User Guide to the Smartcard Manager, v2.2

Configuring readers for smart cards

rf IDEAS, Inc.

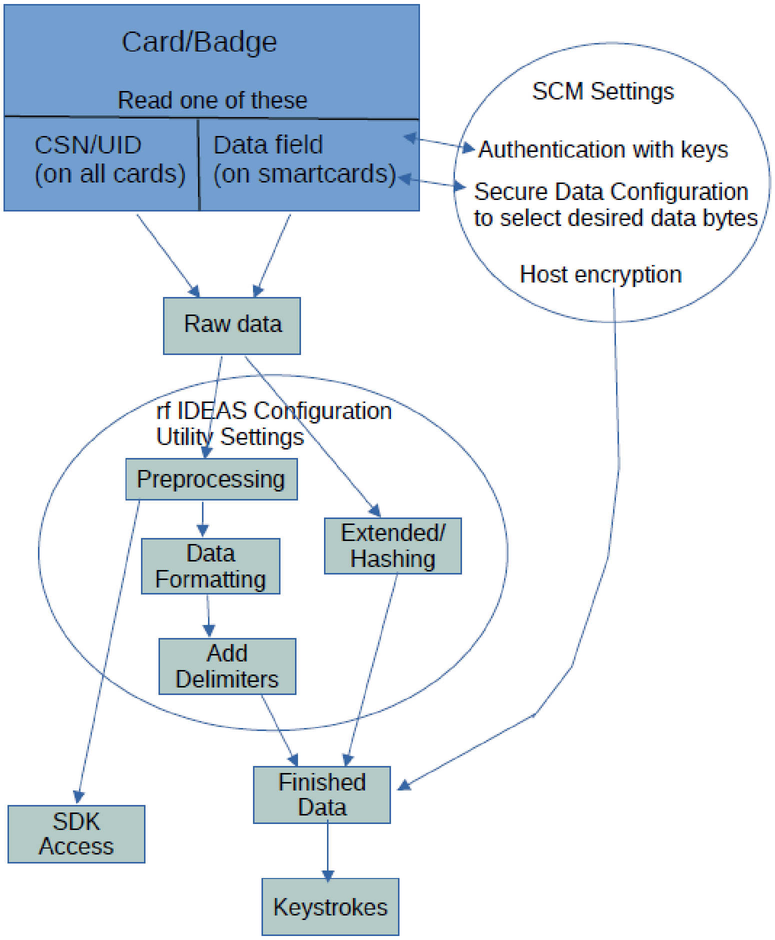
October 2023

Table of Contents

1) Scope

This user guide describes how to use the Smartcard Manager (SCM) application to configure rf IDEAS readers to read secure data. Readers that are capable of reading data fields from contactless cards require additional settings beyond our typical configuration. The SCM supports MFP24, Keystroke and SDK protocols (including CCID and Ibis). The difference in protocols is all handled internally, but may affect availability of some settings. The SCM does not support ethernet, serial or CDC protocols.

2) System Overview

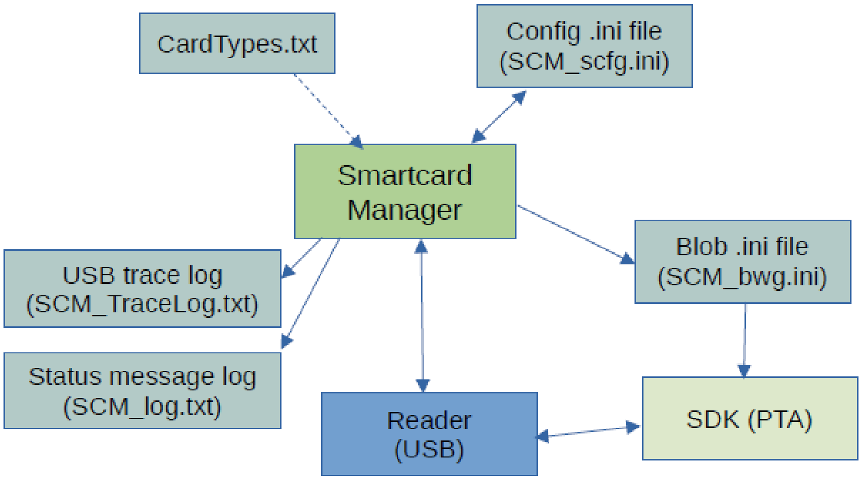


The Smartcard Manager will inform the reader what data bytes to read and what keys are needed to access that data. Then pcProxConfig or the rf IDEAS Configuration Utility can be used for formatting of that data, to get the desired output for keystrokes or accessing by SDK. Data in SDK undergoes less processing than keystroke data. MFP24 readers do not process the raw card data.

NOTE: All numeric entries in the SCM are in hexadecimal!

3) File Overview

There are a number of files associated with the Smartcard Manager. They will be covered in depth later in the document.


CardTypes.txt
Config .ini file (SCM_scfg.ini)
Smartcard Manager
USB trace log (SCM_TraceLog.txt)
Blob .ini file (SCM_bwg.ini)
Status message log (SCM_log.txt)
Reader (USB)
SDK (PTA)

4) Cards and Keys

The following table has a brief overview of smart cards that can be accessed with Smartcard Manager, and appropriate firmware (most firmware will support a subset of this table).

Card Type	**Variations Supported**	**Key type/Protection**	**Memory layout**
LEGIC	Advant (ISO-14443A and ISO-15693), prime	1/2/3/ key 3DES, AES-128, AES-192, AES-256, SAM launch	Segments, accessed by segment number or Stamp ID
MIFARE Classic	Standard, MIFARE Plus at SL1	MIFARE Standard (6-byte) on Key A or B	Blocks (16 bytes) and Sectors (nominally 3 data blocks)
MIFARE Plus	S, SE, C, X at SL3	AES-128	Blocks (16 bytes) and Sectors (nominally 3 data blocks)
MIFARE DESFire	EV1, LEAF, EV1 features of EV2, EV3	AES-128, 1K TDEA, 2K TDEA, 3K TDEA	Applications (AID) containing Files of variable size
MIFARE UltraLight	Standard, C, unprotected portion of EV1	None, 2K TDEA	Pages of 4 bytes each
FeliCa	Standard	None, 3DES, AES-128	Blocks of 16 bytes
FeliCa	Lite/Lite-S	None, AES-128	Blocks of 16 bytes

The complete card list (including those that only report the UID and CSN) is built into the SCM app. This card list can be replaced by including an updated copy of the file “CardTypes.txt” in the same directory as the executable. This file needs to follow a specific format.

5) File Menu

Save Configuration

Save configuration settings in a readable .ini file for all settings and keys that are currently set in the active tabs. To avoid saving a key in a readable format, it is recommended to use the Encrypt button found in the key tab before saving the configuration. This has a security feature preventing changes to the file outside of SCM. The default name is “SCM_scfg.ini”.

Load Configuration

Retrieve configuration settings from a previously stored secure file.

Save Unsecure Configuration

Similar to Save Configuration except that it uses the older format without the security feature. The default name is “SCM_cfg.ini”.

Load Unsecure Configuration

Similar to Load Configuration, but without checking the tamper resistant security feature. This is useful for reading configuration settings that were stored from an earlier version of the SCM.

*Export Blob *.ini File*

Create a file with raw hex codes that can be used by the rf IDEAS SDK to send configuration blobs to the reader. After selecting this, the user needs to do the steps to configure the reader as desired, and all blob output will be redirected to the .ini file. Configuration messages are redirected, not actually sent to the reader, during this time. Configuration status messages are in orange. After configuration steps are complete, stop the export. This .ini file is used by the rf IDEAS SDK API and associated applications.

Start USB Trace Log File

Start recording all USB messages to/from the SCM (primarily for development/debugging uses). It continues until the program exits.

Save Status Log

Write the history of status messages to a log file (primarily for development/debugging uses). This is a maximum of 50 previous messages that have been displayed in the status bar since the app was started.

Exit

Self-explanatory.

6) Options Menu

Reset to Defaults

Send a command to the reader to reset all configuration settings to the default values.

Get Installed Hardware

Get a brief list of installed hardware from the reader, such as SAM chips, low-frequency radio, etc. In some cases, an item may be present but still cannot be used, such as an NXP SAM AVx chip that has an unknown master key.

Read SAM Version Information

Retrieve the version information for any SAMs installed on the reader. Not available on all readers.

Connect to Reader

Looks for a reader connected by USB to the PC. Essentially the same as the Connect/Reconnect button on the General Settings tab.

Disconnect from Reader

End the USB connection to reader.

Get Reader Trace Log

Retrieve the reader trace log, a low-memory log of select reader steps, such as attempts to read a smart card. Not available on all readers. For debug/development purposes.

Get Autotune Values

Retrieve the auto-tune step values during the last card read attempt. For debug/development purposes.

Send Convenience Formatting with Config

Set some common format options when sending the reader configuration (0/0 parity, hex output, etc.) Note that this can conflict with Configuration Utility and *.hwg file settings.

Perform Beep Test

Send a beep command to the reader, to test the connection and help the user verify which reader is connected.

7) Help Menu

About Smartcard Manager

Display version and a short message about the Smartcard Manager.

About Reader

Retrieve various identification values about the reader, including version and model number.

Help with Find Menu

Simple description of items in the Find Menu.

Help with Options Menu

Simple description of items in the Options Menu.

