SAM TOOL USER MANUAL

Version 1.0

Digital Logic Ltd.

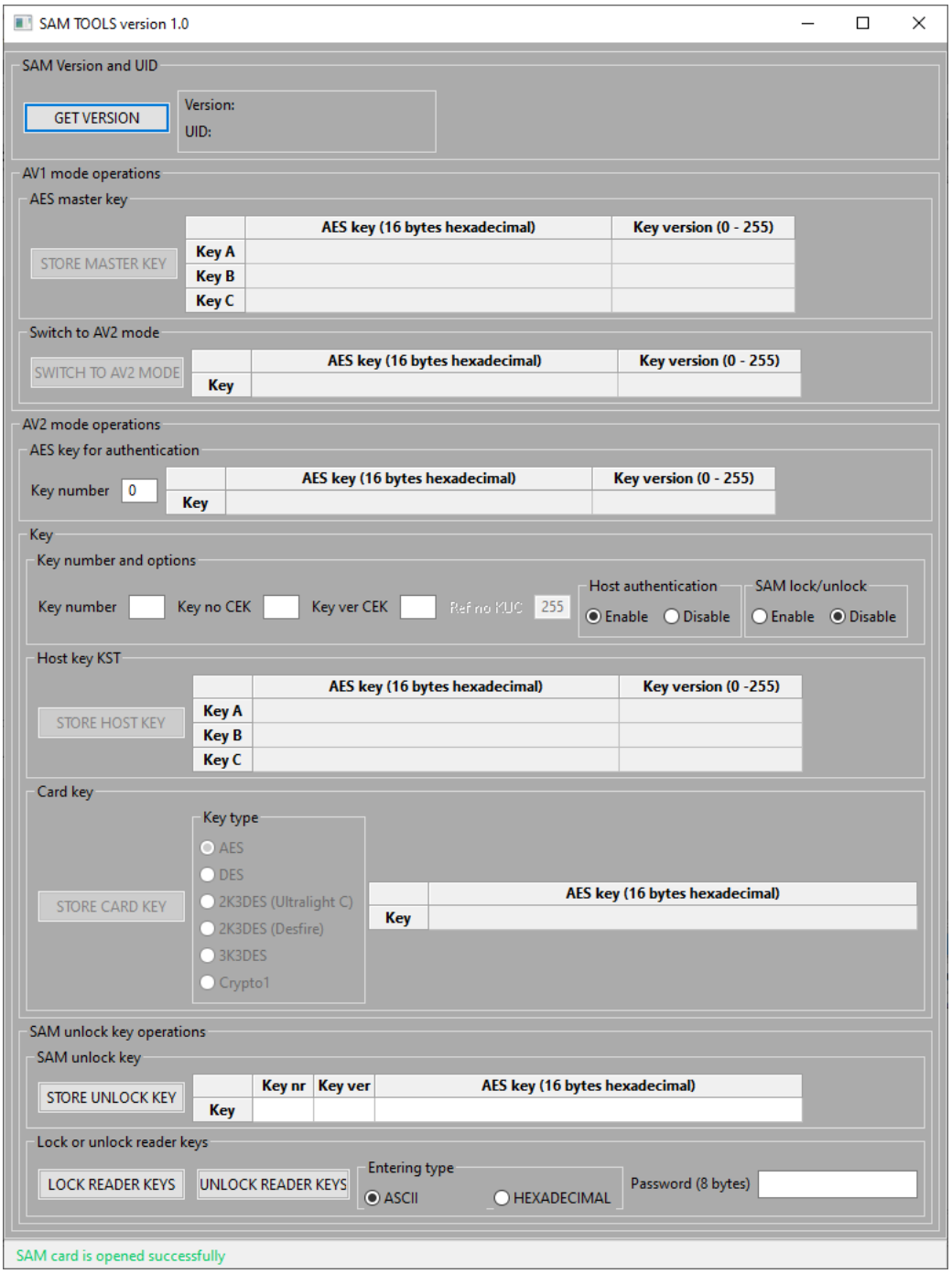
Address: Nemanjina 57a, 12000 Pozarevac, Serbia · Tel: +38112541022· VAT: 111385444 Reg. 21473642
e-mail: office@d-logic.com · www.d-logic.com

