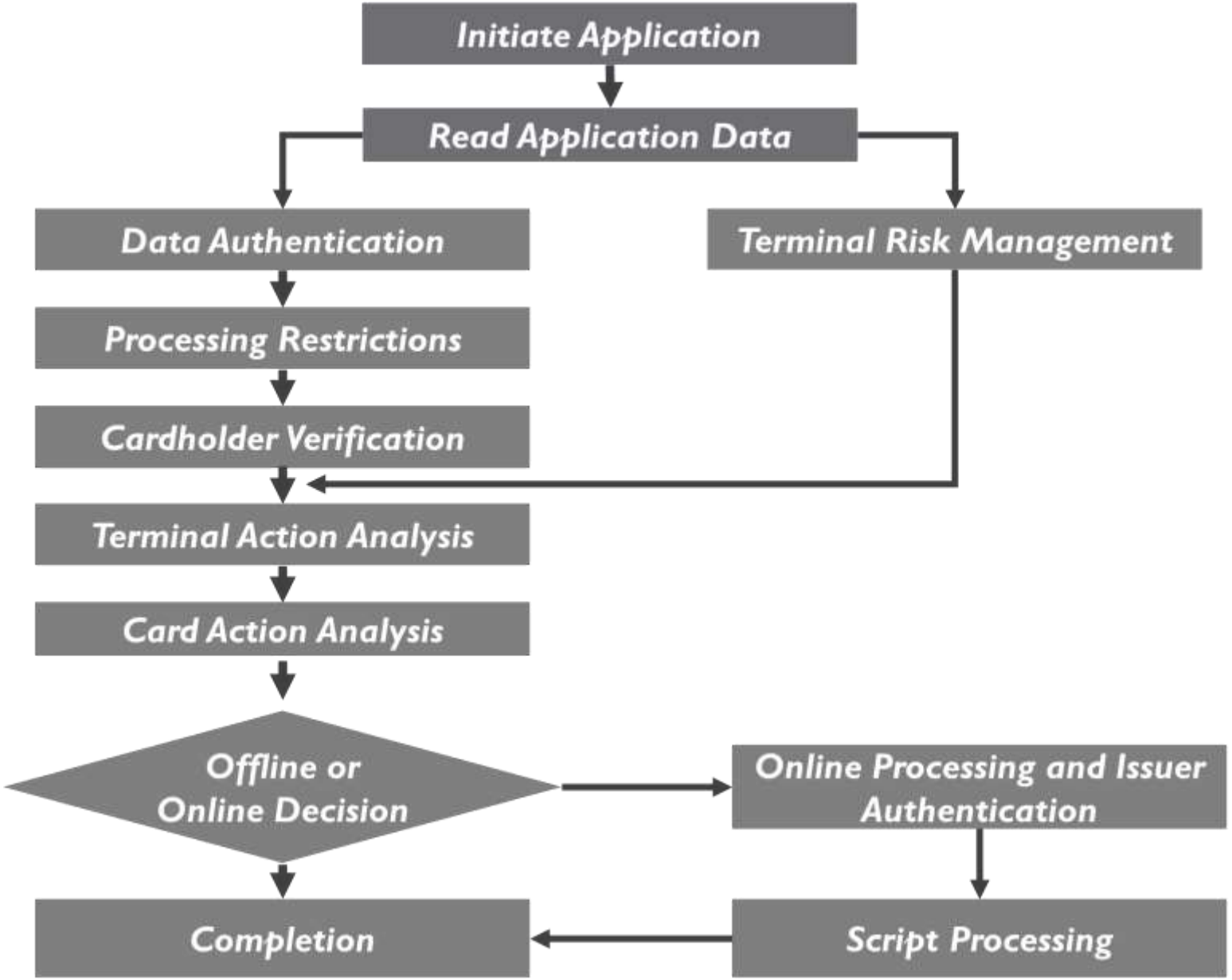
ICMI LEARNING

EMV Transaction Processing: The Flowchart

EMV Transaction Processing: The Flowchart



EMV Transaction Processing: The Flowchart

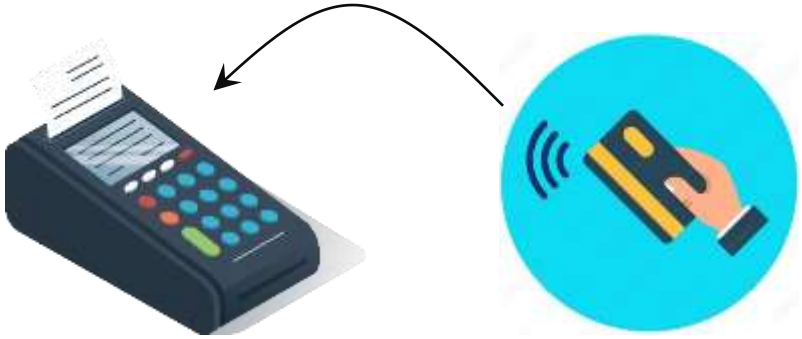
1 Initiate Application

Terminal sends signal to the card, requesting that it initiate the application process

2 Read Application Data

- Application Identifier (AID)
- Cardholder account number (PAN)

Card send data to terminal



EMV Transaction Processing: The Flowchart

3 Data Authentication

To ensure that the card is genuine and that the transaction can proceed

- Static data authentication (SDA)
- Dynamic data authentication (DDA)
- Combined dynamic data authentication (CDA)

3 Terminal Risk Management

Terminal risk management techniques to assess the level of risk involved in the transaction

EMV Transaction Processing: The Flowchart

4 Processing Restrictions

Terminal checks for any processing restrictions

- Transaction amount limits
- Rules set by the card issuer

5 Cardholder Verification

Verifying that the person using the card is a legitimate cardholder

PIN or biometric

Signature

EMV Transaction Processing: The Flowchart

6 Terminal Action Analysis

To determine the next steps in the transaction process

- The results of the data authentication,
- Processing restrictions,
- Cardholder verification

7 Card Action Analysis

Action analysis performed on the data received for the terminal

Determines the actions

Generating an application cryptogram (AC) for the transaction

EMV Transaction Processing: The Flowchart

8 Offline or Online Decision

If the terminal and card are able to complete the transaction offline, then the transaction is completed

If an online transaction is required, the terminal proceeds to the next step.