8) General Settings

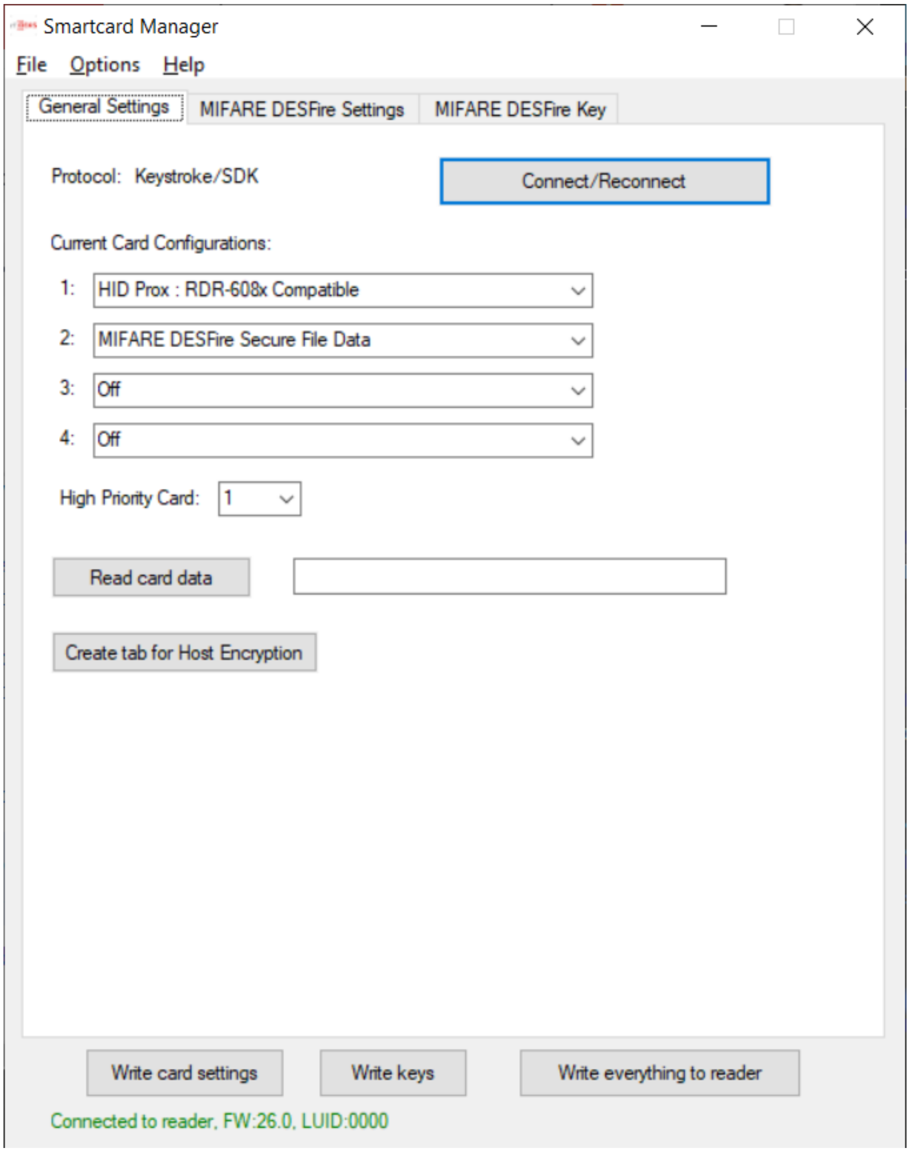
In the General Settings tab, **Connect/Reconnect** will establish connections to the reader, useful when switching readers on the PC (it will only connect to one reader at a time). It reads the current configuration of the reader as part of the connection process.

The General Settings tab is used to display and select the card types. Additional tabs are used to select the specific read/authentication configuration, send keys, and which bytes to read. The rf IDEAS Configuration Utility can be used if additional settings are needed for specialized keystroke output, such as converting the data to decimal or ASCII output. There can be multiple secure file card types set at one time, and a mix of MIFARE card types and/or repeats of a MIFARE card type. LEGIC readers do not read MIFARE secure data and vice versa.

If the same secure file data card type is selected for more than one configuration, then a pull-down Card Configuration Index (1-4) in the relevant tabs will determine which configuration is currently selected.

For newer readers (after LNC firmware version 22.2 and all WNC firmware), then there is an option to create another tab to set the Host Encryption Key. This key is used to encrypt keystroke card data sent to the host from the reader. This affects all keystroke output from the reader. This key can be sent individually from the Host Encryption tab, as well as the bottom button to write all keys.

At the bottom of window, below the tab space, are three buttons for writing settings to the reader:
Write card settings: Write the file configuration settings for all smart cards in the current configuration.
Write keys: Write any entered keys for all smart cards in the current configuration. The key will be written to a SAM (Secure Access Module) or similar 3rd party chip. Depending on the reader, this may be a removable SIM chip. In no case can the reader firmware running on the control processor be able to read back the key for a smart card from a 3rd party chip. If the field for a key is empty, no action is taken (ie. the reader will not send a blank key or all zeros).
Write everything to reader: This is a combination of the other two buttons.



Protocol: Keystroke/SDK

Current Card Configurations:

1: HID Prox : RDR-608x Compatible

2: MIFARE DESFire Secure File Data

3: Off

4: Off

High Priority Card: 1

Connected to reader, FW:26.0, LUID:0000

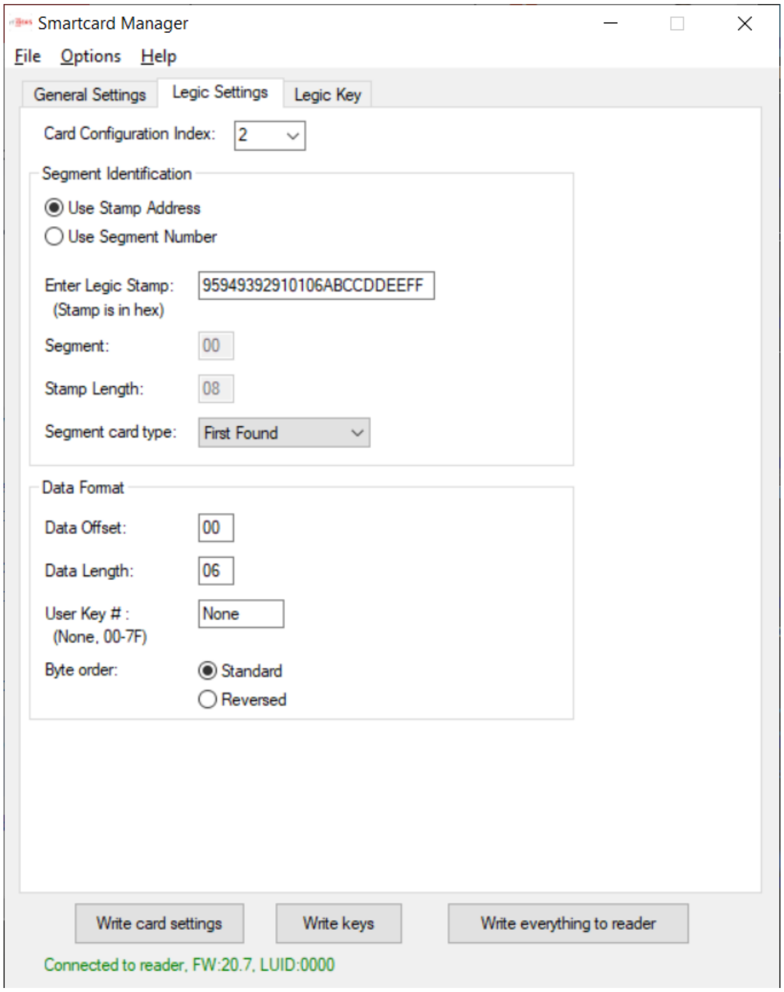
Figure 1 General Settings tab of the Smartcard Manager

9) LEGIC Settings and Key

If a card type is set to LEGIC Stamp, then a tab for LEGIC Settings will appear. For firmware version 20.7 and later, a tab for LEGIC Key will also appear. The LEGIC settings tab has the following fields:

A LEGIC segment can be addressed by the Stamp Address, or by the segment number. When using the segment number, an optional Stamp Length field is available. Entering this will keep the data consistent if both LEGIC advant and prime cards are being used, as the prime card includes the stamp with the card data, while the advant does not.

The Segment Card Type field is useful when using a multi-technology LEGIC card. There are three LEGIC technologies: prime, advant on ISO-14443A, and advant on ISO-15693. On a multi-technology card, there will be a combination of technologies, each with its own range of segments, possibly using the same Stamp address. This field will determine which one is used, or "First Found" is non-discriminatory (default case, and safest choice for the standard single-technology card).



