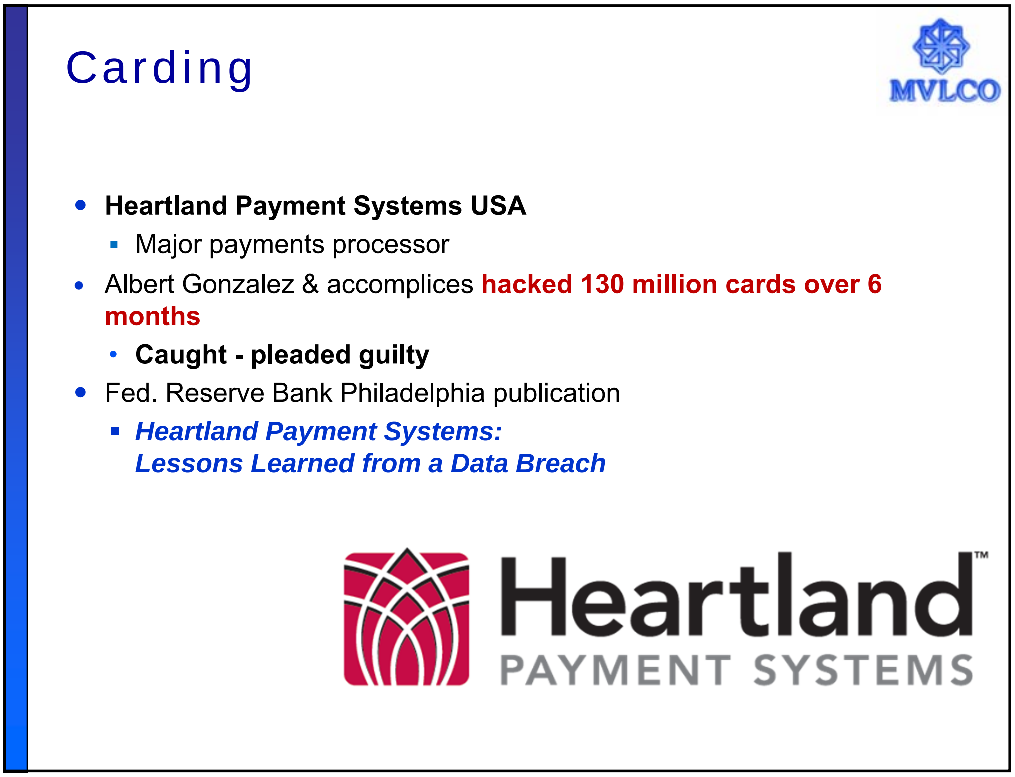
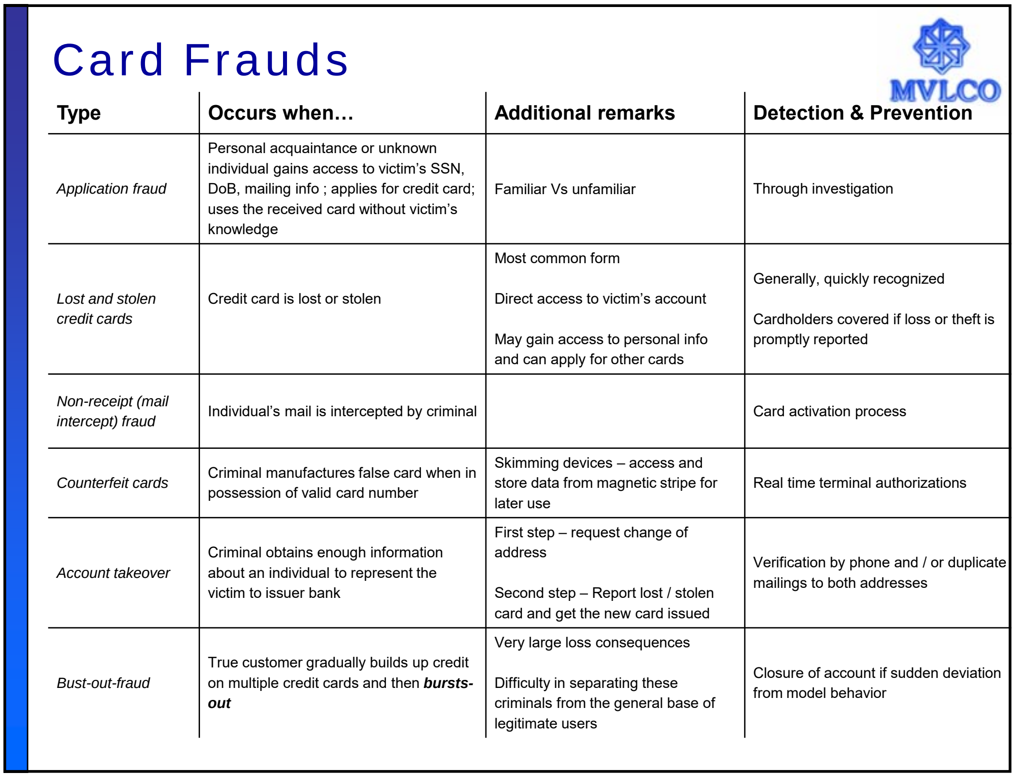


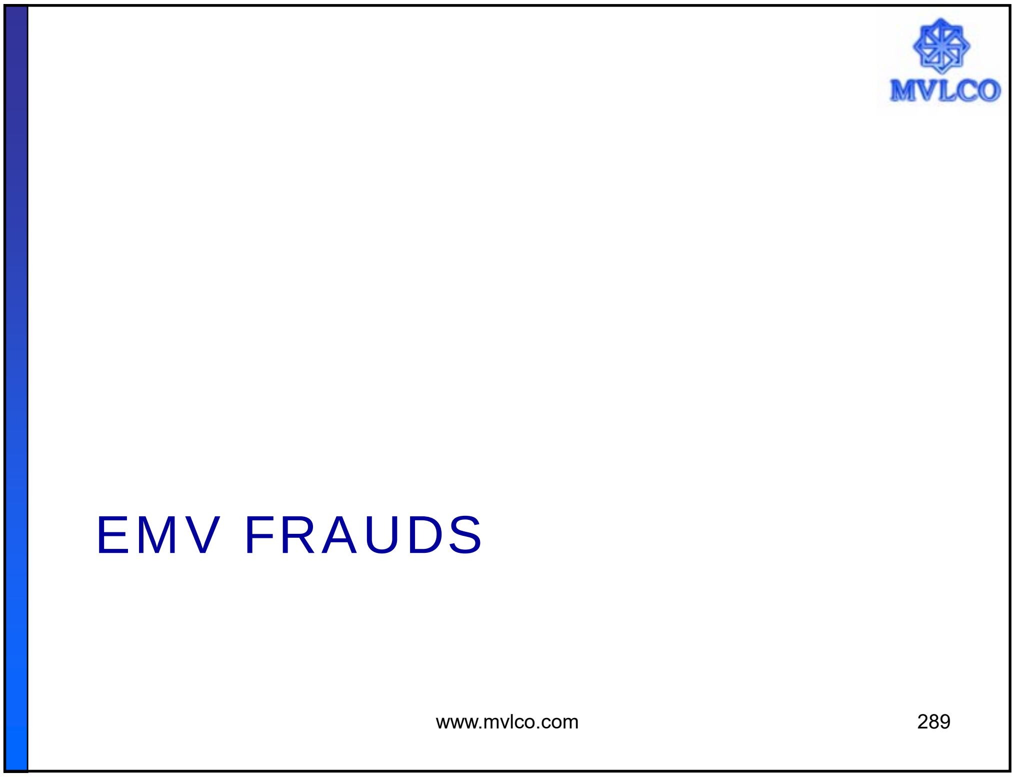
Carding

- **Heartland Payment Systems USA**
  - Major payments processor
- Albert Gonzalez & accomplices **hacked 130 million cards over 6 months**
  - **Caught - pleaded guilty**
- Fed. Reserve Bank Philadelphia publication
  - ***Heartland Payment Systems: Lessons Learned from a Data Breach***



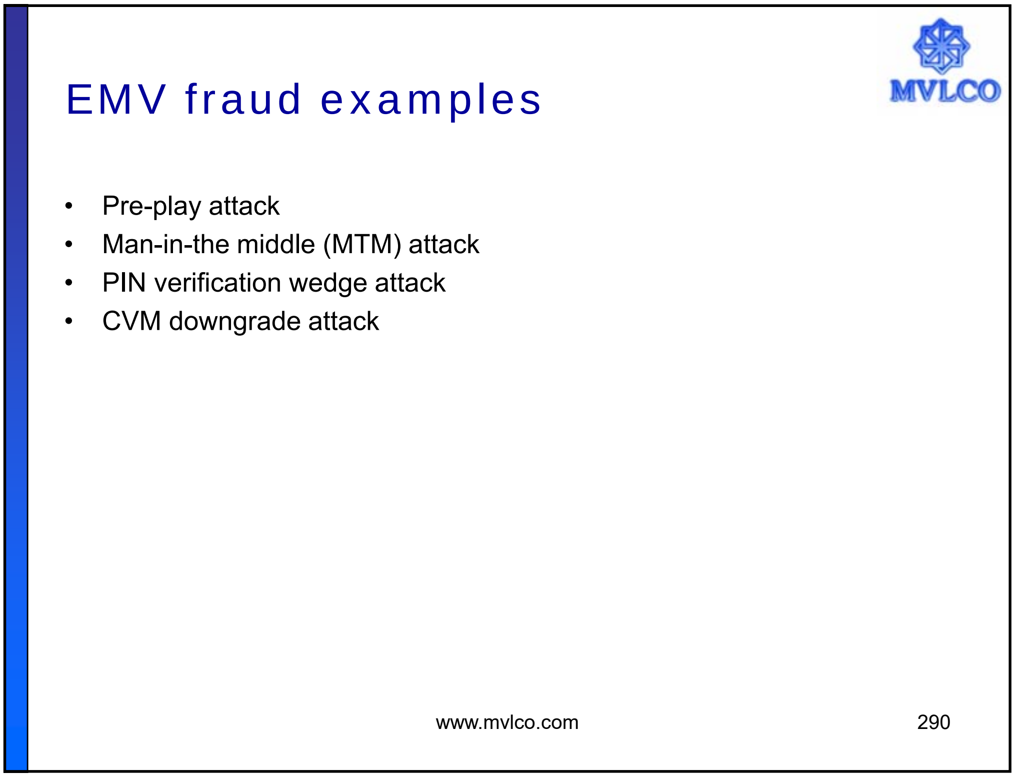
Card Frauds

Type	Occurs when…	Additional remarks	Detection & Prevention
Application fraud	Personal acquaintance or unknown individual gains access to victim's SSN, DoB, mailing info ; applies for credit card; uses the received card without victim's knowledge	Familiar Vs unfamiliar	Through investigation
Lost and stolen credit cards	Credit card is lost or stolen	Most common form Direct access to victim's account May gain access to personal info and can apply for other cards	Generally, quickly recognized Cardholders covered if loss or theft is promptly reported
Non-receipt (mail intercept) fraud	Individual's mail is intercepted by criminal		Card activation process
Counterfeit cards	Criminal manufactures false card when in possession of valid card number	Skimming devices – access and store data from magnetic stripe for later use	Real time terminal authorizations
Account takeover	Criminal obtains enough information about an individual to represent the victim to issuer bank	First step – request change of address Second step – Report lost / stolen card and get the new card issued	Verification by phone and / or duplicate mailings to both addresses
Bust-out-fraud	True customer gradually builds up credit on multiple credit cards and then ***bursts-out***	Very large loss consequences Difficulty in separating these criminals from the general base of legitimate users	Closure of account if sudden deviation from model behavior



