SmartOS-K1

Reference Manual
v.1.1.0

Disclaimer of Liability

The content of this manual has been checked for agreement with the hardware described. Since deviations cannot be precluded entirely, full agreement is not guaranteed. However, the data in this manual are reviewed regularly and any necessary corrections will be included in subsequent versions. Suggestions for improvement are welcomed.

General Information

The smart card SmartOS K1 is a microprocessor smart card with 2K of EEPROM (1,5 taken by the operating system), compliant with ISO7816 and with any PC/SC or CCID smart card reader, that gives a bank of public memory of 255 bytes and a bank of private memory, protected by a PIN, of 255 bytes (protected memory means that read and write operations on private memory can be performed only after PIN verification)
SmartOS K1 is suitable for applications requiring a few memory, low cost and usability readiness such as badges, fidelity cards, memory cards, etc.

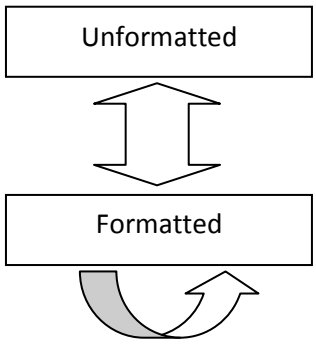
The PIN is an alphanumeric value of max 8 numbers/characters. After 3 wrong trials the PIN is blocked and can be unblocked by the PUK.

The PUK is an alphanumeric value of max 8 numbers/characters. After 3 wrong trials the PUK is blocked and cannot be unblocked.

The Format Key is an alphanumeric value of 10 numbers/characters. After 10 wrong trials the Format Key is blocked and cannot be unblocked.

Life Cycle

The life cycle of the SmartOS K1 has two states: Unformatted and Formatted as shown in the following picture:



After production the smart card is in Unformatted state.
The command Format is used to move from Unformatted to Formatted state.
In Formatted state the smart card can be formatted again, infinite times, using the Format command.

Tecnical Specification

- Microchip with 2KB EEPROM (1,5 taken by OS)
- Protocol T = 1
- Compliant with ISO 7816 1,2,3
- Compliant with any PC/SC, CCID reader
- 255 byte of public memory
- 255 byte of private memory protected by PIN
- PIN to protect private memory - max 8 numbers/characters, max 3 trials (error counter)
- PUK max 8 numbers/characters
- Command set compliant with ISO 7816 4

Default values:

PIN: 12345678
PUK: 12345678
Format Key: 1234567890

Commands

The following table shows the set of commands respect to the state of the card:

Command	Unformatted	Formatted
CHANGE REFERENCE DATA		X
FORMAT	X	X
GET DATA	X	X
READ BINARY		X
UPDATE BINARY		X
VERIFY PIN		X

CHANGE REFERENCE DATA

CLA	INS	P1	P2	LC	DATA	LE
00	24	00	*id*	08	*<empty>*	00

Changed thte PIN or the PUK as specified in P2.
P2 = 1 PIN
P2 = 2 PUK.
DATA fields contains the new value for PIN/PUK.

Conditions:
- PIN or PUK has already been verified by the command Verify PIN

Example
PIN changed in 1234:
00 24 00 01 08 31 32 33 34 FF FF FF FF 00

FORMAT

CLA	INS	P1	P2	LC	DATA	LE
C0	41	00	00	0A	*<format key>*	00

Formats the EEPROM and deletes the content moving the card is *Formatted* state.
DATA field must contain the right *format key*

Example
C0 41 00 00 0A 31 32 33 34 35 36 37 38 39 30 00

GET DATA

CLA	INS	P1	P2	LC	DATA	LE
00	CA	00	*mode*	00	*<empty>*	00

Reads system information specified in P2 as described in the following table:

mode	Description
80	Manufacturer
81	Microchip Identification Code
82	ID operating system (1- SmartOS K1, 2 – SmartOS K2, 3- SmartOS KW, 4- SmartOS CK)
83	Life Cycle: *unformatted* = 10, *formatted* = 20
85	Error counter format key
86	Error counter PIN
87	Error counter PUK

