application protocol data unit (APDU)

Frank Braun

2019-06-07

In the context of smart cards, an *application protocol data unit* (APDU) is the communication unit between a smart card reader and a smart card.

There are two categories of APDUs:

- command APDUs
- response APDUs

Command APDU

A command APDU is sent by the reader to the card — it contains a mandatory 4-byte header (CLA, INS, P1, P2) and from 0 to 65535 bytes of data.

Field name	Length	Description
CLA	1	Instruction class - indicates type of command
INS	1	Instruction code - indicates specific command
P1-P2	2	Instruction parameters for the command
Lc	0, 1 or 3	Encode number (`Nc`) of bytes of command data
Command data	`Nc`	`Nc` bytes of data
Le	0, 1, 2 or 3	Maximum number (`Ne`) expected response bytes

See APUDs at Wikipedia[1] for `Lc` and `Le` encodings.

Command APDU cases:

- Case 1: no command data, no response data: `|Header|`
- Case 2: no command data, response data: `|Header|Le|`
- Case 3: command data, response data: `|Header|Lc|Data|`
- Case 4: command data, response data: `|Header|Lc|Data|Le|`

An *extended APDU* is an APDU (command) with data and/or response of more than 256 bytes and up to 65536 bytes. Otherwise it is a *short APDU*.

[1] https://en.wikipedia.org/wiki/Smart_card_application_protocol_data_unit

Response APDU

A response APDU is sent by the card to the reader — it contains from 0 to 65536 bytes of data, and 2 mandatory status bytes (SW1, SW2).

Field name	Length	Description
Response data	`Nr` (at most `Ne`)	Response data
Response trailer (SW1 SW2)	2	Command processing status

Some status bytes

SW1 SW2	Message
63 CX	Counter provided by `X` (valued from 0 to 15)
69 82	Access conditions not fulfilled
69 85	No currently selected EF, no command to monitor
90 00	Command executed without error

See SW1 SW2 status bytes[2] for more status bytes.

[2] https://web.archive.org/web/20090623030155/http://cheef.ru/docs/HowTo/SW1SW2.info