Table of contents

1. Introduction

Link: https://git.d-logic.net/nfc-rfid-reader-sdk/sam_tool-executable.git
This software uses for SAM (Secure Application Module) personalization in AV1 mode, and key management in AV2 mode. There are the two types of NXP SAM supported: T1AD2060, and T1AR1070. Main frame is shown on the picture:

Digital Logic Ltd.
Address: Nemanjina 57a, 12000 Pozarevac, Serbia · Tel: +38112541022· VAT: 111385444 Reg. 21473642
e-mail: office@d-logic.com · www.d-logic.com



For proper functionality it is need connect the uFR Classic CS with SAM card to the PC. Firmware versions there support SAM are 5.100.xxx. For same hardware exist firmware versions 5.0.xxx, which does not support SAM, instead they uses keys stored into reader.

2. Personalization and key management

Our SAM cards that come with the readers are in AV2 mode.
Master key structure is:
KeyA = , VerA = 0
KeyB = 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00, VerB = 1
KeyC = 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00, VerC = 2
SAM is not locked at power up or reset.
All KST (1 - 127) are reset, key no CEK = 0, key ver CEK = VerA = 0
if a user uses his card in AV1 mode, he can switch to AV2 mode with this software.

2.1. Get version and UID information

For information about SAM type (version) and 7 bytes UID (Unique Identifier) press button GET VERSION.
Supported version of SAM are:

- T1AD2060 AV1 MODE
- T1AD2060 AV2 MODE
- T1AR1070 AV1 MODE
- T1AR1070 AV2 MODE

2.2. AV1 mode personalization

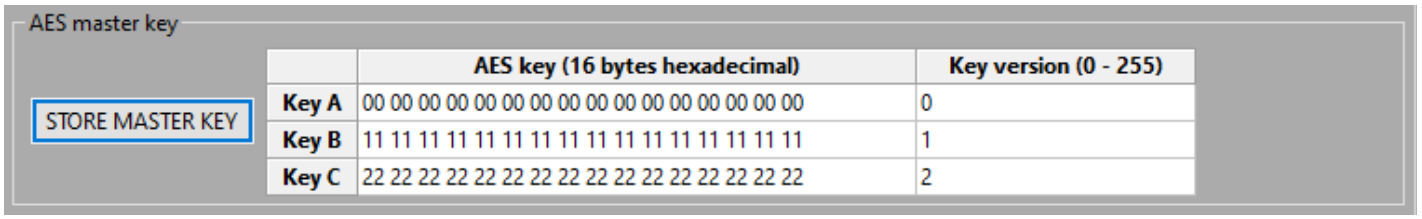
By default, SAM is in AV1 mode, and master key is DES (8 zeros 00 00 00 00 00 00 00 00).
If this SAM card uses in AV1 mode, and master key is not same as factory default, please change it to default value for this software support.

2.2.1. AES master key

First step for personalization in AV1 mode is master key KST (Key Storage Table) definition. It is need to definition 3 AES128 keys (16 bytes long), and versions of these keys (0 - 255), and then press STORE

Digital Logic Ltd.
Address: Nemanjina 57a, 12000 Pozarevac, Serbia · Tel: +38112541022· VAT: 111385444 Reg. 21473642
e-mail: office@d-logic.com · www.d-logic.com

