Advanced Card Systems Ltd.
Card & Reader Technologies

EMV Specification

CARD & READER TECHNOLOGIES

EMV Specifications

- May ‘94 - Version 1.0 EMV Part 1
- Aug ‘94 - Version 1.0 EMV Part 2
- Oct ‘94 - Version 1.0 EMV Part 3
- Jun ‘95 - Version 2.0 EMV
- Jun ‘96 - Version 3.0 EMV’96
- May ‘98 - Version 3.1.1
- Dec ‘2000 - EMV2000 (Version 4.0)

EMV Versions 1 & 2

- Divided into 3 parts:
  - Part 1 : Electromechanical Characteristics, Logical Interface & Transmission Protocol
  - Part 2: Data Elements & Commands
  - Part 3: Transaction Processing

EMV '96

- Divided into 3 documents
- IC Card Specification
  - Part 1: Electromechanical Characteristics, Logical Interface & Transmission Protocol
  - Part 2: Data Elements & Commands
  - Part 3: Application Selection
  - Part 4: Security Aspects

EMV '96

- IC Card Terminal Specification
  - Part 1: General Requirements
  - Part 2: Software Architecture
  - Part 3: Cardholder, Attendant and Acquirer Interface IC Card Terminal Specification
- IC Card Application Specification

EMV 2000

- Book 1 : Application Independent ICC to Terminal Interface Requirement
- Book 2 : Security and Key Management
- Book 3 : Application Specification
- Book 4 : Cardholder, Attendant and Acquirer Interface Requirements

Book 1: Application Independent ICC to Terminal Interface Requirement

- Part 1: Electromechanical characteristics, logical interfaces & transmission protocol equivalent to ISO-7816 parts 1, 2 and 3
- Part 2: File Commands and Application Selection

Book 2: Security & Key Management

- Static & Dynamic Authentication
- PIN Encipherment & Verification
- Application Cryptogram & Issuer Authentication
- Secured Messaging
- CA PK Management Principles & Policies
- Terminal Security & Key Management Requirements

Book 3: Application Specification

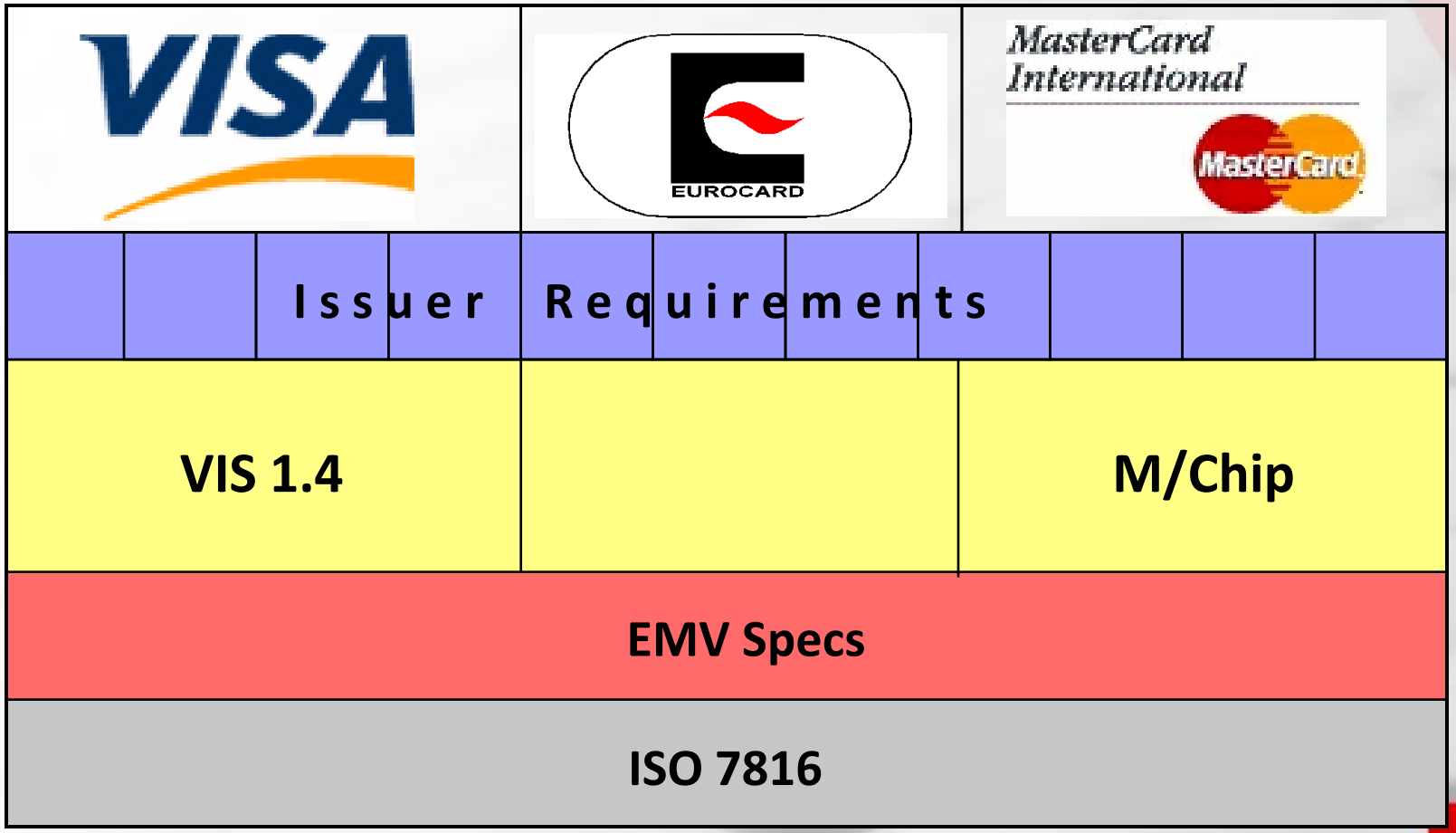
- Part 1: Data Elements & Commands
- Part 2: Debit and Credit Application Specification
  - Files for financial transaction interchange
  - Transaction flow
  - Generate AC coding
  - Functions used in transaction processing

Book 4: Cardholder, Attendant & Acquirer Interface Requirements

- Part 1: General Requirements
  - Terminal types & capabilities
  - Functional requirements
  - Physical characteristics
  - Security requirements
- Part 2: Software Architecture
- Part 3: Cardholder, Attendant and Acquirer Interface

World Coverage

EMV Card


VISA
EUROCARD
MasterCard International
MasterCard
Issuer Requirements
VIS 1.4
M/Chip
EMV Specs
ISO 7816

EMV Specifications: Objectives

- Universal Acceptance of Chip Debit / Credit Card
- Ensure that payment functions are performed consistently & securely at the point of transaction
- Define minimum functionalities to support International interoperability

EUROCARD

MasterCard International

MasterCard

VISA

EMV Concepts

- Offline risk management decision taken by:
  - Terminal (acquirer)
  - Card (issuer)
- 3 possible outcomes:
  - Offline approval of transaction
  - Online approval of transaction
  - Denial of transaction
- Card decision made according to Risk Management Rules defined by the issuer

EMV Concepts

- EMV is a “toolbox.”
- Each issuer is free to decide on the rules on:
  - Security
  - Risk management
  - Implementation
- Each acquirer is free to decide on his own risk management parameters.

EMV Concept: Offline Example

Risk Management Rules

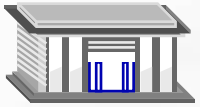
Online if:

- **Transaction > $40**
- **Every 3 offline transactions**

1. I want to make a $20 transaction – OK?

2. Yes. This is the signature.

EMV Concept: Rejected Offline Example



ISSUER

3. Is a $30 online transaction OK?

4. OK.

Risk Management Rules

Online if:

- **Transaction > $40**
- **Every 3 offline transactions**

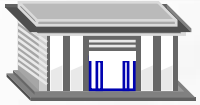
1. I want to make a $30 offline transaction – OK?

2. No. Please ask my issuer bank.

5. Your bank says OK...

6. Here is your signature..

EMV Concept: Online Example

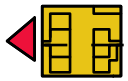


ISSUER

3. Is a $100 online transaction OK?

4. OK.

Risk Management Rules



Online if:

- **Transaction > $40**
- **Every 3 offline transactions**

1. I want to make a $100 online transaction – OK?

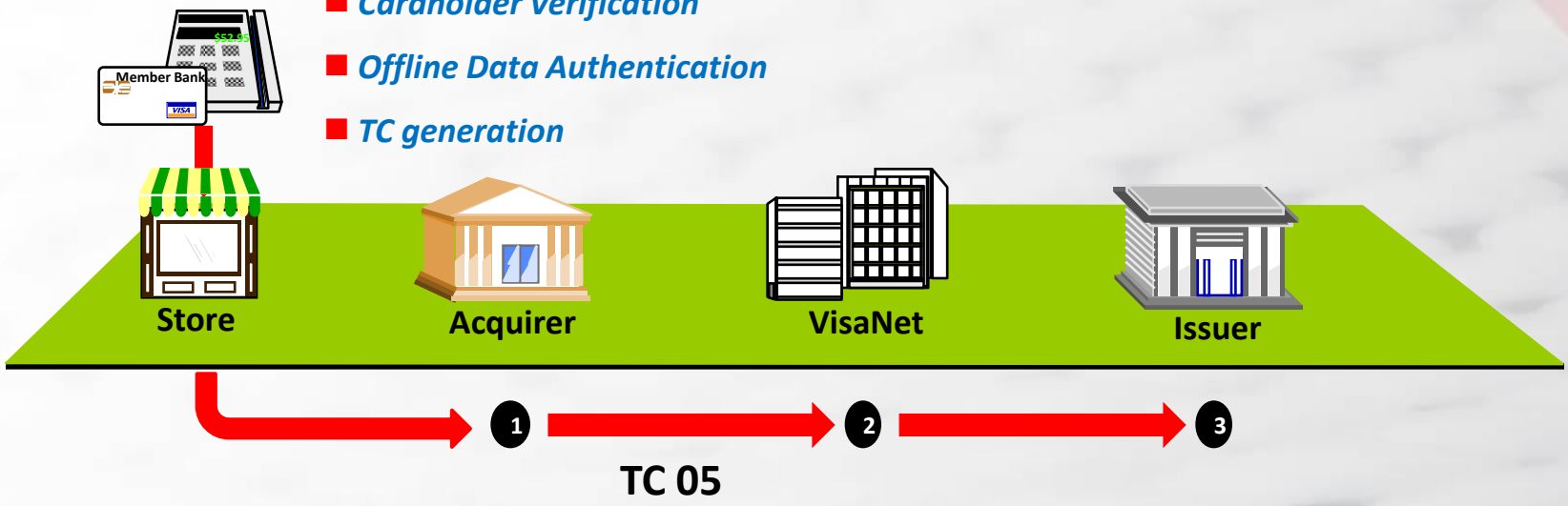
2. Yes. Please ask my issuer bank.