EMV FRAUDS

www.mvlco.com 289

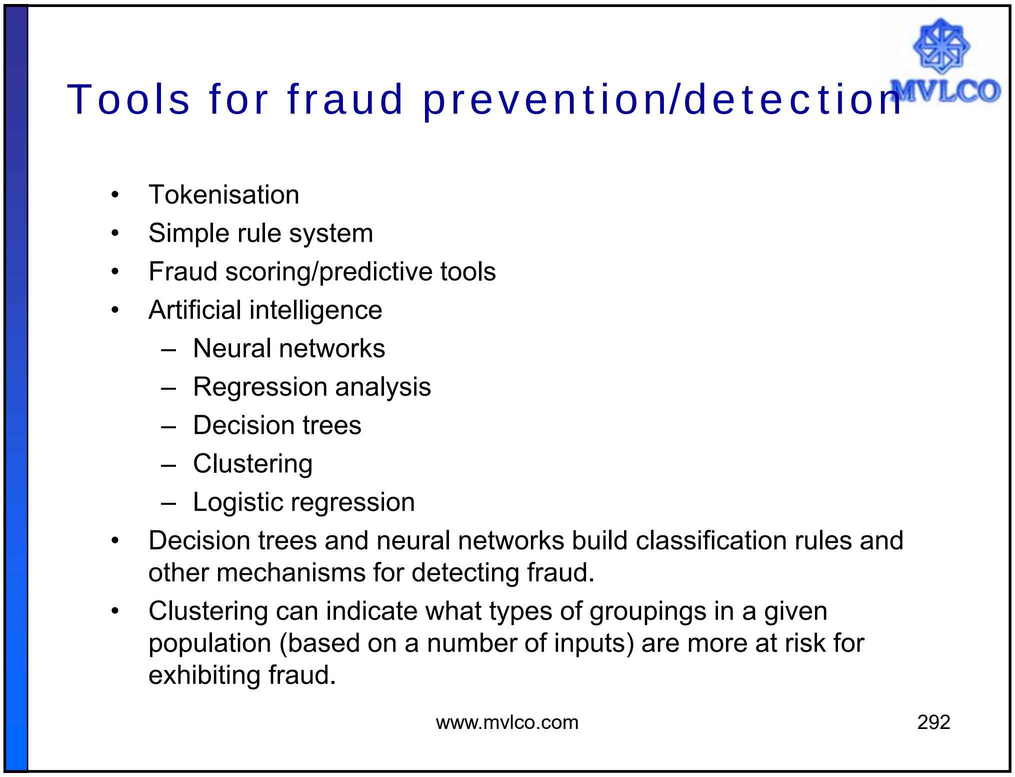


EMV fraud examples

- Pre-play attack
- Man-in-the middle (MTM) attack
- PIN verification wedge attack
- CVM downgrade attack

www.mvlco.com 290

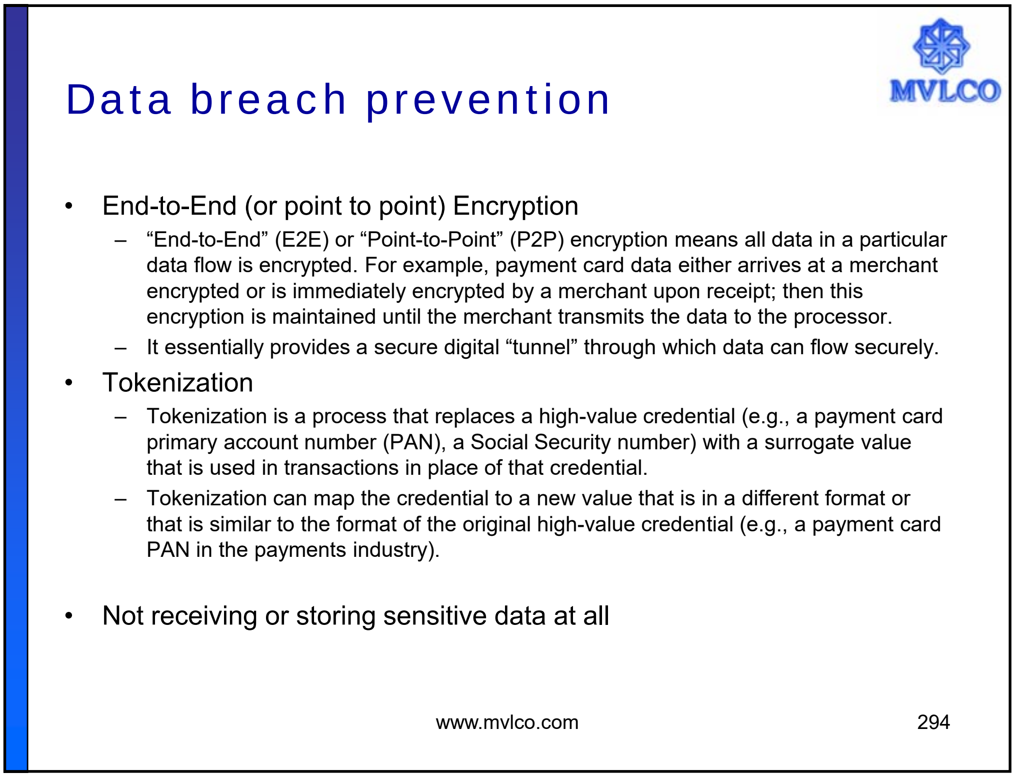
FRAUD PREVENTION



Tools for fraud prevention/detection

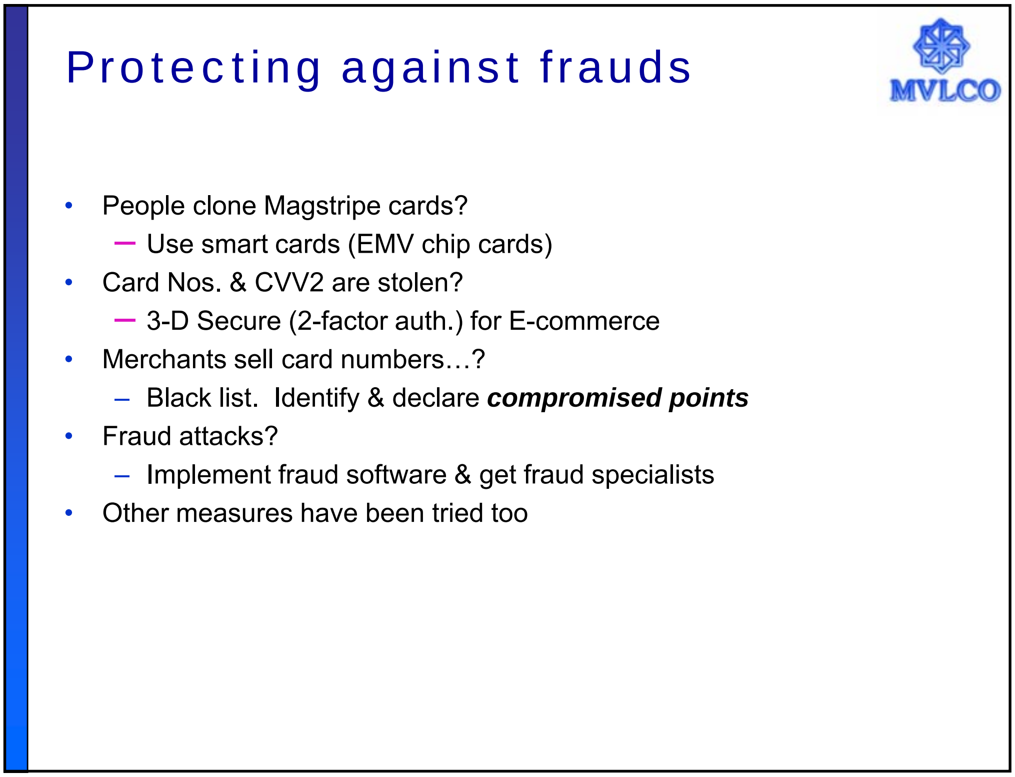
- Tokenisation
- Simple rule system
- Fraud scoring/predictive tools
- Artificial intelligence
  - Neural networks
  - Regression analysis
  - Decision trees
  - Clustering
  - Logistic regression
- Decision trees and neural networks build classification rules and other mechanisms for detecting fraud.
- Clustering can indicate what types of groupings in a given population (based on a number of inputs) are more at risk for exhibiting fraud.

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD



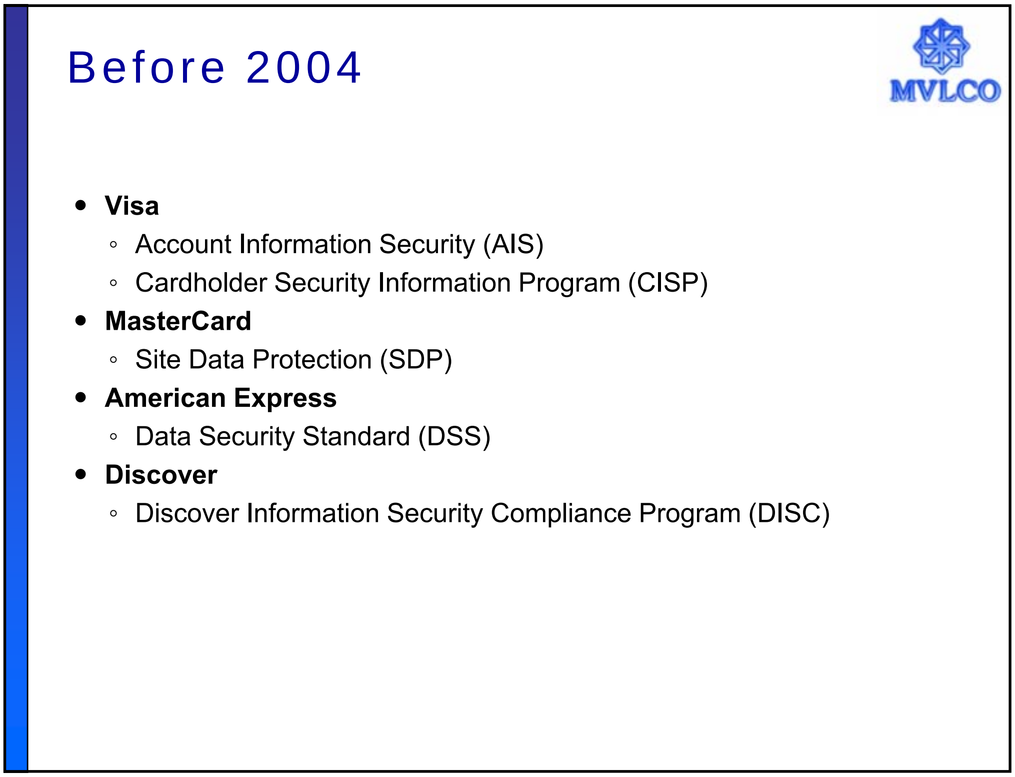
Data breach prevention

- End-to-End (or point to point) Encryption
  - "End-to-End" (E2E) or "Point-to-Point" (P2P) encryption means all data in a particular data flow is encrypted. For example, payment card data either arrives at a merchant encrypted or is immediately encrypted by a merchant upon receipt; then this encryption is maintained until the merchant transmits the data to the processor.
  - It essentially provides a secure digital "tunnel" through which data can flow securely.
- Tokenization
  - Tokenization is a process that replaces a high-value credential (e.g., a payment card primary account number (PAN), a Social Security number) with a surrogate value that is used in transactions in place of that credential.
  - Tokenization can map the credential to a new value that is in a different format or that is similar to the format of the original high-value credential (e.g., a payment card PAN in the payments industry).
- Not receiving or storing sensitive data at all