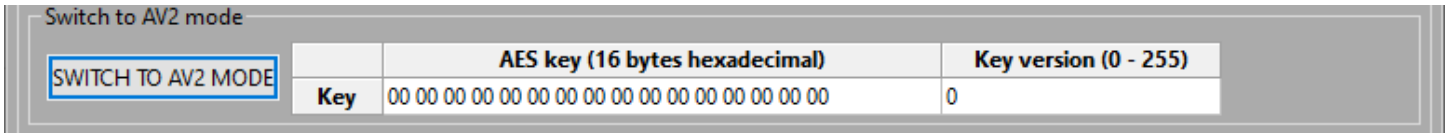
MASTER KEY button



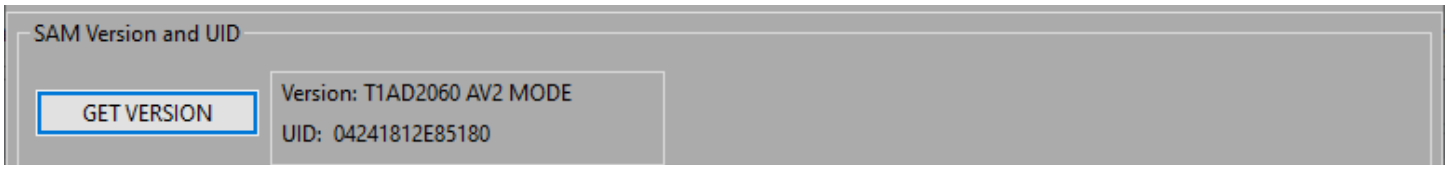
Status of operation will be written in the Status Bar.

2.2.2. Switch to AV2 mode

This is irreversible process. Switch from AV2 mode to AV1 mode is not possible.
Authentication with AES master key is required.
When the SAM switches to AV2 mode, then all KST on SAM, except master key, (key no 1 - 127) will be reset. For KST changing, authentication with master key A, and version of master key A is necessary.



Check if the SAM in AV2 mode



2.3. AV2 mode operations

2.3.1. Host key

The host key is AES key, which uses for host authentication, and/or lock and unlock SAM.
Host authentication is required for changing of any key.
When the key changes for the first time in AV2 mode, host authentication with master key A (key no = 0, key version = version of master key A).

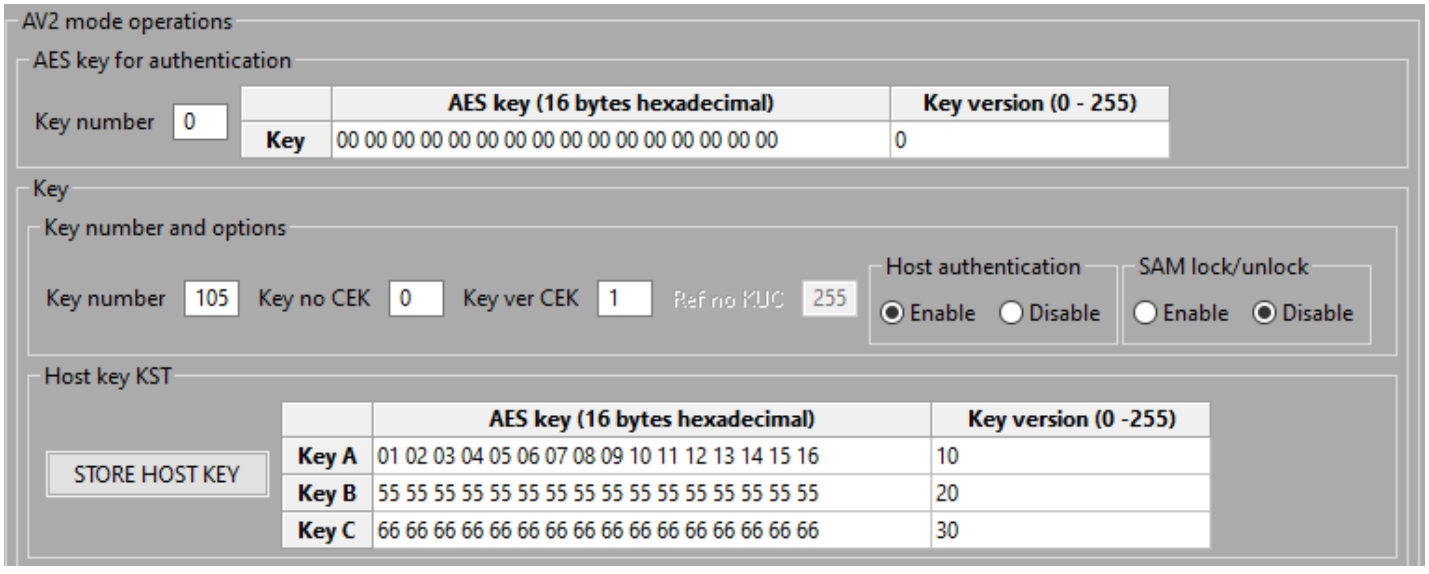
In the panel AES key for authentication is need to enter key number equal to current Key no CEK (Key Reference Number of Change Entry Key) (0 - 127) for KST which will be changed. If uses master key then key number is 0. Key version must be equal to current Key ver CEK (Key Version of Change Entry Key).

