Secure Element Applet API

Communication with a Secure element Applet API is performed through standard APDU commands.

For a detailed description of APDU communication, APDU commands data structure and particular bytes meaning, please refer to ISO/IEC 7816-4 standard.

Commands are grouped into three categories based on the type of usage:

1. Fiscalization
2. Audit

Important Notes

1. All APDU commands are sent to the Smart Card using T1 communication protocol
2. All amount values are submitted to the Secure element using Big-endian. Big-endian is an order in which the "big end" (most significant value in the sequence) is stored first (at the lowest storage address)
3. P1 and P2 values are not considered in the request processing, except for the Select Applet Command
4. All APDU commands are sent to the Smart Card using T1 communication protocol
5. All values are submitted to the Secure element using Big-endian. Big-endian is an order in which the "big end" (most significant value in the sequence) is stored first (at the lowest storage address)

Content

1. General Commands
   Secure Element Applet is installed as a non-default applet on a smart card. Before any APDU command is invoked, the applet is selected using the standard Select command.

2. Fiscalization
   PIN verification is a method that “unlocks” a card for invoice signing and other operations protected by PIN code. PIN is in a decimal format, example PIN:2017 is represented as 0x02, 0x00, 0x01, 0x07

3. Audit
   Returns 259 bytes data structure represents public card key (256 bytes modulus and 3 bytes exponent). This key is used for Audits.

4. Secure Element Specific APDU Error Codes
   This table contains the expected error codes and descriptions that a caller may encounter while working with the Secure Element Applet.