



Acquiring: EMV Transaction Flow. Part 4: PDOL and Contactless Cards, Characteristic Features of qVSDC and qUICS

22 November 2020 • 15829 Views

Introduction

We bring to your attention our new article on «EMV Transaction flow». We will tell you about the characteristic features of the contactless cards' work at the SELECT RESPONSE stage as well as the significant differences that are present in various Payment systems' specifications of exchange via the contactless interface.

In the [previous article](#), we have looked into the following stages of the EMV Transaction Flow:

1. ATR
2. **Select (1PAY.SYS.DDF01)**, an attempt of selection through the **PSE**. In case of denial:
3. **Select (AID)**, selection through the **PSA**. If there is only one applet, the procedure is finished, moving to the next step. If there are two applets:
4. Manual or automatic **application select**.
5. **Get Processing Options with or without PDOL**.

We have also drawn attention to the fact that the work of the «contactless» chips is significantly different at this stage of exchange. And those differences are what we are going to talk about. First of all, this includes the contactless cards of Visa and Union Pay (qVSDC (Quick Visa Smart Debit Credit) specification and qUICS (Quick UnionPay Integrated Circuit Card Specification), respectively). For illustrative purposes, let us compare SELECT RESPONSE for Mastercard and Visa cards.

SELECT RESPONSE, Mastercard:

Tag 6F: File Control Information (FCI) Template

Tag 84: Dedicated File (DF) Name: A0000000041010 — **AID**

Tag A5: File Control Information (FCI) Proprietary Template

Tag 50: Application Label: 4D617374657243617264 — **name of the application, text value «MasterCard»**

Tag 87: Application Priority Indicator: 01— **Application Priority Indicator**

Tag 5F2D: Language Preference: 7275656E — **preferred «communication language»**. Text value «ruen», i.e., the priority language is Russian (ru); if Russian is not supported, it will be English (en)

Tag BF0C: File Control Information (FCI) Issuer Discretionary Template

Tag 9F4D: Transaction Log Entry: 0B0A — **data on the transactions log**. In this case, it is permitted to store the information on the last 10 transactions.

Tag 9F6E: Third Party Data [MasterCard]: 06430000303000 — **specific tag of Mastercard PS**, in this case describing the card's regional affiliation and «form factor». In terms of bytes, it is as follows:

- Bytes 1-2 = 0643 Russian Federation
- Bytes 3-4 = 0000 Unique Identifier
- Bytes 5-6 = 3030 Device Type: Card — **the «form factor», in this case, it is the card**. In the case of a card attached to any *Pay service (GPay, ApplePay, etc.), those bytes will be different.



As we can see, the Mastercard contactless cards have the set of data transmitted at the SELECT RESPONSE stage that has virtually no differences from the contact chip card of that PS previously looked into. We should mention again that the characteristic feature of the Mastercard cards is that they have no PDOL object.

Now, let us see the SELECT RESPONSE of Visa card.

SELECT RESPONSE, VISA:

Tag 6F: File Control Information (FCI) Template

Tag 84: Dedicated File (DF) Name: A0000000031010 — **AID**

Tag A5: File Control Information (FCI) Proprietary Template

Tag 50: Application Label: 56495341 — **name of the application, text value «VISA»**

Tag 5F2D: Language Preference: 7275656E — **preferred «communication language»**. Text value «ruen», i.e., the priority language is Russian (ru); if Russian is not supported, it will be English (en)

9F66049F02069F37045F2A029F1A02 — **main difference, components of PDOL object**.

Let us look into it in greater detail:

Tag 9F66, length 04: Terminal Transaction Qualifiers (TTQ) — **special object peculiar to qVSDC**. This object will be further described in more detail.

Tag 9F02, length 06: Transaction Amount — **Transaction Amount..**

Tag 9F37, length 04: Unpredictable Number (UN) — **the random number generated by the terminal in order to ensure the uniqueness of the transaction's cryptogram.**

Tag 5F2A, length 02: Transaction Currency Code — **Transaction Currency Code..**

Tag 9F1A, length 02: Terminal Country Code — **Terminal Country Code.**

Hence, at this stage of exchange, the card "communicates" to the terminal the parameters that it needs to perform the transaction, namely: device capabilities (TTQ), transaction amount, UN, as well as the currency code and country code. In essence, by transmitting those values to the card in the next command, some equivalent of the «classic» risk management procedure within the EMV is performed, and, based on its results, the decision is made to decline or approve the transaction off-line or send it to the issuer for authorization.

Let us introduce the next command (GPO) as an instance where the parameters listed in PDOL object are transmitted.