In the panel Key number and options is need to enter key number (Key Reference Number) of KST which will be changed, new values for Key no CEK and Key ver CEK, option for host authentication ability and option for SAM lock/unlock ability.
If the master key (key number = 0) host authentication option enabled, then after SAM power up or reset, and unlocking if required, authentication with key with host authentication ability or with master key is required for work with card (PICC Proximity Integrated Circuit Card).
If the master key SAM lock/unlock option enabled, then after SAM power up or reset SAM is locked, and minimal command set is active. SAM can unlocks with key with SAM lock/unlock ability, or host authentication is required for proper work. For detailed read NXP documentation.
uFR reader after SAM activation check if the master key SAM lock/unlock option enabled, and tries to unlock SAM with AES key which stored into reader for this purpose. At this way SAM will be work with cards only on the readers which have proper unlock key.

For other host keys (key number 1 - 127) host authentication option, gives host authentication ability to this host key, and lock/unlock option gives lock/unlock ability to this host key.

Option Ref no KUC (Reference Number of Key Usage Counter) not supported, and number of authentication with key have not limit (Ref no KUC = 255).

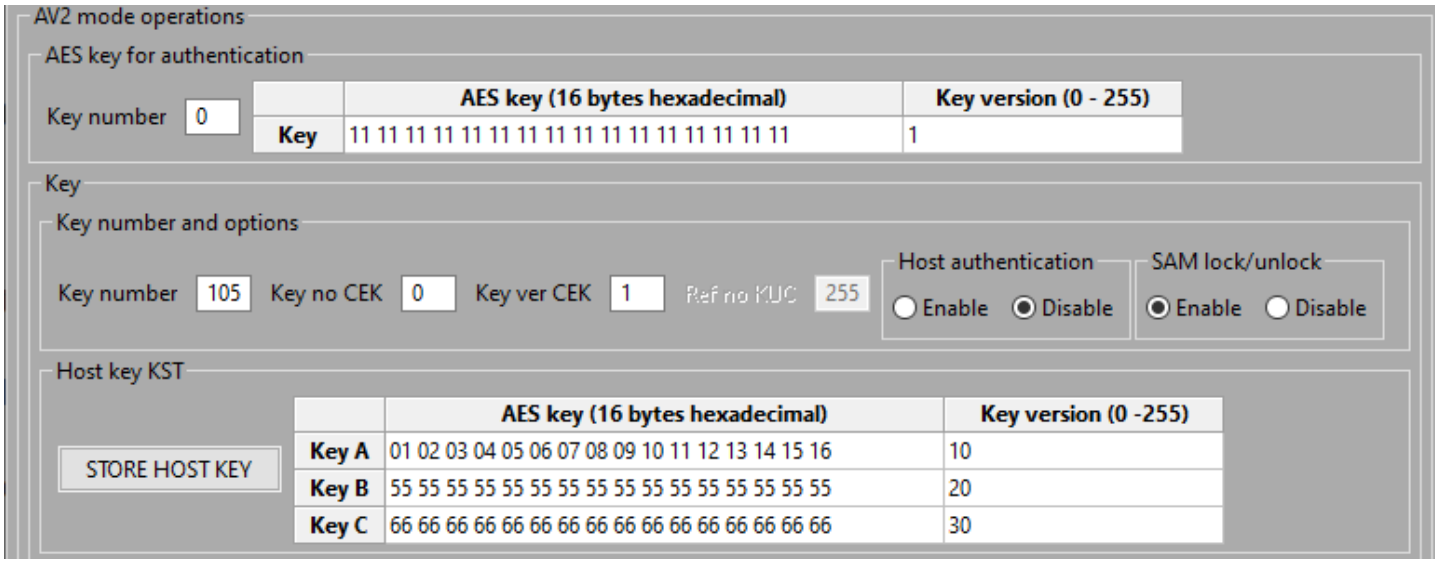
In the panel Host key KST is need to enter 3 AES keys (16 bytes in the hexadecimal format) and their versions (0 - 255). After the all parameters and values entered, press button STORE HOST KEY, to store this KST into SAM.