Example
Gets the PIN error counter:
00 CA 00 86 00 00

READ BINARY

CLA	INS	P1	P2	LC	DATA	LE
00	B0	*mem*	*offset*	00	*< empty >*	*len*

Reads the content of the memory specified in P1 starting from the offset specified in P2.
P1 = 1 public memory.
P1 = 2 private memory.
LE number of bytes to read (up to 127 at a time)

Conditions:
- reading from protected memory can be done only after PIN verification

Example
Reads 10 bytes from public memory starting from 32:
00 B0 01 10 00 0A

UPDATE BINARY

CLA	INS	P1	P2	LC	DATA	LE
00	D6	*hi*	*low*	*len*	*<data>*	*00*

Writes the content in DATA fields in the memory specified by P1 starting from the offset specified in P2.
P1 = 1 public memory
P1 = 2 private memory.
LC must contains the length of the DATA field (up to 127 at a time).

Conditions:
- Writing in protected memory can be done only after PIN verification.

Example
Writes 10 bytes to public memory starting from 32:
00 D6 01 10 0A 31 32 33 34 35 36 37 38 39 30 00

VERIFY PIN

CLA	INS	P1	P2	LC	DATA	LE
00	20	00	*id*	*08*	*<pin>*	*00*

Verifies PIN or PUK as specified in P2
P2 = 1 PIN
P2 = 2 PUK.

If verification succeeds the *PIN*/*PUK* is set to "verified" and the related error counter is cleared.

Example
Verifies the PINwith the value 1234:
00 20 00 01 08 31 32 33 34 FF FF FF FF 00

Error codes

SW1	SW2	Description
Normal Processing		
0x90	0x00	Successful Command
0x61	0xXX	Successful Command, SW2 contains the number of *APDU Response* bytes still available
Warning		
0x62	0x00	Generic Warning
0x62	0x81	Invalid or corrupted data
0x62	0x82	EOF reached
0x62	0x83	The selected file is invalid
0x62	0x84	Invalid File Control Information (FCI)
0x63	0x00	Generic Error
0x63	0x81	File is full
0x63	0xCX	Error meaning depends on the specific command
Processing Errors		
0x64	0xXX	Internal Processing Error
0x65	0x00	Generic Error
0x65	0x81	Storing Error
0x66	0xXX	Reserved for future extensions
Verify Errors		
0x67	0x00	Invalid Command Length (LC)
0x68	0x00	(CLA) Command not supported
0x68	0x81	Channel not supported
0x68	0x83	*Secure Messaging* Mode not supported
0x69	0x00	Command not permitted
0x69	0x81	The Command is incompatible with the file structure
0x69	0x82	Access denied (access permissions not granted)
0x69	0x83	*Security Object* is blocked
0x69	0x84	Invalid Command Data
0x69	0x85	Using conditions unsatisfied
0x69	0x86	Invalid Command, no file selected
0x69	0x87	*Secure Messaging* Object not found
0x68	0x88	Invalid *Secure Messaging* Object
0x6A	0x00	Wrong P1 or P2 field
0x6A	0x80	Wrong Parameters in DATA field
0x6A	0x81	Not Supported Function
0x6A	0x82	File Not Found
0x6A	0x83	Record Not Found
0x6A	0x84	Not enough free space on file or memory
0x6A	0x85	Inconsistent LC field respect to TLV structure
0x6A	0x86	Wrong P1 or P2 field
0x6A	0x87	Inconsistent LC field respect to P1 and P2 fields
0x6A	0x88	Object not found
0x6B	0x00	Wrong P1 and P2 fields
0x6C	0xXX	Wrong LE field. XX indicates the correct size of *APDU Response*'s DATA field
0x6D	0x00	Invalid or not supported INS field
0x6E	0x00	Invalid or not supported CLA field
0x6F	0x00	Internal Error