ICMI LEARNING

EMV application template and application data profile

EMV application template and application data profile

*An application template is a **pre-defined structure**, specifies how the EMV personalization data should be organized for a specific application on the card*

It is a constructed object that is created from base templates, which are pre-defined, generic templates

It can be customized to meet the requirements of the issuer

The application template defines the structure of the personalization data and provides a consistent format for the data to be stored and processed.

EMV application template and application data profile

Application template is represented by ***tag 61***

Tags are numeric identifiers that represent specific data elements stored on the card

Name	Description	Format	Template	Tag	Length
Application template	*Contains one or more data objects relevant to an application directory*	b	70	61	0-252

EMV application template and application data profile

An **application data profile** set of data elements used to define issuer card products such as debit or credit cards

- Application Identifier (AID)
- Application Interchange Profile (AIP)
- Application File Locator (AFL)
- Issuer Action Codes (IAC)
- Card Risk Management Data Object List (CDOL)

EMV application template and application data profile

Application Identifier (AID)	**Tag 61-4F**

This is a unique identifier that identifies the application on the card as per the ISO 7816-5 standard

Application Interchange Profile (AIP)	**Tag 82**

This indicates the card's capabilities to support specific functions in the application

EMV application template and application data profile

Application File Locator (AFL)	Tag 94

AFL indicates the location of the Application Elementary Files (AEFs) on the card.

The AEFs contain the data related to the application

Issuer Action Codes (IAC)	Issuer's conditions for transaction processing

Default	Denial	Online
9F0D	**9F03**	**9F0F**

EMV application template and application data profile

Card Risk Management Data Object List (CDOL)	*It is a list of data objects, along with their tags and lengths*

Passed to the Integrated Circuit Card (ICC) during the first or second Generate Application Cryptogram (AC) command

EMV application template and application data profile

Card Risk Management Data Object List (CDOL)

The card and the payment terminal communicate with each other

They use a messaging standard called ISO 8583 to exchange information

ISO 8583

EMV application template and application data profile

Card Risk Management Data Object List (CDOL)

Card Access data such as

CDOL data

- Transaction amount
- Cardholder account no.
- Expiration date

EMV application template and application data profile

Card Risk Management Data Object List (CDOL)

Types of CDOL data

CDOL 1

First card action analysis

Tag 8C

CDOL 2

Second card action analysis

Tag 8D

EMV application template and application data profile

Card Risk Management Data Object List (CDOL)

The CDOL uses templates to ensure that the required data elements are in the correct format and sequence

The templates define the size and format of each data element

- Transaction amount
- Cardholder account no.
- Expiration date

EMV cardholder data

EMV cardholder data

Various data elements are extracted from the card's chip and magnetic stripe

1. Magstripe track 2 equivalent data
2. Cardholder-related individual data elements
3. Card risk management data
4. The card usage-related data

EMV cardholder data

Magstripe track 2 equivalent data

Primary account number (PAN)	*Can be up to 19 digits in length*
The field separator	
The expiration date	*In YYMM format*
the service code	
discretionary data	*Defined by individual payment systems*

EMV cardholder data

Cardholder-related individual data elements

Primary account number (PAN)	*Uniquely identifies the cardholder's A/c*
PAN Sequence Number (PSN)	*Indicates the order in which multiple cards are issued for a single account*
The expiration date	*Indicates the validity period of the card*
The card service code	*Services available for the card*
PIN-related data	*If offline PIN verification is supported*

EMV cardholder data

Card risk management data

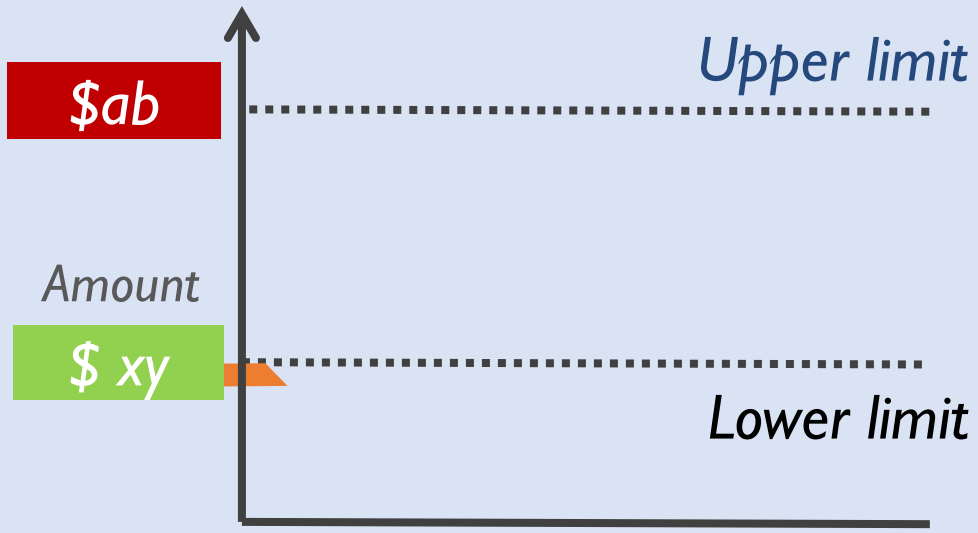
Lower/upper consecutive offline limit (Tag 9F14/Tag 9F23)

