 9F27 Cryptogram Information Data.
    - **9F27 (Cryptogram Information Data - CID):** A single byte indicating the type of cryptogram (ARQC, TC, AAC) and the CVM performed.
    - **9F34 (Cardholder Verification Method (CVM) Results):** The actual CVM that was performed and its result (e.g., Online PIN performed, Signature verified).

        - **9F3B (Application Reference Currency):** If currency conversion is happening.
        - **9F4E (Form Factor Indicator):** Indicates if it's a mobile payment.

**Phase 4: Online Authorization (if required)**

9. **Build Online Authorization Message:**
    - **Action:** If the card generated an **ARQC** (meaning an online authorization is required), the terminal constructs an **ISO 8583 message**.
    - **Key ISO 8583 Data Elements:**
        - **MTI:** 0100 (Authorization Request)
        - **DE 2:** Primary Account Number (PAN) (5A from EMV data)
        - **DE 3:** Processing Code (9C Transaction Type + Account types)
        - **DE 4:** Amount, Transaction (9F02)
        - **DE 7:** Transmission Date and Time
        - **DE 11:** System Trace Audit Number (STAN)
        - **DE 22:** POS Entry Mode (e.g., 05 for EMV chip)
        - **DE 37:** Retrieval Reference Number
        - **DE 41:** Card Acceptor Terminal ID
        - **DE 42:** Card Acceptor ID Code
        - **DE 43:** Card Acceptor Name/Location
        - **DE 49:** Currency Code, Transaction (5F2A)
        - **DE 52:** PIN Data (if online PIN was entered)
        - **DE 55: Integrated Circuit Card (ICC) Data:** This is crucial. It contains *all* the relevant EMV tags exchanged between the card and terminal that the issuer needs to verify the transaction. This is a TLV-encoded string of EMV tags (e.g., 9F26 ARQC, 9F27 CID, 9F10 IAD, 9F36 ATC, 9F34 CVM Results, 95 TVR, 82 AIP, 9F37 UN, 9F02, 9F03, 5F2A, 9A, 9C).

10. **Issuer Processing (Host Side):**
    - **Action:** The authorization request travels through the payment network to the issuing bank. The issuer:

        - **Verifies ARQC:** Uses its secret keys and the data from DE 55 to re-calculate and verify the 9F26 ARQC received from the card. This confirms the card is genuine and the transaction data wasn't altered.
        - **Performs standard authorization checks:** Checks account balance, card status, fraud rules, etc.
        - **Generates ARPC:** If approved, the issuer generates an **ARPC (Authorization Response Cryptogram)**, which is a cryptogram verifying the issuer's response.
    - **Issuer Response:** The issuer sends an ISO 8583 authorization response message back to the terminal.
    - **Key ISO 8583 Data Elements in Response:**
        - **MTI:** 0110 (Authorization Response)
        - **DE 38:** Authorization Identification Response (Approval Code, e.g., A1B2C3)
        - **DE 39:** Response Code (e.g., 00 for Approved, 05 for Do Not Honor)
        - **DE 55:** ICC Data (contains the **ARPC - Tag 9F26**, usually with a new CID 9F27 and sometimes 71 Issuer Script Template 1 or 72 Issuer Script Template 2).

11. **Second Card Action Analysis (GENERATE AC with Issuer Response):**
    - **Action:** The terminal sends the issuer's response (including the ARPC from DE 55) back to the card using a second GENERATE AC command. This time, the command payload contains data requested by the card in **8D (CDOL2)**.
    - **Terminal Command:** GENERATE AC (often with CDOL2 data).
    - **Terminal Data Provided (Examples, as part of the GENERATE AC command payload):**
        - 9F26 (ARPC - from issuer response)
        - 9F27 (CID - from issuer response)
        - 8A (Authorization Response Code - ARC, from DE 39)
        - 91 (Issuer Authentication Data) - Contains the ARPC and sometimes an Issuer Script.

- **Card Action:** The card verifies the ARPC. If the ARPC verification fails, the card might internally decline the transaction even if the issuer approved it (a rare but possible scenario for security). The card may also process **Issuer Scripts** (71, 72) for actions like blocking the card or updating internal parameters.
- **Card Response:** The card provides its final status or a final cryptogram if needed.