Card Configuration Index: 2

Segment Identification

● Use Stamp Address

○ Use Segment Number

Enter Legic Stamp: (Stamp is in hex) 95949392910106ABCCDDEEFF

Segment: 00

Stamp Length: 08

Segment card type: First Found

Data Format

Data Offset: 00

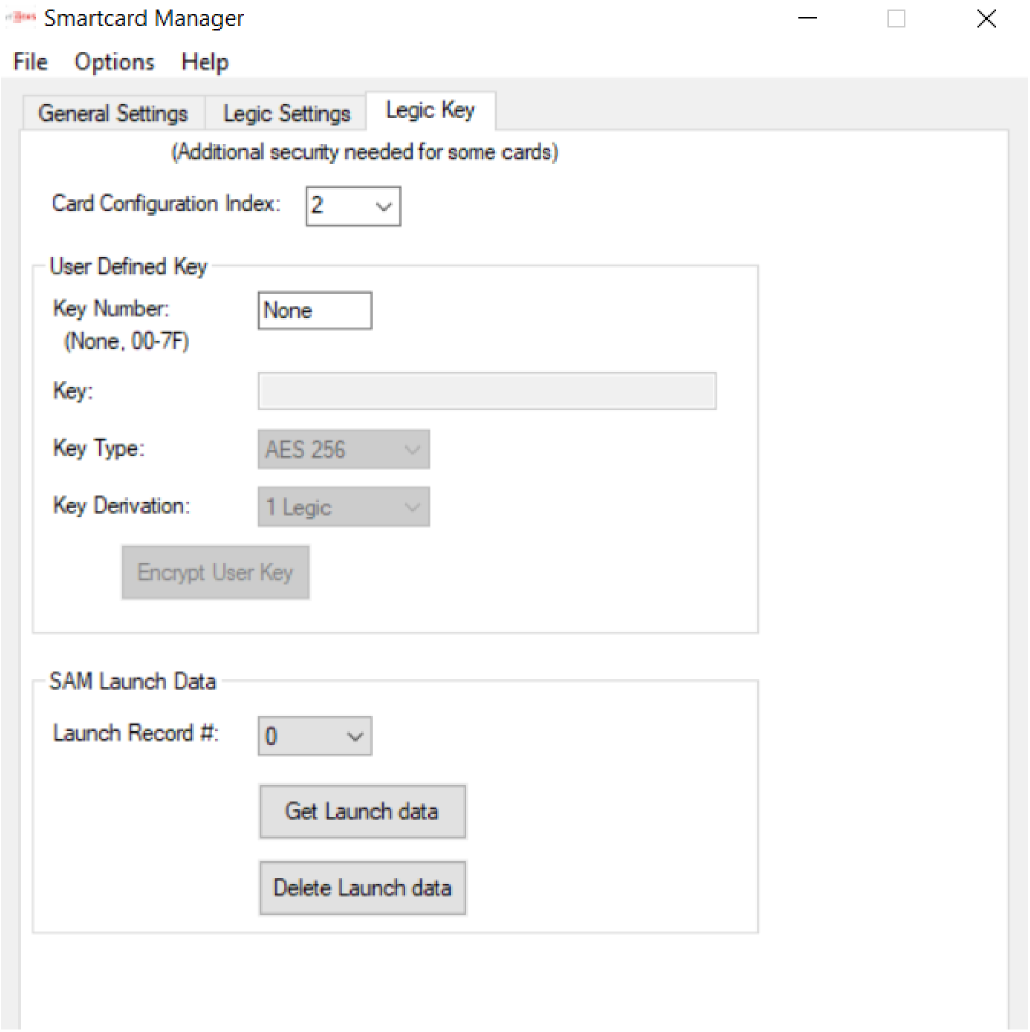
Data Length: 06

User Key # : (None, 00-7F) None

Byte order: ● Standard ○ Reversed

Connected to reader, FW:20.7, LUID:0000

For all WNC firmware, and LNC firmware versions 20.7 and later, a user-defined key number can be entered. This key number is an index to a table stored in the LEGIC chip. The actual key is entered in the next tab, the LEGIC Key tab.



(Additional security needed for some cards)

Card Configuration Index: 2

Key Number: None
(None, 00-7F)

Key:

Key Type: AES 256

Key Derivation: 1 Legic

Launch Record #: 0

The key is entered on this tab, and stored at location Key Number in the LEGIC chip. The key cannot be read back. If desired, the key can be encrypted after it is entered. Thereafter it will be displayed in the encrypted form, stored in the configuration file as encrypted (if a configuration file is created), and it is sent encrypted over USB to the reader.

The bottom section of this tab is used for Launch (baptism) using a SAM-63 card. Some user cards require that a reader be launched before the user data can be read. If LEGIC Stamp is selected as a card type, then any LEGIC reader (including LNC 20.5) can be launched with a SAM-63 card.

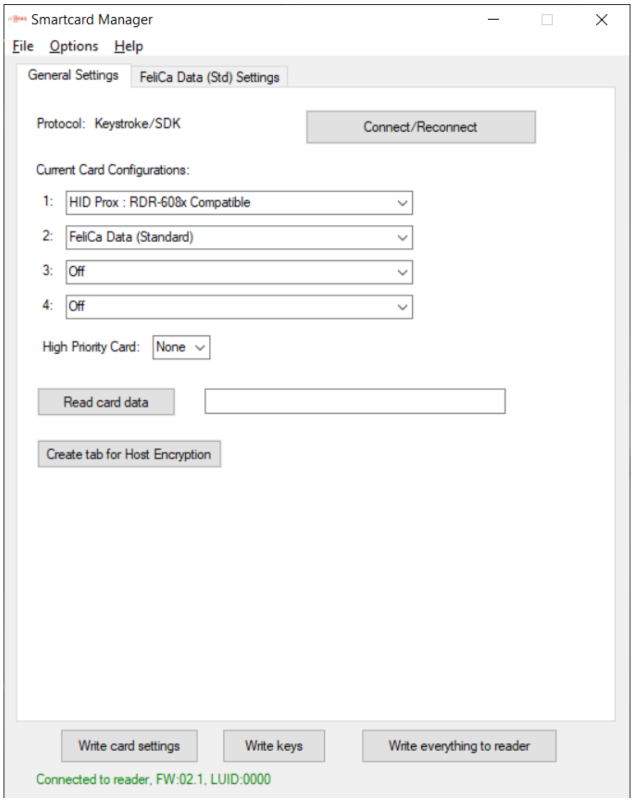
In firmware 20.7 and later, when a SAM-63 card is detected in the field, the usual 15-second window for launching is reduced to 7 seconds, and a beep and/or LED change indicates the launch has occurred. This results in a record being stored in the LEGIC chip. This launch record can be read back, to verify it was launched, and it can also be deleted.

10) FeliCa Standard Card Settings

If a card type is set to FeliCa Data (Standard), then a tab for FeliCa Data (Standard) Settings will appear. This card type is supported starting with firmware version LNC 22.5.

The FeliCa Data (Standard) settings tab has the following sections:

1. SAM Key Configuration
2. Reader Configuration



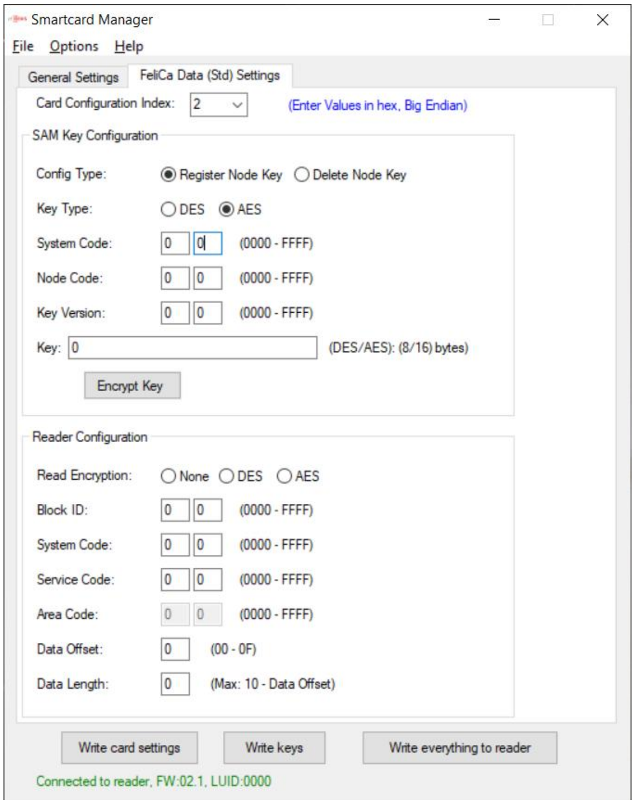
Protocol: Keystroke/SDK

Current Card Configurations:

1: HID Prox : RDR-608x Compatible
2: FeliCa Data (Standard)
3: Off
4: Off

High Priority Card: None

Connected to reader, FW:02.1, LUID:0000



Card Configuration Index: 2 (Enter Values in hex, Big Endian)

SAM Key Configuration

Config Type: ● Register Node Key ○ Delete Node Key
Key Type: ○ DES ● AES
System Code: 0 0 (0000 - FFFF)
Node Code: 0 0 (0000 - FFFF)
Key Version: 0 0 (0000 - FFFF)
Key: 0 (DES/AES): (8/16) bytes)

Reader Configuration

Read Encryption: ○ None ○ DES ○ AES
Block ID: 0 0 (0000 - FFFF)
System Code: 0 0 (0000 - FFFF)
Service Code: 0 0 (0000 - FFFF)
Area Code: 0 0 (0000 - FFFF)
Data Offset: 0 (00 - 0F)
Data Length: 0 (Max: 10 - Data Offset)

Connected to reader, FW:02.1, LUID:0000

1. <u>SAM Key Configuration :</u>

Use this section to program Felica Standard Node key into Sony Felica RW-SAM (RC-S500/S02)
This is independent of any Card Configuration Index.
All fields of this section are disabled if SONY FeliCa RW-SAM is not present in the reader.

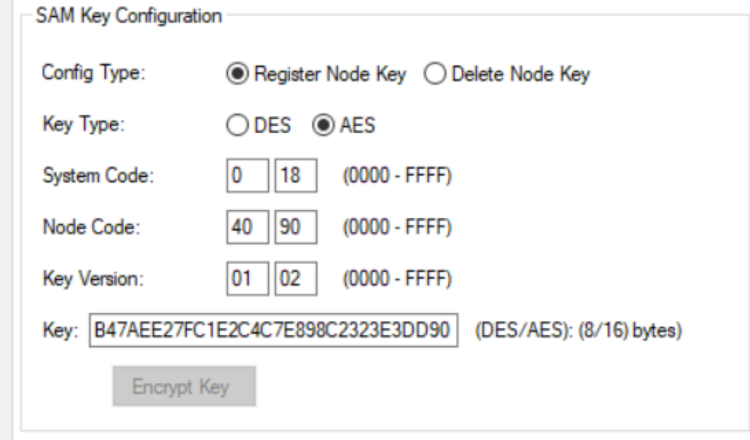
Config Type:
Select if you want to register a key or delete a key.