5. Your bank says OK.

6. Here is your signature.

Offline Transaction

- *Authorization Controls*
- *Cardholder Verification*
- *Offline Data Authentication*
- *TC generation*



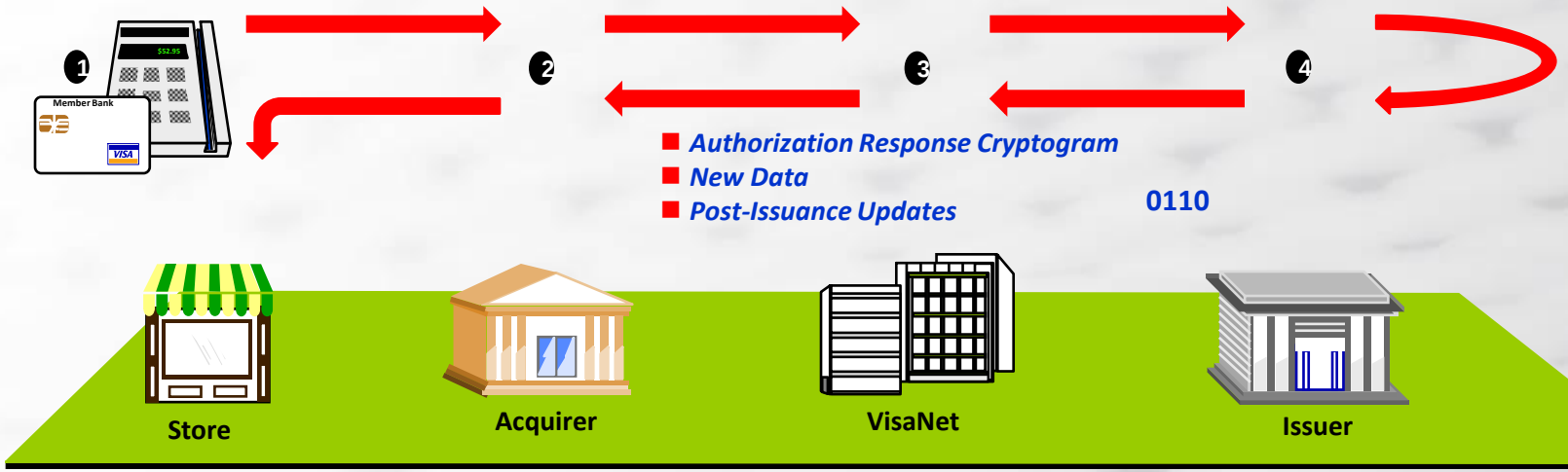
- *Transaction Certificate*
- *New Data*

Online Transaction

- Authorization Controls
- Cardholder Verification
- Offline Data Authentication
- *ARQC generation (for online request)* ★
- *ARPC validation (for online response)* ★
- TC generation (for clearing)

0100

- *Authorization Request Cryptogram*
- *New Data/Results of offline risk management*



- *Authorization Response Cryptogram*
- *New Data*
- *Post-Issuance Updates*

0110

TC 05

- *Transaction Certificate*
- *New Data*

EMV Specification Coverage

- Data Authorization
- Data Collection

- Transaction Storage
- Communication Protocol

Not specified by EMV Specification

Transaction Flow & Data

Interface

Interface & Data

- Risk Management
- Cryptography of transaction
- Personalization

Not specified by EMV Specification

EMV Specification

Terminal Coverage

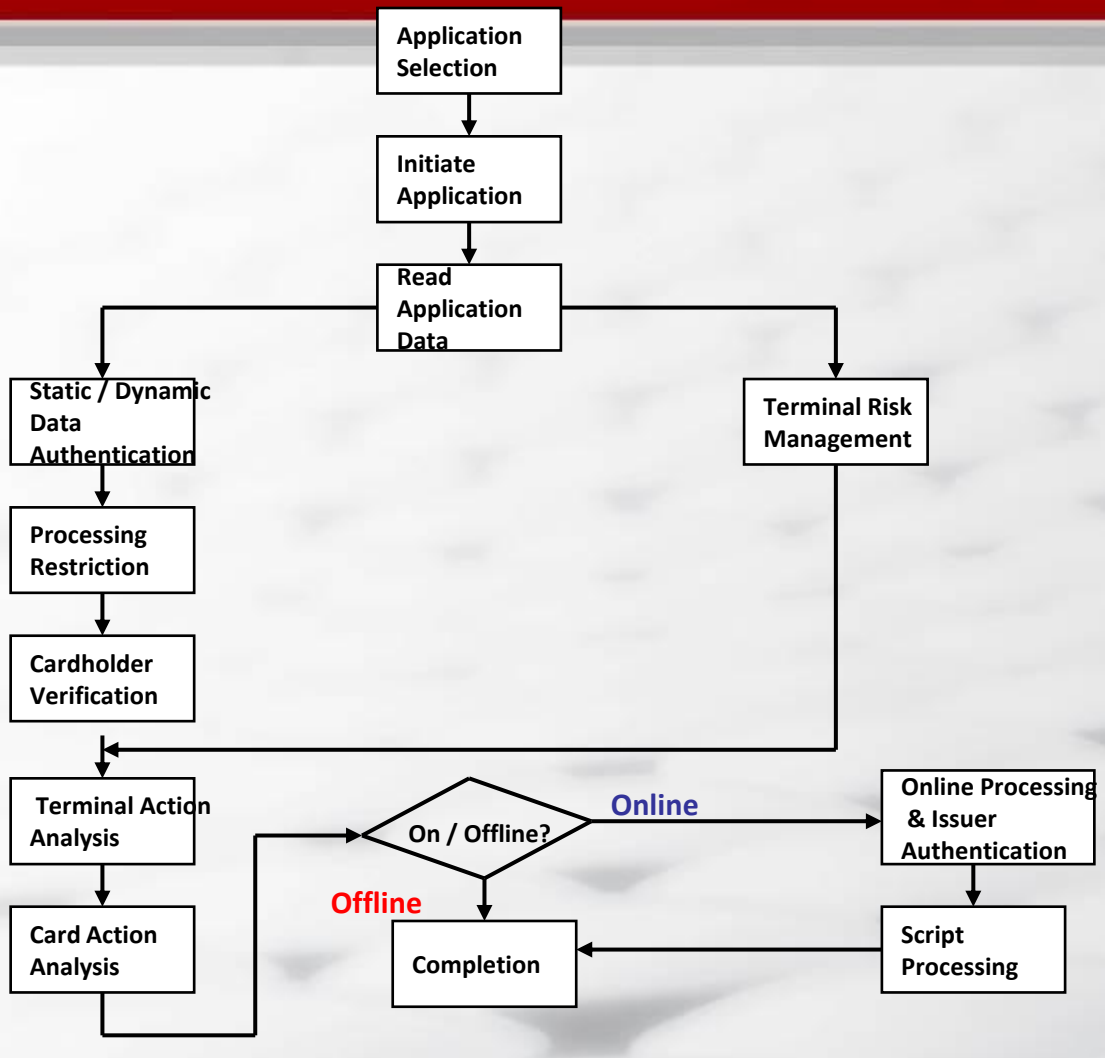
Europay, Mastercard or Visa Requirements

- Acquirer Parameters - Transaction Log - Communication Protocol	- Parameters - Authorization Format - Specific Functions	- Transaction Sequence - Interface

EMV Terminal Application

EMV

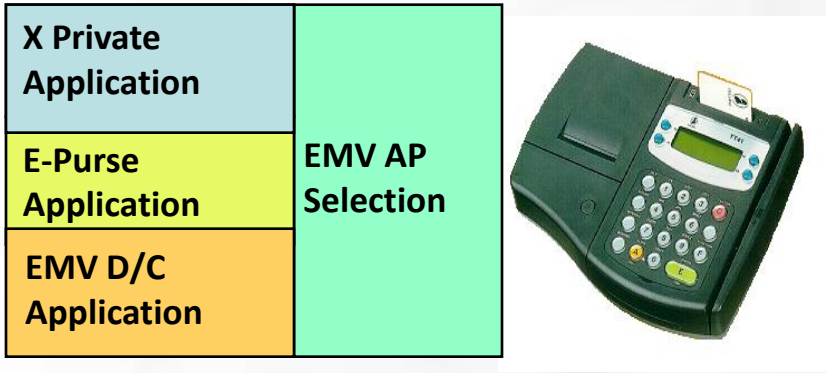
EMV Terminal Transaction Flow

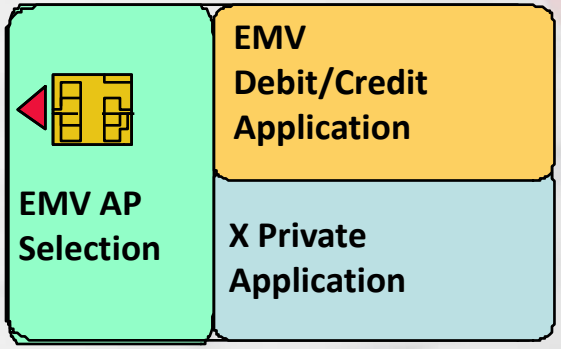


Transaction Functional Blocks

- Application Selection
- Card Authentication
- Cardholder Identification
- Authorization / Acceptance of Transaction
- Script Processing

Application Selection



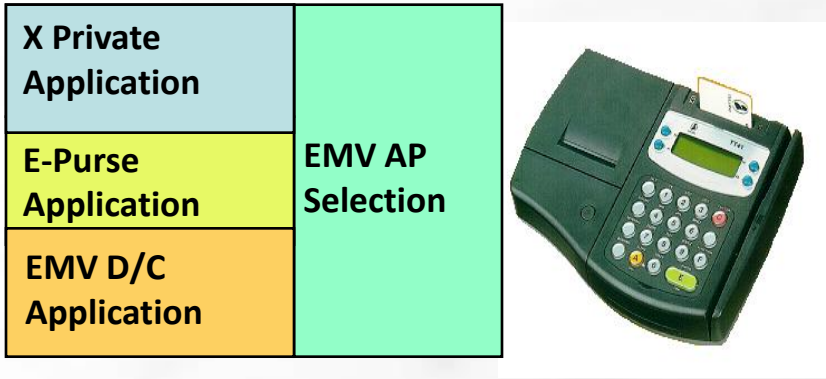


1. What applications do you have ?

2. I have the EMV D/C application and the X Private Application

3. I only know the EMV D/C application and I select the EMV D/C application.

Application Selection

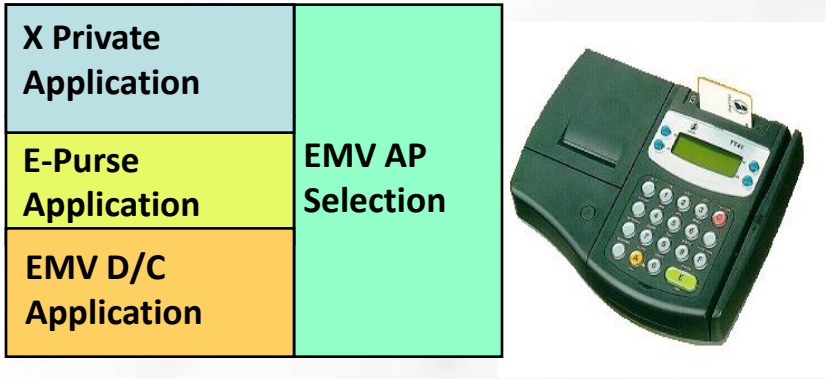


1. What applications do you have ?

2. I have the EMV D/C application and the E-Purse Application

3. I know both but you have priority over the EMV D/C application and therefore I select the EMV D/C application.

Application Selection



1. What applications do you have ?

2. I have the EMV D/C application and the Y Private Application

3. I know both applications but the cardholder has chosen EMV D/C, therefore I select EMV D/C.

EMV Card Capabilities

- Authorization Controls
- Cardholder Verification Methods
- Usage Controls
- Authentication
- Dynamic Data Updates
- Exception Handling
- Multiple Functions

Authorization Controls

- Issuer-defined authorization parameters are based on the risk associated with the transaction type or the POS environment (eg. online authorization, purchase limit and offline transaction counters).
- The chip authorizes the offline transaction.
- Offline authorization reduces fraud and lower costs.
- The issuer may establish default online / offline modes depending on the product or account.
- The offline default may trigger the online mode based on:
  - Reaching a preset limit to the offline activity (time / amount limit)
  - First time use
  - Type of transaction (eg. cashback)
  - Conditions at the POS (eg. PINpad failure)

Usage Controls

The chip manages card use based on conditions at the point of transaction using parameters and the processing power of the chip.

- Geographic
  - Restrict to domestic / international
- Transaction
  - Restrict usage to local goods & services, ATM, goods & services for international transactions, etc.
- Inactive or expired accounts
  - Force online or decline transaction
- Ceiling value of cash or cashback transaction
- Maximum transaction amounts allowed
- Restricted usage based on merchant type or terminal type

Authentication

The chip enables a set of risk management tools, which combat fraud involving cryptology & logical comparison between the transaction and card data, to verify the legitimacy of the card and the host.