9 Online Processing and Issuer Authentication

The terminal sends the transaction data to the card issuer's system for further processing

The issuer verifies the transaction and sends an authorization response back to the terminal.

EMV Transaction Processing: The Flowchart

10 Script Processing

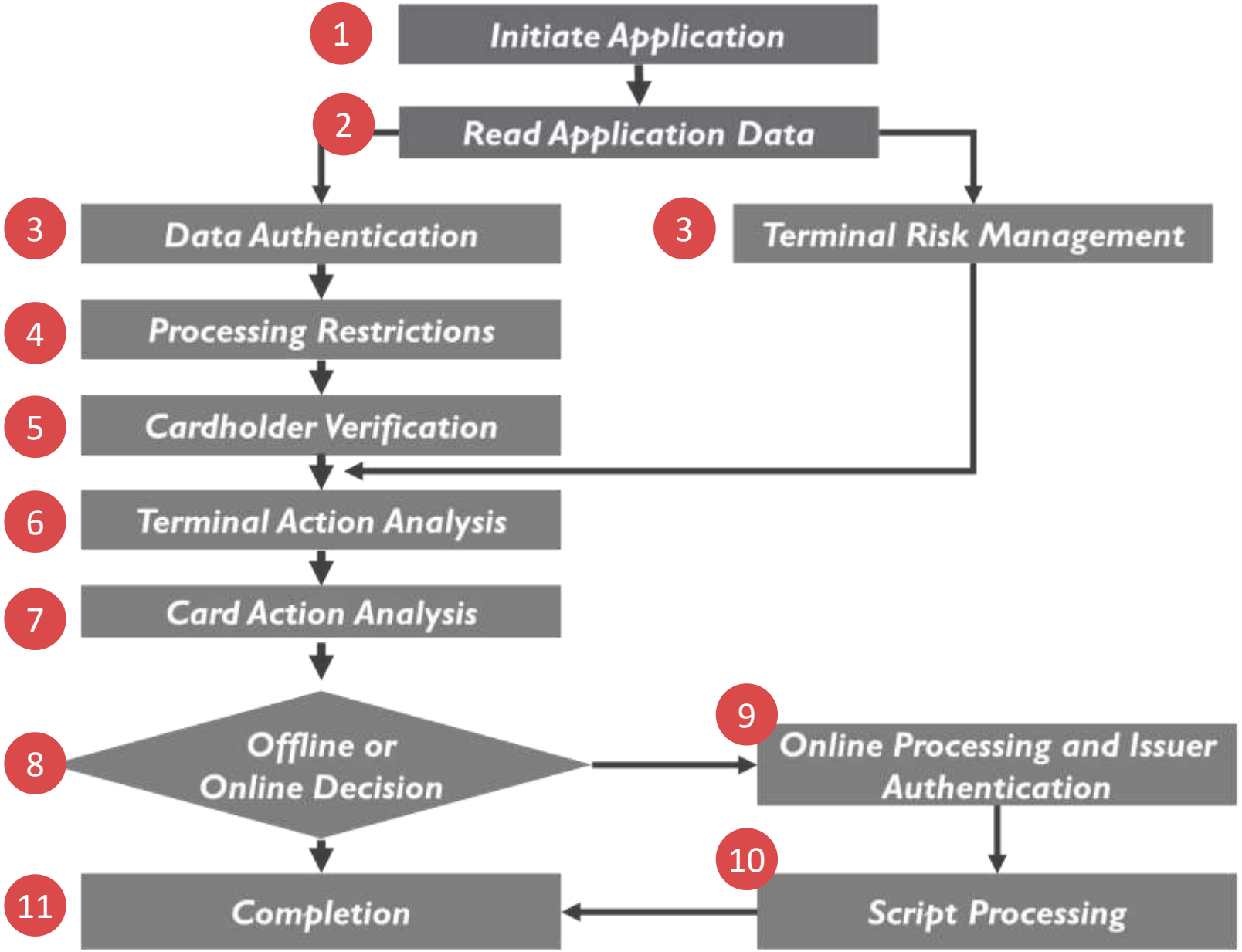
The terminal may receive a script from the issuer to be processed by the card

This script may contain instructions for updating the card's application data or performing other actions

11 Completion

The cardholder receives a receipt or confirmation of the transaction, and the funds are transferred between the cardholder's account and the merchant's account