Term: 831236A0400000000000140036D3EC3906430643 (Get Processing Options)

Cla: 80 — **command class**

Ins: A8 — **instruction code**

P1: 00

P2: 00

Lc: 14

Data: 831236A0400000000000140036D3EC3906430643 — **data field with tag 83 containing concatenation («addition») of values in the same order as they are listed up in the PDOL element of the command to SELECT RESPONSE.** Let us look into them in the same order as they are set out in the example:

Tag 9F66: Terminal Transaction Qualifiers: 36A04000. **In this object, the terminal «tells» about the card and its functionality, namely::**

- Byte 1 bit 8 = 0 Contactless magnetic stripe not supported — **the contactless interface in the magnetic stripe emulation mode is not supported.**
- Byte 1 bit 7 = 0 RFU — **reserved for future use.**
- Byte 1 bit 6 = 1 Contactless qVSDC supported — **the contactless interface in the chip (qVSDC — Quick Visa Smart Debit Credit) emulation mode is supported**
- Byte 1 bit 5 = 1 Contact VSDC supported — **the interface of the contact chip is supported.** This bit is needed for the card to be able to send the command to Switch Interface upon occurrence of certain events, i.e., to suggest the use of the contact chip (see below).
- Byte 1 bit 4 = 0 Reader is Online Capable — **the device has the online authorization capability..**
- Byte 1 bit 3 = 1 Online PIN supported — **«Online PIN» CVM method is supported.**
- Byte 1 bit 2 = 1 Signature supported — **«Signature» CVM method is supported.**
- Byte 1 bit 1 = 0 Offline Data Authentication(ODA) for Online Authorizations not supported — **ODA is not supported.**
- Byte 2 bit 8 = 1 Online cryptogram required — **online transaction cryptogram verification by the issuer is required..**
- Byte 2 bit 7 = 0 CVM not required — cardholder verification is not required. That bit is dynamic and to be introduced depending on the transaction amount and terminal limits. In our case, the transaction amount is small (see below), which is why bit = 0.
- Byte 2 bit 6 = 1 (Contact Chip) Offline PIN supported — **«Offline PIN» CVM method for the contact chip is supported.**

- Byte 2 bit 5 - 1 = 0 RFU — : **bytes 5 to 1 are reserved for future use.**
- Byte 3 bit 8 = 0 Issuer Update Processing not supported — **the capability to transmit the issuer scripts to the card is not supported.**
- Byte 3 bit 7 = 1 Mobile functionality supported (Consumer Device CVM) — **the cardholder verification on the mobile device (password, graphic key, print, etc.) is supported.**

The rest of the bits of the 3rd byte and all bits of the 4th byte are currently reserved for future use.

Tag 9F02: Transaction Amount: 000000001400 — **amount of the transaction. 14.00 rubles.**

Tag 9F37: Unpredictable Number: 36D3EC39 — **random number.**

Tag 5F2A: Transaction Currency Code: 0643 — **code of the transaction currency, rubles.**

Tag 9F1A: Terminal Country Code: 0643 — **country of the terminal, Russian Federation.**

The above example makes it clear that object 9F66 (Terminal Transaction Qualifiers (TTQ)) has in general the same functional purpose as [object 9F33 \(Terminal Capabilities\)](#).



The card's response to the command to GPO follows. Example:

Response:

```
774C8202200057134704340000172834D21122011676600000671F5F2002202F5F3401019F100706011103A000009F2608A4933D887F00
65CE9F2701809F3602004E9F6C023E009F6E04207000009000
```

Tag 77: Response Message Template Format 2 — **format of data presentation in the response.**

Tag 82: Application Interchange Profile: 2000 — **profile of the card application where its functionality is described.** In this case, it is broken down into the following bytes:

- Byte 1 bit 8 = 0 RFU — **reserved for future use.**
- Byte 1 bit 7 = 0 Offline static data authentication is NOT supported for online authorizations — **offline SDA is not supported.**
- Byte 1 bit 6 = 1 Offline dynamic data authentication is supported — **offline DDA is supported.**
- Byte 1 bit 5 - 3 = 0 — **not used.**
- Byte 1 bit 2 = 0 RFU — **reserved for future use.**
- Byte 1 bit 1 = 0 — **not used.**
- Byte 2 bit 8 = 0 MSD is NOT supported — **the magnetic stripe interface is not supported.**
- Byte 2 bit 7 = 0 Mobile handset — **sign that this is a «mobile» device.** I.e., the card attached to any *Pay service (GPay, ApplePay, etc.). In this case, bit = 0, i.e., we deal with an ordinary contactless card.
- Byte 2 bit 6 = 0 Contactless transaction — **sign of a contactless transaction.**
- Byte 2 bit 5 - 1 = 0 RFU — **reserved for future use.**