- Offline data authentication to prevent fraudulent or altered data
- Online card authentication to detect counterfeited card
- Issuer authentication for dynamic data update
- Transaction certificate to provide information confirming that actual steps and processes are performed by the card, the terminal and the merchant during a given transaction.

Risk management tools control fraud & provide information that ensure integrity of card transactions.

Dynamic Data Update

Data inside the chip can be updated at the POS without reissuing the card, thus providing convenience to both the cardholder and issuer, and enhancing risk control.

- Blocking an application or the entire card
- Unblocking an application or the entire card
- Resetting the PIN-try counter
- Changing the upper consecutive offline limit
- Changing the lower consecutive offline limit

Exception Handling

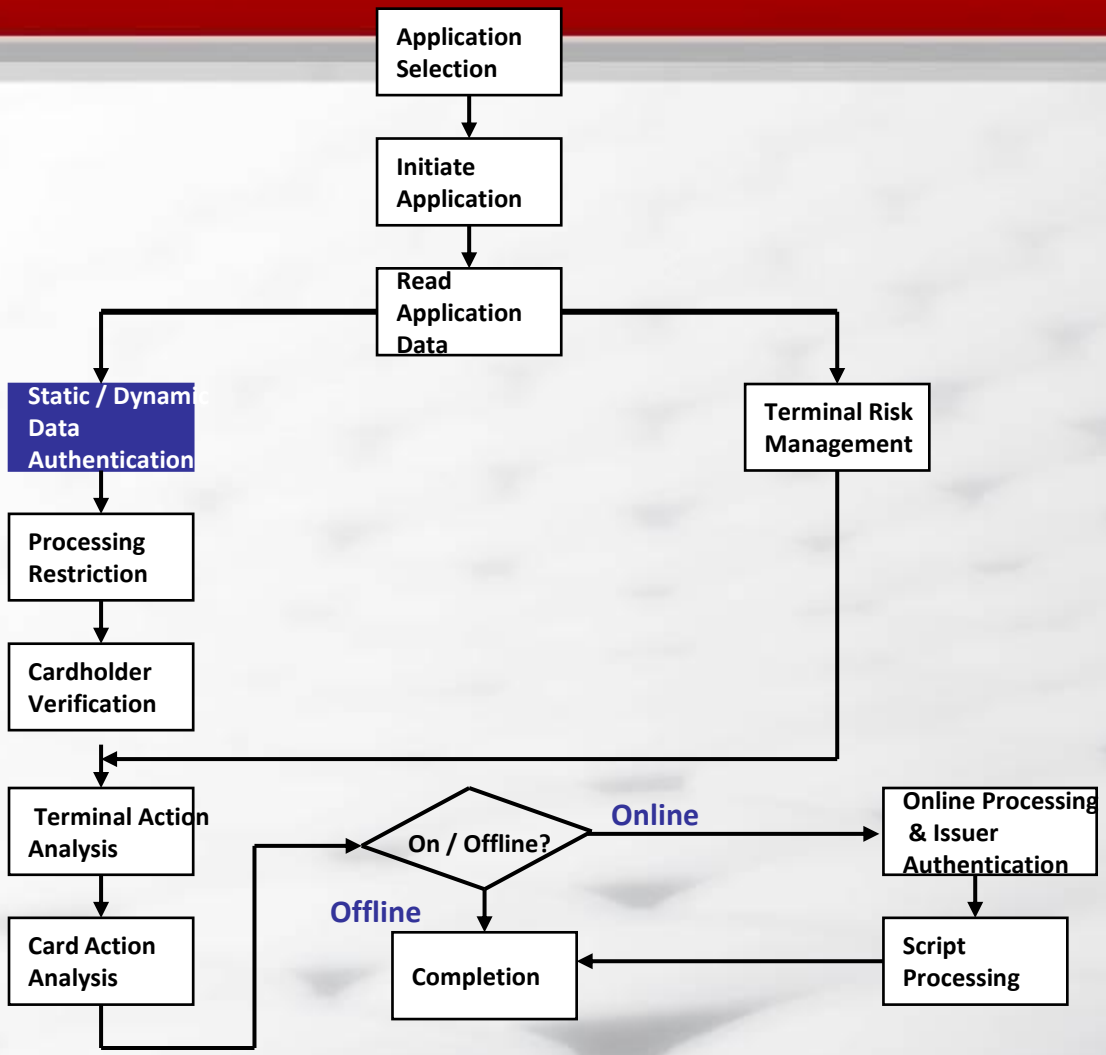
- On-line inoperative
  - The issuer can designate in the card a maximum number of offline transactions when the online processing is no longer operative.
- PIN-try limit exceeded
  - The issuer has the ability to allow more tries under certain circumstances.
- Terminal fault
  - Merchants can accept transactions using magnetic stripe.
- Network fault
  - The processor is allowed to edit the transaction.

This feature provides issuers with greater flexibility to customize payment services on the basis of their risk assessment.

Multiple Function

- The chip can store information about multiple functions.
- The chip can communicate with various devices to allow the selection of different applications at the point of transaction.
- The magnetic stripe can provide access to other services. (eg. ATM)
- It is possible to use the chip for other applications. (eg. loyalty, electronic purse, membership card, etc.)

EMV Terminal Transaction Flow



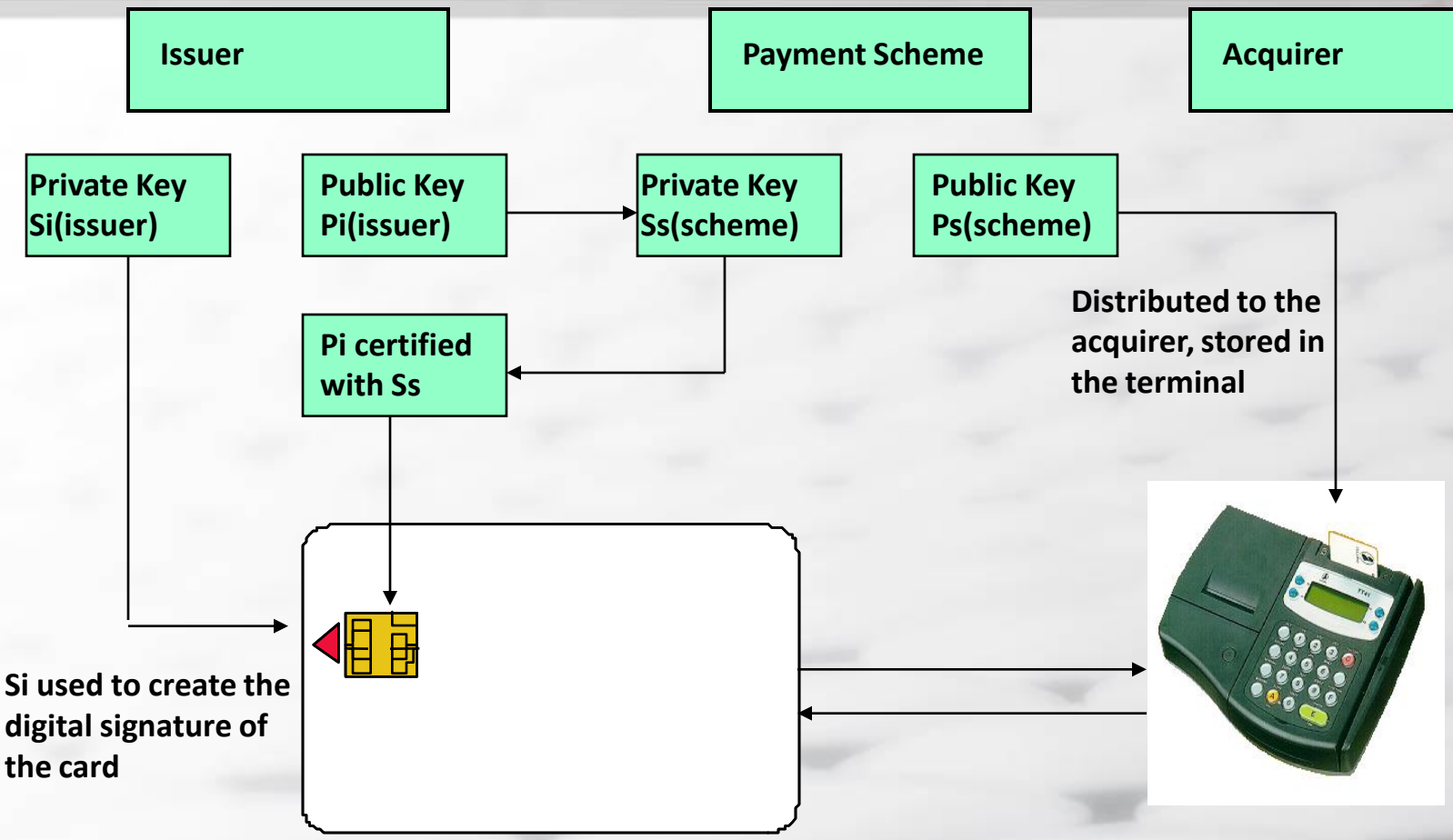
Card Authentication Issues

- Problem of an international environment (eg. problem of sharing secrets)
- Authenticating a Taiwanese EMV card, for instance, in a Japanese terminal
- No direct link established between the card issuer and the terminal application
- Public key cryptography as a solution to this problem

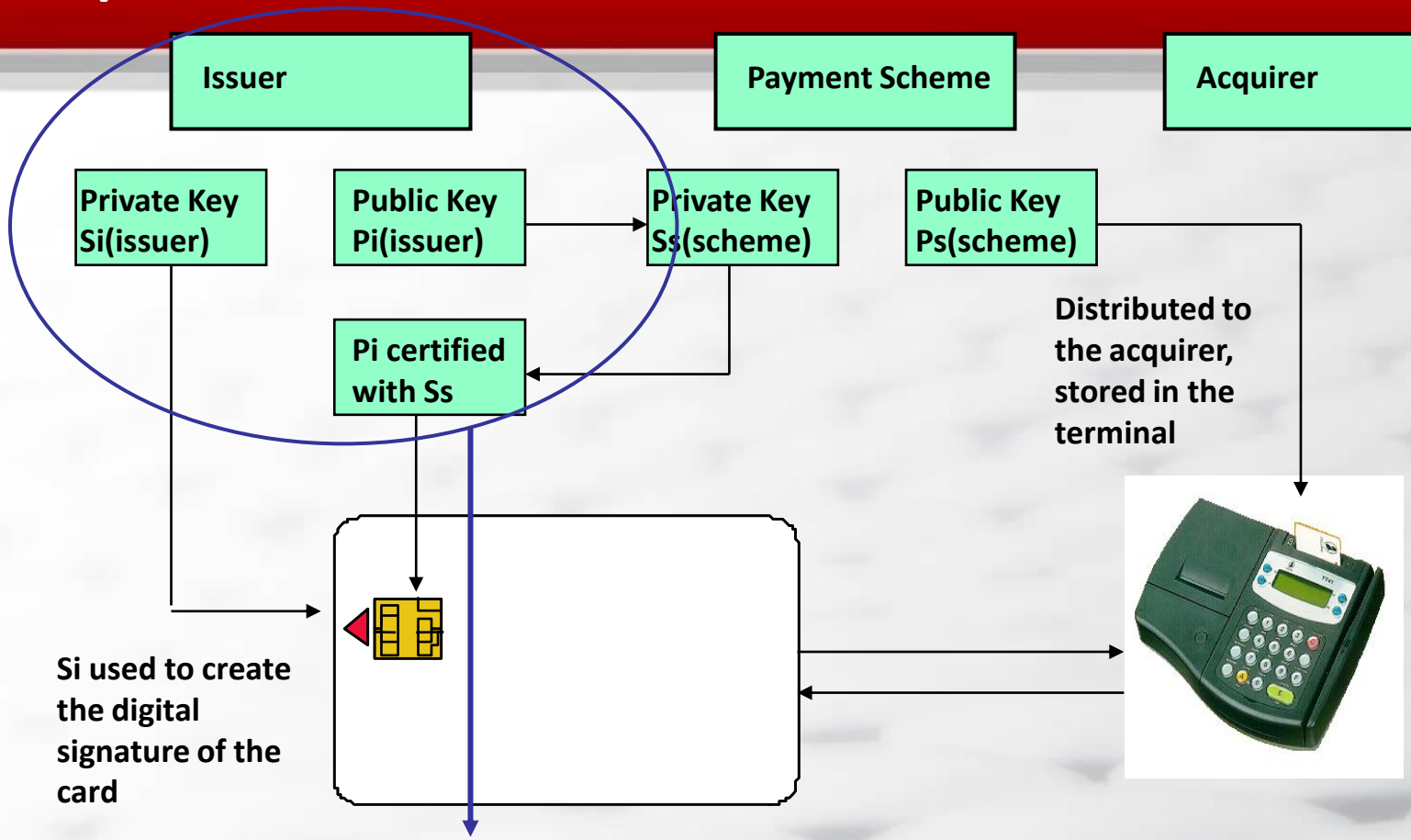
Static/Dynamic Data Authentication

- Public key cryptography (RSA) requires a public/private key pair to be generated by the payment scheme and the issuer.
- The owner of the private key is the **only one** who can sign the message.
- The public key is known to everyone, and hence able to authenticate the author of the message.

