



EMV Application Specification :: Read Application Data

Ahmed Hemdan Farghaly
Senior Manager | Fintech | EFTPOS | mPOS | ISO8583 | EMV | NFC | QR | PCI-DSS | PA-DSS
Veröffentlicht: 22. Nov. 2021

+ Folgen

In this step we'll talk about how a terminal actually reads the application data using AFL collected in the previous step.

Please refer to the previous article about application selection & initiate application processing:

<https://www.linkedin.com/pulse/emv-application-specification-initiate-process-ahmed-hemdan-farghaly/>

In the previous example we showed that after parsing the AFL, the terminal will know the files and record that it needs to read from the card.

Step 1: know what to read

In our example:-

94 (AFL - Application File Locator) 080101011001030018010200

AFL is a group of 4 bytes each represents an SFI and records to read which shall be parsed as follows:

- The 5 most significant bits of the first byte represents SFI (that is 08 -> 00001000 -> 00001 -> SFI = 1).
- The second byte represents the first record number to read from that SFI (that is 01 -> start record = 1), note that this byte must not be zero.
- The third byte represents the last record number to read from SFI (that is 01 -> end record =1), note that this byte must be greater than or equal to the second byte.
- The fourth byte represents number of record that will be involved in offline data authentication step (which we'll talk about in next steps in details).

Using our example, it can be interpreted as follows:

SFI 1 record 1, and 1 record to be used in ODA (starting from record 1).

SFI 2 records 1-3.

SFI 3 records 1-2.

Step 2: read all records

Using the list prepared in step 1, the terminal shall issue a READ RECORD command for each SFI found in the list to reads the required records.

That is: CLA:(00) INS:(B2) P1:(record number) P2: (SFI as described in EMV book 3 Table 21) Le: (record length = 00, we still don't know the actual length of the record)

- SFI 1 record 1, 1 record to be used in ODA:

-> 00B2010C00 (send READ RECORD cmd to read record "1" in SFI "1")

<- 6C 39 (card send error indicate incorrect length with the actual length indicated)

-> 00B2010C39 (send the same command but with the correct record length)

<-
70375A0854133300890200945F24032512315F25030401015F3401469F0702FF009F0D05FC50A000009F0E050000000009F0F05F870A49800 9000 (card reply with a record template tag 70 where the content is TLV formatted data elements)

```
70 EMV Proprietary Template
  5A Application Primary Account Number (PAN)
    5413330089020094
  5F24 Application Expiration Date
    251231
  5F25 Application Effective Date
    040101
  5F34 Application Primary Account Number (PAN) Sequence Number
    46
  9F07 Application Usage Control
    FF00
  9F0D Issuer Action Code - Default
    FC50A00000
  9F0E Issuer Action Code - Denial
    0000000000
  9F0F Issuer Action Code - Online
    F870A49800e
```

- SFI 2 records 1-3:

-> 00B2011400 (send READ RECORD cmd to read record "1" in SFI "2")

<- 6C 40 (card send error indicate incorrect length with the actual length indicated)

-> 00B2011440 (send the same command but with the correct record length)

<-
703E8C209F02069F03069F1A0295055F2A029A039C019F37049F35019F45029F34039B028D08910A8A0295059B028E10000000000000000410342031E031F00 9000

-> 00B2021400 (send READ RECORD cmd to read record "2" in SFI "2")

<- 6C 06 (card send error indicate incorrect length with the actual length indicated)

-> 00B2021406 (send the same command but with the correct record length)

<- 70049F4A0182 9000

-> 00B2031400 (send READ RECORD cmd to read record "3" in SFI "2")

<- 6C 15 (card send error indicate incorrect length with the actual length indicated)

-> 00B2031415 (send the same command but with the correct record length)

<- 70135F20104D54495031352D32204D434420313341 9000

- SFI 3 records 1-2:

-> 00B2011C00 (send READ RECORD cmd to read record "1" in SFI "3")

<- 6C BF (card send error indicate incorrect length with the actual length indicated)

-> 00B2011CBF (send the same command but with the correct record length)

<-
7081BC8F01F19081B019BB432113F7B797AF7661F050463EC5F04C3D1C9983A5DB777CBC7BEF6AA7C8FA5C57C2721FC6B0FD4DDF6C0BF101DC88BAE88406982D9D5A6041889C226B88172B13395A2563D5E22BB5D19A5D0B3401E51983A9BF8606F8BFFD60ED5E40A4F84BCB92AA7A0478D3123496DA3054EF1EFD20C62515231FC9D78C2C1E701EB4155303F928B9E071EA3BEC4709571D4CCCD8E269A2A53A111B61CF48C383B8407614D1E7003970BE77F4B8806B9E7B5C692009F320103 9000

-> 00B2021C00 (send READ RECORD cmd to read record "2" in SFI "3")

<- 6C 3E (card send error indicate incorrect length with the actual length indicated)

-> 00B2021C3E (send the same command but with the correct record length)

<-
703C57115413330089020094D2512201029570106F5F280200565F300202019F080200029F2005029570106F9F3B0209789F420209789F4301029F440100 9000

After reading, terminal shall check that:

- Data read from Record "1" in SFI "3" will later be used in ODA process.
- All mandatory data objects shall be available (check EMV Book 3 section 7.2 for more details)
- Any error occur in the previous steps shall cause the transaction to be terminated. i.e. READ RECORD cmd return 6A82 or 6A83 indicate file/record not found.

Next article will be on ODA

(Offline Data Authentication) process.

Stay tuned...

50 · 1 Kommentar

Gefällt mir

Kommentieren

Teilen

Mawil Hussein

1 Jahr

كيف الاحوال

Gefällt mir





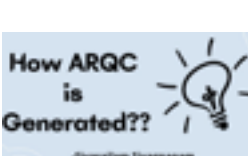

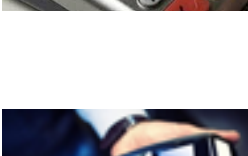
Antworten

Zum Anzeigen oder add a comment [einloggen](#)

Weitere Artikel von dieser Person

EMV Application Specification :: Offline...	EMV Application Specification :: Offline...	EMV Application Specification :: Initiate...	E
11. März 2022	23. Feb. 2022	17. Feb. 2021	S
			1

Ebenfalls angesehen

- **Everything EMV.**
Binoy Baby · 4 Jahre
- **Overloaded "Online vs Offline" in EMV Card Processing**
Kenny Shi · 2 Jahre
- **CDA EMV**
Mahmoud Elshafey · 5 Jahre
- **Full EMV transaction**
Binoy Baby · 4 Jahre
- **EMV Concept - How ARQC is generated | Visa CVN 18 |**
Sivasailam Sivagnanam · 7 Monate
- **How is your PIN validated ???**
Sivasailam Sivagnanam · 1 Jahr
- **EMV Concept - Offline Data Authentication | How an Static Data Authentication Works | SDA | Application of Cryptography in Cards & Payments**
Sivasailam Sivagnanam · 1 Jahr
- PIN Block Part II**
Siddhiganesh Joshi · 1 Woche
- PIN Block**
Siddhiganesh Joshi · 2 Monate
- ARQC and ARPC**
Binoy Baby · 4 Jahre