Key Type:
Select the type of the intended key, between DES key or AES key.
DES key is of 8 bytes. AES key is 16 bytes.

System Code:
Node Code:
Key Version:
Enter two-byte value of System Code, Node Code and Key Version of the intended Key (Big Endian).

Key:
Enter the actual value of the intended Key (Big Endian).
This field is disabled if Config Type selected is Delete Node Key

<u>*Example : System Code - 0x0018, Node Code - 0x4090, Key Version - 0x0102</u>



SAM Key Configuration

Config Type: ● Register Node Key ○ Delete Node Key

Key Type: ○ DES ● AES

System Code: 0 18 (0000 - FFFF)

Node Code: 40 90 (0000 - FFFF)

Key Version: 01 02 (0000 - FFFF)

Key: B47AEE27FC1E2C4C7E898C2323E3DD90 (DES/AES): (8/16) bytes)

Encrypt Key:
After entering the Key, user can encrypt the key using this button. Once the key is encrypted the Encrypt button will be disabled. To re-enable, enter a new key and press tab.

Configure SAM:
Once all the fields are updated and user is ready to send configuration, use the Write keys button, or the Write everything to reader button at the bottom. During configuration, reader flashes Amber and beeps once. Then:
Success: Flashes Green Momentarily and Beeps twice long.
Failure: Flashes Red Momentarily and Beeps twice short.

2. <u>Reader Configuration :</u>

Use this section to program the Reader to read a data block of a FeliCa Standard Card. It is based on Card Configuration Index selected. It supports configuration for reading all 3 three types of FeliCa Standard Cards: AES only, DES only, AES/DES

Read Encryption:
Select the Read Method of the intended Block data. Encrypted (AES/DES) or None.

Block ID:
Specify the 2-byte Block ID of the intended Block data to be read (Big Endian).
For Example : Block ID – 1 is 0001, Block ID – 256 is 0100

System Code, Service Code:
Specify the 2-byte System Code and Service Code of the intended Block data to be read (Big Endian).

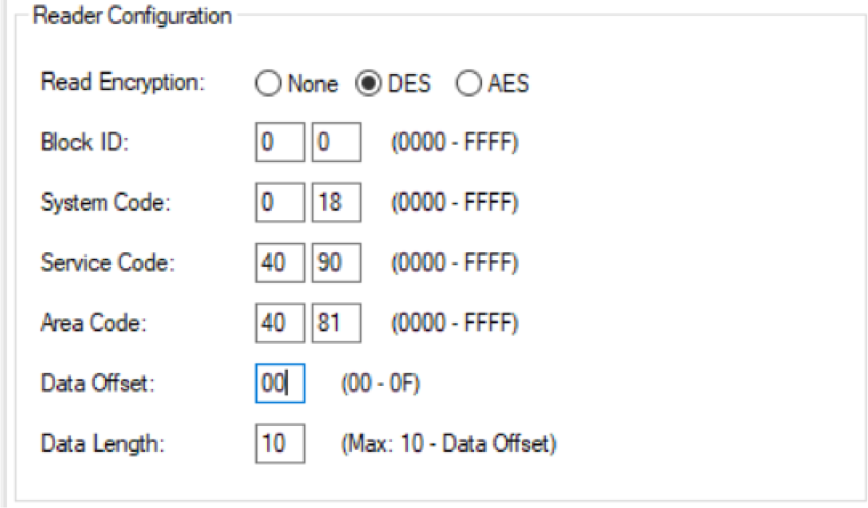
Area Code:
Specify the 2-byte Area Code of the intended Block data to be read (Big Endian).
This field is only used/required, if Read Encryption : DES is selected.
For Read Encryption : None and AES, this field is disabled.

Data Offset:
The Block Data is of 16 bytes, starting from byte 0 … byte 15.
Provide appropriate offset value as per user requirement.

Data Length:
Provide the length of data to be returned by the reader.
Max data length to be read is 16 bytes (0x10), provided Min Data Offset is 0.

Configure Reader:
Once all the fields are updated write the configuration to the reader, using the Write card settings button, or the Write everything to reader button.

<u>*Example : System Code - 0x0018, Service Code - 0x4090, Area Code - 0x4081</u>



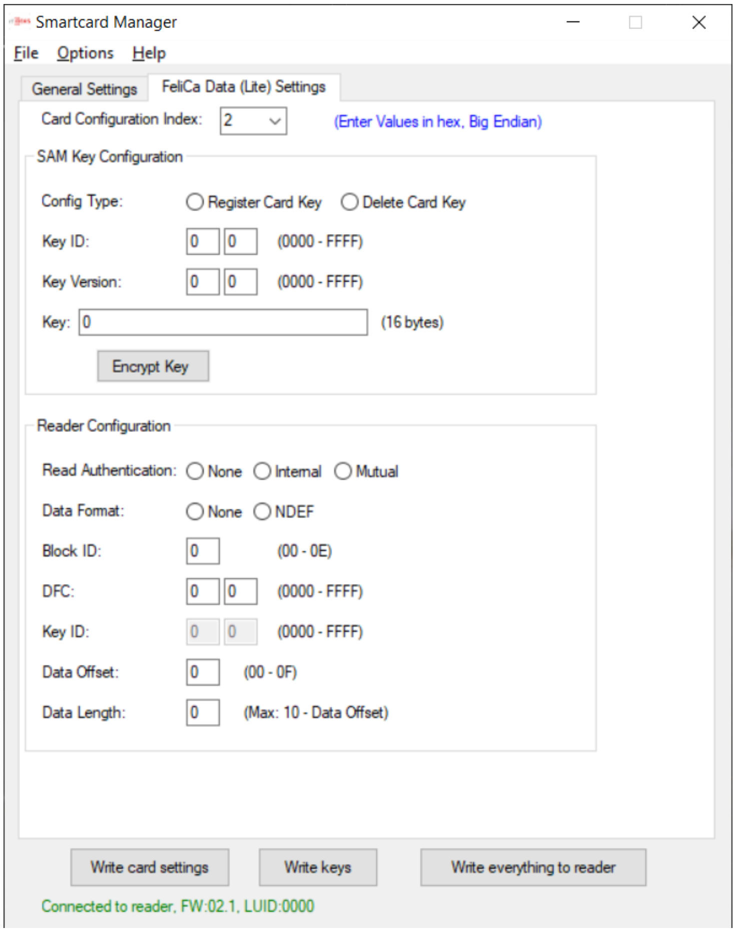
Reader Configuration

Read Encryption: ○ None ● DES ○ AES
Block ID: 0 0 (0000 - FFFF)
System Code: 0 18 (0000 - FFFF)
Service Code: 40 90 (0000 - FFFF)
Area Code: 40 81 (0000 - FFFF)
Data Offset: 00 (00 - 0F)
Data Length: 10 (Max: 10 - Data Offset)

11) FeliCa Lite/Lite-S card Settings

If a card type is set to FeliCa Data (Lite), then a tab for FeliCa Data (Lite) Settings will appear. This card type is supported starting with firmware version LNC 22.5. The FeliCa Data (Lite) settings tab has the following sections:

1. SAM Key Configuration
2. Reader Configuration



Card Configuration Index: 2
(Enter Values in hex, Big Endian)

SAM Key Configuration
Config Type: ○ Register Card Key ○ Delete Card Key
Key ID: 0 0 (0000 - FFFF)
Key Version: 0 0 (0000 - FFFF)
Key: 0 (16 bytes)

Reader Configuration
Read Authentication: ○ None ○ Internal ○ Mutual
Data Format: ○ None ○ NDEF
Block ID: 0 (00 - 0E)
DFC: 0 0 (0000 - FFFF)
Key ID: 0 0 (0000 - FFFF)
Data Offset: 0 (00 - 0F)
Data Length: 0 (Max: 10 - Data Offset)

Connected to reader, FW:02.1, LUID:0000

1. SAM Key Configuration :

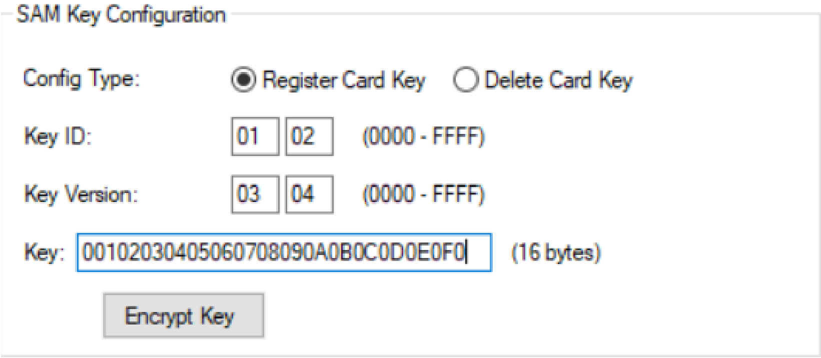
Use this section to program Felica Lite/Lite-S Card key into Sony Felica RW-SAM (RC-S500/S02)
This is independent of any Card Configuration Index.
All fields of this section are disabled if SONY FeliCa RW-SAM is not present in the reader.

Config Type:
Select if you want to register a key or delete a key.

Key ID:
Key Version:
Enter two-byte value of Key ID and Key Version of the intended Key (Big Endian).

