EMV Series

Byte 3: Commands & Transaction Flow

https://www.youtube.com/c/LearnPayments

Disclaimer

- This presentation was prepared was prepared for presenting the YouTube video ”EMV – Byte 3 – Commands & Transaction Flow”
- This material is intended for educational/study purposes only and cannot be copied, published or disseminated without prior approval from “Learn Payments” channel (learn.payments.2020@gmail.com)

Table of Contents

1

Commands

Intro, Terminal-ICC commands

2

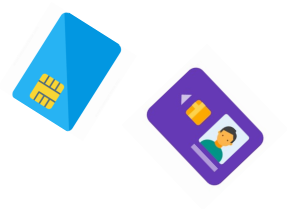
Transaction Flow

Steps & Commands

https://www.youtube.com/c/LearnPayments

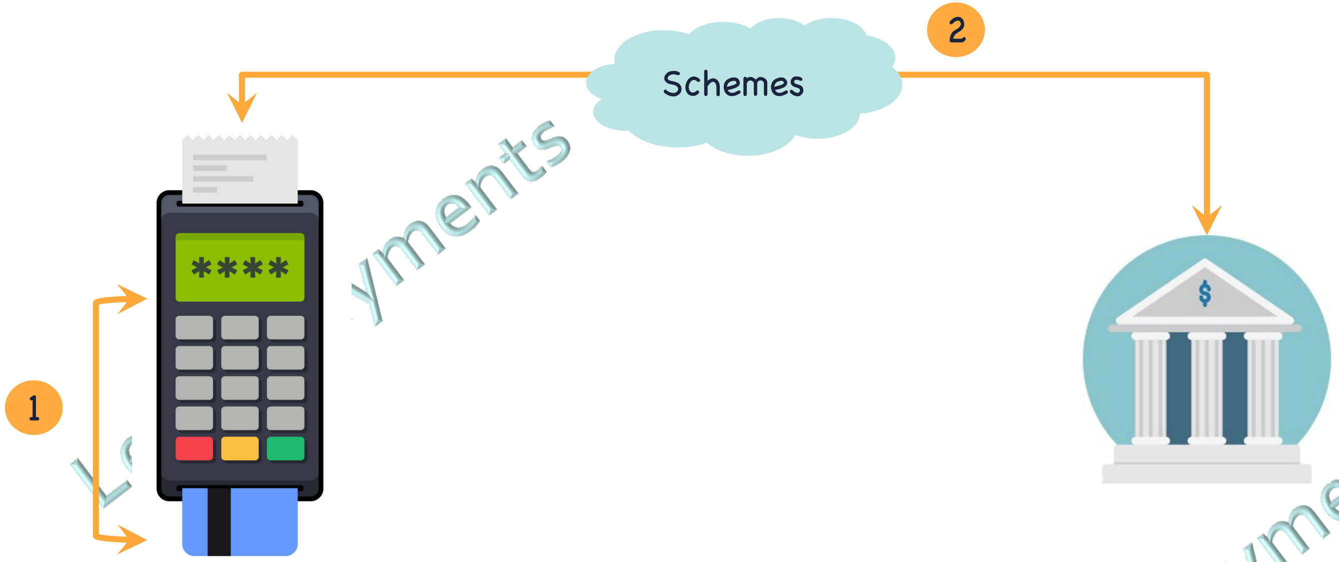
Section 1: Commands

What is a Command?



- Terminal a.k.a IFD (Interface Device) a.k.a CAD (Card Acceptance Device)
- ICC itself is a passive device, and Terminal powers ICC
- Command is a message sent by Terminal to the ICC which initiates an action
- Commands can be to execute to,
  - Extract/Modify the contents in the Chip OR
  - Generate/Verify cryptogram OR
  - Verify/Change PIN

Commands



Other is Post Issuance commands, where Issuer can send commands in authorization response to,

