

You've asked for an **in-depth explanation of TVR**, and yes — what I've given so far **covers nearly everything**, but let's ensure **nothing is missed**. Here's a **complete checklist** of what you might expect when someone says **“explain TVR fully”**:

✅ 1. What is TVR and its Role?

- ✓ 5-byte data structure (Tag: 95) used by the terminal.
 - ✓ Records results of terminal-side checks during an EMV transaction.
 - ✓ Used in **Terminal Action Analysis (TAA)** to decide whether to approve offline, go online, or decline.
-

✅ 2. When is TVR Updated?

- ✓ Dynamically updated as the transaction progresses.
 - ✓ Steps:
 - Application selection
 - Offline data authentication (ODA)
 - Processing restrictions
 - Cardholder verification (CVM)
 - Risk management
 - Terminal Action Analysis
 - Online processing
 - Script processing
-

✅ 3. Byte-by-Byte Breakdown of TVR (Tag 95)

All 40 bits across 5 bytes were explained, including:

- ✓ Byte 1: Offline data auth / ICC data
- ✓ Byte 2: Application expiration, version, restrictions
- ✓ Byte 3: CVM (PIN entry, failure, limits)
- ✓ Byte 4: Terminal risk checks (floor limit, velocity)

- ✓ Byte 5: Issuer auth / script results
-

✓ 4. Offline vs Online Decision Based on TVR

- ✓ Explained how TVR is compared against:
 - IAC-Denial
 - IAC-Online
 - IAC-Default
 - ✓ How specific bits influence the decision to decline/approve or go online
-

✓ 5. Realistic Example Decoded

- ✓ A real TVR (40 00 08 20 00) was broken down bit by bit
 - ✓ Interpreted meaning of each byte
 - ✓ Mapped scenario to likely terminal behavior
-

✓ 6. Values TVR Can Take

- ✓ All zeroes (00 00 00 00 00) → perfect case (offline approval likely)
 - ✓ Examples where bits are set in one or more bytes
 - ✓ Explained meanings and implications of critical bits (SDA failure, expired card, PIN failed, etc.)
-

✓ 7. TVR and Terminal Action Analysis (TAA)

- ✓ Described how TVR is **logically ANDed** with IACs to determine the next action.
 - ✓ Emphasized the terminal doesn't just read TVR — it uses it **programmatically** in TAA logic.
-

✓ 8. Relation to CVM, AIP, TTQ

- CVM-related bits are in **Byte 3**

- Terminal's **capabilities** (e.g. TTQ, AIP) impact which checks happen, and thus which **TVR bits can be set**
-

✓ 9. Impact of TVR on Cryptogram Generation

- The **TVR is part of the input** to Generate AC (GAC) commands:
 - GAC 1: First cryptogram generation
 - GAC 2: Second cryptogram after online processing
 - TVR is present in the **CDOL (Card Data Object List)** and used in **cryptogram generation logic**
-

✓ 10. What Happens If TVR is Not Handled Properly

- May cause:
 - **Wrong cryptogram type generated**
 - **Security issues** (e.g. approving expired card)
 - **Online fallback when not necessary**
 - EMV Level 2 certification requires **proper TVR handling**
-

! Anything Missing?

Here are a few **advanced additions** I can explain further if you're interested:

- ✓ Mapping of TVR with **TTQ / CTQ bits** (how capabilities influence TVR updates)
- ✓ TVR in **Contactless vs Contact** mode differences
- ✓ **TVR in logs** from EMV terminals (used in troubleshooting)
- ✓ How **Terminal Risk Management logic** interacts with TVR (velocity checks, floor limit, etc.)
- ✓ TVR in **fallback and no-CVM** scenarios

The **Terminal Verification Results (TVR)** is one of the most important components in the EMV (Europay, MasterCard, and Visa) transaction flow. It's a 5-byte (40-bit) data object used by the terminal to track and record the results of **various checks** during the EMV transaction process.

◆ What is TVR?