Tag 57: Track 2 Equivalent Data: 4704123456789000D21122011676600000671F — **equivalent of the magnetic stripe's second track.** Its structure includes:

- PAN = 4704123456789000 — **card number itself.**
- Separator field = D — **separator.**
- Expiry Date = 21/12 — **card expiry date.** Through December 2021.
- Service Code = 201 — **service code.**
- Discretionary Data = 1676600000671F — **so-called «discretionary data» where the values such as CVV/CVV2 can be encoded.**

Tag 5F20: Cardholder Name: 202F — **name of the cardholder.** It should be mentioned that contactless cards never contain the cardholder name. It is done for the security purposes. For this reason, tag 5F20 is either completely missing in the card profile, or has a certain random set of data. In our case, the cardholder name is = «/».

Tag 5F34: Application PAN Sequence Number: 01 — **sequence number of the card.** Its initial purpose was to be used in the profiles that have more than one application on one physical card. Currently, it is often used in the cryptographic procedures related to the card authenticity verification by the issuer's host.

Tag 9F10: Issuer Application Data: 06011103A00000 — **data of the card application.** Its structure includes:

- **Length Indicator** = 06
- **Derivation Key Index** = 01
- **Cryptogram Version Number** = 11
- **Card Verification Results (CVR)** = 03A00000, dynamic object based on the previous steps of exchange within the transaction. In our case, its values are the following:
 - Byte 1 bit 8-1 = 00000011 **Length indicator.**
 - Byte 2 bit 8-7 = 10 AC returned in 2nd GENERATE AC: Not requested — **since the card is contactless, the second cryptogram will not be requested.**
 - Byte 2 bit 6-5 = 10 AC returned in 1st GENERATE AC: ARQC is the **cryptogram resulting from the exchange - ARQC (Authorisation Request Cryptogram), i.e., the online request to the issuer.**

- Byte 2 bit 4 = 0 Issuer Authentication successful or not performed — **the authentication of the issuer was either not performed or successful.** In essence, it means that the authentication of the issuer did not fail.
- Byte 2 bit 3 = 0 **Offline PIN verification not performed.**
- Byte 2 bit 2 = 0 Offline PIN verification passed or not performed — **in essence, it means that the offline PIN verification did not fail.**
In our case, there is no verification failure, because there was no verification.
- Byte 2 bit 1 = 0 Able to go online or offline transaction — **in essence, it means that there is no failure cryptogram.**
- Byte 3 bit 8 = 0 Last online transaction completed — **sign of successful completion of the last online transaction.**
- Byte 3 bit 7 = 0 PIN Try Limit not exceeded — **sign that the PIN code entry attempts limit is not exceeded.**
- Byte 3 bit 6 = 0 Velocity checking counters not exceeded — **sign that the transactions velocity checking counters limit is not exceeded** (This value is used as a part of the offline transactions approval functionality).
- Byte 3 bit 5 = 0 No new card — **sign that this is not a new card.** In essence, it means that this is not this card's first transaction.
- Byte 3 bit 4 = 0 Issuer Authentication successful on last online transaction or not performed — **the authentication of the issuer on the last online transaction was either successful or not performed.** In essence, it means that the authentication of the issuer on the last online transaction did not fail.
- Byte 3 bit 3 = 0 Issuer Authentication performed after online authorization or offline transaction — **issuer authentication was performed.**
- Byte 3 bit 2 = 0 Application not blocked by card — **sign that the card application is not blocked.**
- Byte 3 bit 1 = 0 Offline static data authentication passed or was not performed on last transaction — **in essence, it means that the offline SDA did not fail.**
- Byte 4 bit 8-5 = 0000 Number of Issuer Script Commands : '0' — **number of scripts sent to the card by the issuer.** They are missing in our case.
- Byte 4 bit 4 = 0 Issuer Script processing passed — **in essence, it means that the issuer scripts sending procedure did not fail.**
- Byte 4 bit 3 = 0 Offline dynamic data authentication passed or was not performed on last transaction — **in essence, it means that the offline DDA did not fail.**
- Byte 4 bit 2 = 0 Offline dynamic data authentication not performed — **sign that the offline DDA was not performed.**
- Byte 4 bit 1 = 0 PIN verification command received for a PIN-Expecting card or card does not expect PIN (i.e. Offline PIN verification not supported) — **sign that the offline PIN was not verified because it was not supported (due to this being a contactless card).**