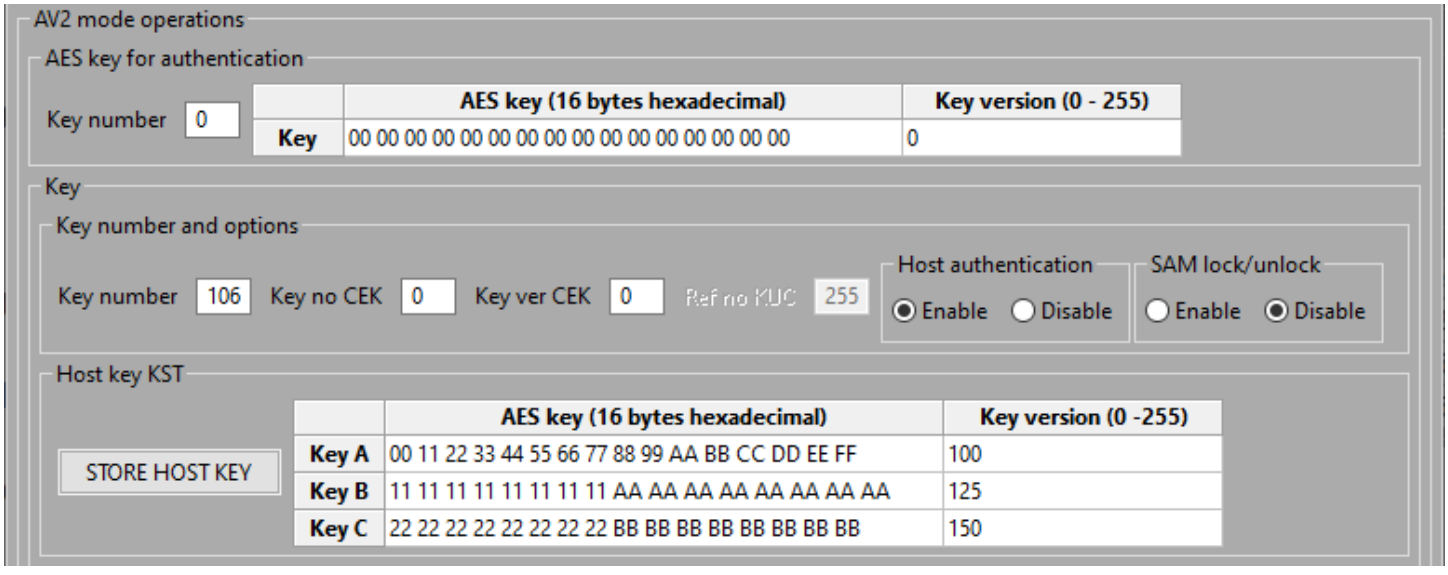
This host key has parameters: key number = 105, current Key no CEK = 0, current Key ver CEK = 0 (first key changing with master key A), futured Key no CEK = 0, futured Key ver CEK = 1 (futured key changing with

master key B (version of master key B = 1)), host authentication ability enabled, lock/unlock ability disabled. KST values are: Key A = 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16, Key A version = 10, Key B = 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55 55, Key B version = 20, Key C = 66 66 66 66 66 66 66 66 66 66 66 66 66 66 66 66, Key C version = 30.

For example change this host key 105, to key which has lock/unlock ability only. Other parameters, and values are unchanged.



Make host key 106 for host authentication.



2.3.2. Card key

The card (PICC) key uses for authentication on PICC.

This key may be:

- AES (16 bytes) for desfire and mifare plus card
- DES (8 bytes) for desfire card
- 2K3DES (16 bytes) for ultralight C card
- 2K3DES (16 bytes) for desfire card
- 3K3DES (24 bytes) for desfire card
- Crypto1 (6 bytes) for mifare classic card