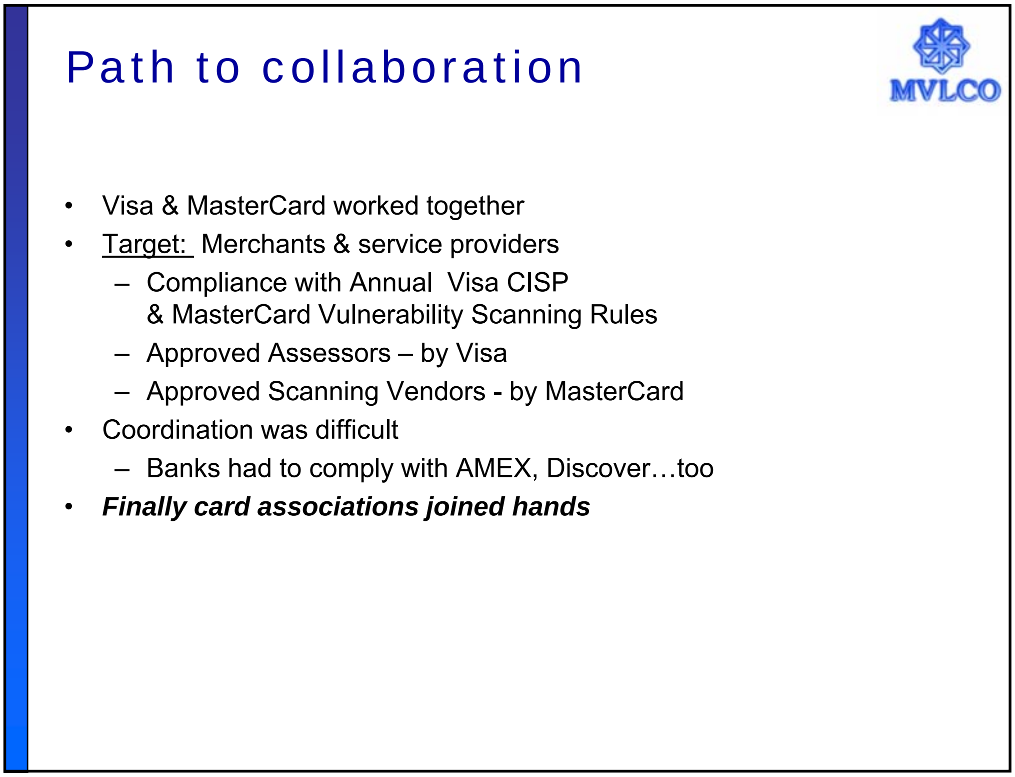
Protecting against frauds

- People clone Magstripe cards?
  - Use smart cards (EMV chip cards)
- Card Nos. & CVV2 are stolen?
  - 3-D Secure (2-factor auth.) for E-commerce
- Merchants sell card numbers…?
  - Black list. Identify & declare ***compromised points***
- Fraud attacks?
  - Implement fraud software & get fraud specialists
- Other measures have been tried too



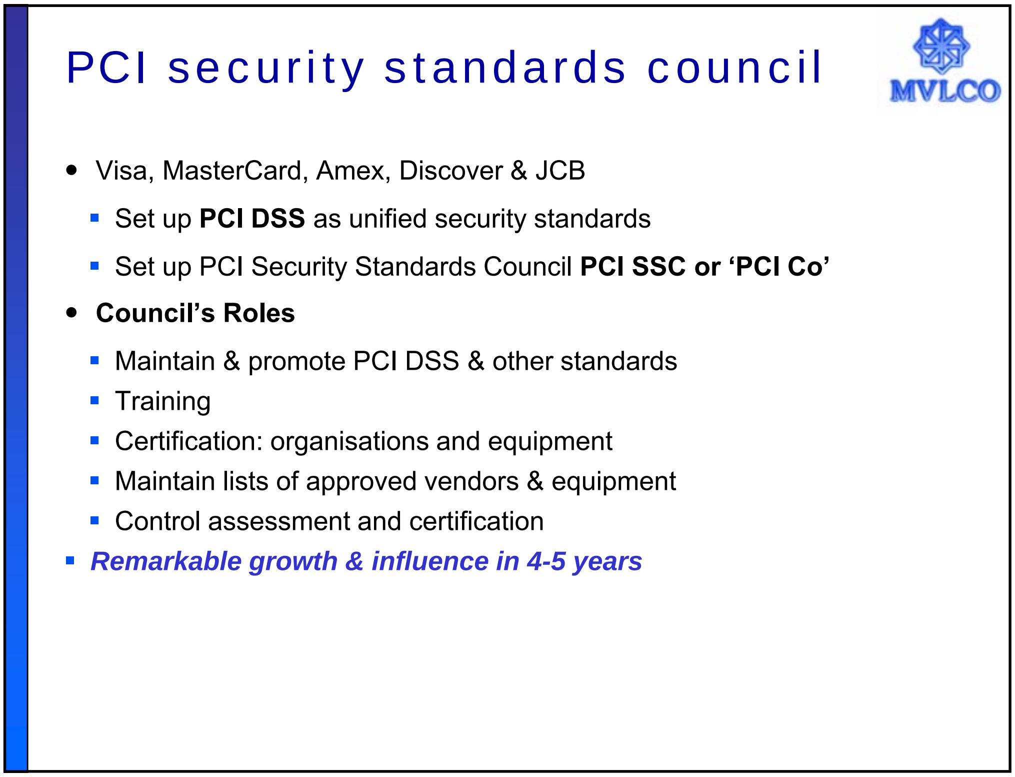
Before 2004

- **Visa**
  - Account Information Security (AIS)
  - Cardholder Security Information Program (CISP)
- **MasterCard**
  - Site Data Protection (SDP)
- **American Express**
  - Data Security Standard (DSS)
- **Discover**
  - Discover Information Security Compliance Program (DISC)



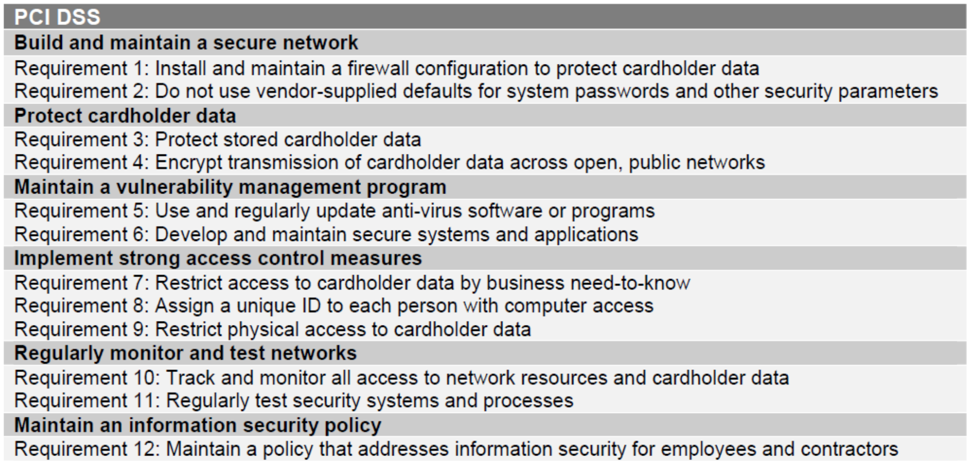
Path to collaboration

- Visa & MasterCard worked together
- Target: Merchants & service providers
  - Compliance with Annual Visa CISP
    & MasterCard Vulnerability Scanning Rules
  - Approved Assessors – by Visa
  - Approved Scanning Vendors - by MasterCard
- Coordination was difficult
  - Banks had to comply with AMEX, Discover…too
- ***Finally card associations joined hands***

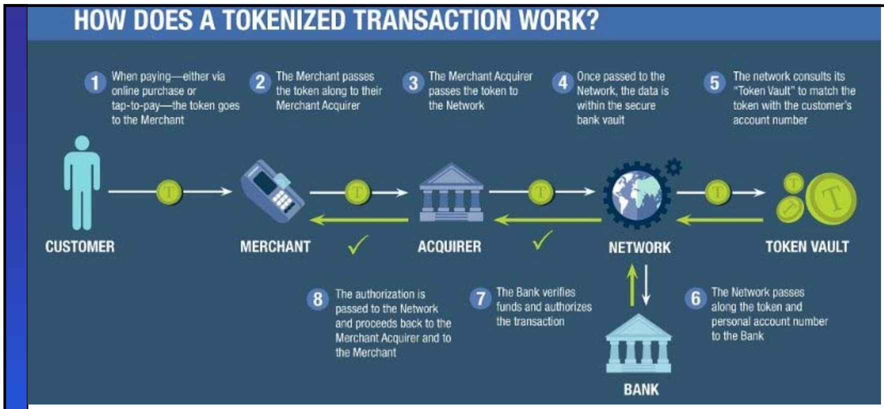


PCI security standards council

- Visa, MasterCard, Amex, Discover & JCB
  - Set up **PCI DSS** as unified security standards
  - Set up PCI Security Standards Council **PCI SSC or 'PCI Co'**
- **Council's Roles**
  - Maintain & promote PCI DSS & other standards
  - Training
  - Certification: organisations and equipment
  - Maintain lists of approved vendors & equipment
  - Control assessment and certification
- ***Remarkable growth & influence in 4-5 years***



PCI DSS
Build and maintain a secure network
Requirement 1: Install and maintain a firewall configuration to protect cardholder data Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters
Protect cardholder data
Requirement 3: Protect stored cardholder data Requirement 4: Encrypt transmission of cardholder data across open, public networks
Maintain a vulnerability management program
Requirement 5: Use and regularly update anti-virus software or programs Requirement 6: Develop and maintain secure systems and applications
Implement strong access control measures
Requirement 7: Restrict access to cardholder data by business need-to-know Requirement 8: Assign a unique ID to each person with computer access Requirement 9: Restrict physical access to cardholder data
Regularly monitor and test networks
Requirement 10: Track and monitor all access to network resources and cardholder data Requirement 11: Regularly test security systems and processes
Maintain an information security policy
Requirement 12: Maintain a policy that addresses information security for employees and contractors



HOW DOES A TOKENIZED TRANSACTION WORK?

1 When paying—either via online purchase or tap-to-pay—the token goes to the Merchant

2 The Merchant passes the token along to their Merchant Acquirer

3 The Merchant Acquirer passes the token to the Network

4 Once passed to the Network, the data is within the secure bank vault

5 The network consults its "Token Vault" to match the token with the customer's account number

6 The Network passes along the token and personal account number to the Bank

7 The Bank verifies funds and authorizes the transaction

8 The authorization is passed to the Network and proceeds back to the Merchant Acquirer and to the Merchant

TOKENISATION

Let us have a detailed discussion on Tokenisation.