Key:
Enter the actual value of the intended Key (Big Endian).
This field is disabled if Config Type selected is Delete Node Key

<u>*Example : Key ID - 0x0102, Key Version - 0x0304</u>



SAM Key Configuration

Config Type: ● Register Card Key ○ Delete Card Key

Key ID: 01 02 (0000 - FFFF)

Key Version: 03 04 (0000 - FFFF)

Key: 00102030405060708090A0B0C0D0E0F0 (16 bytes)

Encrypt Key:
After entering the Key, user can encrypt the key using this button.
Once, the key is Encrypted the field will be disabled. To re-enable field, change the key and press tab.
This field is also disabled if Config Type selected is Delete Card Key

Configure SAM:
Once all the fields are updated and user is ready to send configuration, use the Write keys button, or the Write everything to reader button at the bottom. During configuration, reader flashes Amber and beeps once. Then:
Success: Flashes Green Momentarily and Beeps twice long.
Failure: Flashes Red Momentarily and Beeps twice short.

2. <u>Reader Configuration :</u>

Use this section to program the Reader, to read a Block Data of a FeliCa Lite/Lite-S Card.
It is based on Card Configuration Index selected. The configuration for reading both FeliCa Lite and Lite-S cards is the same.

Read Authentication:
Select the Method of Authentication for intended Block data: Internal, Mutual or None.

Data Format:
Select NDEF if the format of intended block data to be read is NDEF (NFC Data Exchange Format).
If not select None.

Block ID:
Specify the 1-byte Block ID of the intended Block data to be read (Big Endian).
Lite/Lite-S cards only have block numbers in user area from 00 – 0E.

DFC:
Specify the 2-byte Data Format Code of the intended Block data to be read (Big Endian).
If unknown, specify: 0x0000. This field is only used/required if Data Format : None is selected.
For Data Format : NDEF, this field is disabled.

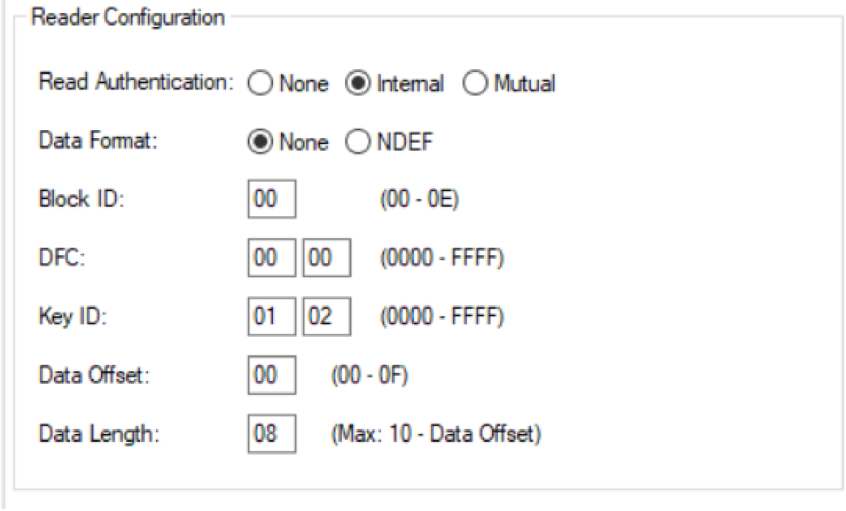
Key ID:
Specify the 2-byte Key ID of the intended Block data to be read (Big Endian).
This field is only used/required, if Read Authentication : Internal or Mutual is selected.
For Read Authentication : None, this field is disabled.

Data Offset:
The Block Data is of 16 bytes, starting from byte 0 … byte 15.
Provide appropriate offset value as per user requirement.

Data Length:
Provide the length of data to be returned by the reader.
Max data length to be read is 16 bytes (0x10), provided Min Data Offset is 0.

Configure Reader:
Once all the fields are updated. Press Configure Reader button, to program the Reader Configuration setting for the chosen Card Configuration Index.

*Example : Block ID - 0x00, DFC - 0x0000, Key ID - 0x0102

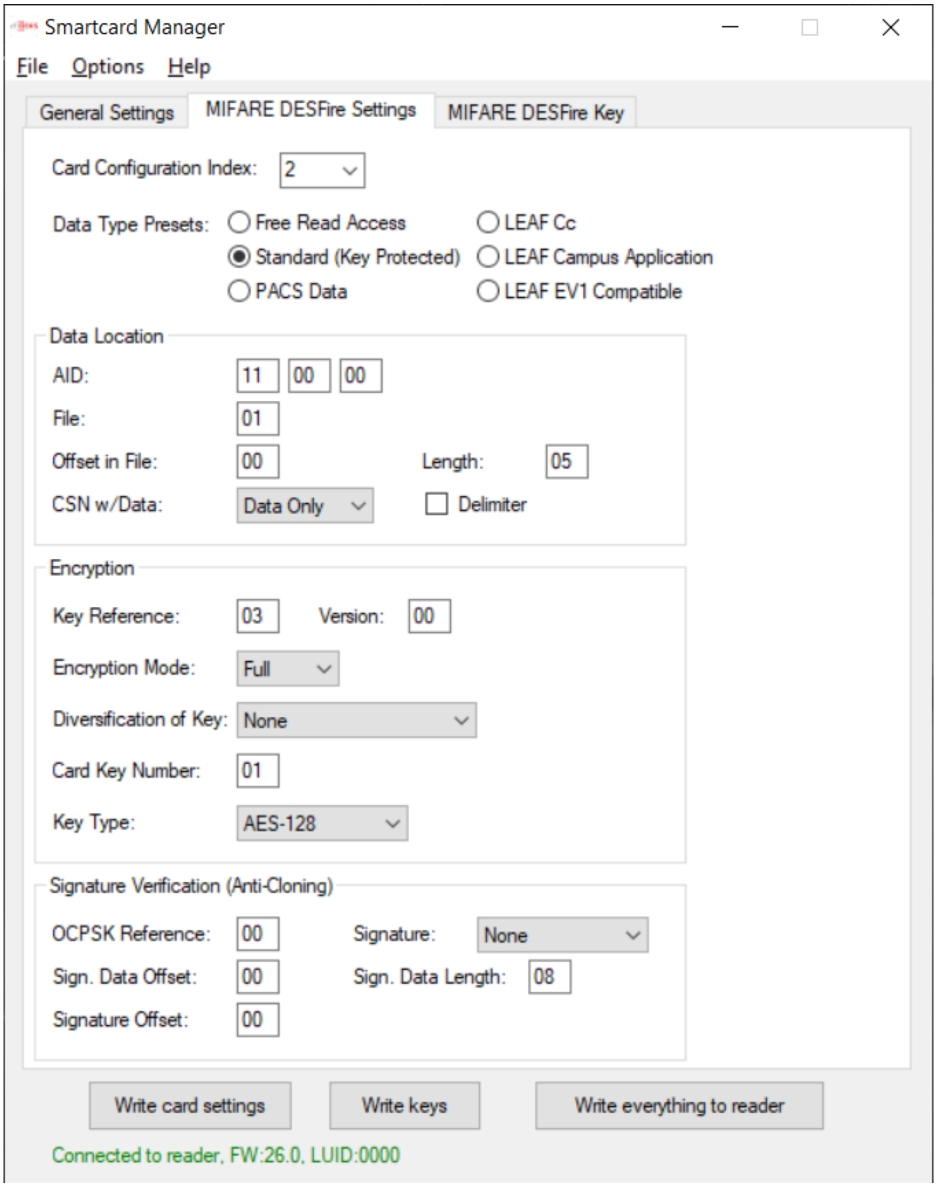


Reader Configuration

Read Authentication: ○ None ● Internal ○ Mutual
Data Format: ● None ○ NDEF
Block ID: 00 (00 - 0E)
DFC: 00 00 (0000 - FFFF)
Key ID: 01 02 (0000 - FFFF)
Data Offset: 00 (00 - 0F)
Data Length: 08 (Max: 10 - Data Offset)

12) MIFARE DESFire Settings

If a card type is set to MIFARE DESFire Secure File Data, then a tab for MIFARE DESFire Settings will appear. This tab contains the following fields needed for reading a DESFire card:



Card Configuration Index: 2

Data Type Presets:
○ Free Read Access
● Standard (Key Protected)
○ PACS Data
○ LEAF Cc
○ LEAF Campus Application
○ LEAF EV1 Compatible

Data Location
AID: 11 00 00
File: 01
Offset in File: 00
Length: 05
CSN w/Data: Data Only
☐ Delimiter

Encryption
Key Reference: 03
Version: 00
Encryption Mode: Full
Diversification of Key: None
Card Key Number: 01
Key Type: AES-128

Signature Verification (Anti-Cloning)
OCPSK Reference: 00
Signature: None
Sign. Data Offset: 00
Sign. Data Length: 08
Signature Offset: 00

Connected to reader, FW:26.0, LUID:0000

The Data Type Presets at the top are quick presets for common uses. For example, the LEAF Cc and LEAF EV1 Compatible presets will fill in the fields to read the Badge ID from a standard LEAF card. The other options are for more customizable data selection.

The rest of the page is organized into three sections:

- Data Location – where the data is located on the card, and what bytes to return.
- Encryption – how the data is protected and with what key.
- Signature Verification – for optional anti-cloning protection.

Data Location:
The MIFARE DESFire cards store data in Application spaces, referred to by their Application ID (AID). Each AID has one or more Files where the data is stored. The AID is sometimes described in big endian format (most significant number first) or little endian format (least significant number first). Smartcard Manager uses the latter, following the lead of NXP tools, but card documentation may vary.

Encryption
The Key Reference is an index into keys stored on the SAM AV2 chip inserted into the reader. The Key can also be programmed at this time using the DESFire Key tab, or can be programmed at another time, even on a different reader or device. In any case, the Key Reference value (and Version, if non-zero) on this page must match the Key ID and Version used when storing the key. The index is a value in the range of hexadecimal values 01 to 7F, the version is a value from 00 to 03.