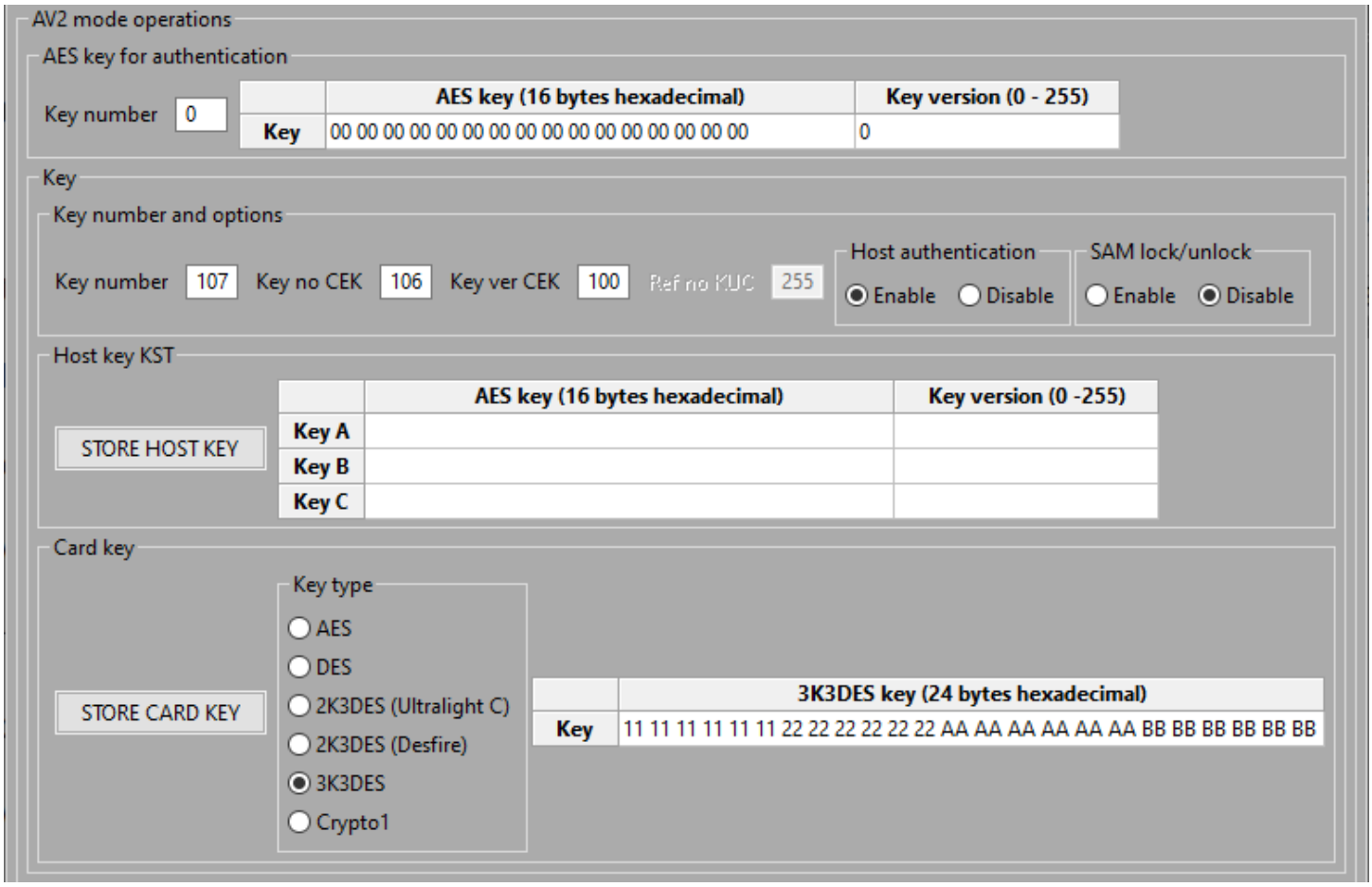
Parameters and values for host authentication key enter into panel AES key for authentication in the same manner as for host key.

In the panel Key number and option is need to enter Key number, Key no CEK, and Key ver CEK. Other parameters are ignored.

In the panel Card key, chose the type of key, and enter value of key. For Crypto1 key type, enter two keys (KeyA and KeyB) continuously (first KeyA 6 bytes and then KeyB 6 bytes, 12 bytes in total). When the all parameters and values entered, press button STORE CARD KEY to store card key into SAM.