EMV Transaction Processing: The Flowchart

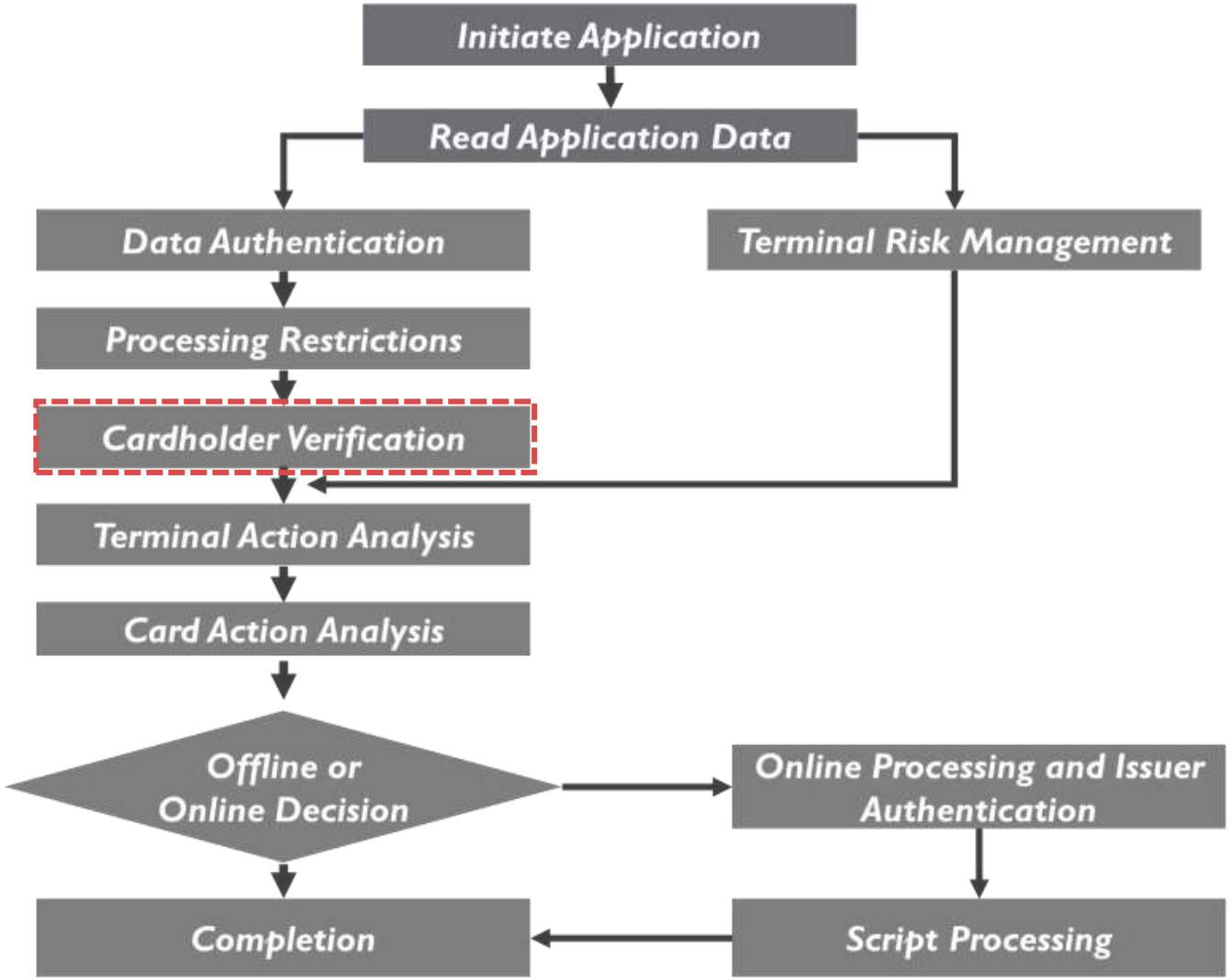


Cardholder Verification in EMV Transactions

ICMI LEARNING

Cardholder Verification in EMV Transactions

To ensure that the person presenting the card is a legitimate cardholder



Cardholder Verification in EMV Transactions

The cardholder verification method (CVM) list, which is read from the card, is used by the terminal to determine the type of verification

CVM list consists of a priority order of verification methods

The list is established based on the capabilities of the POS terminal and the card issuer

Cardholder Verification in EMV Transactions

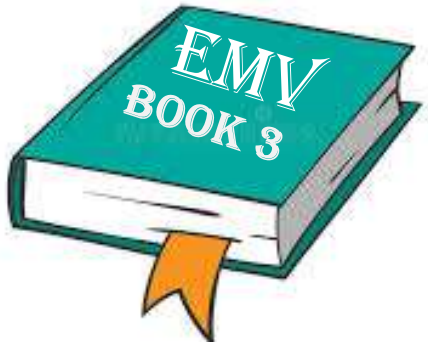
Different terminals support different CVMs

Availability of certain methods may vary based on the terminal type and location

Cardholder Verification in EMV Transactions

CVM methods includes

- Signature verification
- Offline PIN verification
- Online PIN verification
- Biometric authentication



The terminal will select the highest-priority method that it supports from the CVM list and prompt the cardholder to provide the necessary information

Cardholder Verification in EMV Transactions

CVM list is encoded in the card, contains thresholds and information about how to apply CVM

For each CVM, list includes two elements, or two bytes

CVM code	CVM condition code
Define CVM type to performed	Defines conditions when the CVM method is applicable
Next step when the CVM fails	Example, always enforce online PIN for ATM withdrawals

CVM code

ICMI LEARNING

CVM code

Possible values for the card verification method (CVM) codes in an EMV transaction

No CVM is required	011111b
No verification is required for the transaction	

Fail CVM processing	000000b
CVM processing failed & transaction cannot be completed	

CV Rule Byte 1 (Leftmost): Cardholder Verification Method (CVM) Codes

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0								RFU
	0							Fail cardholder verification if this CVM is unsuccessful
	1							Apply succeeding CV Rule if this CVM is unsuccessful
		0	0	0	0	0	0	Fail CVM processing
		0	0	0	0	0	1	Plaintext PIN verification performed by ICC
		0	0	0	0	1	0	Enciphered PIN verified online
		0	0	0	0	1	1	Plaintext PIN verification performed by ICC and signature (paper)
		0	0	0	1	0	0	Enciphered PIN verification performed by ICC
		0	0	0	1	0	1	Enciphered PIN verification performed by ICC and signature (paper)
		0	x	x	x	x	x	Values in the range 000110-011101 reserved for future use by this specification
		0	1	1	1	1	0	Signature (paper)
		0	1	1	1	1	1	No CVM required
		1	0	x	x	x	x	Values in the range 100000-101111 reserved for use by the individual payment systems
		1	1	x	x	x	x	Values in the range 110000-111110 reserved for use by the issuer
		1	1	1	1	1	1	This value is not available for use