EMV®*

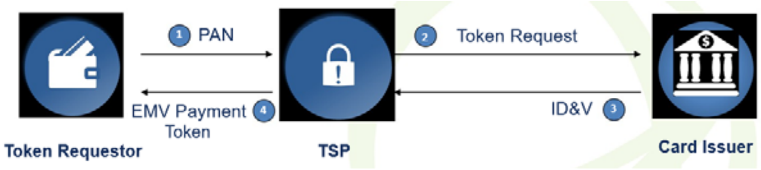
Payment Tokenisation Specification

Token issue process

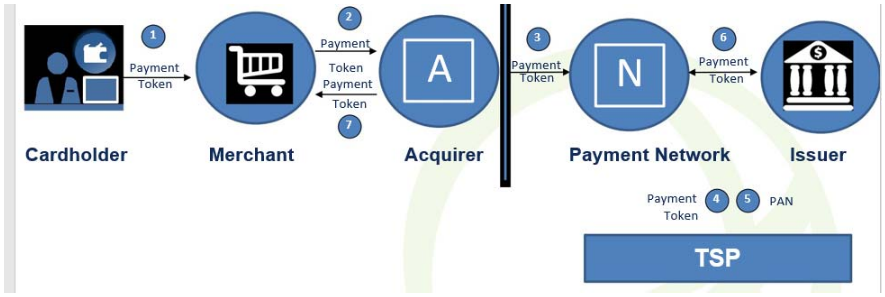
EMV Payment Token requests are made to a TSP. The token requestor, TSP and card issuer can all participate in ID&V. A token requestor can be a wallet, merchant, etc.

Process:

1. Token requestor sends a cardholder PAN to the TSP (a request)
2. As part of the token request process, the TSP alerts the card issuer that ID&V is needed
3. Card issuer (or TSP on issuer's behalf) performs ID&V and passes results to the token vault (Binding)
4. TSP passes the registered EMV Payment Token to the token requestor



Token usage process



(1) Cardholder initiates a purchase with a payment instrument i.e. EMV Payment Token.

(2) and (3) Payment Token flows through the merchant and acquirer as if it were a PAN

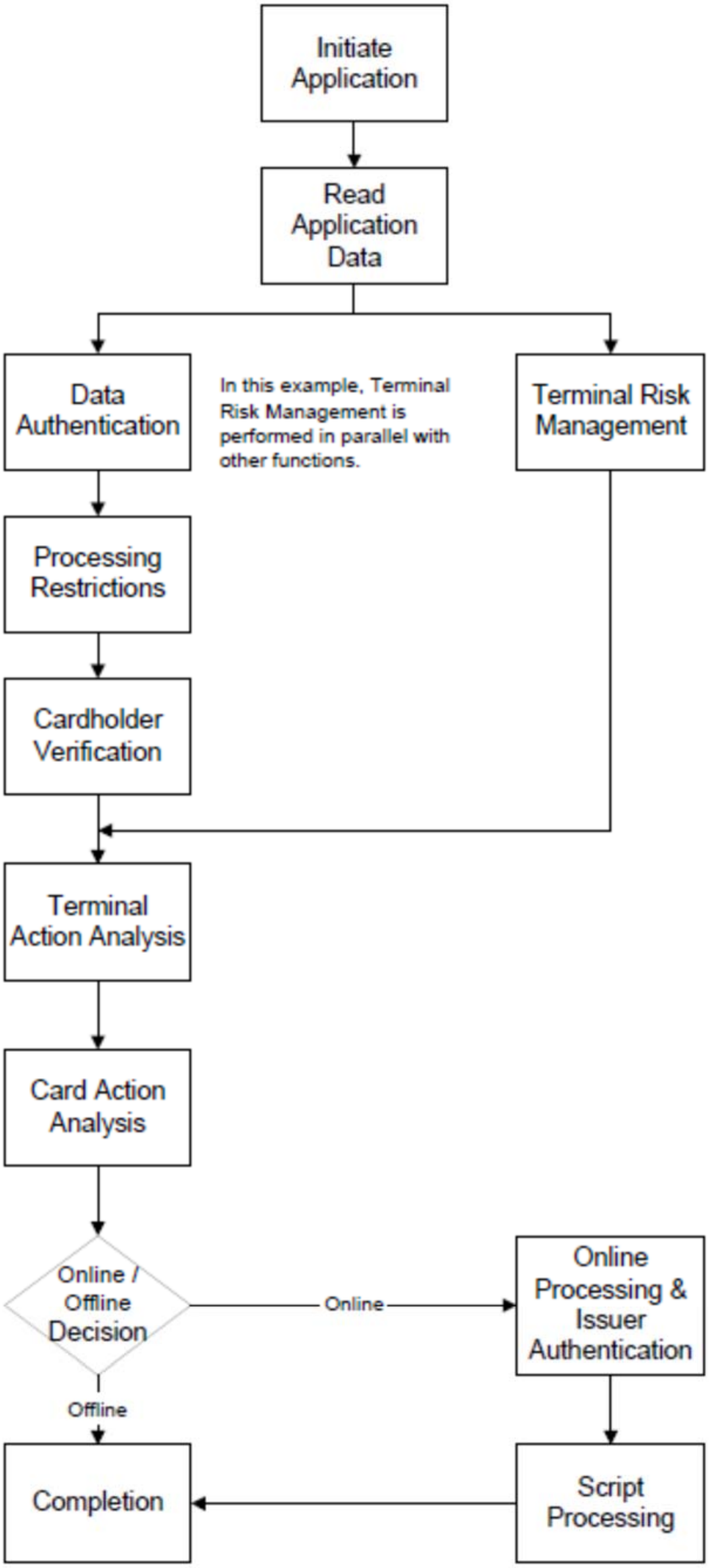
(4) and (5) Payment token is de-tokenised into a PAN by the TSP; card issuer makes authorization decision and returns PAN to TSP

(6) and (7) TSP re-tokenises the PAN and the authorisation response flows back through the acquirer to the merchant

MVLCO

Thank You !

EMV Process Flow Charts



In this example, Terminal Risk Management is performed in parallel with other functions.

Figure 6: Transaction Flow Example

EMV Process Flow Charts

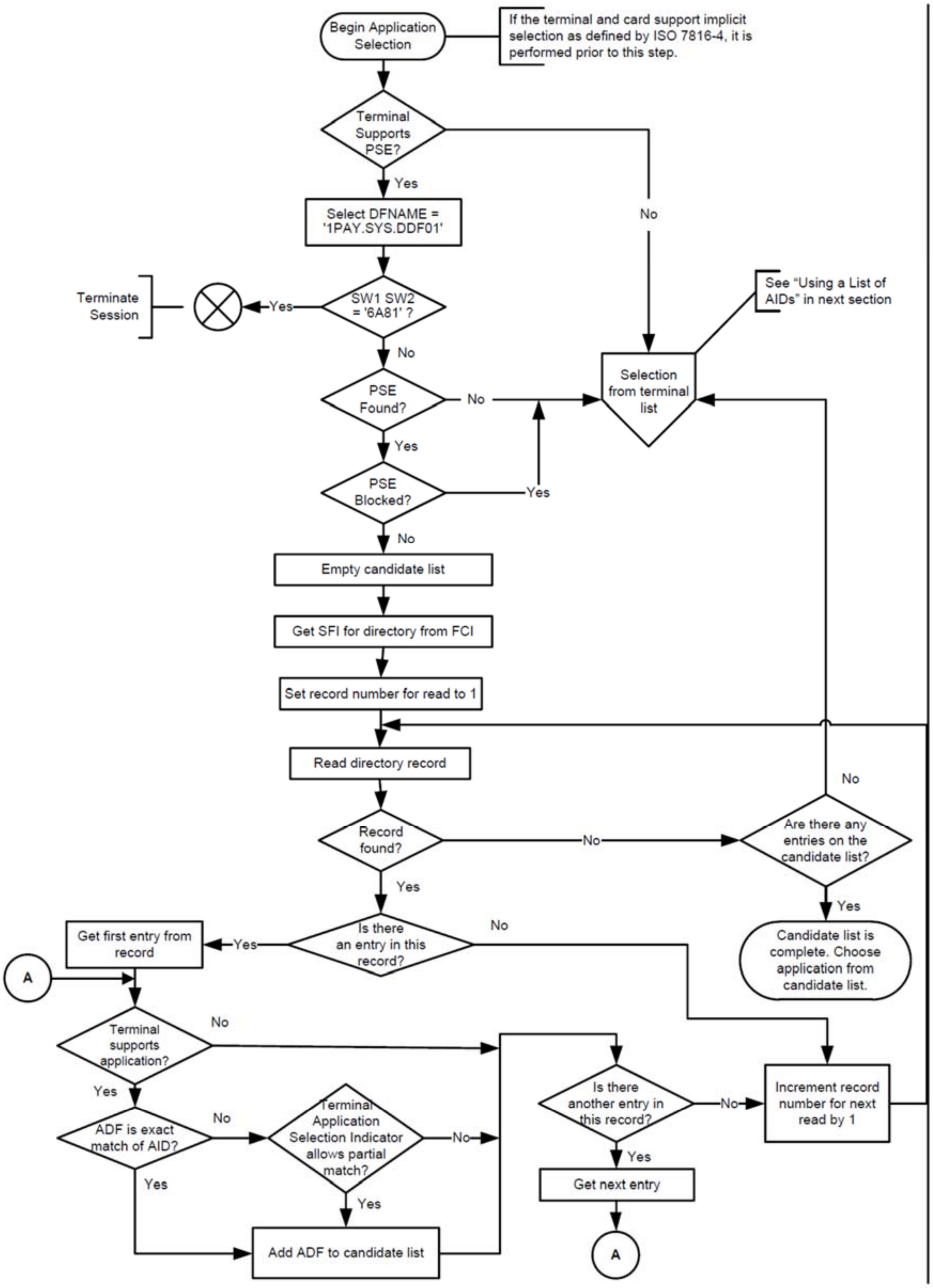

Begin Application Selection
If the terminal and card support implicit selection as defined by ISO 7816-4, it is performed prior to this step.
Terminal Supports PSE?
Yes
No
Select DFNAME = '1PAY.SYS.DDF01'
Terminate Session
Yes
SW1 SW2 = '6A81' ?
No
See "Using a List of AIDs" in next section
Selection from terminal list
PSE Found?
No
Yes
PSE Blocked?
Yes
No
Empty candidate list
Get SFI for directory from FCI
Set record number for read to 1
Read directory record
No
Record found?
No
Are there any entries on the candidate list?
Yes
Yes
Candidate list is complete. Choose application from candidate list.
Get first entry from record
Yes
Is there an entry in this record?
No
A
Terminal supports application?
No
Yes
ADF is exact match of AID?
No
Terminal Application Selection Indicator allows partial match?
No
Yes
Yes
Add ADF to candidate list
Is there another entry in this record?
No
Increment record number for next read by 1
Yes
Get next entry
A