A diversified key is one that is modified, in part by the card's CSN, so the resulting key is unique to each card. There are different methods of diversification, some are proprietary to a particular vendor. At this time, the options are:

- None
- Encryption (Classic) which is standard AV1 method
- Encryption UID CKN (AV1, but card key number is part of diversification)
- CMAC UID (AV2 method using only UID for diversification input)
- Safetrust (Specific to Safetrust cards)

Card key number refers to which key on the MIFARE card is used for access to the data on this AID/File. This is typically 01, but values can be 00 to 0D. Card key number of 0E is reserved for Free Read Access (no key needed).

Key Types:

- AES-128 (uses a 16 byte, 32 character key)
- 2KTDEA-DES (16 byte 3DES using MIFARE DESFire implementation). For single DES, repeat the 8-byte key.
- 2KTDEA-ISO and 3KTDEA (3DES using ISO-10116). 3KTDEA takes 24 bytes.

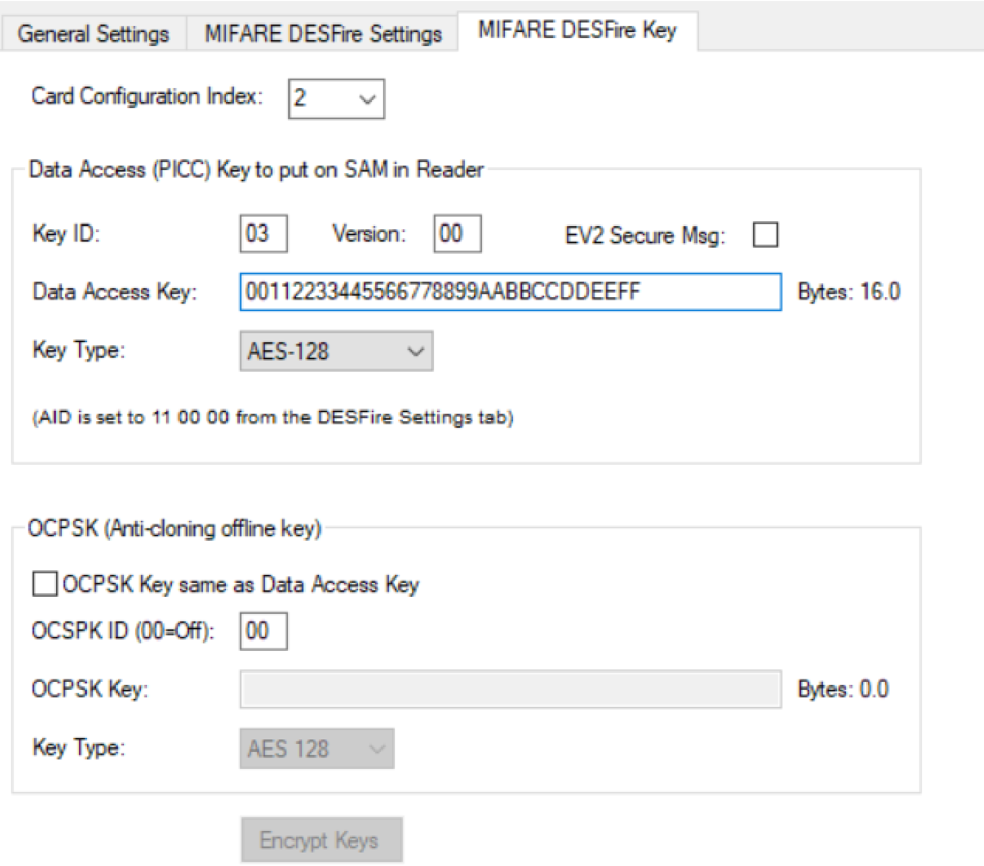
Signature Verification
This involves computing a signature from the data and comparing it to a value on the card, using a key and process distinct from data encryption. The key used to make the signature is not stored on the card being read and uses diversification, so a cloned card will fail the signature verification test. The Signature Verification process uses an additional key reference to the Originality and Cloning Protection System Key (OCPSK).

TIMING NOTE: Signature Verification requires additional data to be read and an additional encryption step. On a standard LEAF Cc card for instance, it nearly doubles the read and response time to about 1.5 seconds.

13) MIFARE DESFire Key

Unless the file data is Free Access, a key will be needed to access the data. The key is stored on the NXP AV2 or AV3 SAM (built-in or inserted). This key is kept separate from reader configuration and other settings and connect be read back. It is not changed if the reader is set to defaults or bootloaded with new firmware. In standard situations, keys can be programmed onto an NXP SAM card on one reader, and then the SAM card can be moved to another reader for use there. (The readers need to be powered off when moving a SAM).

For DESFire, there are two places a key can be used, so there are two sections on this tab. First is Data Access (stored as a PICC key on the SAM). The NXP SAM needs the AID stored with the key, that uses the AID set in the DESFire Settings tab. The second section is for OCPSK (available on some cards for signature verification, stored as an Offline key on the SAM). This can use the same key value as above if desired. AID is not needed for the OCPSK. The OCPSK ID needs to be entered with a non-zero value before the Send OCPSK button is enabled. Both keys can be encrypted for better security in storage (local configuration file) and transit (sending key to the reader).



Card Configuration Index: 2

Data Access (PICC) Key to put on SAM in Reader

Key ID: 03 Version: 00 EV2 Secure Msg: ☐

Data Access Key: 00112233445566778899AABBCCDDEEFF Bytes: 16.0

Key Type: AES-128

(AID is set to 11 00 00 from the DESFire Settings tab)

OCPSK (Anti-cloning offline key)

☐ OCPSK Key same as Data Access Key

OCSPK ID (00=Off): 00

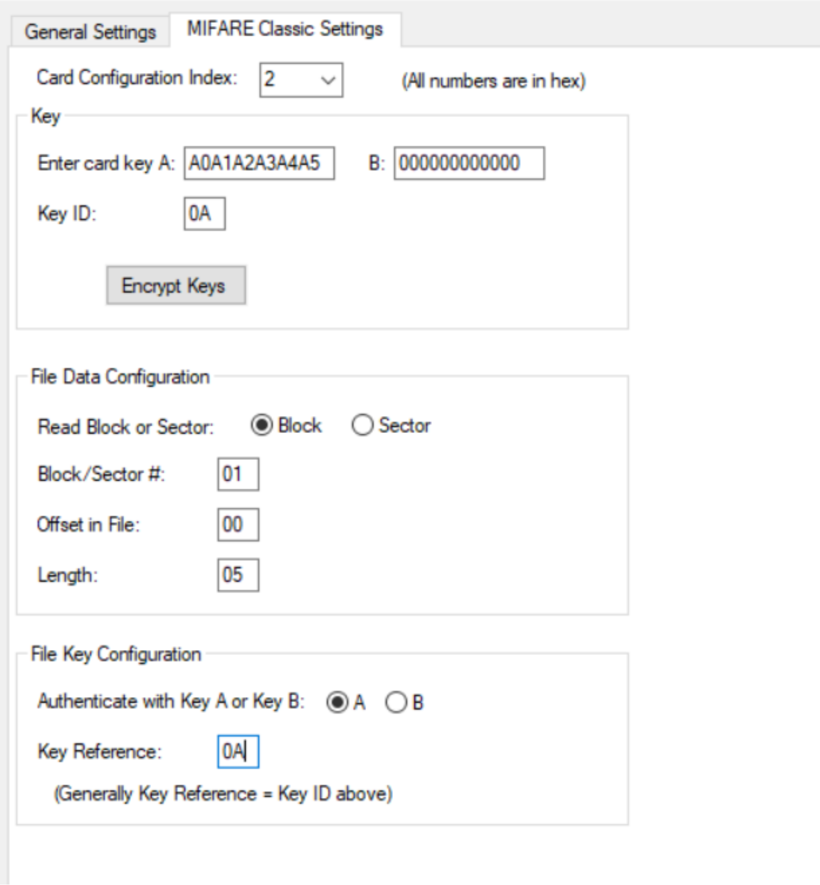
OCPSK Key: Bytes: 0.0

Key Type: AES 128

14) MIFARE Classic Settings Tab

The MIFARE Classic card is simpler than the DESFire. Memory is also arranged differently, with sectors composed of blocks. Typically, a sector has four blocks: three data blocks, and the last block has key and access information. They count from 0, so block 4 is the first data block of sector 1. Each block has 16 bytes, and each sector has 48 bytes of data.

There are two keys, each 6 bytes long. By default, Key A is used, but Key B is also possible. The two keys fit into one entry in the SAM AV2. Key ID and Key Reference values behave the same as in MIFARE DESFire.



Card Configuration Index: 2

(All numbers are in hex)

Key

Enter card key A: A0A1A2A3A4A5 B: 000000000000

Key ID: 0A

File Data Configuration

Read Block or Sector: ● Block ○ Sector

Block/Sector #: 01

Offset in File: 00

Length: 05

File Key Configuration

Authenticate with Key A or Key B: ● A ○ B

Key Reference: 0A

(Generally Key Reference = Key ID above)

Note: The reader firmware has been extended to be able to keystroke up to 48 bytes of data (a typical sector of MIFARE Classic). The SDK (API) interface, however, still has a maximum of 32 bytes. This is only noticeable if the configured length is more than 32 (hexadecimal 20), and the rf IDEAS Configuration Utility (or similar application using our DLL) is used to retrieve data. The first 32 bytes are returned, and it reports a maximum of 255 bits of data.

15) MIFARE Plus

MIFARE Plus uses the same memory layout as Classic, with blocks and sectors. Plus has four security levels.