CVM code

Possible values for the card verification method (CVM) codes in an EMV transaction

Signature-Paper	011110b

The cardholder provides a signature on a paper receipt

Enciphered PIN verified online	000010b

Cardholder enters an encrypted PIN on the terminal, and verified online by the issuer

CV Rule Byte 1 (Leftmost): Cardholder Verification Method (CVM) Codes

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0								RFU
	0							Fail cardholder verification if this CVM is unsuccessful
	1							Apply succeeding CV Rule if this CVM is unsuccessful
		0	0	0	0	0	0	Fail CVM processing
		0	0	0	0	0	1	Plaintext PIN verification performed by ICC
		0	0	0	0	1	0	Enciphered PIN verified online
		0	0	0	0	1	1	Plaintext PIN verification performed by ICC and signature (paper)
		0	0	0	1	0	0	Enciphered PIN verification performed by ICC
		0	0	0	1	0	1	Enciphered PIN verification performed by ICC and signature (paper)
		0	x	x	x	x	x	Values in the range 000110-011101 reserved for future use by this specification
		0	1	1	1	1	0	Signature (paper)
		0	1	1	1	1	1	No CVM required
		1	0	x	x	x	x	Values in the range 100000-101111 reserved for use by the individual payment systems
		1	1	x	x	x	x	Values in the range 110000-111110 reserved for use by the issuer
		1	1	1	1	1	1	This value is not available for use

CVM code

Possible values for the card verification method (CVM) codes in an EMV transaction

Plaintext PIN verification performed by ICC	000001b

The cardholder enters a PIN on the card's chip, which is then verified by the chip itself

Plaintext PIN AND Signature-Paper	000011b

The cardholder provides a signature on a paper receipt also enters a plaintext PIN

CV Rule Byte 1 (Leftmost): Cardholder Verification Method (CVM) Codes

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0								RFU
	0							Fail cardholder verification if this CVM is unsuccessful
	1							Apply succeeding CV Rule if this CVM is unsuccessful
		0	0	0	0	0	0	Fail CVM processing
		0	0	0	0	0	1	Plaintext PIN verification performed by ICC
		0	0	0	0	1	0	Enciphered PIN verified online
		0	0	0	0	1	1	Plaintext PIN verification performed by ICC and signature (paper)
		0	0	0	1	0	0	Enciphered PIN verification performed by ICC
		0	0	0	1	0	1	Enciphered PIN verification performed by ICC and signature (paper)
		0	x	x	x	x	x	Values in the range 000110-011101 reserved for future use by this specification
		0	1	1	1	1	0	Signature (paper)
		0	1	1	1	1	1	No CVM required
		1	0	x	x	x	x	Values in the range 100000-101111 reserved for use by the individual payment systems
		1	1	x	x	x	x	Values in the range 110000-111110 reserved for use by the issuer
		1	1	1	1	1	1	This value is not available for use

CVM code

Possible values for the card verification method (CVM) codes in an EMV transaction

Enciphered PIN by ICC	000100b

Cardholder enters an encrypted PIN on the card's chip, and verified offline by the chip

Enciphered PIN by ICC AND Signature-Paper	000101b

Cardholder provides a signature on a paper receipt, as we as enters an encrypted PIN

CV Rule Byte 1 (Leftmost): Cardholder Verification Method (CVM) Codes

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0								RFU
	0							Fail cardholder verification if this CVM is unsuccessful
	1							Apply succeeding CV Rule if this CVM is unsuccessful
		0	0	0	0	0	0	Fail CVM processing
		0	0	0	0	0	1	Plaintext PIN verification performed by ICC
		0	0	0	0	1	0	Enciphered PIN verified online
		0	0	0	0	1	1	Plaintext PIN verification performed by ICC and signature (paper)
		0	0	0	1	0	0	Enciphered PIN verification performed by ICC
		0	0	0	1	0	1	Enciphered PIN verification performed by ICC and signature (paper)
		0	x	x	x	x	x	Values in the range 000110-011101 reserved for future use by this specification
		0	1	1	1	1	0	Signature (paper)
		0	1	1	1	1	1	No CVM required
		1	0	x	x	x	x	Values in the range 100000-101111 reserved for use by the individual payment systems
		1	1	x	x	x	x	Values in the range 110000-111110 reserved for use by the issuer
		1	1	1	1	1	1	This value is not available for use

CVM condition code

ICMI LEARNING

CVM condition code

Second element, or byte, referred to as the CVM condition code

Specifies the condition that must be met in order to apply the CVM method

Breakdown of each CVM condition code

Value	Meaning
'00'	Always
'01'	If unattended cash
'02'	If not unattended cash and not manual cash and not purchase with cashback
'03'	If terminal supports the CVM
'04'	If manual cash
'05'	If purchase with cashback
'06'	If transaction is in the application currency and is under X value
'07'	If transaction is in the application currency and is over X value
'08'	If transaciton is in the application currency and is under Y value
'09'	If transaciton is in the application currency and is over Y value
'0A'-'7F'	RFU
'80'-'FF'	Reserved for use by individual payment systems

X is referred to the amount field
Y is referred to the second amount field

CVM condition code

Code 00 Always be applied, regardless of the transaction type or amount

Code 01 CVM is applied only for transactions that involve cash or cash back

Code 02 CVM is applied only for transactions that do not involve cash or cashback