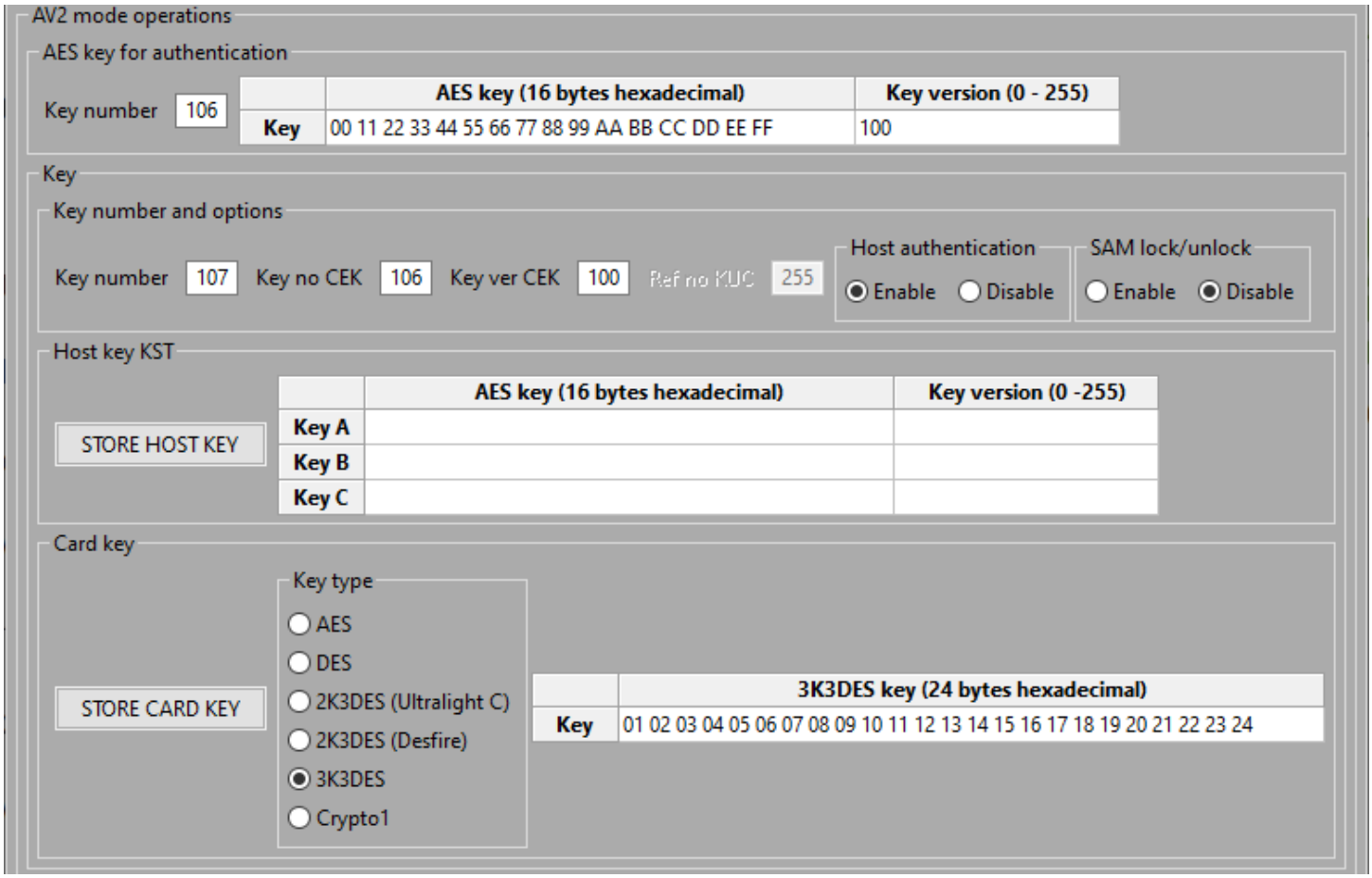
In one KST, stores just one card key, for compatibility reason of internal reader key using. Internal reader key index for Crypto1 keys is from 0 to 31, and for AES, DES, 2K3DES or 3K3DES is from 0 to 15. SAM card key index may be from 1 to 127, except host key indexes.

Address: Nemanjina 57a, 12000 Pozarevac, Serbia · Tel: +38112541022· VAT: 111385444 Reg. 21473642
e-mail: office@d-logic.com · www.d-logic.com



Card key parameters and values: Key no = 107, current Key no CEK = 0, current Key ver CEK = 0 (first key changing with master key A), futured Key no CEK = 106, futured Key ver CEK = 100 (Key A of KST 106), type of card key is 3K3DES (24 bytes), value of key 11 11 11 11 11 11 22 22 22 22 22 22 AA AA AA AA AA AA BB BB BB BB BB BB.