Static Data Authentication (SDA)

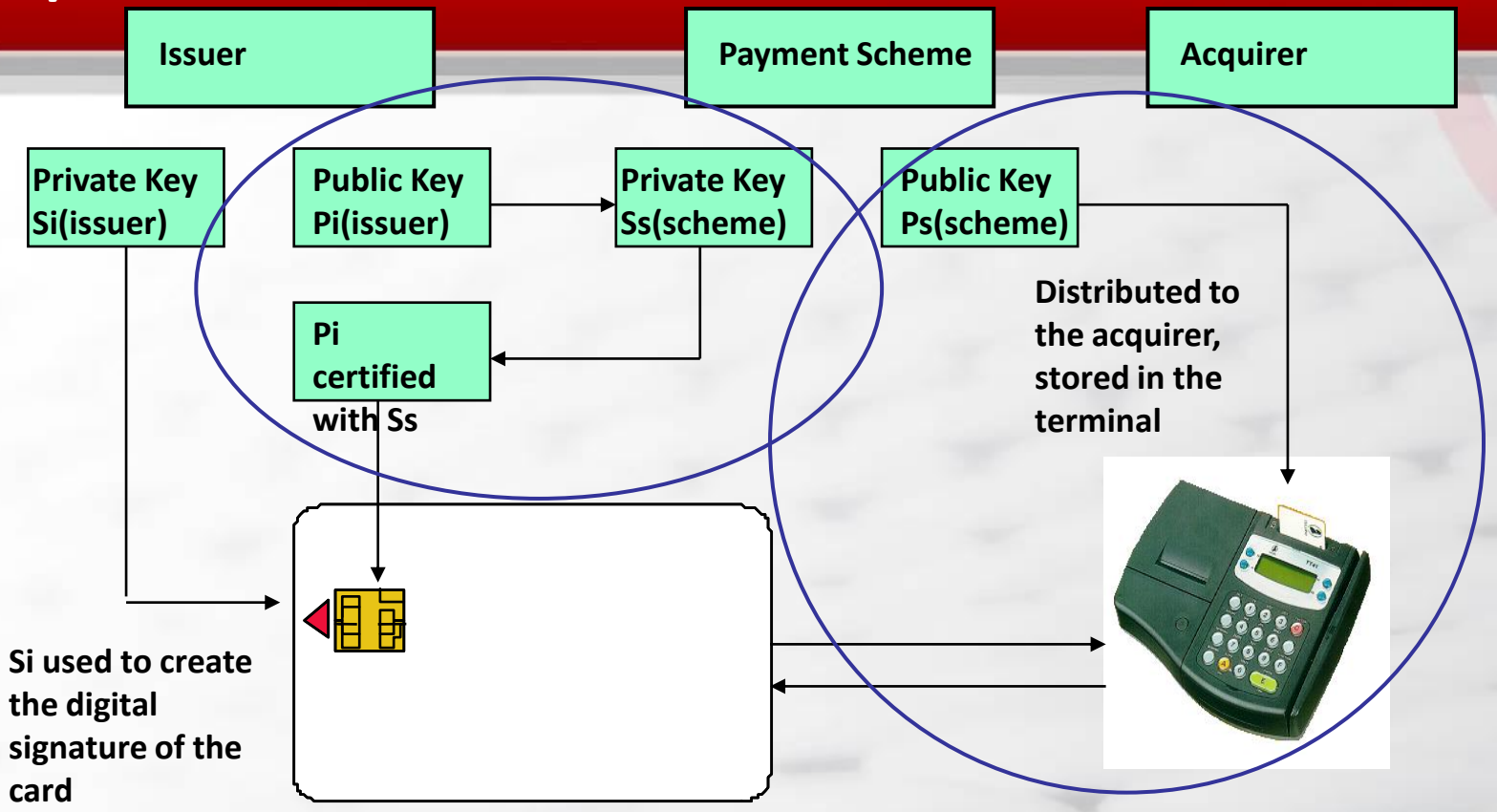


Step 1: Certification of Pi



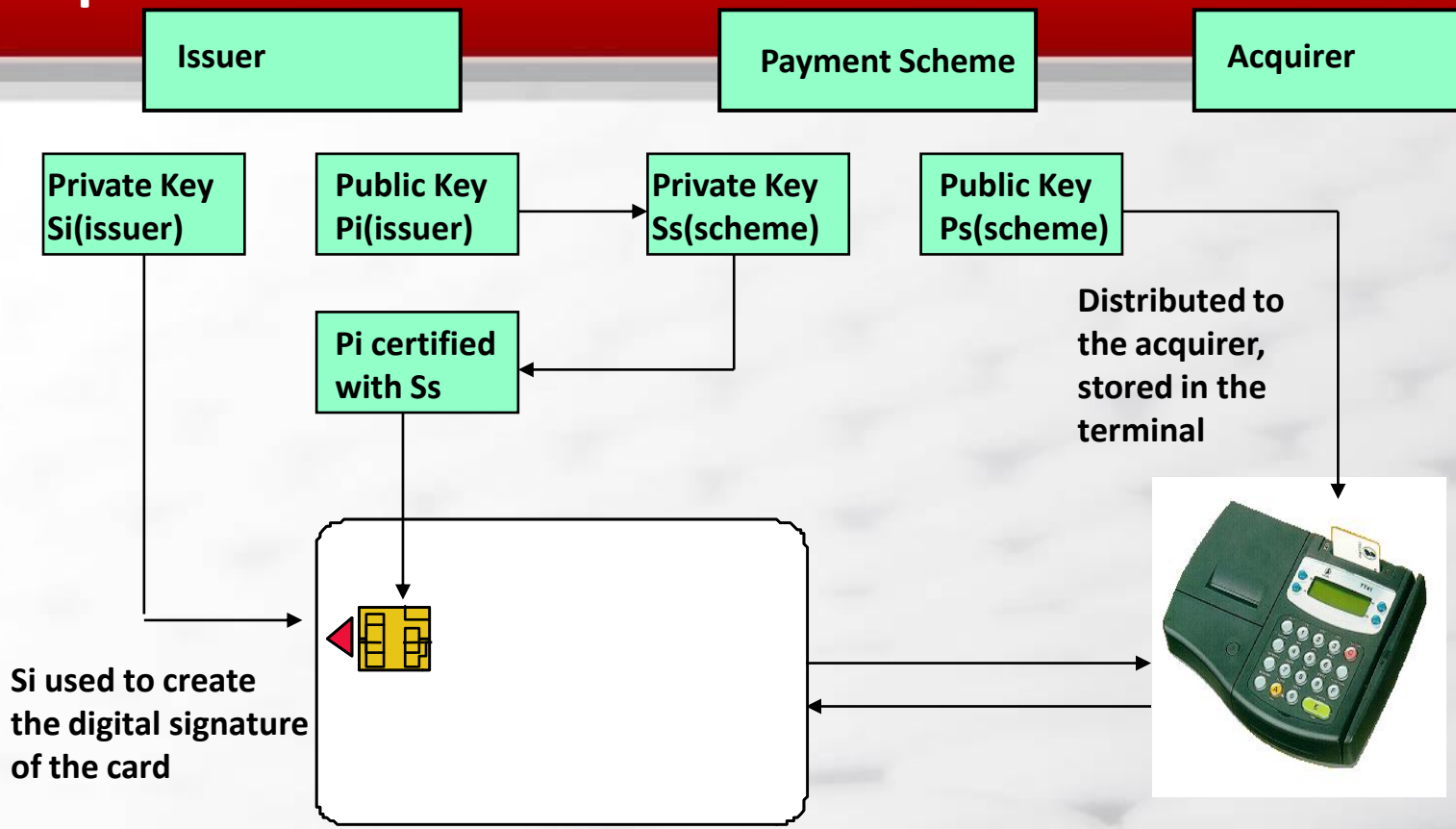
- The issuer certifies the card.
- The issuer stores the result (SDA) in the card.

Step 2: Personalization



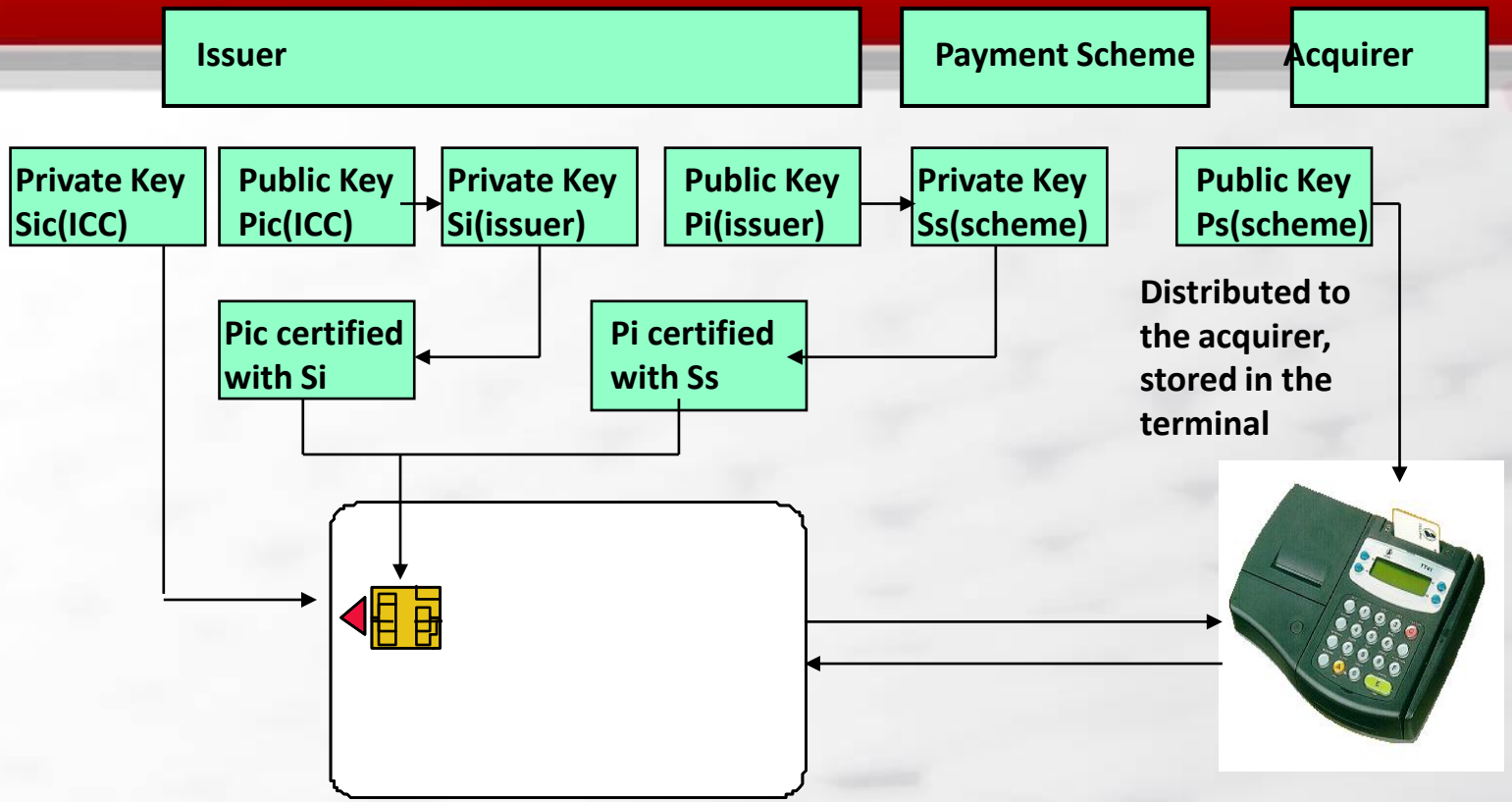
- The payment organization acts as a certification authority.
- The payment organization's Ss is used to certify the issuer's Pi.