The maximum number of consecutive transactions that can be completed without online authorization	The maximum value of cumulative offline transactions that can be completed before requiring online authorization

EMV cardholder data

3 Card risk management data

Lower/upper consecutive offline limit (Tag 9F14/Tag 9F23)



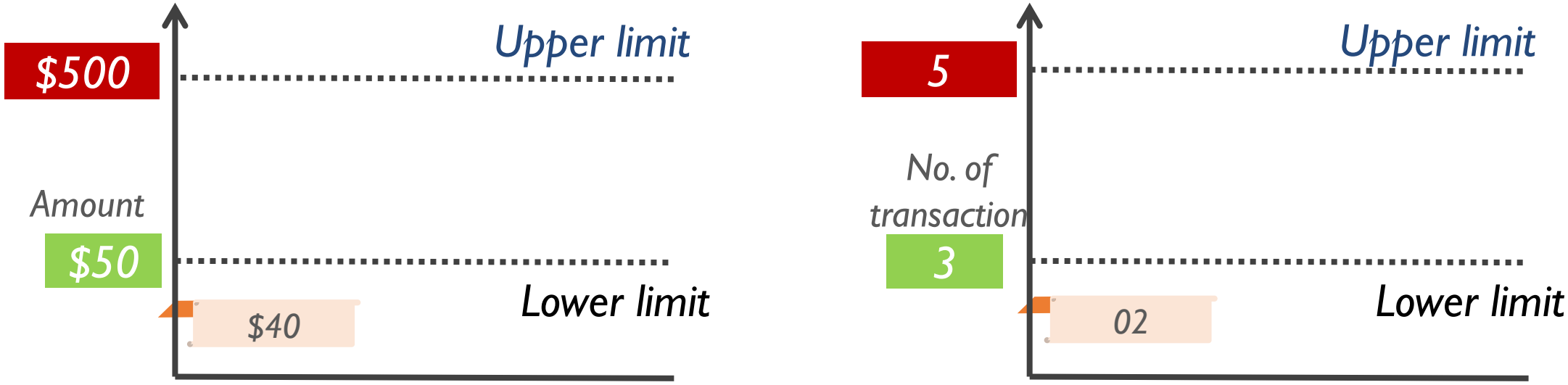
Lower and upper limit

Control & Limit the amount and number of transaction performed by the card offline

EMV cardholder data

3 Card risk management data

Lower/upper consecutive offline limit (Tag 9F14/Tag 9F23)

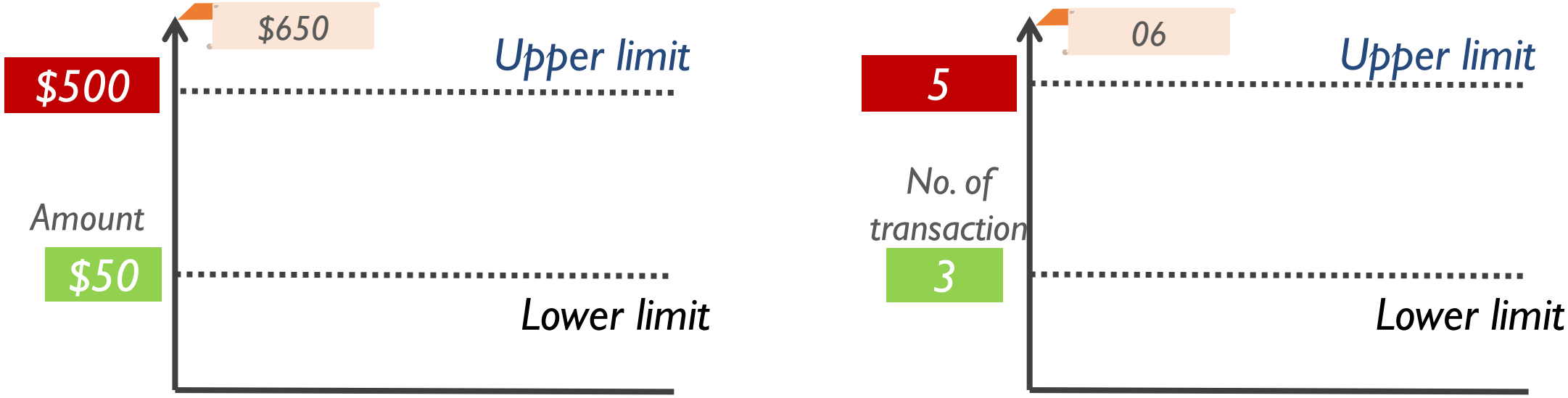


Any transaction below $50 or before making 3 transactions can be authorized ***OFFLINE*** *without connecting to the issuer*

EMV cardholder data

3 Card risk management data

Lower/upper consecutive offline limit (Tag 9F14/Tag 9F23)

