Byte 2: EMV Chip Application

(A Gentle) Introduction to Files & Data inside Chip

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

Disclaimer

- This presentation was prepared was prepared for presenting the YouTube video ”EMV – Byte 2 – EMV Chip Application – (A Gentle) Introduction to Files & Data Inside Chip”
- 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)

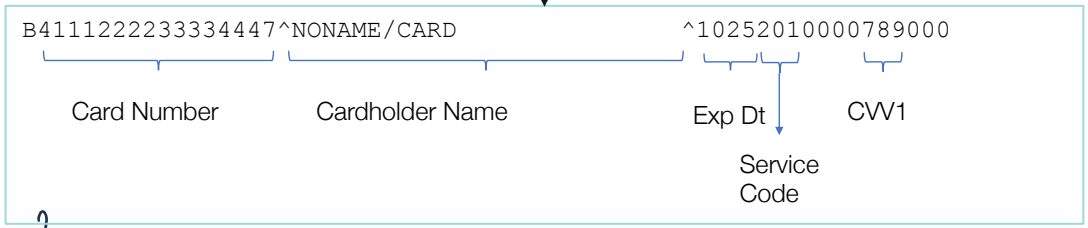
https://www.youtube.com/c/LearnPayments

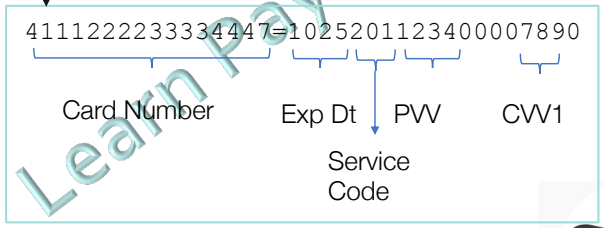
Table of Contents

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

Background: Magnetic Stripe

- One Card per Product (per Account or Scheme product)
- Minimal information storage
- Data format was not flexible
- Can not update after issuance





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

Background: Magnetic Stripe (contd.)

- "Card Authentication" means ensure that the card is a "valid" card
- "Cardholder Authentication" means ensuring cardholder is "valid"
- In case of Magnetic stripe,
  - Card Authentication is by <u>looks of card</u>
  - Cardholder Authentication is always <u>online using PIN</u> or Merchant verifies the Signature

Advantages of EMV

Memory more >16kb and allowing multiple records allowed to be stored in EMV chip Card

Flexible File Organization grouped by "Files", "Records" & "Data elements" in "BER-TLV Format"

EMV cards are devised to store multiple products (account/scheme in the form of "Applications")

Enhanced Card authentication using cryptography. Supports intelligent Cardholder Authentication

Limited records (bytes) of Info

Rigid standard for Data Representation

Only one card per product

Restrictive or Dependent Card & Cardholder Authentication methods

Section 1:
File Organization

What is Application?

An Application corresponds to a unique product.

Product here refers to Scheme products

Say if there is a MasterCard Credit card & Maestro debit card.

- MasterCard Credit Card has its own Application &
- Maestro's Debit Card has its own Application

Applications are referred by it's AID (Application Identifier).

Say MasterCard Credit Card is "A0000000041010"

Maestro Debit Card is "A0000000043060"

What is Application?

Application AID has 2 components

- RID (Registered Application Provider Identifier): This is unique to scheme
- PIX (Proprietary Application Identifier Extension): Number that unique identifies products within schemes

- Say MasterCard has RID = A000000004, Visa = A000000003

  Within MasterCard,

  Credit/Debit Card has PIX = 1010

  Maestro = 3060

  MasterCard Credit Card "A0000000041010"

  Maestro Debit Card "A0000000043060"

What is Application?


HDFC BANK
We understand your world

HDFC BANK

DATE :
MID :
TID : 41158929
BATCH NUM : 001259
INV. NUM : 044185
BILL NUM :
1070100016

Sale

512967******9069
Chip
EXP DATE : XX/XX
CARD TYPE : MASTERCARD
TXN ID : 2949455241
APP: HDFC BANK MC DC
AID: A0000000041010
TVR: 0000048000
TSI: E800
TC : 2D06D7CF6966BDAA