Value	Meaning
'00'	Always
'01'	If unattended cash
'02'	If not unattended cash and not manual cash and not purchase with cashback
'03'	If terminal supports the CVM
'04'	If manual cash
'05'	If purchase with cashback
'06'	If transaction is in the application currency and is under X value
'07'	If transaction is in the application currency and is over X value
'08'	If transaciton is in the application currency and is under Y value
'09'	If transaciton is in the application currency and is over Y value
'0A'-'7F'	RFU
'80'-'FF'	Reserved for use by individual payment systems

X is referred to the amount field
Y is referred to the second amount field

CVM condition code

Code 03 CVM is applied only if the terminal is adequately equipped to support the CVM method

Code 06 to 09 CVM is applied only when the transaction currency code (tag 5F2A in the terminal) of the authorized amount is the same as the application currency code (tag 9F42 in the ICC)

Value	Meaning
'00'	Always
'01'	If unattended cash
'02'	If not unattended cash and not manual cash and not purchase with cashback
'03'	If terminal supports the CVM
'04'	If manual cash
'05'	If purchase with cashback
'06'	If transaction is in the application currency and is under X value
'07'	If transaction is in the application currency and is over X value
'08'	If transaciton is in the application currency and is under Y value
'09'	If transaciton is in the application currency and is over Y value
'0A'-'7F'	RFU
'80'-'FF'	Reserved for use by individual payment systems

X is referred to the amount field
Y is referred to the second amount field

CVM condition code

CVM condition codes provide additional information to the terminal about **when** and **how** to apply the CVM methods listed in the first byte of the CVM list

Both the CVM codes and condition codes are defined during the personalization process of the card

Test Your Knowledge!

What is the purpose of the Cardholder Verification Method (CVM) list in EMV transactions?

1. Is it used to track the cardholder's transaction history
2. To determine the method of cardholder verification to be used

PIN Verification and Retry Counter in EMV Transactions

ICMI LEARNING

PIN Verification and Retry Counter in EMV Transactions

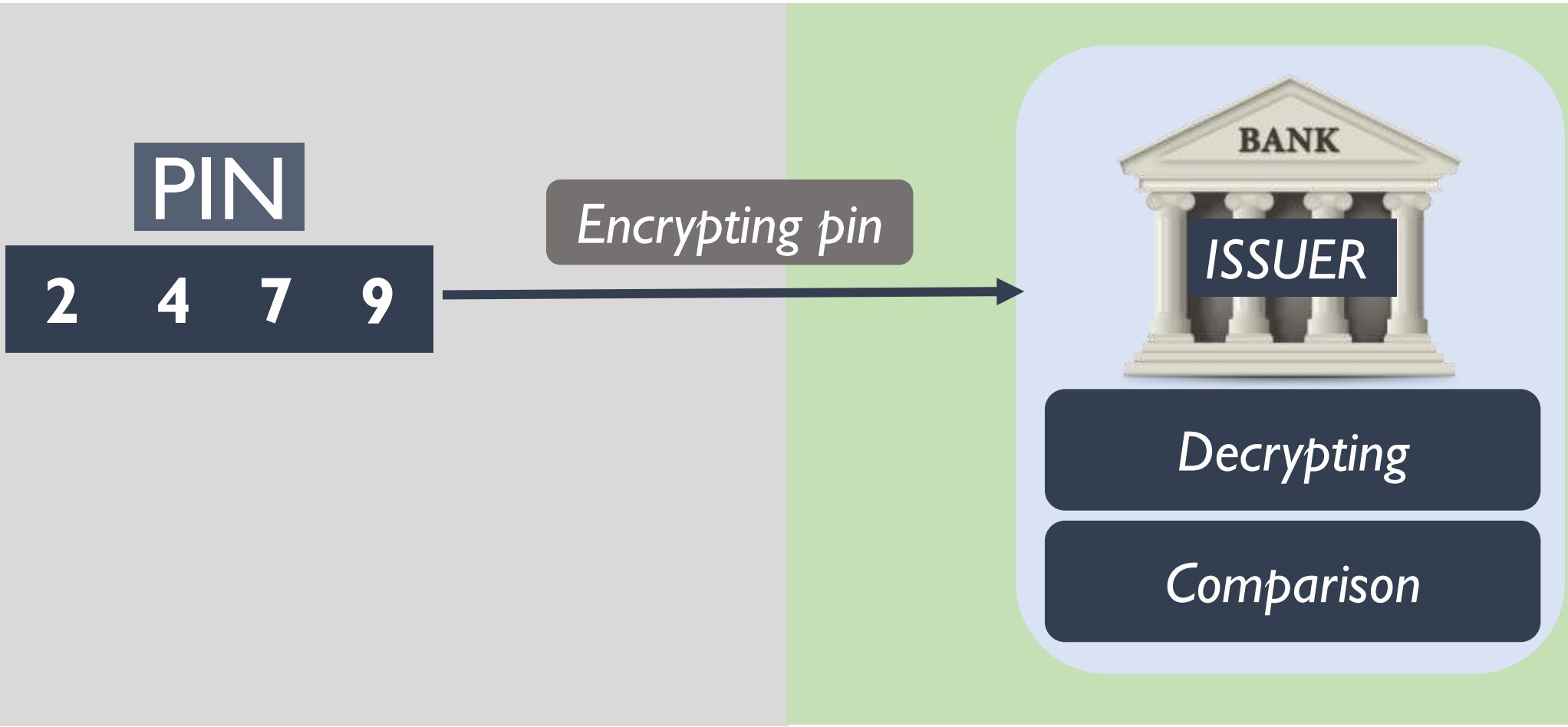
Card Verification Method list is used to determine the appropriate method for verifying the cardholder's identity

011111b	000000b	011110b	000010b
000001b	000011b	000100b	000101b

When a PIN is used for verification in an EMV transaction, it can be verified either online or offline