Change value of key 107 to 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24. Other parameters are unchanged.

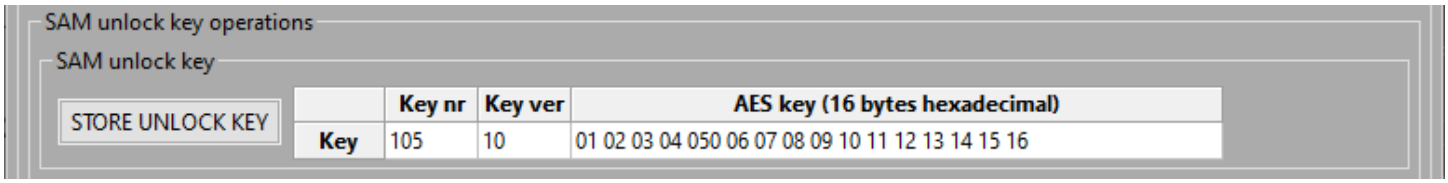


2.4. SAM unlock key operations

2.4.1. SAM unlock key store into reader

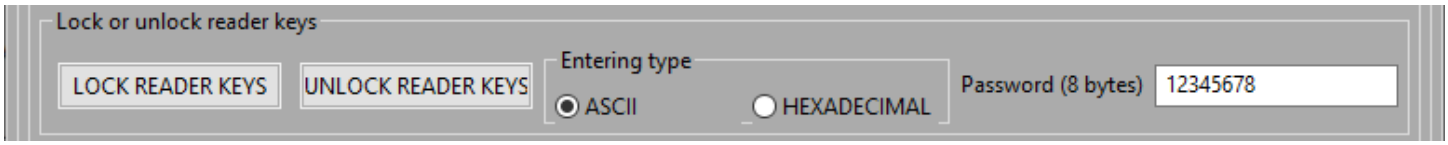
If master key has enabled lock/unlock parameter, then SAM unlock with key with lock/unlock ability is required. uFR reader tries to unlock SAM with key which stored into reader.
In the panel SAM unlock key enter parameters and value of key with lock/unlock ability which is stored into SAM.
When the all parameters and value entered press key STORE UNLOCK KEY to store key into reader.
If the reader internal keys are locked, operation will be rejected, then the internal keys unlocking is required.

For example store the key A no 105 into reader. Key 105 has lock/unlock ability, and has not host authentication ability.

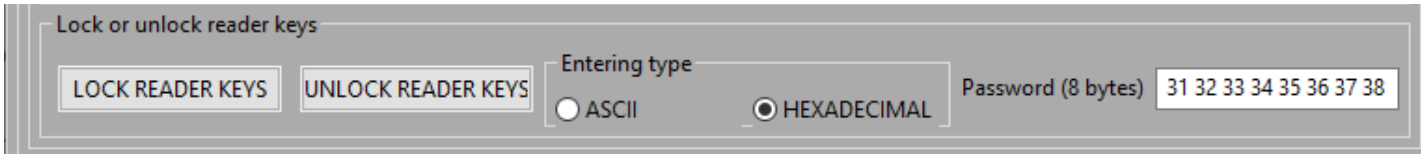


2.4.2. Lock or unlock reader keys

For unlock reader keys is need to enter valid password (8 bytes), and press button UNLOCK READER KEYS in panel Lock or unlock reader keys.
For lock reader keys in need to enter any password (8 bytes). Reader keys must be unlocked. This is factory default state.
Password may be entered in two ways: ASCII and hexadecimal.
There are examples of entering of same password in the different ways:
ASCII



Hexadecimal



Digital Logic Ltd.
Address: Nemanjina 57a, 12000 Pozarevac, Serbia · Tel: +38112541022· VAT: 111385444 Reg. 21473642
e-mail: office@d-logic.com · www.d-logic.com

Revision history

Date	Version	Comment
2019-09-09	1.0	Base document

Digital Logic Ltd.

Address: Nemanjina 57a, 12000 Pozarevac, Serbia · Tel: +38112541022· VAT: 111385444 Reg. 21473642
e-mail: office@d-logic.com · www.d-logic.com