Figure 17: Terminal Logic Using Directories

EMV Process Flow Charts

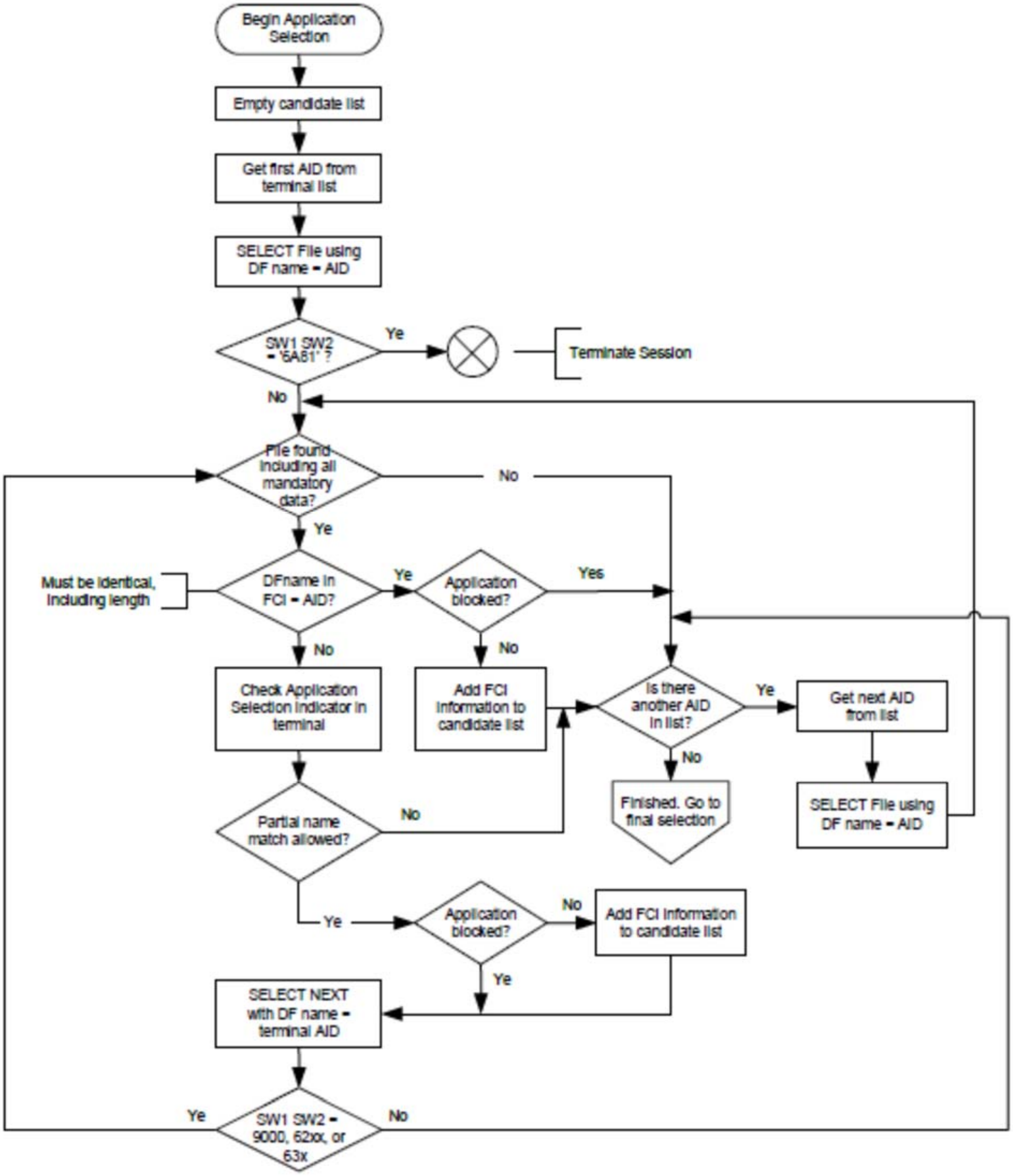

Begin Application Selection
Empty candidate list
Get first AID from terminal list
SELECT File using DF name = AID
SW1 SW2 = '6A81' ?
Ye
Terminate Session
No
File found including all mandatory data?
No
Ye
Must be identical, including length
DFname in FCI = AID?
Ye
Application blocked?
Yes
No
No
Check Application Selection indicator in terminal
Add FCI information to candidate list
Is there another AID in list?
Ye
Get next AID from list
No
Finished. Go to final selection
SELECT File using DF name = AID
Partial name match allowed?
No
Ye
Application blocked?
No
Add FCI information to candidate list
Ye
SELECT NEXT with DF name = terminal AID
Ye
SW1 SW2 = 9000, 62xx, or 63x
No

Figure 18: Using the List of AIDs in the Terminal

EMV Process Flow Charts

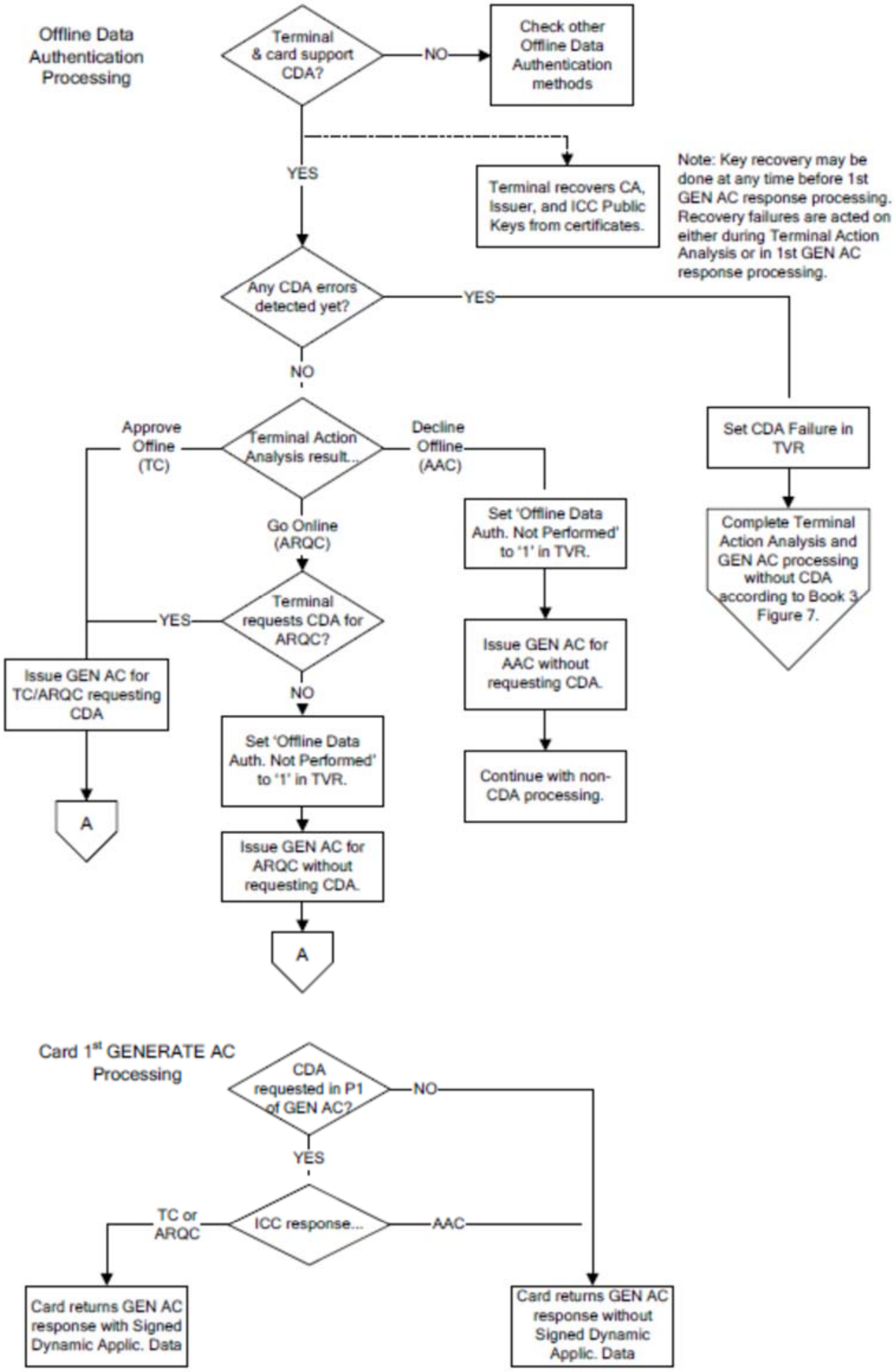

Offline Data Authentication Processing
Terminal & card support CDA?
NO
Check other Offline Data Authentication methods
YES
Terminal recovers CA, Issuer, and ICC Public Keys from certificates.
Note: Key recovery may be done at any time before 1st GEN AC response processing. Recovery failures are acted on either during Terminal Action Analysis or in 1st GEN AC response processing.
Any CDA errors detected yet?
YES
NO
Set CDA Failure in TVR
Complete Terminal Action Analysis and GEN AC processing without CDA according to Book 3 Figure 7.
Approve Offline (TC)
Terminal Action Analysis result...
Decline Offline (AAC)
Go Online (ARQC)
Set 'Offline Data Auth. Not Performed' to '1' in TVR.
Issue GEN AC for AAC without requesting CDA.
Continue with non-CDA processing.
YES
Terminal requests CDA for ARQC?
NO
Issue GEN AC for TC/ARQC requesting CDA
A
Set 'Offline Data Auth. Not Performed' to '1' in TVR.
Issue GEN AC for ARQC without requesting CDA.
A
Card 1st GENERATE AC Processing
CDA requested in P1 of GEN AC?
NO
YES
TC or ARQC
ICC response...
AAC
Card returns GEN AC response with Signed Dynamic Applic. Data
Card returns GEN AC response without Signed Dynamic Applic. Data