Step 3: Authentication



- The terminal verifies the Pi certificate to ensure issuer authenticity.
- The terminal then verifies the data certificate to ensure card authenticity.
- The proof of card authenticity is **static**.

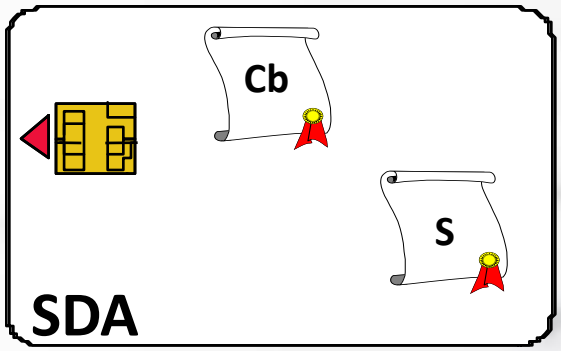
Dynamic Data Authentication (DDA)

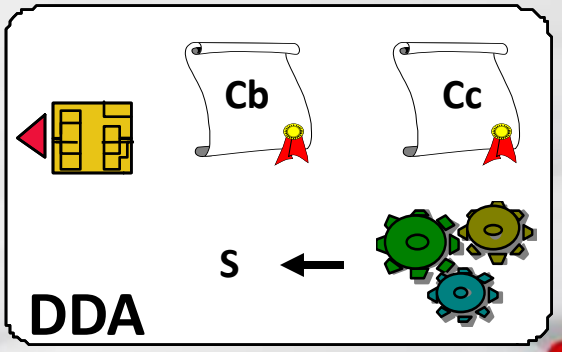


- Payment organization certifies the issuer
- The issuer certifies the card
- The card **dynamically** proves its authenticity to the terminal

Card Authentication

- SDA is the storage of:
  - A certificate for issuer authentication
  - A digital signature for card authentication
- DDA is storage of:
  - A certificate for issuer authentication
  - A certificate for card authentication
- Dynamic generation of signature for authentication

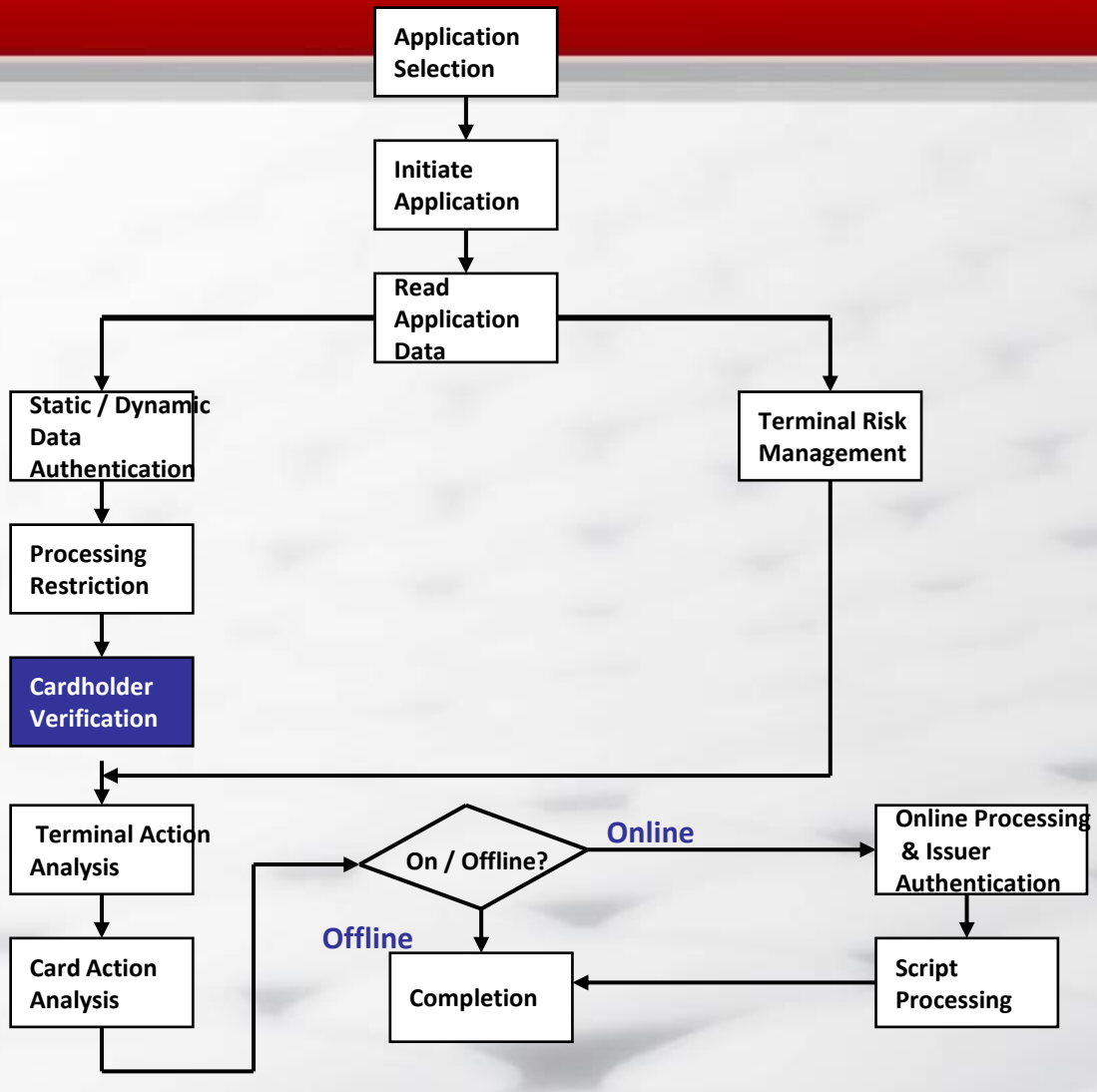




DDA

- RSA calculation needs a smart card with a cryptographic co-processor.
- The time it takes to produce a digital signature (1024 bits) is approximately 800 ms.

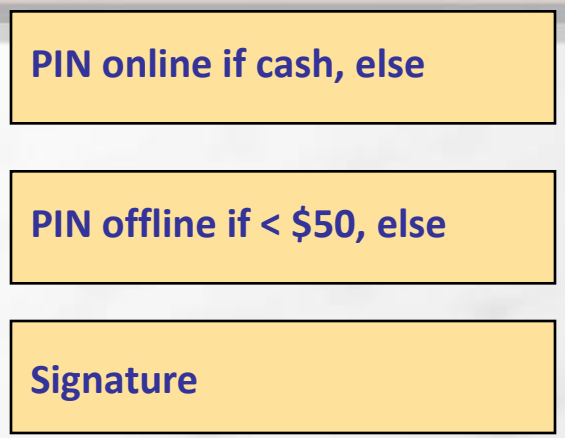
EMV Terminal Transaction Flow



Cardholder Verification

- The issuer defines a method and the conditions for identification.
- The terminal executes according to the agreed methods and conditions.
- Confirmation of holder identity (photo) & acceptance of the transaction (signature panel) occurs.
- Offline PIN verification is done by comparing it with the PIN in the chip.
- Encrypted online PIN verification is done by the host.
- The PIN is optional and dependent on issuer market requirements, merchant segments and terminal types.
- The chip stores and processes issuer instructions on which CVMs are to be used in different situations.
- This process enhances security and improves issuer control.

Cardholder Verification Example



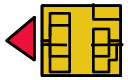
- PIN Online if the transaction is cash
- Otherwise, PIN offline if the transaction < $50
- Otherwise, paper signature if the PIN offline is incorrect

Offline Cardholder Identification

Plain

Verify PIN 1233

PIN OK!



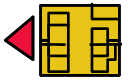
PIN 1234 = Card PIN?

Ciphered

Verify PIN "#$&@"

PIN OK!

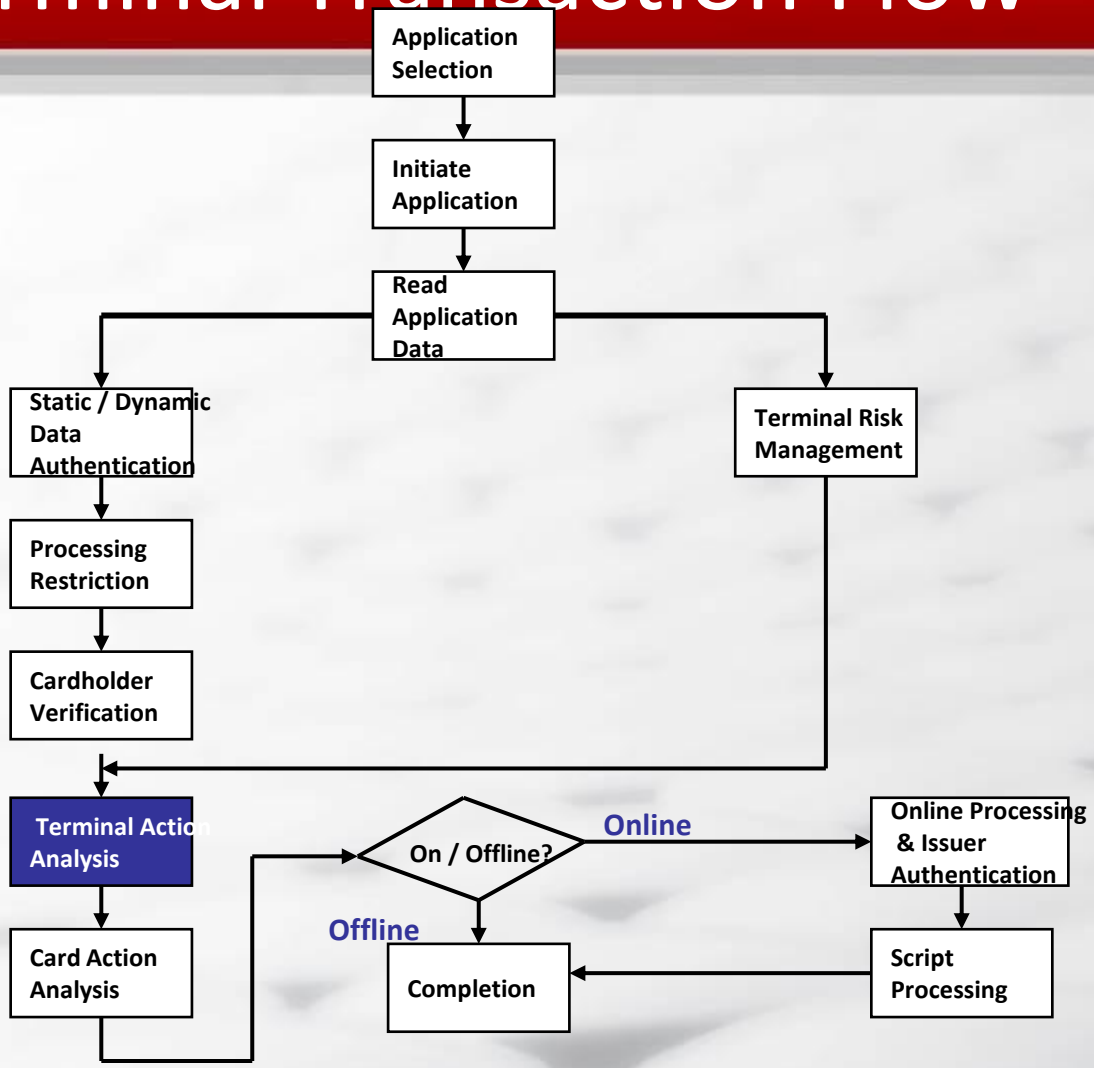
Deciphering #$&@



Equals Card PIN?