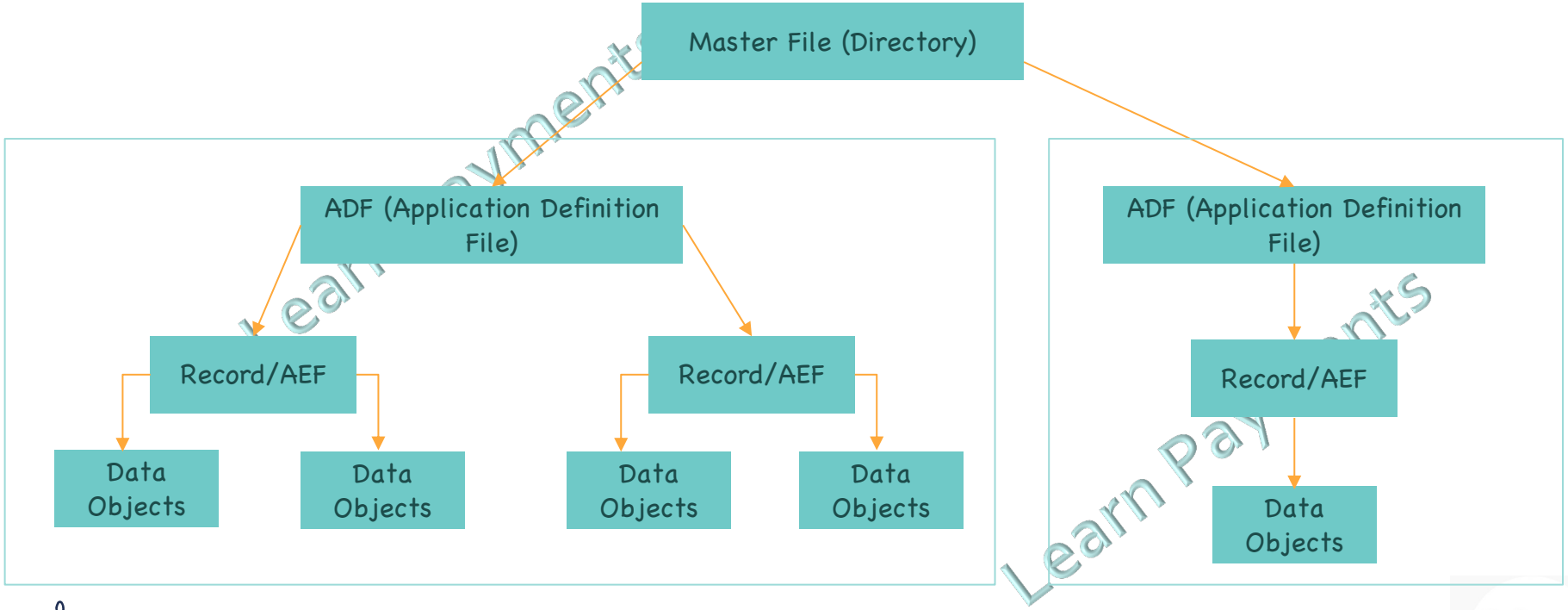
BASE AMT. : INR
PIN VERIFIED OK
SIGNATURE NOT REQUIRED

I AGREE T GREEMENT
**** CUSTOMER COPY ****
THANK YOU!
Plutus v1.49.3 MT HDFC
PRIVACY POLICY AS ON https://www.pinelabs.com/pr

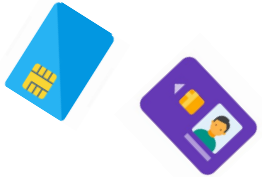
Application ID & Name on the payment receipt

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

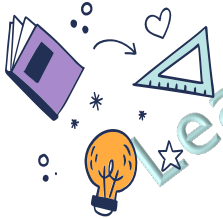
File Organization: Basics



Point 1: Data elements & Objects



- Data element is smallest piece of information
  - Eg: PAN number, Cardholder Name, Track 1, Track 2, Service Code, Currency Code
- Each Data element is assigned a unique tag
- Every DE is stored in the format of "Tag-Length-Value". It is called Data Object
- Example:
  - PAN = 5441 2232 9999 8888
  - Tag for PAN number is 5A
  - Length of PAN is, 16 - when represented in BCD, PAN takes 8 bytes (54 41 22 32 99 99 88 88)
  - So, Data Object is **5A 08 54 41 22 32 99 99 88 88**



Point 1.1: Data Elements & Tags

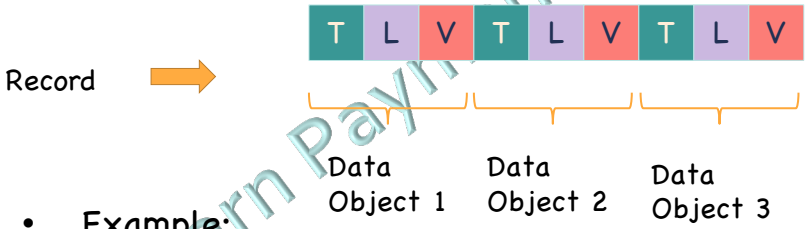
A2 Data Elements by Tag

Name	Template	Tag
Issuer Identification Number (IIN)	'BF0C' or '73'	'42'
Application Dedicated File (ADF) Name	'61'	'4F'
Application Label	'61' or 'A5'	'50'
Track 2 Equivalent Data	'70' or '77'	'57'
Application Primary Account Number (PAN)	'70' or '77'	'5A'
Cardholder Name	'70' or '77'	'5F20'
Application Expiration Date	'70' or '77'	'5F24'
Application Effective Date	'70' or '77'	'5F25'
Issuer Country Code	'70' or '77'	'5F28'
Transaction Currency Code	—	'5F2A'
Language Preference	'A5'	'5F2D'
Service Code	'70' or '77'	'5F30'
Application Primary Account Number (PAN) Sequence Number	'70' or '77'	'5F34'

