

CORE SMART CARD

ABC4T Types:

- GROUP
- CREDENTIAL
- BLOB ITEM
- ...

APDU Payload Types:

- APDU_SET_GROUP_COMPONENT
- APDU_READ_AUTHENTICATION_KEY
- ...

Global variables:

- Variables found in Session, Public & Static in the original code. Kept as global variables.

Subroutines:

- Functions called *Subroutines* in original code.
- Used exclusively by APDU Handler.

Constants definitions:

- INS byte values
- ERROR codes
- Data sizes
- Other constants

MULTOS Types:

- BYTE (1B)
- WORD (2B)
- DWORD (4B)
- ...

APDU Handler:

- handle_APDU(); → switch:case
- handle_INS_GET_MODE()
- ...

MULTOS reimplemented C-API:

- Reimplementation of the needed CAPI functions following MULTOS documentation.

INTERFACES

Modular Arithmetic:

- Addition
- Subtraction
- Multiplication
- Exponentiation
- Modulo

Criptography:

- AES128
- SHA256
- Random Number Gen.

Memory:

- memmove
- memcpy
- memcmp
- memset

Smart Card Status Serialization:

- [PoC] Json file de/serialization

APDU I/O:

- Parse APDU Command
- Compose APDU Response

EXTERNAL UTILITIES

[PoC] Base64 encoding/decoding:

- Nibble And A Half's ANSI C Base64 library.
- Used for serialization.

[PoC] cJSON:

- Dave Gamble's ANSI C JSON parser.
- Used for serialization.

[PoC] GMP Lib:

- The GNU Multiple Precision Arithmetic Library.
- Used for modular arithmetic.

[PoC] OpenSSL:

- Cryptography and SSL/TLS Toolkit.
- Used for the Cryptography interface.