Tag 9F26: Application Cryptogram (AC): A4933D887F0065CE — **the cryptogram itself.**

Tag 9F27: Cryptogram Information Data (CID): 80 — **information on the cryptogram.** Its structure includes:

- Byte 1 bit 8-7 = 10 ARQC — **i.e., the online authorization.**
- bit 6-5 = 00 Payment System specific cryptogram
- bit 4 = 0 No advice required
- bit 3-1 = 000 No information given

Tag 9F36: Application Transaction Counter (ATC): 004E — **card transactions counter.** Digital value: 78.

Tag 9F6C: Card Transaction Qualifiers: 3E00 — **qVSDC-specific object of CTQ describing the card capabilities.** In terms of bits:

- Byte 1 bit 8 = 0 **Online PIN is not required.** That bit is dynamic and to be introduced depending on the transaction amount and terminal limits. In our case, the transaction amount is small (see above), which is why bit = 0.
- Byte 1 bit 7 = 0 **Signature is not required.** That bit is dynamic and to be introduced depending on the transaction amount and terminal limits. In our case, the transaction amount is small (see above), which is why bit = 0.

- Byte 1 bit 6 = 1 Go online if Offline Data Authentication fails and Reader is online capable — **go online if ODA fails and if the terminal supports the online exchange.**
- Byte 1 bit 5 = 1 Switch interface if Offline Data Authentication fails and Reader supports contact chip — **switch to the contact chip if ODA fails and if the terminal supports the contact chip.**
- Byte 1 bit 4 = 1 Go Online if Application Expired — **go online if the application expires.**
- Byte 1 bit 3 = 1 Switch interface for Cash Transactions — **switch interface to the contact chip for «Cash withdrawal» transactions.**
- Byte 1 bit 2 = 1 Switch interface for Cashback Transactions — **switch interface to the contact chip for «Purchase with cashback» transactions.**
- Byte 1 bit 1 = 0 Valid for contactless ATM transactions — **work with contactless ATMs is supported.**
- Byte 2 bit 8 = 0 Consumer Device CVM not performed — **the cardholder verification on the mobile device (password, graphic key, print, etc.) is not supported.**
- Byte 2 bit 7 = 0 Card does not support Issuer Update Processing at the POS — **the issuer script processing procedure is not supported.**
- Byte 2 bit 6-3 = 0 RFU — **bits 6 to 3 are reserved for future use.**
- Byte 2 bit 2 = 0 valid at ATMs — **work with ATMs is supported.**

Tag 9F62 Form Factor Indicator 20700000 — **reserved for future use.** So called «form factor indicator». The object describes the technological type of this particular mean of payment.

- Byte 1 bit 8-6 = 001 Form Factor Indicator Version Number: 1 — **FFI version.**
- Byte 1 bit 5-1 = 00000 Payment Device Form Factor: Standard Card — **the form factor is the card.**
- Byte 2 bit 8 = 0 Payment Device is not passcode capable
- Byte 2 bit 7 = 1 Payment Device has a signature panel
- Byte 2 bit 6 = 1 Payment Device has a hologram
- Byte 2 bit 5 = 1 Payment Device is capable of CVV2
- Byte 2 bit 4 = 0 Payment Device is incapable of two-way messaging
- Byte 2 bit 3 = 0 Payment Device is not using cloud-based payment credentials
- Byte 2 bit 2 = 0 Payment Device is using Biometric Cardholder Verification not Capable
- Byte 2 bit 1 = 0 RFU
- Byte 3: 00 RFU
- Byte 4 bit 8-5: RFU
- Byte 4 bit 4-1: 0000 Payment Transaction Technology: Proximity contactless interface using ISO 14443

As it was mentioned before, in addition to the contactless Visa, the scenario of exchange using the special objects is also available within the specifications of qUICS (Quick UnionPay Integrated Circuit Card Specification) of Union Pay International Payment System.

Another characteristic distinction of the implementation of those two IPS' «contactless» devices is a significant «laconization» of the exchange scenario where many parts of the functionality usual for the classical EMV, have been forgone (Thanks to which the scenario became so compact that we have already pretty much completely described it in this article). In essence, the entire cycle consists of the commands to Select PSE, Select PSA and Get Processing Options (in some cases, the command to READ RECORDS is available if fDDA(Fast Dynamic Data Authentication) is supported). In addition to that, the procedure of decision-making regarding TVR — Terminal Action Code/Issuer Action Code is not carried out. Instead, the mechanism using TTQ/CTQ is used. We should also mention that the value of TVR is always zero (which results from what we have mentioned before), but its presence in Field 55 in case of online exchange is mandatory, because in some cases it is a part of the cryptogram generation.