- Ciphering 1234 = #$&@

EMV Terminal Transaction Flow



Transaction Authorization/Validation

- Acquirer Risk Management
- Terminal's Decision
- Card's Decision
- Issuer Risk Management

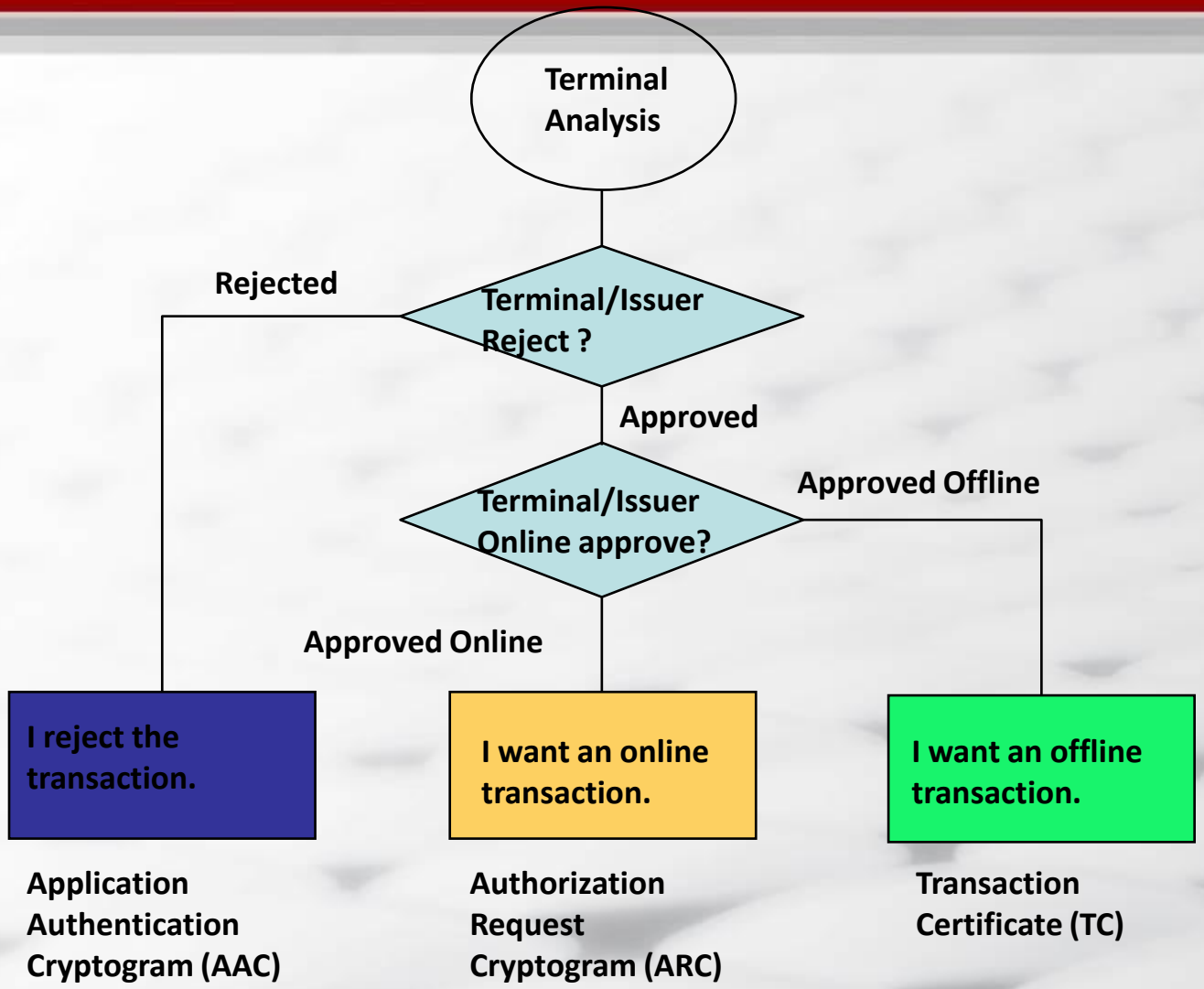
Acquirer Risk Management

- Terminal risk management is defined by the acquirer.
- It consists of:
  - Checking floor limit: compare with the transaction amount
  - Random transaction selection: to perform transaction online
  - Velocity checking: after a number of consecutive offline transactions, the transaction should go online depending on consecutive limits, cumulative total, international limits, dual currency amount and limits

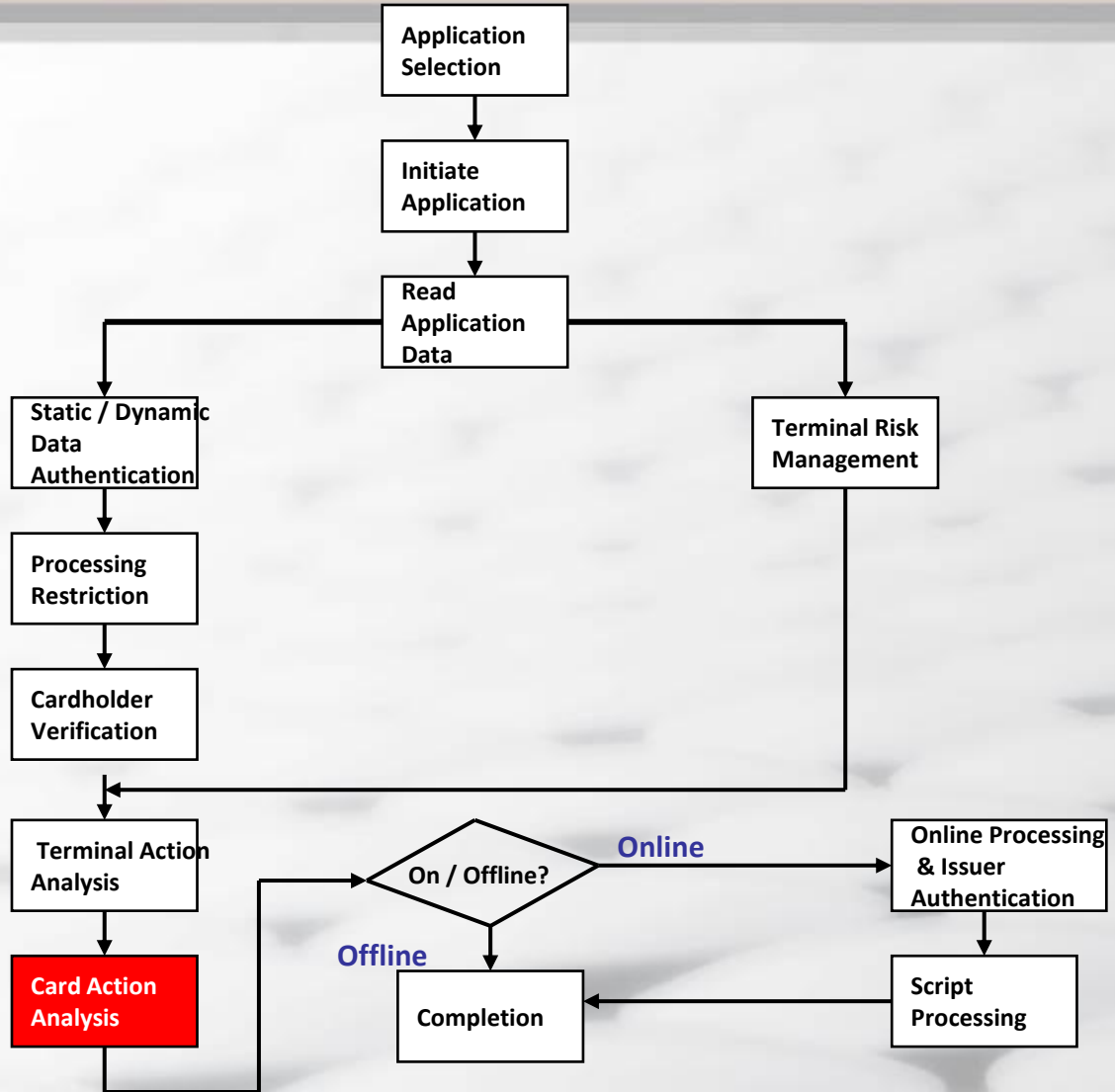
Terminal Decision

- Analyze the result of previous functions.
  - Card authentication result
  - Cardholder identification result
  - Acquirer risk management result
- Based on the result, a joint acquirer-issuer decision is made.