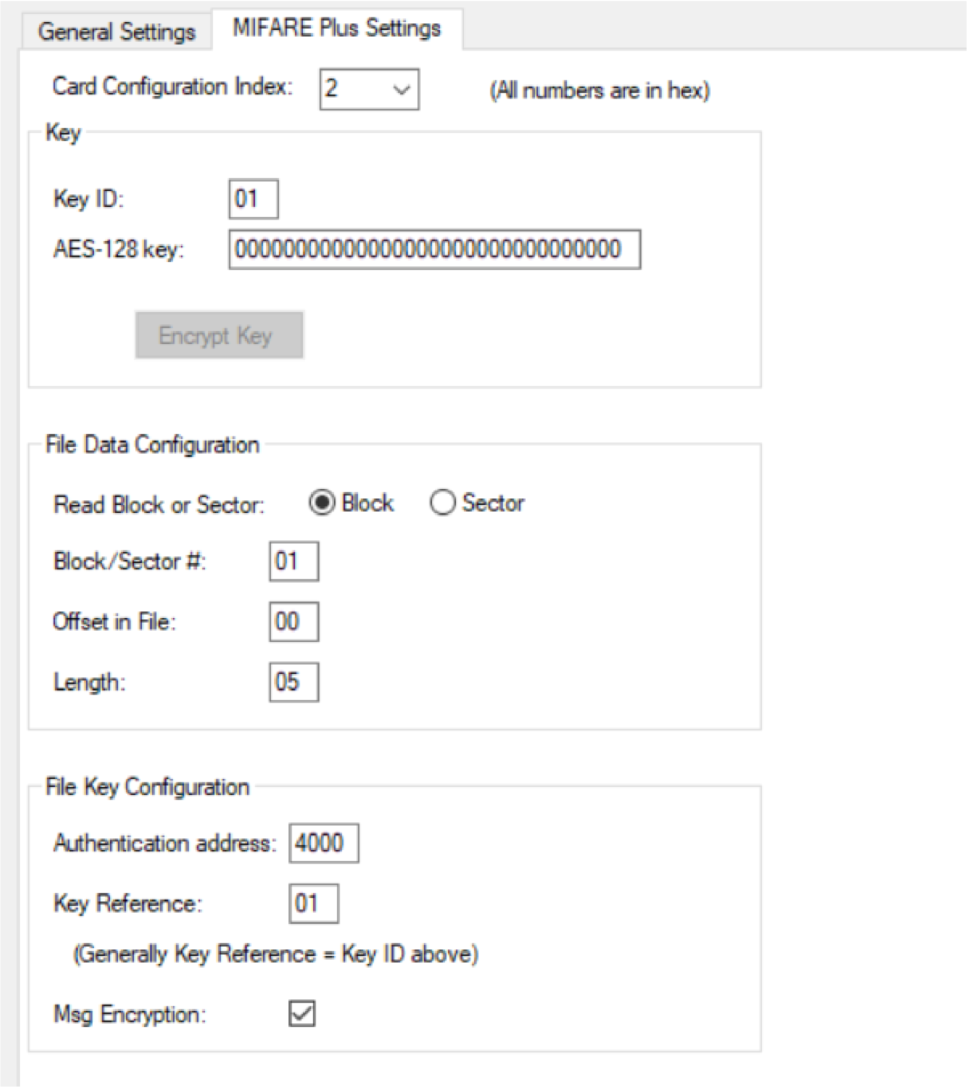
- Security Level 0 (SL0) is straight from the factory, with no data or keys programmed.
- SL1 is in Classic mode and can be read using the MIFARE Classic Secure File card type.
- SL2 (SL1/SL3 mix mode) has not been tested.
- SL3 is “normal” Plus mode, use MIFARE Plus Secure File card type to read this card.

Instead of MIFARE Classic keys (6 bytes), SL3 uses AES-128 keys (16 bytes). It still uses Key A and Key B as authentication options for each sector, but because of memory issues, the keys are moved from the trailing configuration block to a separate Authentication address space.

Authentication Address	**Sector**	**Key A/B**	**Data Blocks (in hex)**
0x4000	0	Key A	0-2
0x4001	0	Key B	0-2
0x4002	1	Key A	4-6
0x4003	1	Key B	4-6
0x4004	2	Key A	8-10 (0x08 - 0x0A)
:	:	:	:

Like other secure file configurations, the Key Reference number needs to match the Key ID. These are kept as separate fields because the Key (and associated Key ID) can be written to the NXP SAM AV2/AV3 chip at any time, including by a 3rd party at a different location.

The Message Encryption checkbox is needed to read MIFARE Plus S and SE cards. Those flavors of MIFARE Plus do not use encryption for data sent between the reader and the card (authentication with a key is still in place).



Card Configuration Index: 2

(All numbers are in hex)

Key

Key ID: 01

AES-128 key: 00000000000000000000000000000000

File Data Configuration

Read Block or Sector: ● Block ○ Sector

Block/Sector #: 01

Offset in File: 00

Length: 05

File Key Configuration

Authentication address: 4000

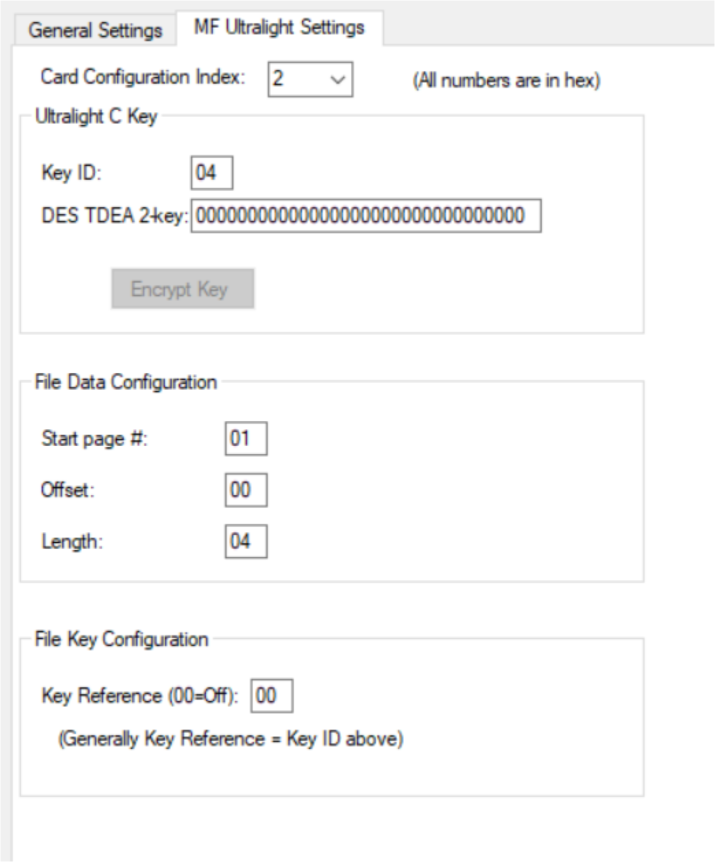
Key Reference: 01

(Generally Key Reference = Key ID above)

Msg Encryption: ☑

16) MIFARE Ultralight

Ultralight uses Pages of 4 bytes each as the basic memory unit. All flavors of Ultralight can be read if the access rights allow open reads. Ultralight C can be set up to require a TDEA key, so the tab for MIFARE Ultralight Settings includes key information. In many cases a key will not be needed and only the page number, offset and length are needed.



Card Configuration Index: 2

(All numbers are in hex)

Ultralight C Key

Key ID: 04

DES TDEA 2-key: 00000000000000000000000000000000

File Data Configuration

Start page #: 01

Offset: 00

Length: 04

File Key Configuration

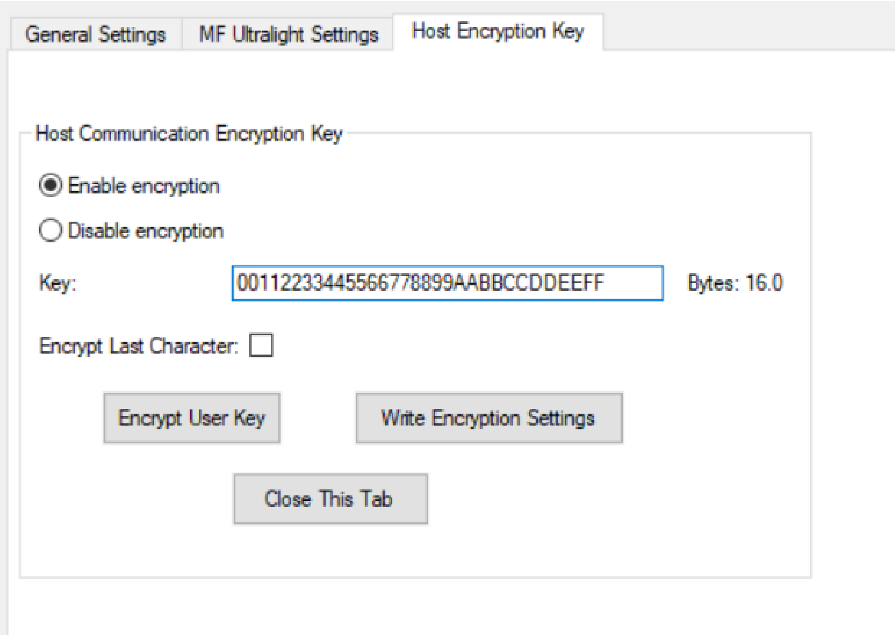
Key Reference (00=Off): 00

(Generally Key Reference = Key ID above)

17) Host Encryption

A feature added in reader firmware version LNC 22.3 is encryption of the keystroke output. This applies to all card data being keystroked by the reader, regardless of the type of card that was presented to the reader. There has been a button added to the General Settings tab to create a new tab for these settings.