- **Tag:** 95
 - **Length:** 5 bytes (fixed)
 - **Format:** Binary
 - **Purpose:** The TVR records the outcome of checks performed by the terminal (e.g., card data validity, risk management checks, offline data authentication, etc.).
 - It is part of the **Terminal Action Analysis (TAA)** phase and helps in deciding whether to:
 - Approve the transaction offline,
 - Decline offline,
 - Or go online.
-

◆ When is the TVR updated?

TVR is **updated dynamically during the EMV transaction flow**, particularly during the following phases:

EMV Step	Description	TVR Bits Affected
1. Card Insertion / Contactless Tap	Terminal reads the card data	ICC Data issues (Byte 1), Expiry date, Application not found
2. Read Application Data	Terminal reads AIP, AFL, and other data	Byte 1, 2
3. Offline Data Authentication (ODA)	Terminal verifies data using SDA/DDA/CDA	Byte 2, Byte 3
4. Processing Restrictions	Checks like application version, usage control, etc.	Byte 2

EMV Step	Description	TVR Bits Affected
5. Cardholder Verification (CVM)	PIN entry / signature	Byte 3
6. Risk Management	Checks like floor limit, random transaction selection, velocity checking	Byte 4
7. Terminal Action Analysis	Terminal evaluates the TVR, IACs	All bytes may contribute
8. Online Processing (if needed)	If online authorization is performed	Byte 5
9. Completion	Final decision and script processing	May further update some bits

◆ TVR Byte-Wise Breakdown

Each byte has 8 bits, each representing a specific check result:

■ Byte 1 – ICC Data

Bit Meaning


- 8 Offline data authentication was not performed
- 7 SDA failed
- 6 ICC data missing
- 5 Card appears on terminal exception file
- 4 DDA failed
- 3 CDA failed
- 2 Reserved
- 1 Reserved

✓ Updated during: Offline Data Authentication phase and reading card data.

■ Byte 2 – Application and Expiry

Bit Meaning


- 8 ICC and terminal have different application versions
- 7 Expired application
- 6 Application not yet effective
- 5 Requested service not allowed for card product
- 4 New card
- 3-1 Reserved

 Updated during: Processing Restrictions and Application Selection.

Byte 3 – CVM (Cardholder Verification)

Bit Meaning

- 8 CVM not successful
- 7 Unrecognized CVM
- 6 PIN Try Limit exceeded
- 5 PIN entry required and PIN pad not present/working
- 4 PIN required but not entered
- 3 Online PIN entered
- 2 Reserved
- 1 Reserved

 Updated during: CVM Processing.

Byte 4 – Terminal Risk Management

Bit Meaning

- 8 Transaction exceeds floor limit
- 7 Lower consecutive offline limit exceeded

Bit Meaning

- 6 Upper consecutive offline limit exceeded
- 5 Transaction selected randomly for online processing
- 4 Merchant forced transaction online
- 3-1 Reserved

✅ Updated during: Risk Management and Terminal Action Analysis.

Byte 5 – Issuer/Script/Other

Bit Meaning

- 8 Default TDOL used
- 7 Issuer authentication failed
- 6 Script processing failed before final GENERATE AC
- 5 Script processing failed after final GENERATE AC
- 4-1 Reserved

✅ Updated during: Online Authorization and Script Processing.

◆ Example TVR Values

Let's walk through a few scenarios:

✅ Offline Approval Case (no issues)

plaintext

CopyEdit

TVR: 0000000000

Meaning: All checks passed; no issues.

⚠️ Offline Decline Case

plaintext

CopyEdit

TVR: 4000000000

Bit 7 of Byte 1: SDA failed → critical security failure.

→ Terminal declines transaction offline.

Online Authorization Case

plaintext

CopyEdit

TVR: 0000000010

Bit 5 of Byte 4: Merchant forced online.

→ Terminal sends transaction to issuer.