Figure 3: CDA Sample Flow Part 1 of 3

EMV Process Flow Charts

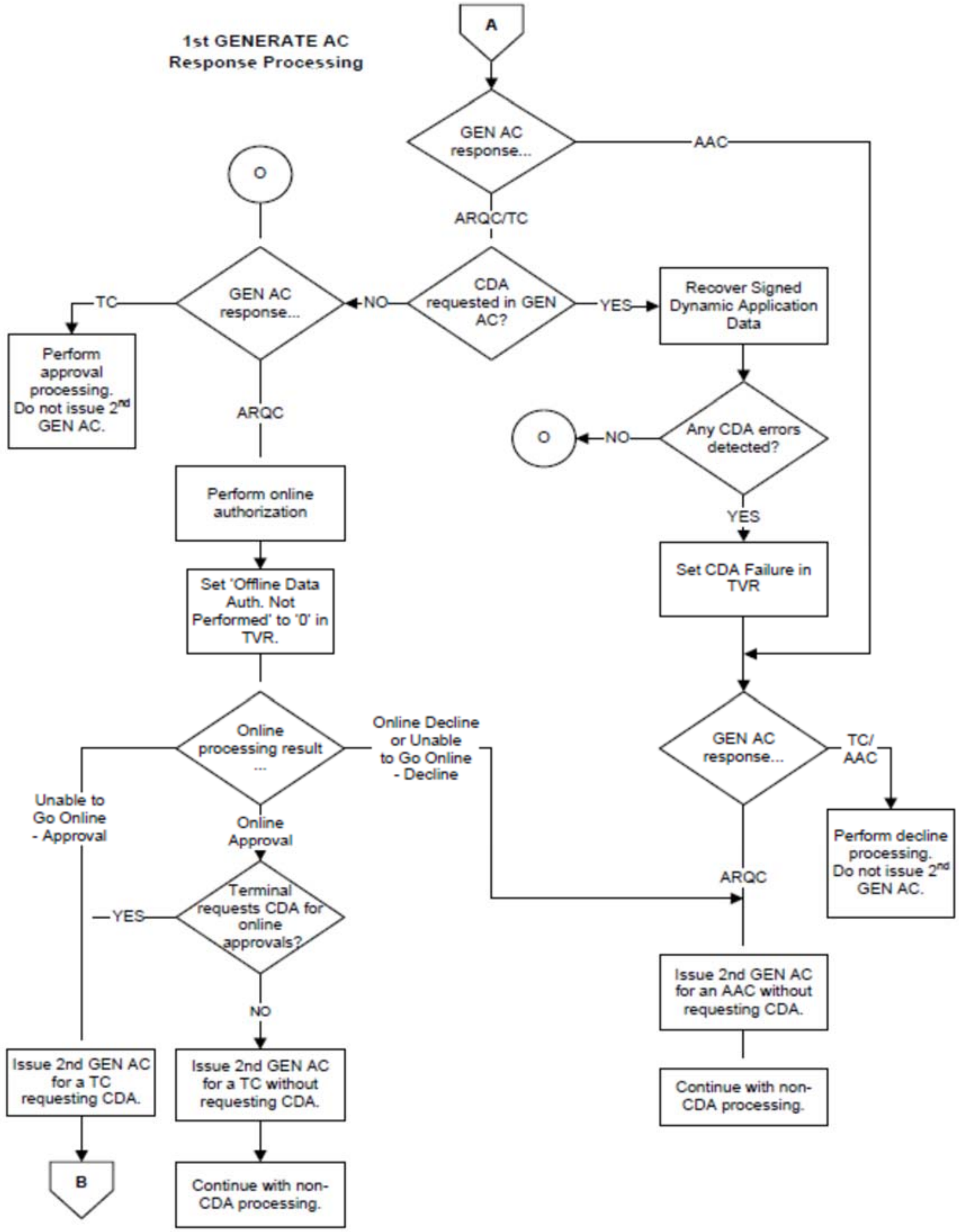

1st GENERATE AC
Response Processing
A
GEN AC response...
AAC
ARQC/TC
O
CDA requested in GEN AC?
NO
YES
Recover Signed Dynamic Application Data
GEN AC response...
TC
Perform approval processing. Do not issue 2nd GEN AC.
ARQC
Any CDA errors detected?
O
NO
YES
Perform online authorization
Set CDA Failure in TVR
Set 'Offline Data Auth. Not Performed' to '0' in TVR.
Online processing result ...
Online Decline or Unable to Go Online - Decline
GEN AC response...
TC/ AAC
Unable to Go Online - Approval
Online Approval
Perform decline processing. Do not issue 2nd GEN AC.
ARQC
Terminal requests CDA for online approvals?
YES
NO
Issue 2nd GEN AC for an AAC without requesting CDA.
Issue 2nd GEN AC for a TC requesting CDA.
Issue 2nd GEN AC for a TC without requesting CDA.
Continue with non-CDA processing.
B
Continue with non-CDA processing.

Figure 4: CDA Sample Flow Part 2 of 3

EMV Process Flow Charts

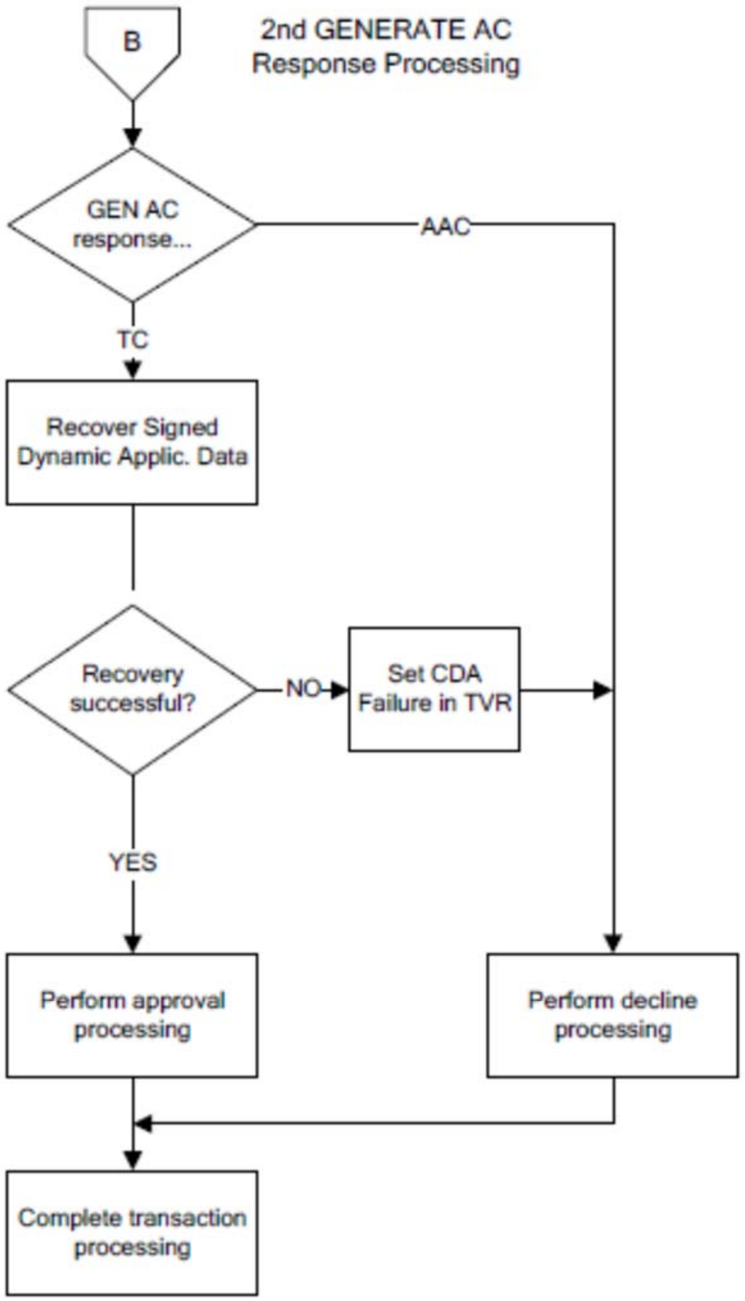


Figure 5: CDA Sample Flow Part 3 of 3

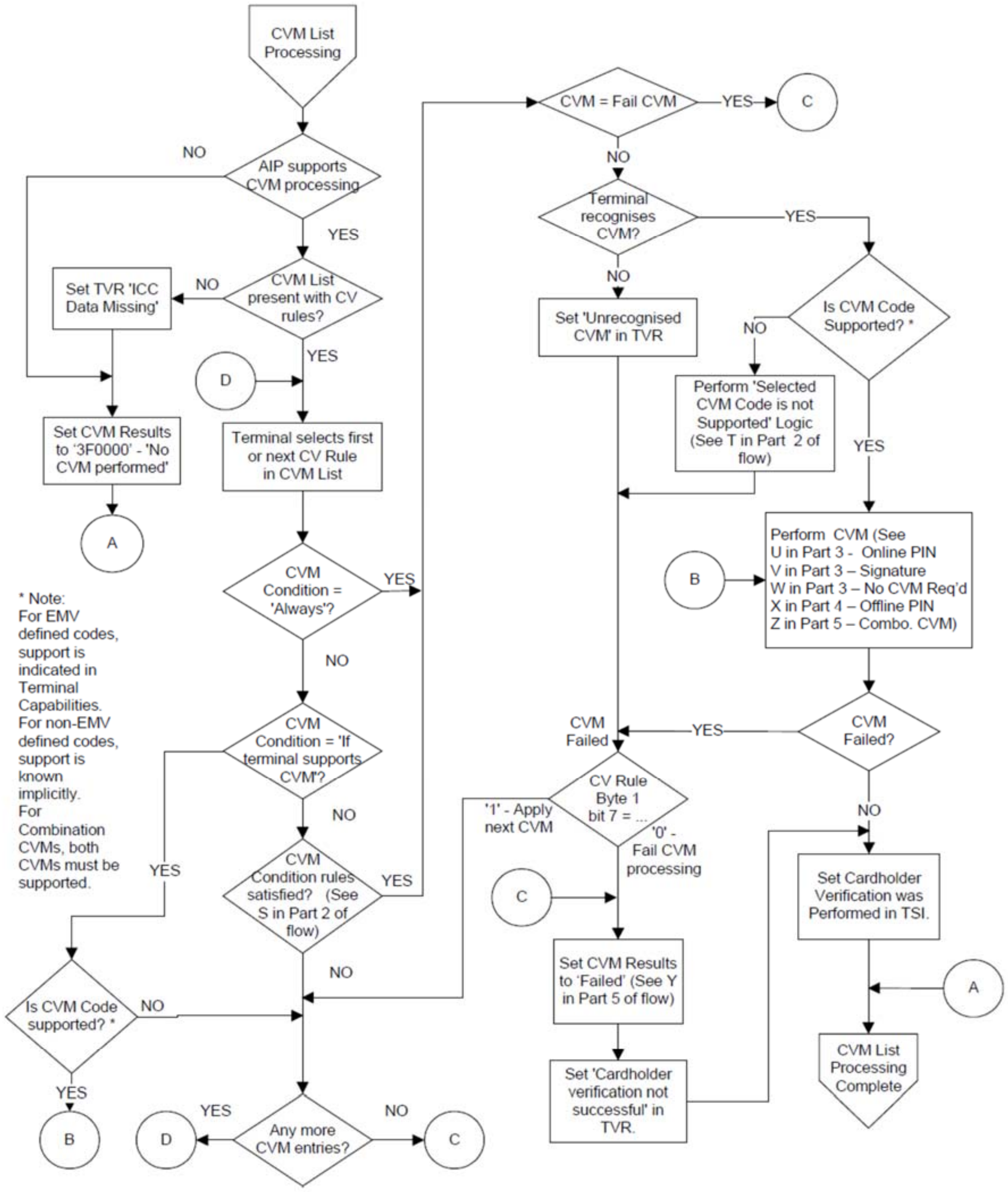
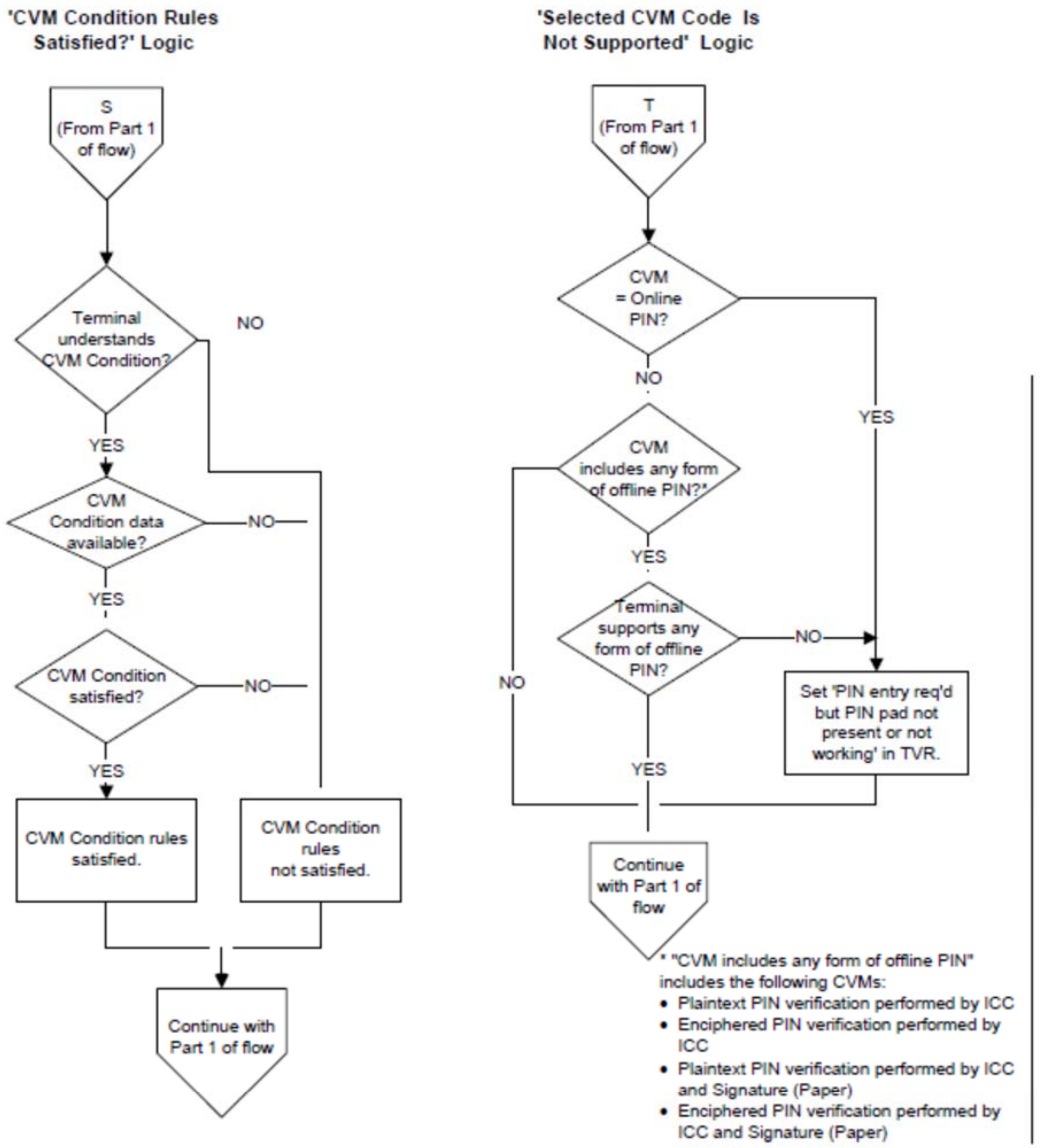