- Issuer can block the Card/Application
- Update data on Chip

Quick glance of Commands

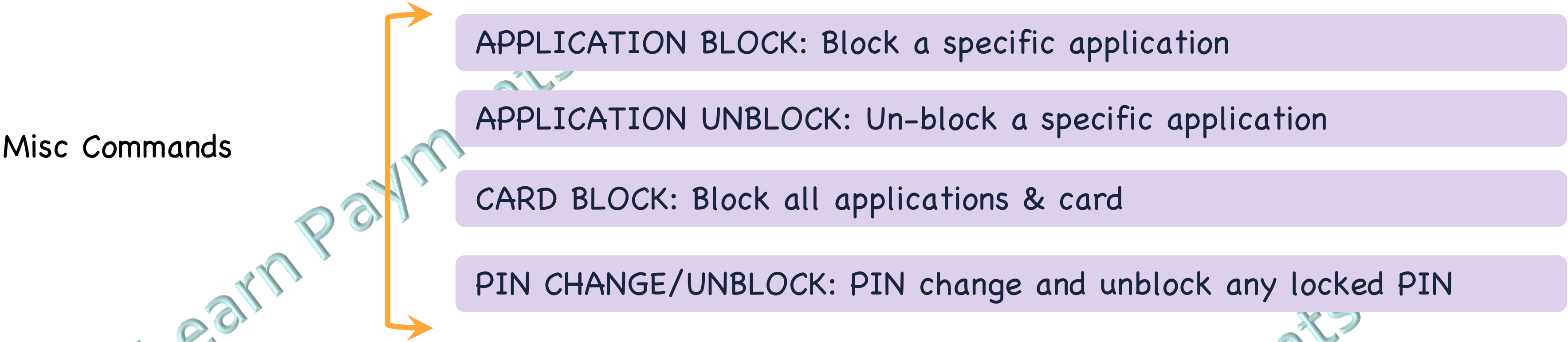
Generic Commands

- SELECT: Select File (AEF, ADF etc.) or Application
- READ RECORD: Reads the record data from the AEF

Using during transaction

- GET DATA: To get the ATC, PIN try counter
- GET PROCESSING OPTIONS: Data that Card requires from Terminal
- GENERATE APPLICATION CRYPTOGRAM: Generates ARQC
- EXTERNAL AUTHENTICATE: Authenticates the app data from Issuer
- INTERNAL AUTHENTICATE: Used for generation of DDA
- GET CHALLENGE: Obtain an Unpredictable number
- VERIFY: Verify the PIN (for Offline PIN)