◆ **Offline vs Online – Impact on TVR**

Flow	TVR Impact
Offline Approval	Must ensure bits in TVR don't match the IAC-Denial mask.
Offline Decline	If critical failures (e.g., SDA failure, expired app), TVR bits set cause terminal to decline.
Online Authorization	Certain bits (like floor limit exceeded, PIN failed, etc.) cause terminal to go online.

TVR is **compared with**:

- **IAC-Denial**
- **IAC-Default**
- **IAC-Online**

Whichever matches based on the set bits, the corresponding path is taken (offline decline / go online / approve).

◆ **Summary**

Key Point	Detail
What	5-byte record of terminal-side checks

Key Point	Detail
Tag	95
Format	Binary
Updated When	Throughout transaction: from card read to final decision
Usage	Compared with IACs to decide next action
Offline	Used heavily to determine approve/decline
Online	Helps decide whether to go online, and holds issuer script failures

If you'd like, I can walk you through a **real sample TVR value**, map it to actual bit meanings, and explain what decision the terminal would take with that TVR.

You said:

yes

ChatGPT said:

Great! Let's walk through a **real-world TVR value** example and deeply analyze each bit to understand what happened during the transaction.

Sample TVR

Let's say the terminal has this TVR after completing pre-online checks:

ini

CopyEdit

TVR = 40 00 08 20 00

Now let's break it down **byte by byte, bit by bit**.

◆ **Byte 1: 40 → 0100 0000**

Bit Value Meaning

8 0 Offline Data Authentication was performed

7 1  **SDA failed**

Bit Value Meaning

6	0	ICC data present
5	0	Card not on exception file
4	0	DDA passed or not used
3	0	CDA passed or not used
2	0	Reserved
1	0	Reserved

✅ **This is critical. SDA failure** is a serious integrity issue. Terminal may decline or go online.

◆ Byte 2: 00 → 0000 0000

No issues found with:

- Expiry date
- Application version
- Service usage
- Application activation date

👍 Nothing to worry about here.

◆ Byte 3: 08 → 0000 1000

Bit Value Meaning

8	0	CVM performed successfully or not required
7	0	CVM recognized
6	0	PIN Try Limit not exceeded
5	1	✅ PIN pad not working or not present but PIN required
4	0	PIN was entered
3	0	No online PIN

Bit Value Meaning

2 0 Reserved

1 0 Reserved

✓ Terminal required PIN entry but PIN pad was unavailable → **serious fallback or bypass.**

◆ Byte 4: 20 → 0010 0000

Bit Value Meaning

8 0 Transaction within floor limit

7 0 Lower consecutive offline limit not exceeded

6 1 ✓ **Upper consecutive offline limit exceeded**

5 0 Not selected randomly for online

4 0 Not forced online by merchant

3-1 0 Reserved

✓ Too many offline approvals — issuer requires online to evaluate card risk behavior.

◆ Byte 5: 00 → 0000 0000

No post-online or script failures.

Final Breakdown Summary

Component Description

Byte 1 SDA failed — high risk

Byte 3 PIN pad not present when PIN was required

Byte 4 Upper offline limit exceeded

Other Bytes OK

💡 What will the terminal do?

This depends on **IACs** (Issuer Action Codes), which define what to do if certain TVR bits are set.

Let's assume:

- **IAC-Denial** includes Bit 7 of Byte 1 (SDA failed)
- **IAC-Online** includes Byte 4 Bit 6 (upper offline limit) or Byte 3 Bit 5 (PIN not entered)

So options:

● **Case A: TVR matches IAC-Denial**

→ Immediate offline decline.

● **Case B: TVR does not match IAC-Denial, but matches IAC-Online**

→ Terminal sends transaction online to issuer.

If issuer accepts → approve; else → decline.

📌 **Conclusion**

This sample:

- Highlights **integrity failure (SDA)**
- Shows **PIN bypass/failure**
- Indicates **risk threshold exceeded**

In most real-world terminals, this combination leads to **going online**, unless the terminal is strictly offline — in which case, it would **decline**.