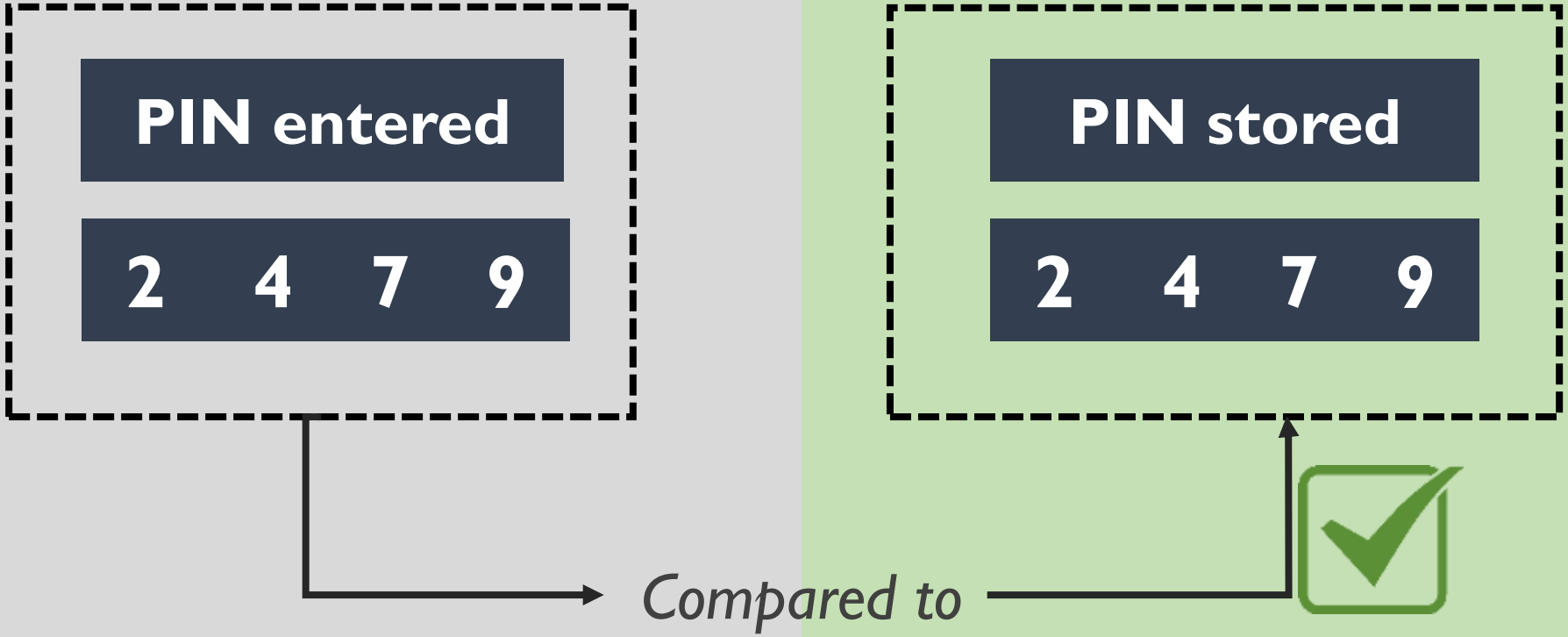
PIN Verification and Retry Counter in EMV Transactions