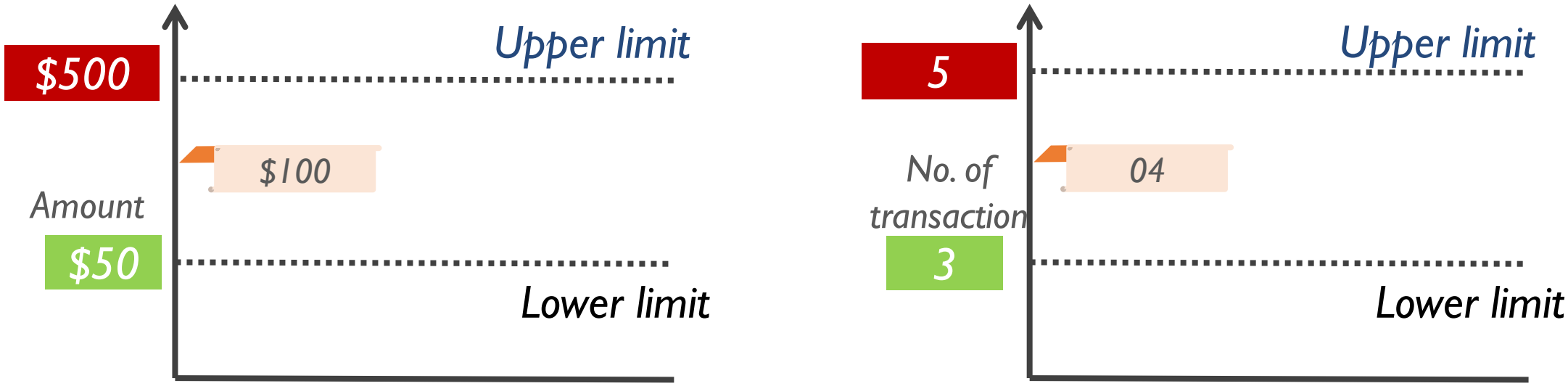


*Any transaction above **$500** or after making 5 transactions will require the card to connect to the issuer for authorization*

EMV cardholder data

3 Card risk management data

Lower/upper consecutive offline limit (Tag 9F14/Tag 9F23)

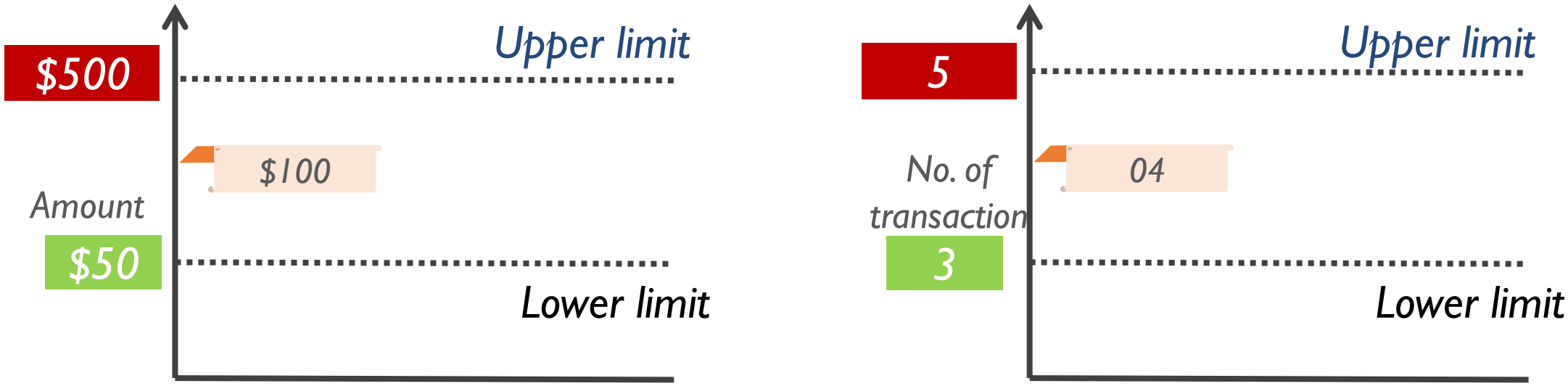


Transaction between lower and upper limit must be authenticated by the issuer on the terminals, which are able to go online, or must be approved offline

EMV cardholder data

3 Card risk management data

Lower/upper consecutive offline limit (Tag 9F14/Tag 9F23)



Limits are set by issuer and adjust based on cardholder usage pattern , risk profile, other factors

EMV cardholder data

4 Card usage-related data

Data includes the application usage control (tag 9F07)

Data includes information about

How the card can be used

Types of transactions are allowed

Types of conditions

Include restrictions on spent per transaction, per day, or per month

EMV cardholder data

4 Card usage-related data

Data includes the application usage control (tag 9F07)

Data is usually stored on the card's chip and can be read by the terminal during a transaction

EMV cardholder data

Some examples of card usage-related data include

Application Usage Control (AUC)

Transactions allowed (such as purchases, cash withdrawals, or balance inquiries)

Terminal Action Code (TAC)

Terminal respond if certain condition are met (such as if the transaction amount exceeds a certain limit)

Other types of data

- *Limits on the number of transactions*
- *Geographical restrictions*