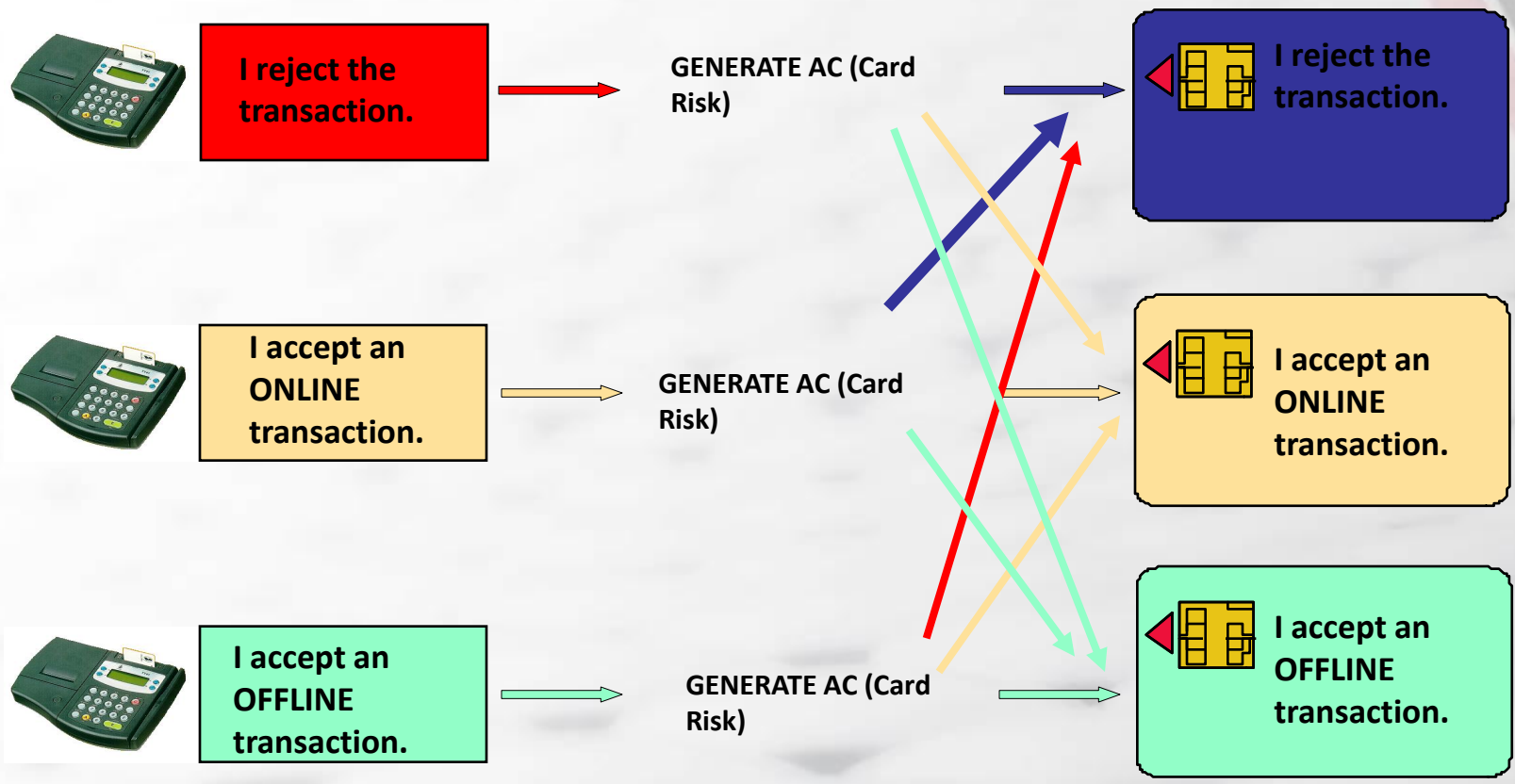
Terminal Action Analysis



EMV Terminal Transaction Flow



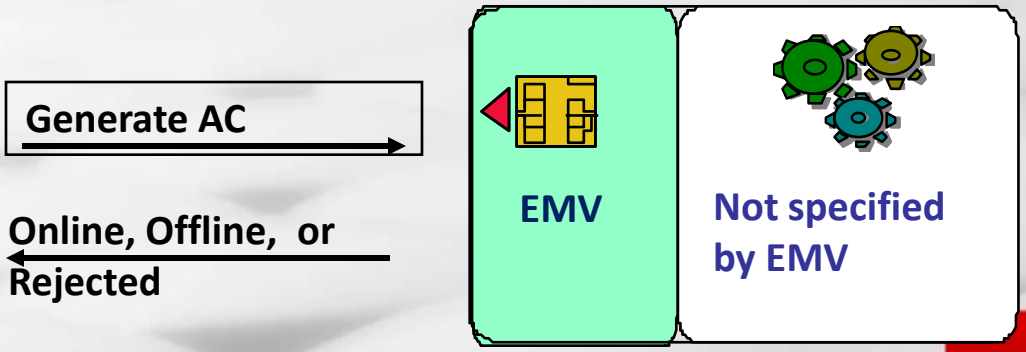
Card Action Analysis



- The card performs its own risk management (not specified by EMV) and makes the final decision.

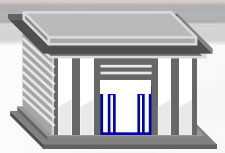
Issuer Risk Management

- Performed by the Generate AC Command
- Issuer decides its own rules
- Examples of possible rules:
  - Counting total consecutive number of offline transactions
  - Counting total consecutive amount of offline transactions
  - Incorrect identification of cardholder
  - Verification of previous transaction
  - And more…



Script Processing Mechanism

Card Issuing Bank 1



ISSUER

Direct link between the card & the issuer

Risk Management Rules

Online if:

- **Transaction > $40**
- **Every 3 offline transactions**

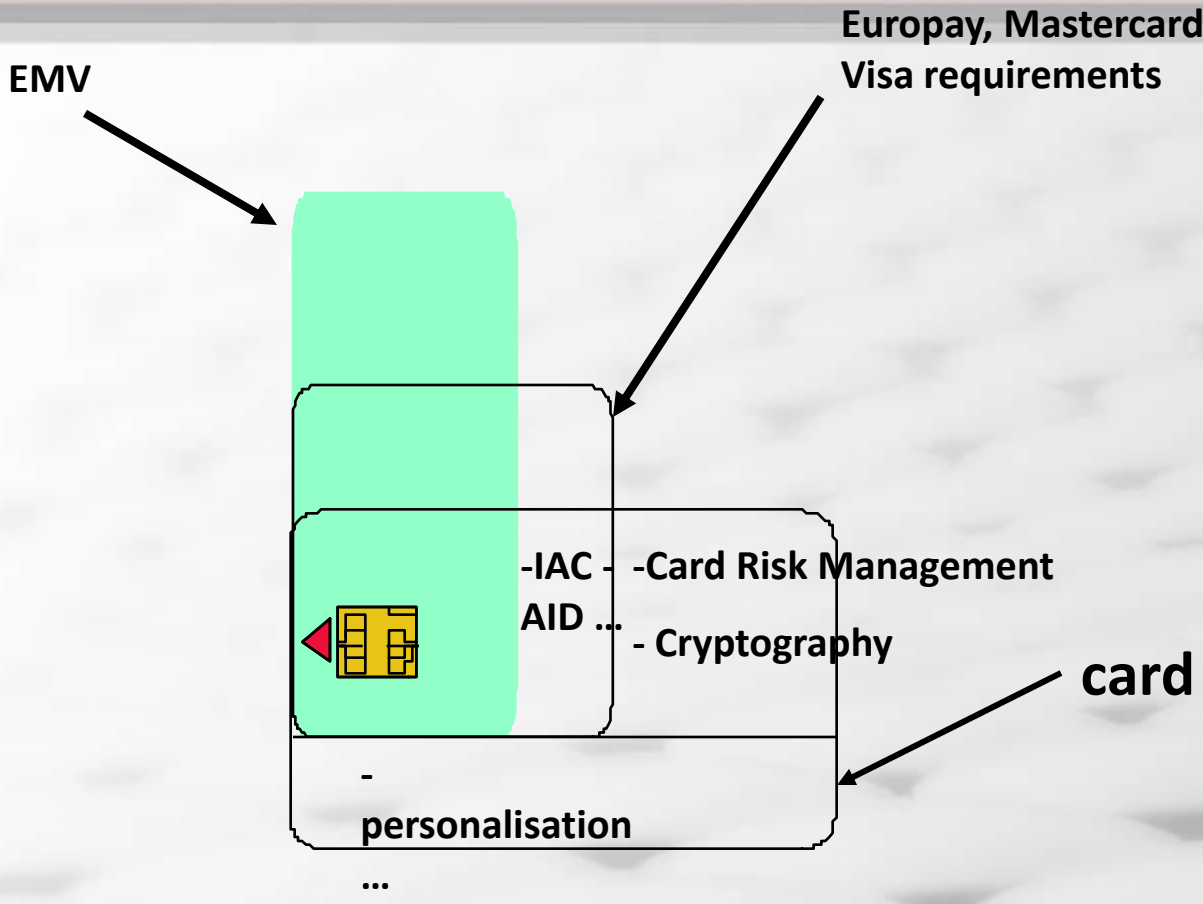
Bank 2 Country 2 Terminal

Bank 1 Country 1 Card

Script Processing Mechanism

- Allows issuer to be in contact with their cards during online transactions
- Independence of country and acquirer
- To do what?
  - Change card parameters
  - Blocking and unblocking of application
  - And more…

EMV Card Application



EMV '96

- ICC Specifications for Payment Systems
  - Part 1: Electromechanical Characteristics, Logical Interface and Transmission Protocols
  - Part 2: Data Elements and Commands
  - Part 3: Application Selection
  - Part 4: Security Aspects

EMV '96

- ICC Terminal Specification for Payment Systems
  - Part 1: General Requirements
  - Part 2: Software Architecture
  - Part 3: Cardholder, Attendant & Acquirer Interface
- ICC Application Specification for Payment Systems

Card Specification

Prerequisite documents to understand Part 1: ISO-7816 1,2,3

- Essentially the EMV implementation of ISO-7816 parts 1,2,3
- Defines Answer To Reset (ATR) characters
- Requires a warm reset if ATR is different
  - Possible migration from proprietary/national system to co-exist with EMV without modification of existing systems (eg. Taiwan FISC, Singapore CashCard, etc.)
- Allows the card to support either the T=0 or T=1 protocol
- Does not require Vpp

Card Specification

Prerequisite document to understand Part 2: ISO-7816-4,6

- Defines all data objects (more than 100)
- Data objects are in TLV format
- Can be a primitive data object (eg. TLV or a constructed data object like TL(TLV)..(TLV))
- Defines the range of the SFI (file name) to be used
- Defines the EMV command set
- And more...

EMV Card Commands

8x 1E	Application Block
8x 18	Application Unblock
8x 16	Card Block
0x 82	External Authentication
8x AE	Generate Application Cryptogram
0x 84	Get Challenge (added in EMV2000)
8x CA	Get Data
8x A8	Get Processing Options
0x 88	Internal Authentication
8x 24	PIN Change / Unblock
0x B2	Read Record
0x A4	Select
0x 20	Verify
8xDx, 8xEx,9xxx, Exxx	Reserved

Application Selection

- Terminal cold reset card; If not an EMV card, warm reset
- SELECT PSE DDF name = 1PAY.SYS.DDF01
- Read FCI using Get Response
- Read DIR EF SFI using READ RECORD
- Read supported applications using READ RECORD & match supported applications
- Select the highest priority application supported by the terminal using the SELECT command on the ADF

Data Elements for Financial Transaction

- ICC data objects are stored in:
  - Fixed sized records
  - Variable size records
- All objects are in TLV format.

Primitive data object:

Tag (1 or 2 bytes)	length (1 byte)	value

Constructed data object:

TL	(TLV)(TLV) . . . (TLV)

The value field of a constructed object (TLV)(TLV) . . . (TLV) is called a template.

Tag Structure

- Primitive object tag – 0x,4x,5x,8x,9x,Cx,Dx
- Constructed object tag – 2x,3x,6x,7x,Ax,Bx,Ex,Fx
- 2 bytes tag – odd F (eg. 7Fxx, 9Fxx)
- Tag is always within the range of 1F to 7F

Examples of Data Objects

Tag	Length	Value
5F24	3	Application Expiry Date
5A	10	Application Primary Account Number
8C	Variable	Card Risk Management Data Object List 1
8D	Variable	Card Risk Management Data Object List 2

The above are mandatory data objects.

Examples of Data Objects

Tag	Length	Value
8F	1	Certification Authority Public Key Index
90	40-128	Issuer Public Key Certificate
93	40-128	Signed Application Data
92	1-34	Issuer Public Key (Remainder)
9F32	1-32	Issuer Public Key (Exponent)

The above are static data authentication data objects.

Record Data Object

- Record in SFI 1 – 10 must be in BER-TLV.
  - SFI 1 to 10 is governed by the EMV specification.
  - SFI 11 to 20 is proprietary data of payment systems.
  - SFI 21 to 30 is proprietary data of the issuer.
- The tag of a record data object is 70, indicating that it is a constructed data object.
- The Application File Locator (AFL) indicates files & records used for transaction processing.