Source: *EMV ICC Specifications for Payment Systems Book 3 – Application Specification v4.3*

Point 2: Records/AEF

Multiple data objects forms a Record. This is also referred to as an "AEF – Application Elementary File"



- Example:

9f 1f 18 32 34 39 35 30 30 30 30 30 30 30 30 30 30 30 31 30 31 30 30 30 30 30 30

57 13 54 11 11 88 88 88 88 82 d1 20 32 01 12 34 56 78 90 00 0f

5f 20 1a 53 4d 49 54 48 2f 4a 4f 48 4e 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

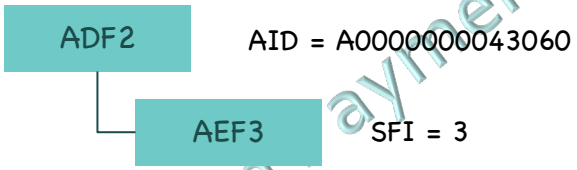
Tag for this Data Element is 9F 1F and length is 24 (BCD 18 = 24)

Track 1 Discretionary Data = 32 34 39 35 30 30 30 30 30 30 30 30 30 30 30 31 30 31 30 30 30 30 30 30

Point 3: ADF – Application Definition File

ADF (Application Definition File)

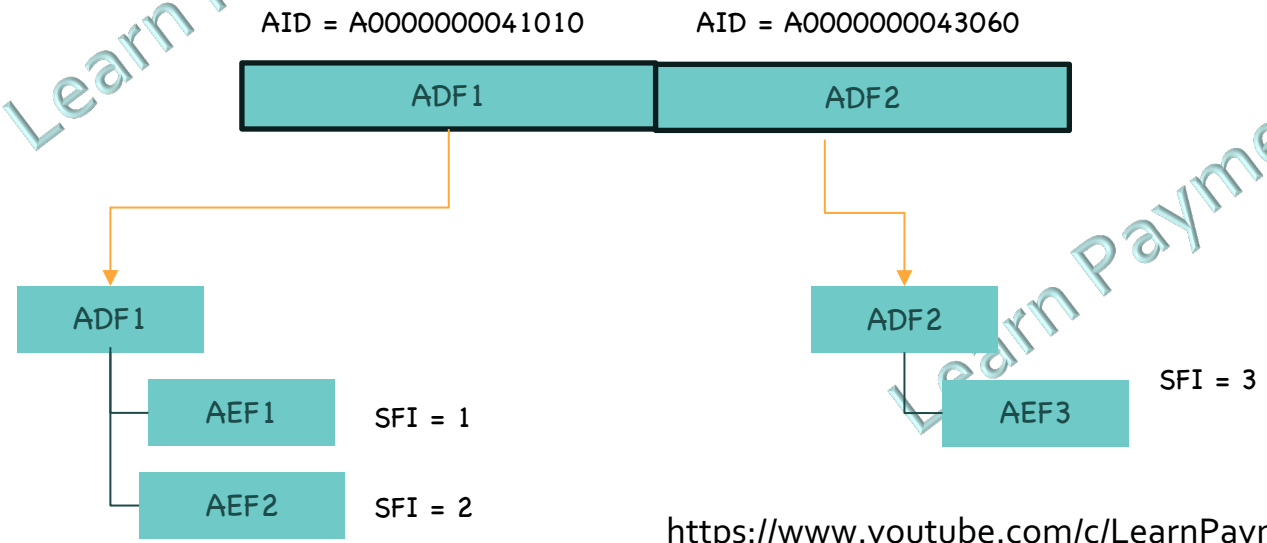
- Multiple AEFs grouped together form an ADF
- Every unique Application has an ADF
- Within ADF, each AEF would have a unique SFI (Short File Identifier) with which the AEF would be addressed



Point 4: Directory Definition File (DDF)

Directory Definition File

- It's a directory (index) to all ADFs
- Used to locate the ADF based on the Application ID
- For chip cards this file name should be **"1PAY.SYS.DDF01"**



Section 2: Key Data Elements

Important Data Elements

Application Data

- Application Identifier (AID)
- Application Label
- Application Preferred Name
- Application Priority Indicator
- Issuer Country Code
- Default Currency Code

Cardholder Data

- Cardholder Name
- PAN Number
- PAN Sequence
- Service Code
- Track Data

Card Authentication

- Issuer Action Code
- Signed Static Application Data

Cardholder Authentication

- CVM List
- Offline PIN (Encrypted)

Misc Data

- Application Transaction Counter (ATC)
- PIN Try Counter
- CDOL 1 & 2
- PDOL

What Next in Byte 3?

- Look at EMV Commands & How data gets exchanged between ICC & Terminal
- EMV Transaction Flow

Thank YOU

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