Here's a detailed table of **Application Interchange Profile (AIP)** bits and their meaning in the EMV transaction flow, along with **in-depth explanations** of each bit's function:

📘 AIP: Application Interchange Profile

- Sent by the card in response to the **GPO (Get Processing Options)** command.
- Tells the terminal what the **card supports** in terms of capabilities/features.
- It is **2 bytes** (16 bits) – though some implementations may use more.
- Helps terminal to decide:
  - Which data authentication method to use.
  - Whether the card can perform offline processing.
  - Whether CVM (Cardholder Verification Method) is supported.

🧾 AIP Format (16 bits total)

Byte	Bit	Value	Feature Name	Detailed Explanation
1	8 (MSB)	80	**Offline Static Data Authentication (SDA)** supported	Card supports SDA – a basic offline method to verify card authenticity using digital signature of static data.
1	7	40	**Offline Dynamic Data Authentication (DDA)** supported	Card supports DDA – uses a challenge-response mechanism and dynamic signature; more secure than SDA.
1	6	20	**Cardholder Verification Method (CVM)** supported	Card can handle PIN, signature, or other CVM methods. Required for most attended terminals.
1	5	10	**Terminal risk management is to be performed**	Instructs terminal to check for risk rules like floor limits, exception files, random selection.
1	4	08	**Issuer Authentication** is supported	Card can perform online issuer authentication (ARQC and ARPC exchange).

Byte	Bit	Value	Feature Name	Detailed Explanation
1	3	04	**Offline Enciphered PIN** supported	Card supports secure offline PIN entry using encryption with card's public key.
1	2	02	**Offline Plaintext PIN** supported	Card supports plaintext PIN sent directly to card (insecure; deprecated).
1	1 (LSB)	01	**Signature (paper-based) CVM** supported	Indicates fallback support for paper-based signature if PIN isn't available.
2	8	80	**Combined DDA / Application Cryptogram Generation (CDA)** supported	Advanced method combining DDA and AC generation, offering highest security for offline auth.
2	7–1	-	Reserved for future use	Bits 7 to 1 are RFU (Reserved for Future Use). Must be zero unless specified by spec.

🔍 Key AIP Use Cases and Implications

Feature	Why It Matters
SDA/DDA/CDA	Helps the terminal determine which **offline data authentication method** it can perform. If card supports only SDA, terminal can't use dynamic auth.
CVM Supported	If card doesn't support CVM, terminal may skip PIN/signature verification.
Issuer Authentication	Indicates if card supports **online ARQC/ARPC** process.
PIN Support (Offline)	Determines if the terminal can request PIN validation **offline** instead of online.
Terminal Risk Management	Helps terminal decide whether to apply **floor limits, velocity checks, etc.**

💡 Example AIP = 50 80

Breakdown:

- **First Byte = 0x50 = 0101 0000**
  - Bit 7: DDA supported ✅
  - Bit 5: Terminal risk management ✅
- **Second Byte = 0x80 = 1000 0000**
  - Bit 8: CDA supported ✅

🔍 This means:

- Card supports DDA and CDA (secure authentication methods).
- Card wants terminal to perform risk management.
- It does **not support CVM or issuer authentication** in this case.

🧬 **Used In:**

- GPO command response TLV: 77 or 80 template contains AIP as 82 tag.
- Terminal parses 82 tag to know what steps it should execute.

✅ **Summary of Critical Bits**

Feature	Byte.Bit	Value	Required For
SDA	1.8	80	Basic offline authentication
DDA	1.7	40	Secure offline dynamic check
CDA	2.8	80	Highest offline security
CVM	1.6	20	Verifying cardholder
Issuer Auth	1.4	08	Online auth (ARPC)
Terminal Risk Mgmt	1.5	10	Offline transaction control