Data Object Existence

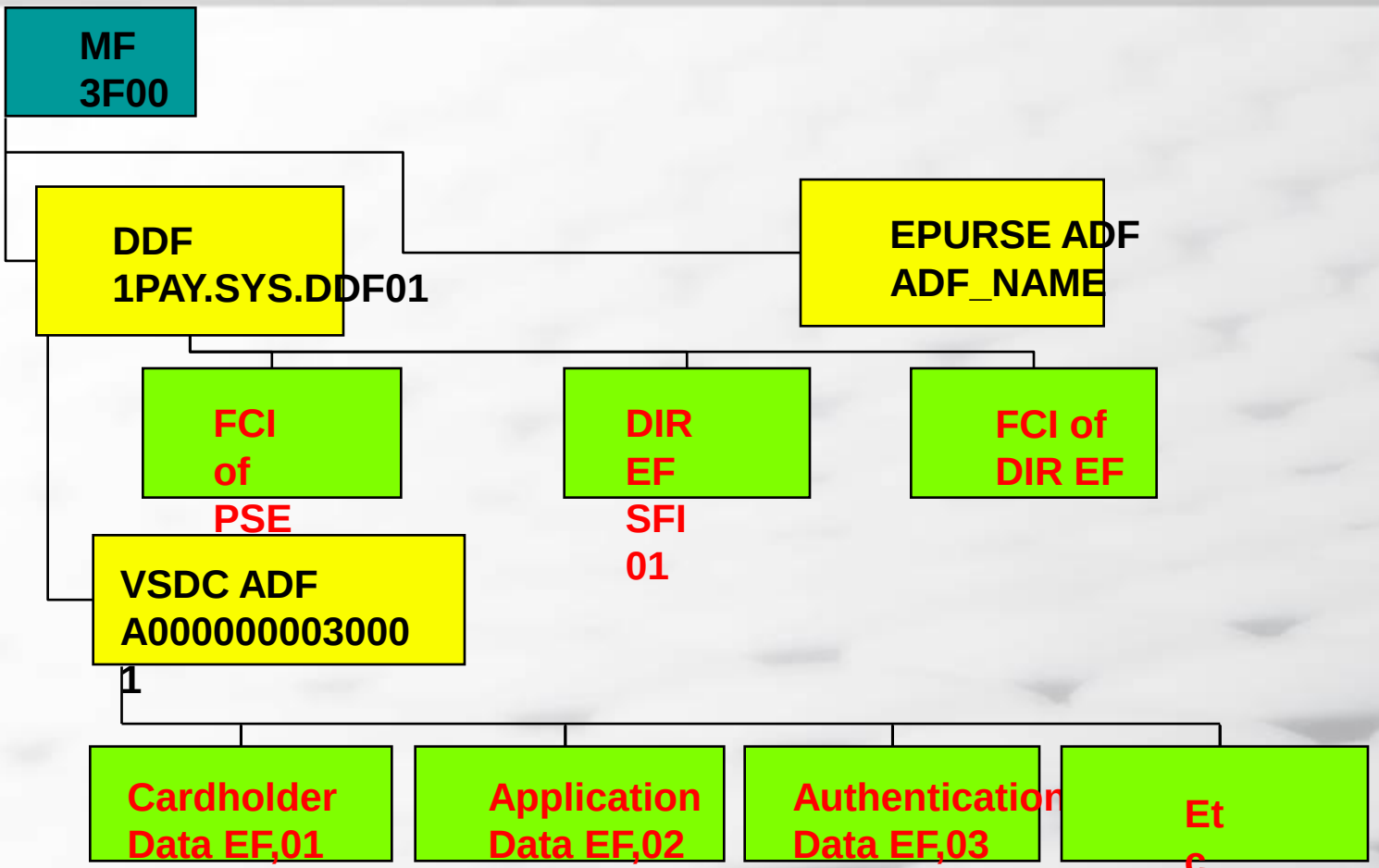
- M = Mandatory, must be present to allow terminal transaction processing
- R = Required, terminal should not terminate transaction if not received
- C = Conditional, necessary under certain conditions
- O = Optional, necessary under certain conditions

R and C are defined by Visa in the VSDC Requirements for Common Personalization document

IC Card Structure

- MF : Master File, equivalent to root directory
- DF : Dedicated File, equivalent to sub-directory
- EF : Elementary File, equivalent to a data file; also called AEF or Application EF
- DIR File : EF containing a list of applications supported by the card
- DDF: Directory Definition File
- ADF : Application Definition File, contains a list of AEF's for this application

EMV Card Organization



- ***PSE is usually also the MF.***

DIR EF

- An EF residing inside a DDF
- SFI must be between 1 to 10, where value is in DDF FCI
- Used in the Application Selection process
- Each entry is a record of the Application Template (tag 61)
- An Application Template is a constructed object

Tag	Length	Value	Presence
4F	5-16	ADF name (AID)	Mandatory
50	1-16	Application Label	Mandatory
9F12	1-16	Application Preferred Name	Optional
87	1	Application Priority	Optional

DIR EF Content

70h	15h to 2Fh	61h	13h to 2Dh	4Fh	05h to 10h	AID of Application,5 to16 bytes (M) eg A000 0000 0310 1001 = Visa Credit A000 0000 0310 1002 = Visa Debit
				50h	01h to 10h	Application Label, up to 16 bytes (M)

9F12h	01h to 10h	Application Preferred Name, (O) Up to 16 bytes
87h	01h	Application Priority Indicator,1 byte (O)

73h	04h	CEh	02h	EFID of application's DF, 2 bytes (O)

70h = template proprietary to this application
61h = application template

DDF

- Implemented as a DF inside the card
- Mandatory to have the 1PAY.SYS.DDF01 DDF, the Payment System Environment (PSE)
- Get Response after Select DDF returns the FCI template
- A template is a constructed data object
- One implementation of FCI uses a transparent EF inside the DF to store the Get Response content

PSE DDF FCI

Tag	Value	Presence
6F	FCI Template	Mandatory
84	DF Name	Mandatory
A5	FCI Proprietary Template	Mandatory
88	SFI of DIR EF	Mandatory
5F2D	Language Preference	Optional
9F11	Issuer Code Table Index	Optional
9F3B	Application Reference Currency	Optional
BF0C	FCI Issuer Discretionary Data	Optional
XXXX	Additional object as in book 3	Optional

Other DDF FCI

Tag	Value	Presence
6F	FCI Template	Mandatory
84	DF Name	Mandatory
A5	FCI Proprietary Template	Mandatory
88	SFI of DIR EF	Mandatory
BF0C	FCI Issuer Discretionary Data	Optional
XXXX	Additional object as in book 3	Optional

ADF

- Implemented as a DF inside the card
- Can have many ADFs, with one ADF per application (eg. Credit Card, Electronic Purse, etc.)
- Each ADF entry can be found in the DIR EF of the 1PAY.SYS.DDF01
- The Application Priority byte indicates:
  - Application selected without holder's confirmation
  - Application selected with holder's confirmation
  - The priority of the selection from 1(highest) to 15 or none
  - Catered for RFU (reserved for future use)

ADF FCI

Tag	Value	Presence
6F	FCI Template	Mandatory
84	DF Name	Mandatory
A5	FCI Proprietary Template	Mandatory
87	Application Priority Indicator	Mandatory
9F38	Processing Options Data Object List	Optional
BF0C	FCI Issuer Discretionary Data	Optional

Interchange

- EMV specifications only define:
  - The structure
  - The commands to access files
  - Data objects
- The issuer will map the appropriate data objects to files (SFI 1-10) according to their needs, BUT in compliance with the rules
  - Linear FREE READ, but may be a conditional UPDATE
  - Each record is limited to 254 bytes, including tag & length
  - Each record is a constructed data object, tag 70
- AFL defines the file & record required for application processing, a response from Get Processing Options.

Cardholder-related Data File

Tag	Value	Presence
5F24	Application Expiry Date	M
5A	Application PAN	M
5F25	Application Effective Date	O
5F34	Application PAN Sequence Number	O
5F20	Cardholder Name	O
9F0B	Cardholder Name Extended	O
5F28	Issuer Country Code	O
5F30	Service Code	O
9F1F	Track 1 Discretionary Data	O
57	Track 2 Equivalent Data	O
9F20	Track 2 Discretionary Data	O

Application-related Data File

Tag	Value	Presence
8C	Card Risk Management Data Object List1	M
8D	Card Risk Management Data Object List2	M
9F05	Application Discretionary Data	O
9F07	Application Usage Control	O
9F08	Application Version Number	O
9F14	Lower Consecutive Offline Limit	O
9F23	Upper Consecutive Offline Limit	O
8E	Cardholder Verifcation Method List	O
97	Transaction Certificate DOL	O
9F0D	Issuer Action Code - Default	O
9F0E	Issuer Action Code - Denial	O
9F0F	Issuer Action Code - Online	O

Application-related Data File

Tag	Value	Presence
9F42	Application Currency Code	O
9F44	Application Currency Component	O
9F4A	Static Data Authentication Tag List	O

Static Data Authentication Data File

Tag	Value	Presence
8F	Certification Authority Public Key Index	M
90	Certified Issuer Public Key	M
93	Signed Application Data	M
92	Issuer Public Key Index	O

VEE – Visa Easy Entry

- Quick, easy and cost-effective implementation of ICC programs
- Infra-structure supporting future ICC products
  - Multiple applications
  - Global interoperability
  - Co-existence with non-Visa programs
  - Avoidance of confusion
- And more…

VEE – Visa Easy Entry

- Complies with ICC Specification Part 1
- Complies with ICC Specification Part 3 - Application Selection
- Supports a card file with 1 record
  - Track 2 data
  - Track 1 - Cardholder name and track 1 discretionary data
- Complies with the EMV data coding scheme
- Processes transactions using a message format identical to the current magnetic transaction
- **No longer in use**

VSDC Card

- Can be a native card (eg. conventional chip operating system powered type of card)
- Can also be a Global Platform Java Card

Data Preparation before Personalization

- Issuer public key certificate, remainder, exponent
- Signed static application data
- Uniquely Derived Key (derived from PAN and protected by Key for card authentication)
- MAC Derived Key
- ENC Derived Key
- Offline PIN

3 Alternatives for VSDC

- Quick Start data elements in VSDC
- Jump Start data elements in VSDC
- Full data elements in VSDC

What QuickStart **Cannot** Do

- Velocity Checking
- Static Data Authentication
- Dynamic Data Authentication
- Script Processing
- Offline PIN
- Offline

What Jump Start **Cannot** Do

- Velocity Checking
- Dynamic Data Authentication
- Script Processing
- Offline PIN
- Offline

Data Elements in VSDC

- Magnetic Stripe Image (MSI)
- Authorization Control (AuthC)
- Static Data Authentication (SDA)
- Dynamic Data Authentication (DDA)
- Online Card / Issuer Authentication (CAM / IAuth)
- Issuer Script for Post Issuance Update(IS)

Possible VSDC Templates

Template

1. Magnetic Stripe Image
2. Authorization Control
3. Enhanced Cardholder Verification Method (PIN)
4. Offline Static Data Authentication (SDA)
5. Online Card and Issuer Authentication (CAM)
6. SDA, Offline PIN, and Authorization Controls
7. SDA, Offline PIN and CAM
8. SDA, Offline PIN, CAM, and Authorization Controls
9. SDA, CAM, and Authorization Controls
10. Offline Dynamic Data Authentication (DDA)
11. Post Issuance Updates (Issuer Script – IS)

Application Interchange Profile (AIP)

- Card indicates processing capabilities
- Returns via Get Response after Get Processing Options APDU
- Returned data – domestic & international AIP, AFL:
  - Tag 80, L=var AIP (2 bytes) AFL(n*4bytes)
  - Tag 80, L=var AIP (2 bytes) AFL (n*4bytes)

AIP Definition:

Byte 2 Bit 4 = Terminal Risk Management

Byte 2 Bit 3 = Issuer Authentication

Byte 2 Bit 2,1 = RFU

Byte 1, Bit 8-1 = RFU

Byte 2 Bit 4 = Terminal Risk Management

Byte 2 Bit 3 = Issuer Authentication

Byte 2 Bit 2,1 = RFU

Byte 1, Bit 8-1 = RFU

VSDC Template & AIP

VSDC Template	X	SDA	DDA	Cardholder_ Verification	Terminal_Risk_ Management	Issuer_Authetication	
1. MSI	0	0	0	1	1	0	00 00000000
2. Authorization Control	0	0	0	1	1	0	00 00000000
3. Enhanced CVM (PIN)	0	0	0	1	1	0	00 00000000
4. SDA	0	1	0	1	1	0	00 00000000
5. Online Card & Issuer Auth (CAM)	0	0	0	1	1	1	00 00000000
6. SDA, Offline PIN & Authorization	0	1	0	1	1	0	00 00000000
7. SDA, Offline & CAM	0	1	0	1	1	1	00 00000000
8. SDA, Offline, CAM & Auth Control	0	1	0	1	1	1	00 00000000
9. SDA , CAM & Auth Control	0	1	0	1	1	1	00 00000000
10. DDA	0	1	1	1	1	0	00 00000000
11. Post Issuance Update (IS)	0	1	0	1	1	1	00 00000000

Application File Locator - AFL

- Each AFL is a 4 byte-pointer
  - First byte – SFI
  - Second byte – record # of first record (r1) to be read
  - Third byte – record # of last record (r2) to be read
  - Fourth byte – number of consecutive records involved in the SDA starting from r1

Questions?