Clicking that button will open a new tab with the following options:



● Enable encryption
○ Disable encryption
Key: 00112233445566778899AABBCCDDEEFF Bytes: 16.0
Encrypt Last Character: ☐

Keystroke encryption button will enable/disable encryption of keystrokes. The key is currently a 16-byte (32 hexadecimal characters) field, for AES-128 encryption (initial div input of 0x00). Other key types may be available in the future.

Encrypt Last Character is an option for including the final keystroke character - typically a carriage return key - with the encrypted message, or for sending that character in the clear. Some host programs need that character in the clear in order to detect the end of transmission.

The data can be decrypted using the same key on the host side. There are a number of online AES-128 decryption tools.

The key itself can be encrypted before storing in a local config file or sending to the reader. Use the Write Encryption Settings tab to send the host encryption key to the reader (or to disable it).

18) MIFARE Key Storage overview

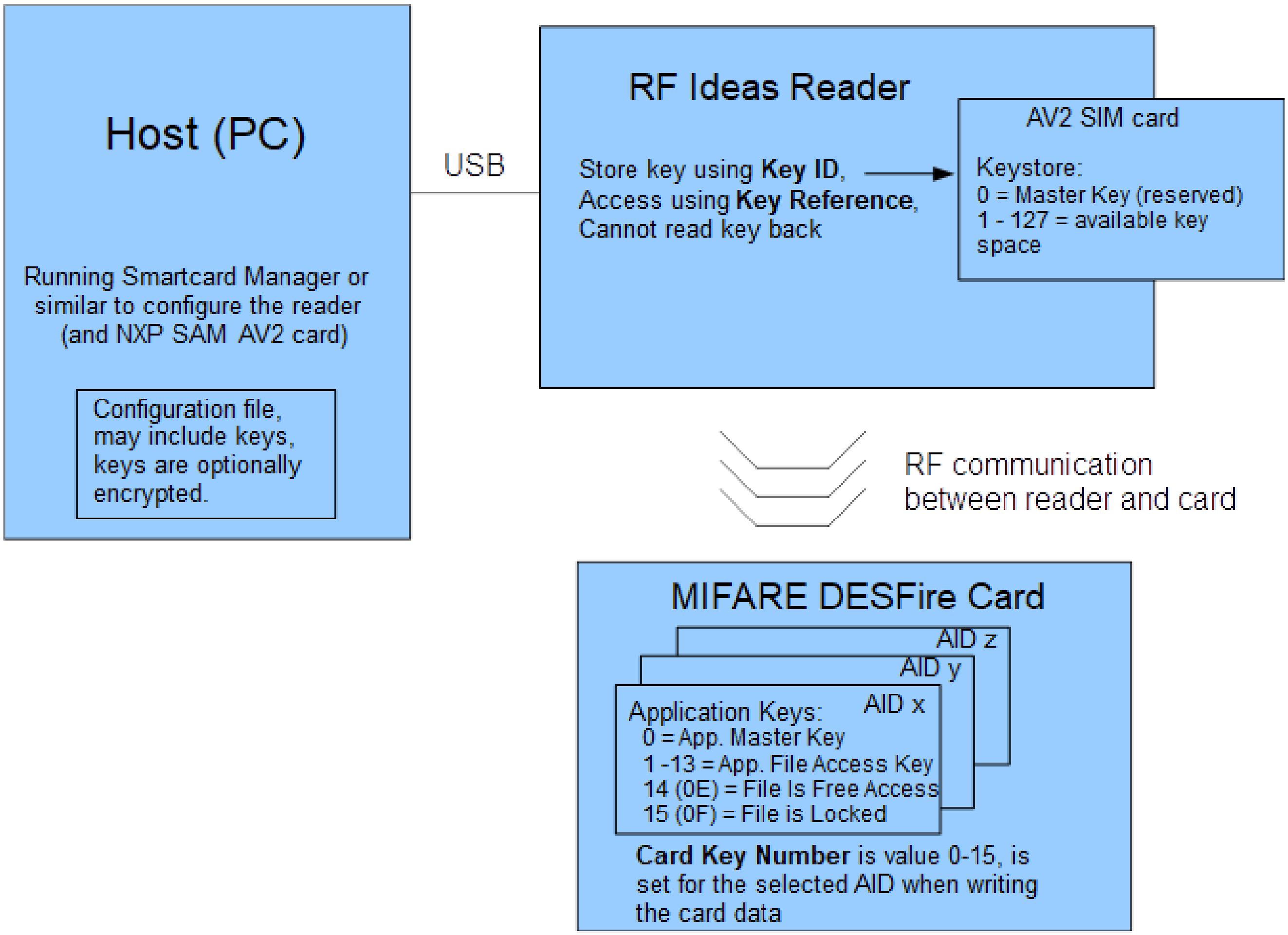
The Key ID used when storing a key to the NXP SAM AV2 or AV3 chip must be the same value that later will be used as the Key Reference when reading the card data. The Key ID has a valid range of 1 to 127 (01 to 7F). MIFARE reserves key 0 as a Master Key. The Card Key Number is an index to the key stored on the card. Additionally, each Key ID has 3 “versions”. Starting with SCM v1.19 and select readers, the versions can be individually written, or use 00 to write to all 3 versions, as was done in earlier revisions of the SCM and firmware.

Outline of Key Store on NXP SAM

Key ID	**Version A**	**Version B**	**Version C**	**Comments**
0	16 bytes	16 bytes	16 bytes	Reserved for SAM Master Key
1	16 bytes	16 bytes	16 bytes	Used for DESFire Config Card on some systems
2-127	16 bytes	16 bytes	16 bytes	Available for all uses

All three versions for a given Key ID must have the same key type (AES-128, TDEA, Classic A&B). Sometimes 1, 2, 3 are used in documentation for the versions instead of A, B, C. The SCM uses value 0 to set all versions of a given Key ID to the same key (the default behavior in earlier systems), 1 = Version A only, 2 = Version B, 3 = Version C. AES-192 (future) and 3K TDEA use 24 bytes, so they have a stretched Version A and Version B, there is no Version C in that case.

See the following figure for how keys are stored on various systems. This figure uses the MIFARE DESFire card as an example as it is the most complicated. Card key numbers on a DESFire card have a value 0 to 15, with up to 13 keys for each AID. Card key number 14 (0E) is reserved for Free Access, and card key number 15 (0F) is No Access. Even though it is always called the Card Key Number, it might be more intuitive to call it the AID Key Number.


Host (PC)
Running Smartcard Manager or similar to configure the reader (and NXP SAM AV2 card)
Configuration file, may include keys, keys are optionally encrypted.
USB
RF Ideas Reader
Store key using Key ID, Access using Key Reference, Cannot read key back
AV2 SIM card
Keystore:
0 = Master Key (reserved)
1 - 127 = available key space
RF communication between reader and card
MIFARE DESFire Card
AID z
AID y
AID x
Application Keys:
0 = App. Master Key
1 -13 = App. File Access Key
14 (0E) = File Is Free Access
15 (0F) = File is Locked
Card Key Number is value 0-15, is set for the selected AID when writing the card data

19) Release Notes

Version 2.2, October 2023:
Enhancements

- Add MFP24 card types, including Felica
- More support for Wren (WNC) MFP24 and Nestle, including Safetrust diversification, Data+CSN options, installed hardware report and retrieving SAM version information
- Add key length indicator and change color if key being entered is not in hexadecimal on DESFire and Host keys (keys that can be over 16 characters in length)
- Automatically close blob (bwg) ini file if not manually close when program exits. While the blob ini file is active, configuration status messages are in orange, so user knows output is redirected.
- Removed checkboxes (added in 2.1), added buttons instead for writing settings to the reader

Bug Fixes

- Blob length in LEGIC must be multiple of four, ini output was failing production tools
- LEGIC TXP selection (prime, advant 14443A, advant 15693, first-found) was not being picked up correctly from the reader

Version 2.1, July 2023:
Enhancements

- Add ability to save MIFARE DESFire keys that work with EV2-secure messaging
- Add HID Apple Wallet (0102) card type
- Add checkboxes for more control over what gets sent on a Config Reader command (file settings, key settings on a configuration-by-configuration basis). Send Key button removed from Key tabs.
- “Convenience formatting” of parity, hex/decimal output no longer sent by default (could conflict with hwg+ file settings from rf IDEAS Configuration Utility)
- Report the hex file name in “About Reader” message box.

Bug Fixes

- Some configurations not being sent when all card types (1-4) are smart cards (internal naming conflicts)
- Enable Host Encryption and Trace Log features on Wren readers
- NXP SAM Version info wasn’t showing the mode byte (4th byte of version information)

Version 2.0, April 2023 (cumulative major changes since 1.11):
Enhancements

- Added hex code of card types to config ini file
- Add command to read installed hardware and version information
- Recognize more Felica readers (based on reported model number)
- Added Reset to Defaults option
- CCID and CBORD support
- Added EOF security check field to config files (similar to secure hwg+ files)
- Added blob ini (bwg) file export
- Added SafeTrust diversification
- Added support for Wavelynx MyPass BLE

- Corrections & updates to built-in card list
- Can update card list by including "cardtypes.txt" file in the directory
- Updated to NFC wallet (Wavelynx)
- DESFire key versions added to stored config file
- Ability to read old unsecure and new config files (with/without EOF)
- Can send keys & config together (by customer request)
- Polls reader every 3 seconds for connection status

Bug Fixes

- Fixed MIFARE Plus bug when storing key
- Bug fixes for Felica
- Bug fixes with *.ini files
- Wavelynx BLE has parity 1/1
- Fixes for Apple Pay & Google Pay tabs not always showing up