CVM List Processing
AIP supports CVM processing
NO
YES
CVM List present with CV rules?
NO
YES
Set TVR 'ICC Data Missing'
Set CVM Results to '3F0000' - 'No CVM performed'
A
D
Terminal selects first or next CV Rule in CVM List
CVM Condition = 'Always'?
YES
NO
CVM Condition = 'If terminal supports CVM'?
YES
NO
CVM Condition rules satisfied? (See S in Part 2 of flow)
YES
NO
Is CVM Code supported? *
NO
YES
B
Any more CVM entries?
YES
D
NO
C
* Note:
For EMV defined codes, support is indicated in Terminal Capabilities.
For non-EMV defined codes, support is known implicitly.
For Combination CVMs, both CVMs must be supported.
CVM = Fail CVM
YES
C
NO
Terminal recognises CVM?
YES
NO
Set 'Unrecognised CVM' in TVR
Is CVM Code Supported? *
NO
Perform 'Selected CVM Code is not Supported' Logic (See T in Part 2 of flow)
YES
Perform CVM (See
U in Part 3 - Online PIN
V in Part 3 – Signature
W in Part 3 – No CVM Req'd
X in Part 4 – Offline PIN
Z in Part 5 – Combo. CVM)
B
CVM Failed?
YES
CVM Failed
NO
CV Rule Byte 1 bit 7 = ...
'1' - Apply next CVM
'0' - Fail CVM processing
C
Set CVM Results to 'Failed' (See Y in Part 5 of flow)
Set 'Cardholder verification not successful' in TVR.
Set Cardholder Verification was Performed in TSI.
A
CVM List Processing Complete

Figure 8: CVM Processing (Part 1 of 5)

EMV Process Flow Charts



'CVM Condition Rules Satisfied?' Logic

'Selected CVM Code Is Not Supported' Logic

S
(From Part 1 of flow)
Terminal understands CVM Condition?
NO
YES
CVM Condition data available?
NO
YES
CVM Condition satisfied?
NO
YES
CVM Condition rules satisfied.
CVM Condition rules not satisfied.
Continue with Part 1 of flow
T
(From Part 1 of flow)
CVM = Online PIN?
NO
YES
CVM includes any form of offline PIN?*
YES
NO
Terminal supports any form of offline PIN?
NO
YES
Set 'PIN entry req'd but PIN pad not present or not working' in TVR.
Continue with Part 1 of flow

* "CVM includes any form of offline PIN" includes the following CVMs:

- Plaintext PIN verification performed by ICC
- Enciphered PIN verification performed by ICC
- Plaintext PIN verification performed by ICC and Signature (Paper)
- Enciphered PIN verification performed by ICC and Signature (Paper)

Figure 9: CVM Processing (Part 2 of 5)

EMV Process Flow Charts

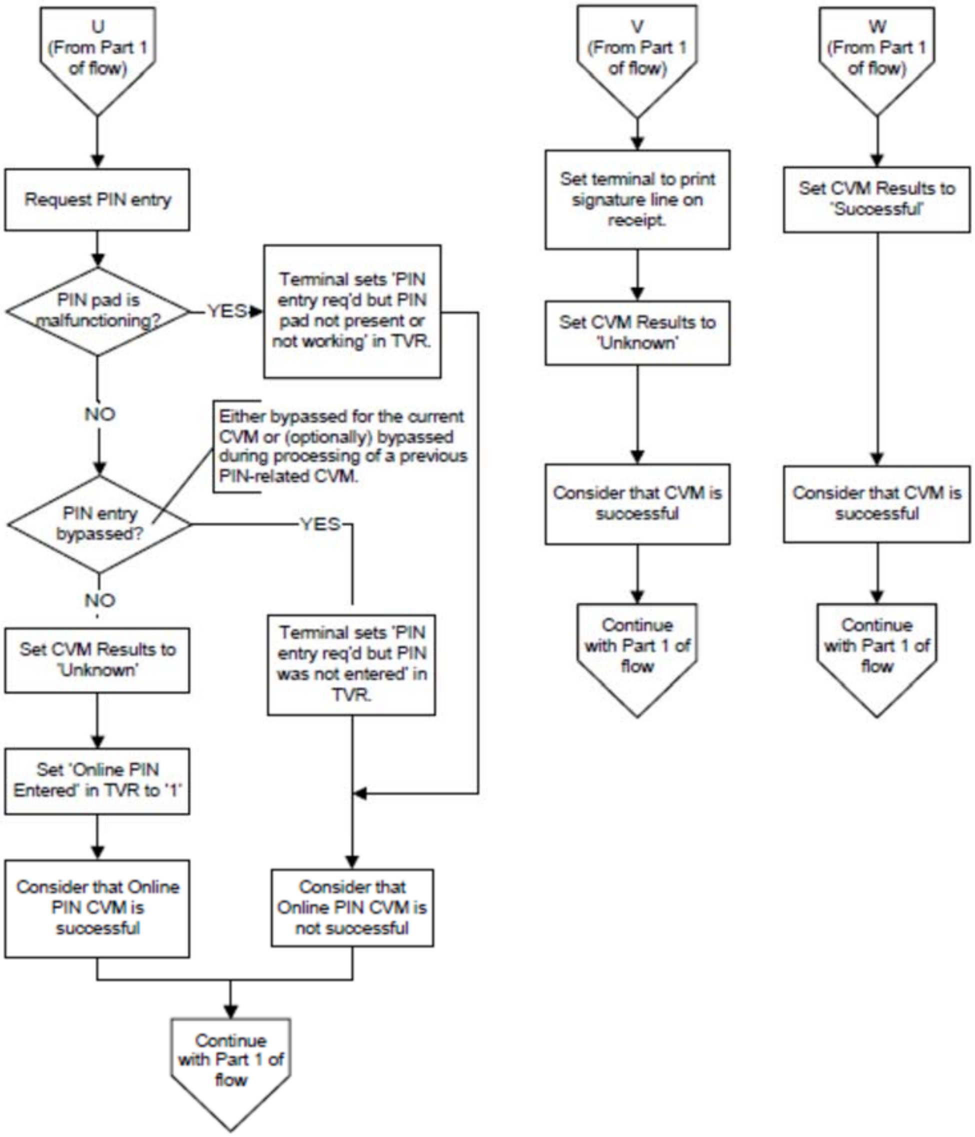

U (From Part 1 of flow)
Request PIN entry
PIN pad is malfunctioning?
YES
Terminal sets 'PIN entry req'd but PIN pad not present or not working' in TVR.
NO
Either bypassed for the current CVM or (optionally) bypassed during processing of a previous PIN-related CVM.
PIN entry bypassed?
YES
NO
Set CVM Results to 'Unknown'
Terminal sets 'PIN entry req'd but PIN was not entered' in TVR.
Set 'Online PIN Entered' in TVR to '1'
Consider that Online PIN CVM is successful
Consider that Online PIN CVM is not successful
Continue with Part 1 of flow
V (From Part 1 of flow)
Set terminal to print signature line on receipt.
Set CVM Results to 'Unknown'
Consider that CVM is successful
Continue with Part 1 of flow
W (From Part 1 of flow)
Set CVM Results to 'Successful'
Consider that CVM is successful
Continue with Part 1 of flow

Figure 10: CVM Processing (Part 3 of 5)