**Phase 5: Transaction Completion**

12. **Terminal Displays Result & Card Removal:**
    - **Action:** The terminal displays the final transaction result to the cardholder (Approved, Declined). It may print a receipt.
    - **Outcome:** The cardholder removes the card. The transaction details are stored locally for batching and clearing.

---

**Summary of Key EMV Tags (Non-exhaustive but highly important):**

- **4F (AID):** Application Identifier
- **50 (Application Label):** Human-readable name of the application.
- **5A (Application PAN):** Cardholder's primary account number.
- **5F20 (Cardholder Name):** Name on the card.
- **5F24 (Application Expiration Date):** Card expiry.
- **5F2A (Transaction Currency Code):** Currency of the transaction.
- **5F34 (Application PAN Sequence Number):** Differentiates cards with same PAN.
- **82 (AIP - Application Interchange Profile):** Card capabilities (e.g., supports DDA, CVMs).
- **84 (Dedicated File Name - DFN):** Used in application selection (same as AID '4F').
- **87 (Application Priority Indicator):** Priority of application on card.
- **8A (Authorization Response Code - ARC):** Issuer's response to the ARQC (maps to ISO 8583 DE 39).
- **8C (CDOL1):** Card Data Object List for GENERATE AC (for ARQC).

- **8D (CDOL2):** Card Data Object List for GENERATE AC (for ARPC).
- **8E (CVM List):** Prioritized list of cardholder verification methods.
- **8F (Certification Authority Public Key Index - CA PKI):** Index of the CA public key used for authentication.
- **90 (Issuer Public Key Certificate):** Issuer's digital certificate.
- **91 (Issuer Authentication Data):** Contains ARPC and/or Issuer Script.
- **94 (AFL - Application File Locator):** List of files on the card to read.
- **95 (TVR - Terminal Verification Results):** 5-byte field indicating results of various terminal checks (e.g., ODA failed, CVM failed, floor limit exceeded). Critical for risk management.
- **9A (Transaction Date):** Date of transaction.
- **9C (Transaction Type):** Type of transaction (e.g., purchase, cashback).
- **9F02 (Amount, Authorised):** Transaction amount.
- **9F03 (Amount, Other):** Secondary amount (e.g., cashback).
- **9F10 (Issuer Application Data - IAD):** Proprietary issuer data, often used in ARQC/ARPC verification.
- **9F1A (Terminal Country Code):** Country where terminal is located.
- **9F1E (Interface Device Serial Number):** Serial number of the terminal.
- **9F26 (Application Cryptogram - AC):** This is the **ARQC**, **TC**, or **AAC**.
- **9F27 (Cryptogram Information Data - CID):** Indicates the type of cryptogram generated.
- **9F33 (Terminal Capabilities):** Terminal's capabilities (e.g., CVMs, security features).
- **9F34 (CVM Results):** Result of cardholder verification.
- **9F35 (Terminal Type):** Type of terminal (e.g., unattended, merchant).
- **9F36 (Application Transaction Counter - ATC):** A sequential counter maintained by the card for each transaction.
- **9F37 (Unpredictable Number):** Random number generated by the terminal for cryptogram generation.
- **9F38 (PDOL - Processing Options Data Object List):** List of data elements terminal requests from card during GPO.

- **9F41 (Transaction Sequence Counter):** Similar to STAN, but internal to the terminal.
- **9F46 (ICC Public Key Certificate):** Chip's public key certificate.
- **9F47 (ICC Public Key Exponent):** Chip's public key exponent.
- **9F48 (ICC Dynamic Data):** Used in DDA.
- **9F4A (Signed Data):** For SDA verification.
- **9F4B (Signed Dynamic Application Data):** For DDA verification.
- **71 (Issuer Script Template 1):** Commands from issuer to card.
- **72 (Issuer Script Template 2):** Commands from issuer to card.

Understanding this flow and these tags is fundamental for anyone implementing or troubleshooting EMV payment systems, as it details the secure and dynamic nature of chip card transactions.