Online PIN verification



PIN Verification and Retry Counter in EMV Transactions

Offline PIN verification



PIN Verification and Retry Counter in EMV Transactions

Enciphered PIN verification provides additional layer of security

PIN entered

2 4 7 9

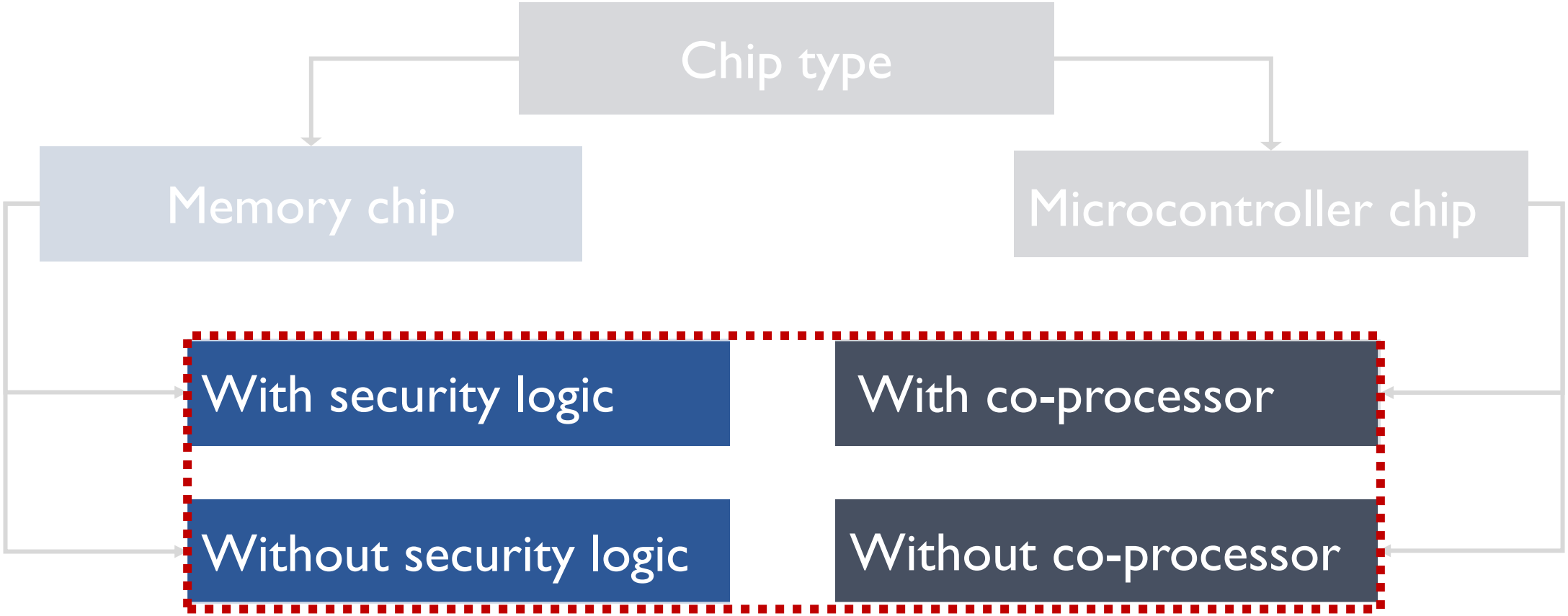
Enciphered PIN

Encrypted PIN

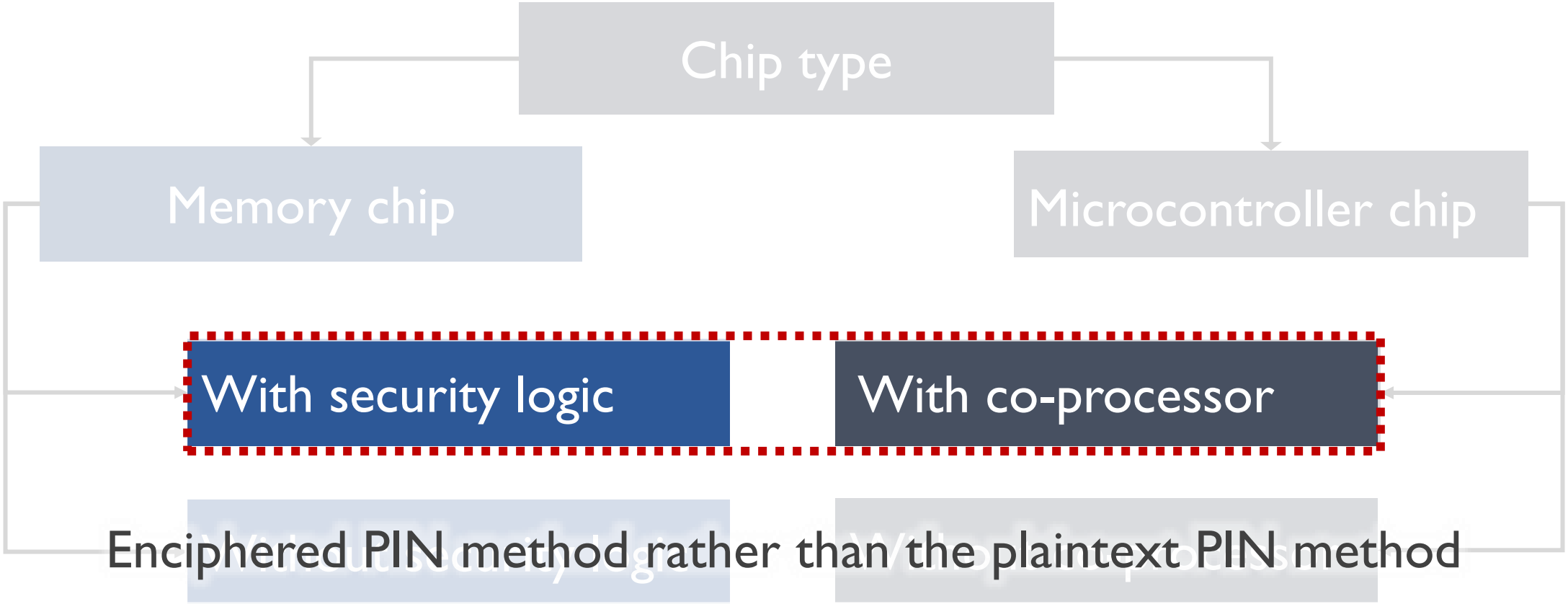
D % q 3

Difficult to intercept or steal the PIN

PIN Verification and Retry Counter in EMV Transactions



PIN Verification and Retry Counter in EMV Transactions



Enciphered PIN method rather than the plaintext PIN method

Pre-requisites for CVM

ICMI LEARNING

Pre-requisites for CVM

The prerequisites for cardholder verification methods

There are several types of CVM, and each requires certain prerequisites to be met

Let's take a look at the prerequisites for each type

Pre-requisites for CVM

Signature verification	
Card	Must retain signature
Terminal	
Acquirer host system	
Issuer host system	
Transaction time	Signature collection and checking time

Pre-requisites for CVM

Offline plaintext PIN verification	
Card	
Terminal	Must support a PIN pad
Acquirer host system	
Issuer host system	Must personalize the card with a PIN
Transaction time	PIN entry time

Pre-requisites for CVM

Offline enciphered PIN verification	
Card	Must support RSA
Terminal	Must support PIN pad & RSA
Acquirer host system	
Issuer host system	Must personalize the card with a PIN and ICC key
Transaction time	PIN entry and RSA time

Pre-requisites for CVM

Online PIN verification	
Card	
Terminal	Must support a PIN pad and be online
Acquirer host system	Must support the secure transport of an online pin to the authorization system
Issuer host system	Must support online pin verification as part of the authorization
Transaction time	PIN entry and online authorization time

Consumer Device Cardholder Verification Method (CDCVM)

ICMI LEARNING

Consumer Device Cardholder Verification Method (CDCVM)

Traditional cardholder verification methods, performed by entering pin at payment terminal

Increasing use of mobile devices for payment transactions consumer authentication can be performed on consumer's device

Consumer Device Cardholder Verification Method (CDCVM)