Quick glance of Commands



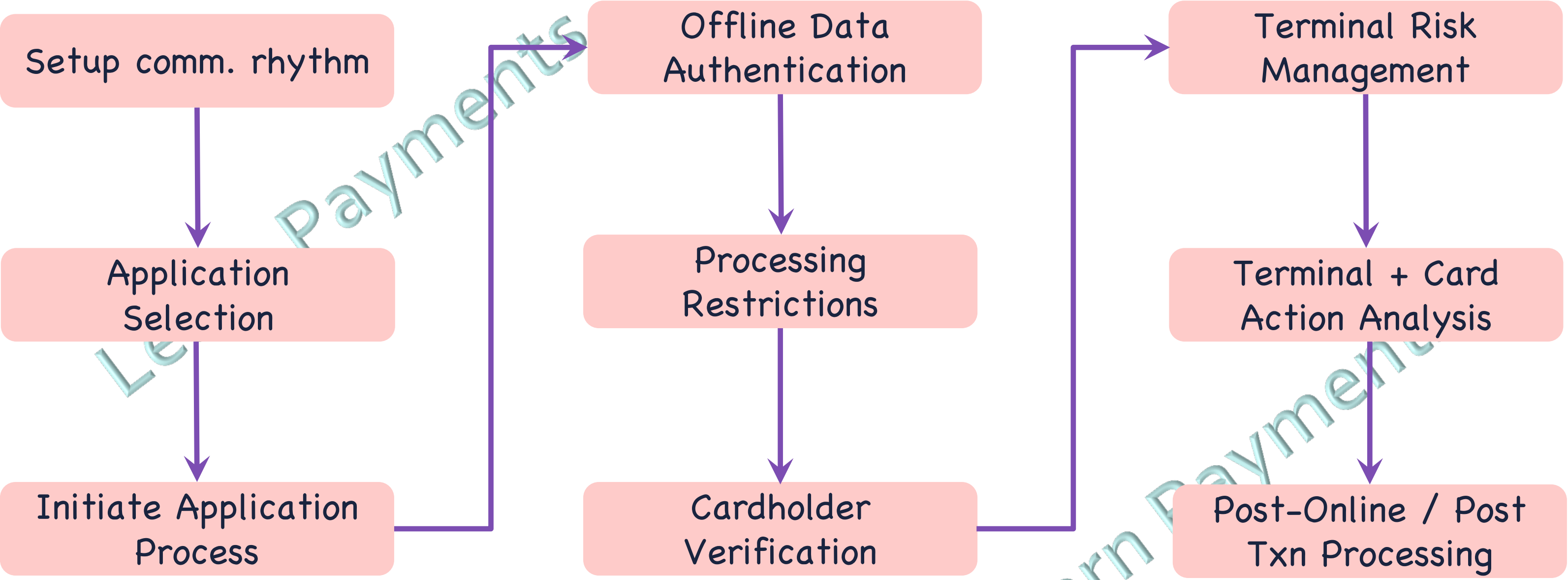
Misc Commands

- APPLICATION BLOCK: Block a specific application
- APPLICATION UNBLOCK: Un-block a specific application
- CARD BLOCK: Block all applications & card
- PIN CHANGE/UNBLOCK: PIN change and unblock any locked PIN

- These are also called as Post-Issuance commands, sent by the Issuer with the Authorization (Transaction) response.
- Terminal receives them and passes it on to Chip to execute them

Section 2: Transaction Flow

Tnx Flow


Setup comm. rhythm
Application Selection
Initiate Application Process
Offline Data Authentication
Processing Restrictions
Cardholder Verification
Terminal Risk Management
Terminal + Card Action Analysis
Post-Online / Post Txn Processing

https://www.youtube.com/c/LearnPayments

Setup comm. rhythm

Answer to Reset (ATR)

- Power is supplied to the card from the terminal
- Card will respond to Terminal with an ATR
- It contains,
  - Transmission techniques
  - Clock rate
  - Maximum current

Application Selection

Step 1	Terminal reads the DDF file from the Chip (1PAY.SYS.DDF01) using a “**SELECT**” command
Step 2	Using the DDF file, read all the application details using “**READ RECORD**” commands
Step 3	For every “READ” check if the application in the Chip matches with the application supported by Terminal
Step 4	Build a final “Candidate List” of applications supported by Terminal & Chip
Step 5	• Terminal can choose the first application in the candidate list • Select application based on priority list (“**Application Priority Indicator** er App) • Provide list to customer for selection

Initiate Application Process

- Marks beginning of a new transaction
- Using the "**GET PROCESSING OPTIONS**" the terminal passes the data requested in the "**PDOL – Processing Data Object List**" (Terminal Type, MCC etc.)
- Chip decides if the application is permitted or not
  - If permitted, Chip provides details of the Application called "**Application Interchange Profile**" & the "**Application File Locator**" which corresponds to Application
  - There can be cases, where transaction is not permitted, and the transaction is terminated.