EMV Process Flow Charts

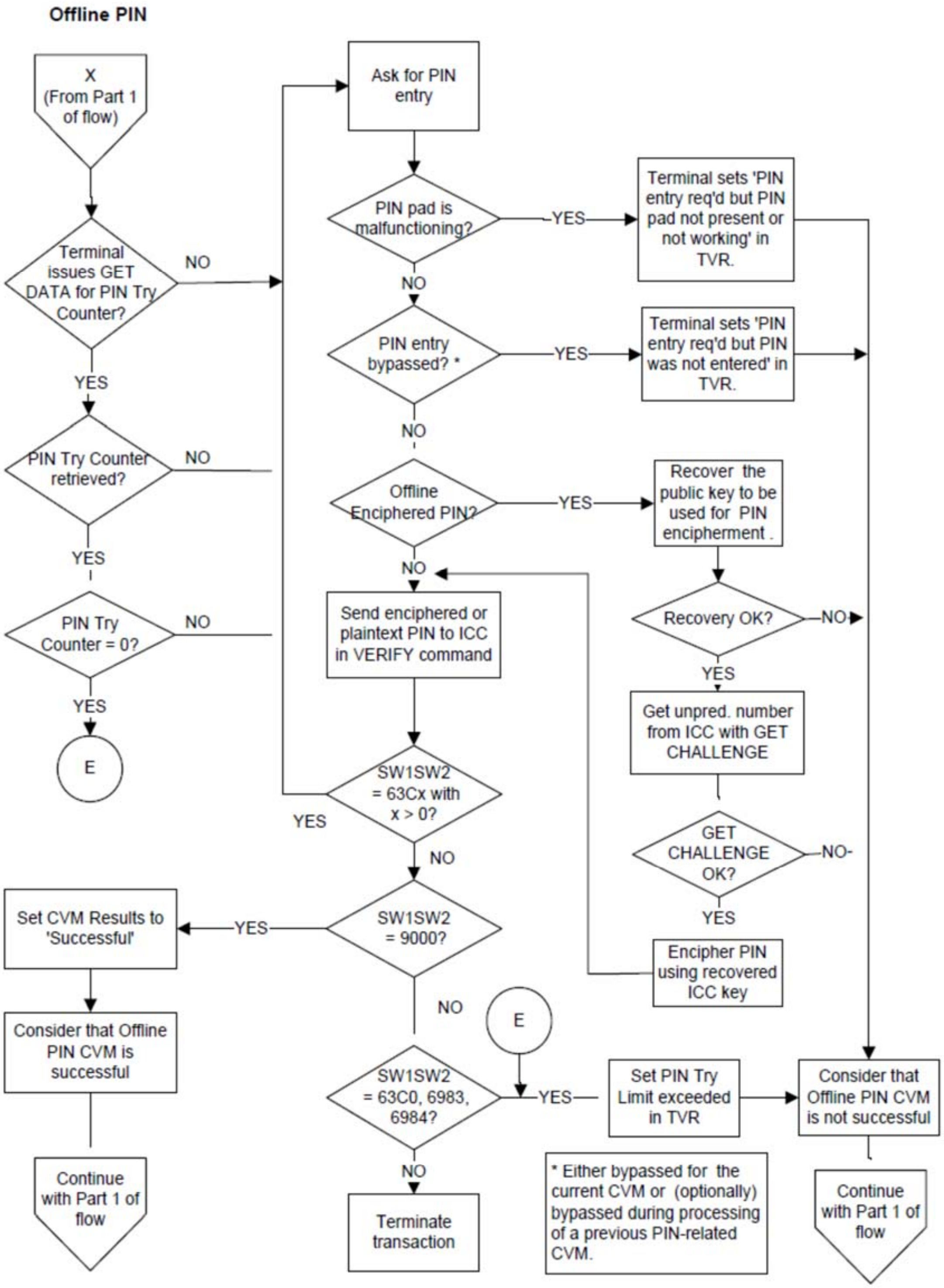
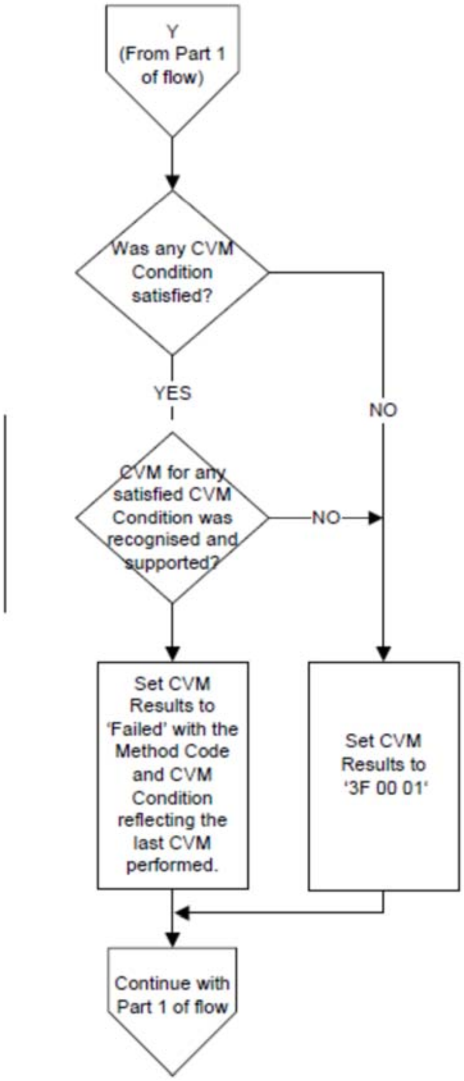

Offline PIN
X (From Part 1 of flow)
Terminal issues GET DATA for PIN Try Counter?
NO
YES
PIN Try Counter retrieved?
NO
YES
PIN Try Counter = 0?
NO
YES
E
Ask for PIN entry
PIN pad is malfunctioning?
YES
Terminal sets 'PIN entry req'd but PIN pad not present or not working' in TVR.
NO
PIN entry bypassed? *
YES
Terminal sets 'PIN entry req'd but PIN was not entered' in TVR.
NO
Offline Enciphered PIN?
YES
Recover the public key to be used for PIN encipherment .
NO
Recovery OK?
NO
YES
Get unpred. number from ICC with GET CHALLENGE
GET CHALLENGE OK?
NO
YES
Encipher PIN using recovered ICC key
Send enciphered or plaintext PIN to ICC in VERIFY command
SW1SW2 = 63Cx with x > 0?
YES
NO
SW1SW2 = 9000?
YES
Set CVM Results to 'Successful'
Consider that Offline PIN CVM is successful
Continue with Part 1 of flow
NO
E
SW1SW2 = 63C0, 6983, 6984?
YES
Set PIN Try Limit exceeded in TVR
Consider that Offline PIN CVM is not successful
Continue with Part 1 of flow
NO
Terminate transaction
* Either bypassed for the current CVM or (optionally) bypassed during processing of a previous PIN-related CVM.

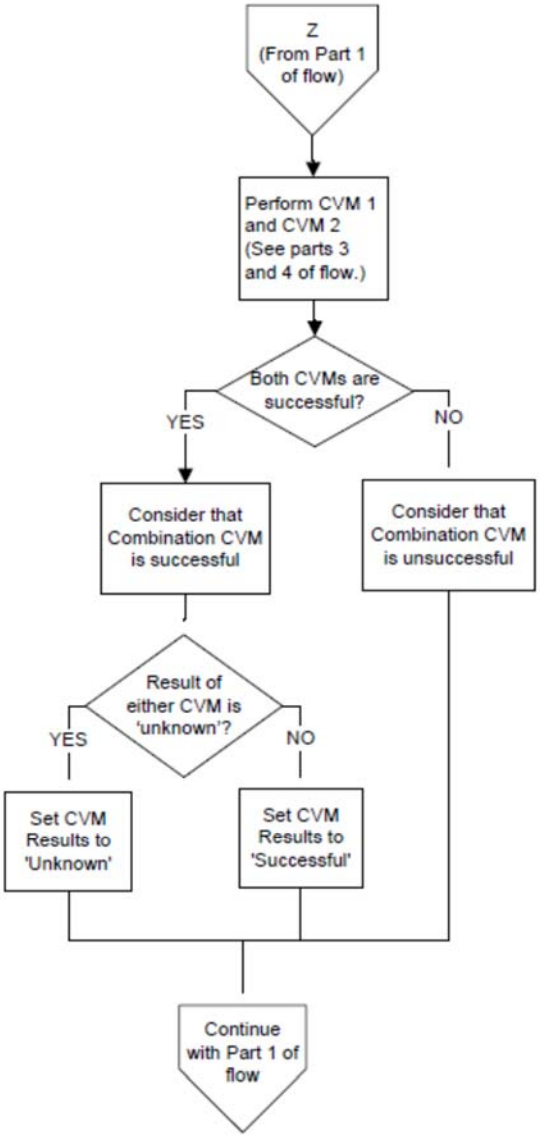
Figure 11: CVM Processing (Part 4 of 5)

EMV Process Flow Charts

Setting CVM Results to Failed



Combination CVMs



EMV Process Flow Charts

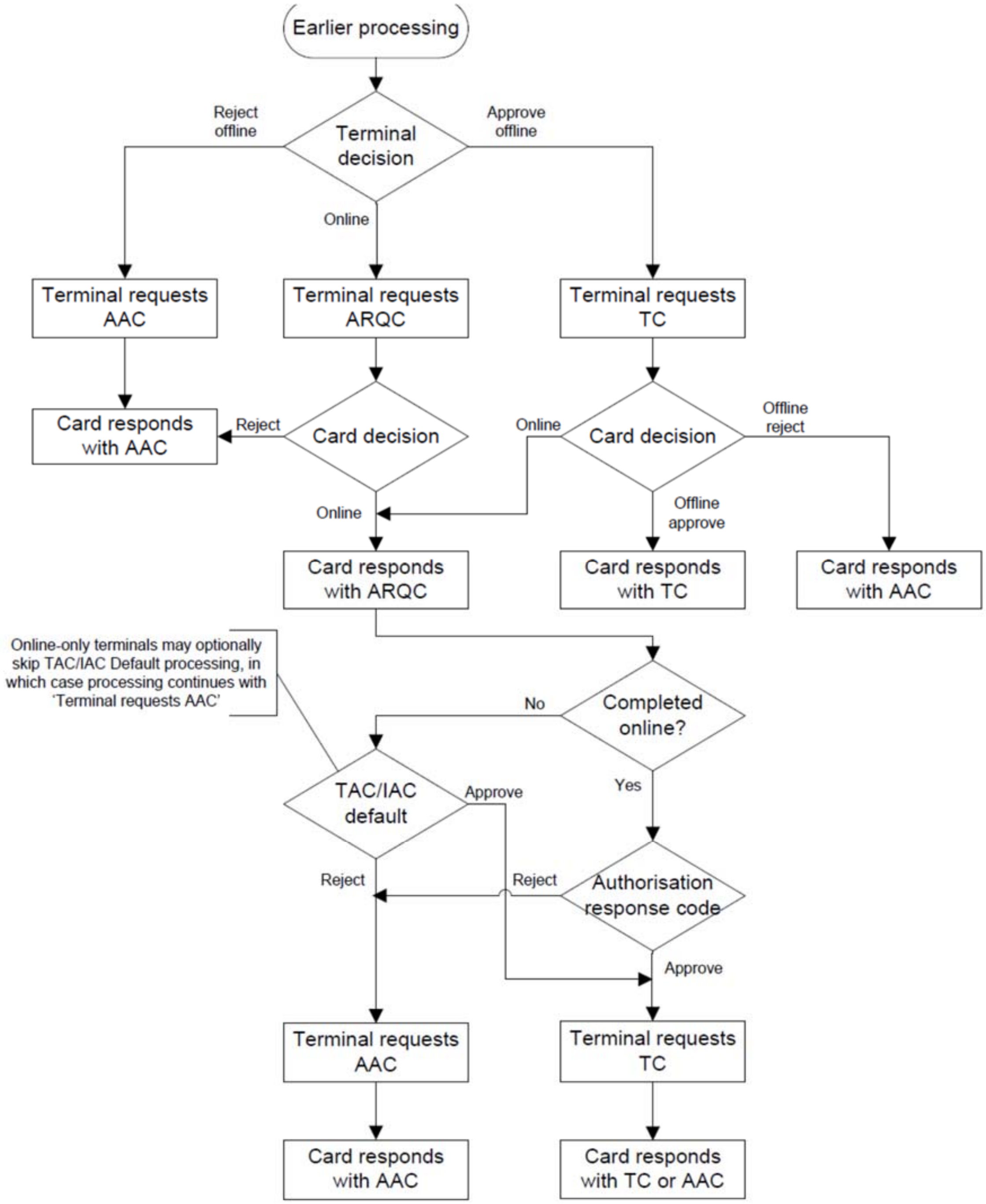


Figure 7: Use of GENERATE AC Options