In conclusion, to complete the picture, let us give the examples of SELECT RESPONSE for the contactless cards of American Express and Mir NSPK (National Payment Card System), accompanied by our comments, as usually.

SELECT RESPONSE, American Express:

Tag 6F: File Control Information (FCI) Template

Tag 84: Dedicated File (DF) Name: A000000025010403 — AID

Tag A5: File Control Information (FCI) Proprietary Template

Tag 50: Application Label: 414D45524943414E2045585052455353 — **name of the application, text value «AMERICAN EXPRESS»**

Tag 87: Application Priority Indicator: 01 — **Application Priority Indicator.**

Tag 9F38: Processing Options Data Object List (PDOL): 9F3501 — **PDOL object, which, as we can see, consists of only one tag 9F35, the length of which is 01.**

Tag 5F2D: Language Preference: 656E — **communication language.** Without «en» scenarios.

PDOL of the contactless American Express card includes object [9F35 \(Terminal Type\)](#), describing the technological type of the terminal.

SELECT RESPONSE, Mir NSPK:

Tag 6F: File Control Information (FCI) Template

Tag 84: Dedicated File (DF) Name : A0000006581099 — **AID**

Tag A5: File Control Information (FCI) Proprietary Template

Tag 87: Application Priority Indicator: 01 — **Application Priority Indicator**.

Tag 9F38: Processing Options Data Object List (PDOL): 9F7A015F2A029F02069F35019F40059F1A029F3303 — **PDOL**, see the explanation below:

Tag 9F7A, length 01: LVP Support Indicator — **sign of «LVP» (Low Value Payments, i.e., the small-amount transactions) functionality support by the terminal.**

Tag 5F2A, length 02: **Transaction Currency Code**.

Tag 9F02, length 06: **Transaction Amount**.

Tag 9F35, length 01: **Terminal Type**.

Tag 9F40, length 05: [Additional Terminal Capabilities](#).

Tag 9F1A, length 02: **Terminal Country Code**.

Tag 9F33, length 03: **Terminal Capabilities**.

After PDOL, SELECT RESPONSE of Mir card includes the following objects:

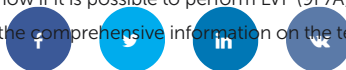
Tag 5F2D: Language Preference : 7275656E — **preferred «communication language»**. Text value «ruen», i.e., the priority language is Russian (ru); if Russian is not supported, it will be English (en).

Tag BF0C: File Control Information (FCI) Issuer Discretionary Template

Tag 9F4D: Transaction Log Entry: 0B0A — **data on the transactions log**. In this case, it is permitted to store the information on the last 10 transactions.

Tag 50: Application Label: 4D495220436C617373696320435244 — **name of the application, text value «MIR Classic CRD»**.

Consequently, the contactless card of Mir wants to know if it is possible to perform LVP (9F7A), as well as the currency and the amount of transaction (5F2A and 9F02). Besides that, it requires the comprehensive information on the terminal and its capabilities (9F40 and 9F33) and its location (9F1A).



Nonetheless, all of the above-mentioned examples make it clear **More articles** American Express and Mir operate with the objects that are, one way or another, characteristic for the classic EMV/CPA. Which is not the case of Visa and Union Pay. This, along with the significant reduction of the exchange scenario, is the main difference between them.



[Acquiring: EMV Transaction Flow. Part 4: PDOL and Contactless Cards, Characteristic Features of qVSDC and qUICS](#)

22 NOVEMBER 2020

[Acquiring: EMV Transaction Flow. Part 2: PSE and AID, Candidate List and Application Selection](#)

5 AUGUST 2020

[Acquiring: EMV Transaction Flow. Part 3: GET PROCESSING OPTIONS with and without PDOL](#)

14 AUGUST 2020

[Resetting TAMPER on VeriFone VX520 terminal](#)

11 AUGUST 2017

[Acquiring: EMV Transaction Flow. Part 5: READ RECORDS](#)

7 DECEMBER 2020

[Payment Solutions](#) [Payment Services](#) [Smart City](#) [Machine Learning](#) [Custom Development](#) [Infrastructure](#)

[Company](#) [Documents](#) [News](#) [Partners](#)



2024. MST Company — system integrator (DUNS Number: 505535797).

[Terms of Use](#)