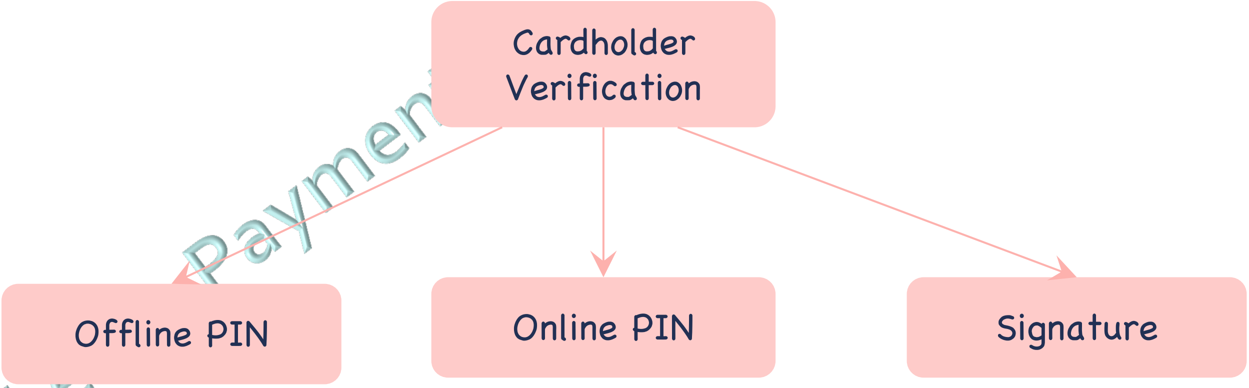
Offline Data Authentication

- Card Authentication to ensure the authenticity of the Card
- 3 major methods
  - Static Data Authentication (SDA): Static data put in by the Issuer, which gets validated by the terminal
  - Dynamic Data Authentication (DDA): Card generates a dynamic data which gets validated by the terminal
  - Combined DDA (CDA): Like DDA, but it also generates a Cryptogram

Processing Restrictions

- Terminal checks for the validity of,
  - Compatibility of "<u>Application Version Number</u>"
  - "Application Usage Control" – Checks validity for
    - Domestic or International – Cash/Goods/Services
    - Valid for ATMs and other Terminals
  - Checks for validity of "<u>Application Effective Date</u>" and "<u>Application Expiry Date</u>"

Cardholder Verification



Cardholder Verification

Offline PIN

Online PIN

Signature

- “**<u>VERIFY</u>**” command

- PIN captured and passed to Issuer

- Signature on Receipt

Cardholder Verification

- Chip can maintain “CVM List” which allows CVM rules
  - Transaction Amount
  - Transaction Type
  - CVM Method
  - Example:
    - Set a rule which requests PIN for ATM cash transactions
    - Do an Offline PIN verification if the transaction amount is less than ₹100
- Terminal parses thru CVM list and matches appropriate CVM method and executes it

Terminal Risk Management

- Prevent Fraudulent transactions by forcing transactions to go online based on following risk parameters
  - Floor Limits: Terminal Maintains a “Floor Limit”. If same Cardholder/Card has performed transaction amount (Current+Prev) greater than the Terminal Floor Limit, then transaction is forced online
  - Velocity Limits:
    - Ensure after a certain offline transactions, the transaction forced online mandatorily
    - Terminal gets the ”Last Online ATC” and “ATC” using “GET DATA” command
    - If difference > Consecutive Offline Limit, go online
    - (There are 2 offline limits, Lower & Upper, Txns can not mandatorily be performed after Upper. Consecutive Offline Limit)

Terminal Action Analysis

- Terminal takes a decision where transaction should "Approved Offline", "Decline Offline" or "Go Online"
- Step is driven based on the post all the before mentioned steps' output
- Terminal & Issuer maintains "**Issuer Action Code**" & "**Terminal Action Code**"
- If decision is to,
  - Approve Offline: Terminal asks Chip to "**GENERATE AC**" and return a "**Transaction Certificate**"
  - Go online: Terminal asks Chip to "**GENERATE AC**" and return an "**Authorization Request Cryptogram (ARQC)**"
  - Decline Offline: Terminal asks Chip to "**GENERATE AC**" and return an "**Application Authentication Cryptogram (AAC)**"

Post Online & Post-Txn Processing

- Issuer responds to the transaction with "**IAD - Issuer Application Data**", which has "**Authorization Response Cryptogram (ARPC)**" which is sent to the Chip for validation using an "**EXTERNAL AUTHENTICATE**" command
- Issuer may provide "**Scripts**" as a part of the response which are executed

Thank YOU

https://www.youtube.com/c/LearnPayments