Passcodes

Patterns

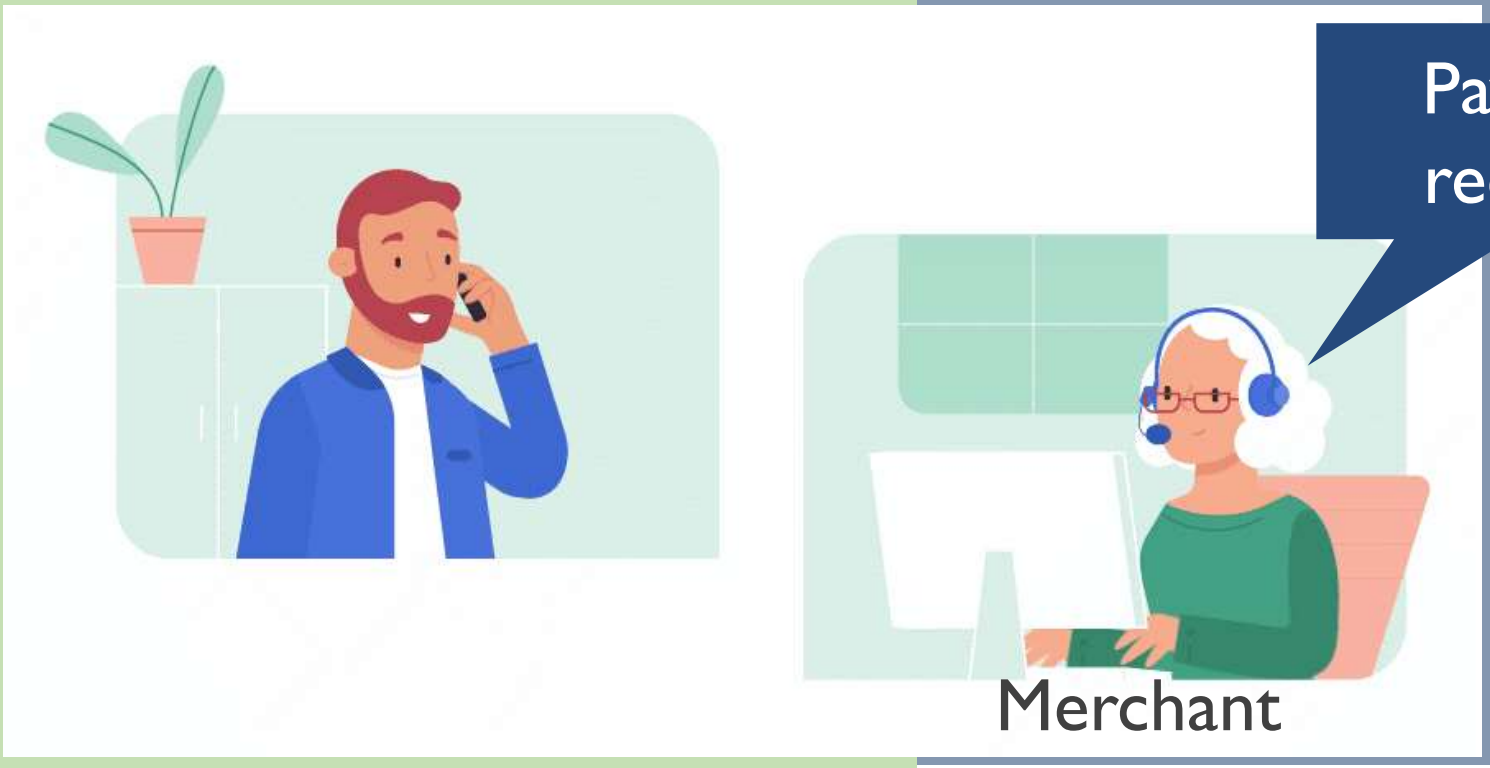
fingerprint

Iris

Facial recognition

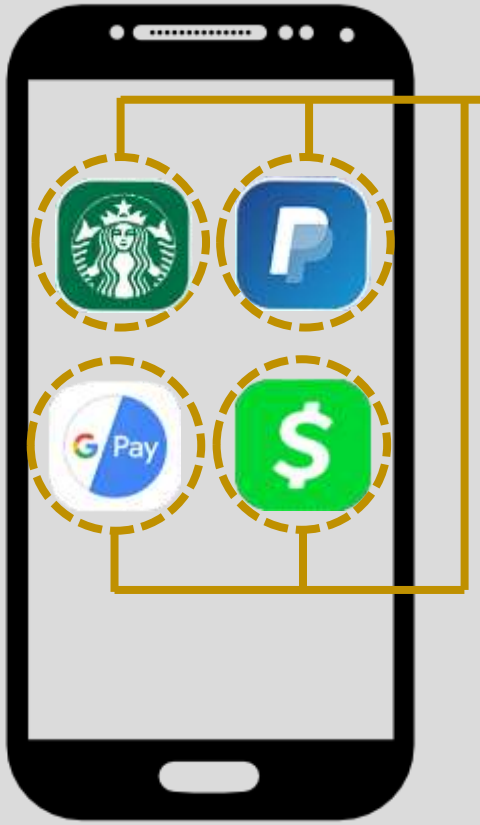
This type of authentication on a consumer's own device is called the Consumer Device Cardholder Verification Method **(CDCVM)**

Consumer Device Cardholder Verification Method (CDCVM)



CDCVM, payment application is able to authenticate the cardholder without relying on the merchant's system, so provides an added layer of security

Consumer Device Cardholder Verification Method (CDCVM)



Multiple payment applications on consumer's device share same CDCVM and associated result

Shared CDCVM

Seamless	Convenient

Consumer only needs to authenticate themselves once for all payment applications that support shared CDCVM