Contents

Manual Revision History

Revision	Date	Description
1	2020-08-01	Initial Release for 1.5.0

Operation

Overview

TODO

Security Considerations

- The KFDtool as a computer peripheral has several important considerations to keep in mind when secure keyloading is required.
    - What this means
        - Because the KFDtool keyloader is made up of a USB peripheral and software for use on a Windows PC, precautions have to be taken to preserve the integrity of the encryption keys due to the complex nature of the systems involved.
- The following points are only valid with unmodified software, firmware, and hardware. With physical access to the PC or adapter, the software, firmware, or hardware could be modified to covertly retain the plaintext keying material.
    - What this means
        - With physical access to the KFDtool adapter or computer running the KFDtool software, someone could modify them in a way to record or transmit the encryption keys without your knowledge. Therefore, you should physically secure the KFDtool adapter and the computer used for keyloading.
- Plaintext keying material is present in the PC's RAM, over the USB connection, in the adapter's RAM, and over the keyload connection. Therefore, you must trust the PC that the software is running on, or air gap it.
    - What this means
        - If the computer you use for keyloading is connected to a network, it is possible that the encryption keys could be accessed without your knowledge due to vulnerabilities in Windows or other software installed on your computer. Therefore, it is recommended that you use a computer that is not connected to any networks, and that you only install software and connect devices to it that you trust.
- It is possible that plaintext keying material in the PC's RAM is paged out to disk. It is also possible that Windows crash dumps may contain plaintext keying material. Therefore, it is recommended that the PC's hard drive is protected using full disk encryption such as BitLocker and powered off when unattended.
    - What this means
        - Windows is a complex operating system, and there are many ways for the encryption keys to end up on the hard drive without your knowledge. Therefore, encrypting the hard drive of the computer you use for keyloading is a good idea as it provides another layer of security against unauthorized users accessing the encryption keys without your knowledge.
- After the KFDtool adapter has been disconnected from the USB port, any residual plaintext keying material present in the microcontroller's RAM will be lost.
    - What this means
        - When unplugging the KFDtool adapter from the computer, any encryption keys are lost due to the memory type used. The KFDtool adapter by design does not store any encryption keys.

- When certain non-default logging is enabled, plaintext keying material is written out to the log file on disk. This logging should only be enabled when diagnostic information needs to be collected, and only used with dummy keying material.
    - What this means
        - There are options in the KFDtool software configuration files that can be set to write detailed information to the hard drive for use to diagnose issues. If you are directed to change these files to enable logging to diagnose an issue, understand that the keys you use may be included in these logs. Therefore, you should not use your production keys when collecting these logs.

Features

Overall

Title Bar

Displays the KFDtool software version and selected function.

Menu Items

File -> Exit

Exits the application.

Help -> Manual

Opens the PDF manual in the system's default PDF viewer.

Help -> Website

Opens the KFDtool website in the system's default web browser.

Help -> About

Displays the software version and copyright information in a dialog.

Container

Overview

The container feature allows individual keys and groups of keys to be stored and used in other features of the software. The container can be saved on disk and opened on the same or another machine.

Security

When saved to disk, the container is encrypted with the AES-256 symmetric encryption algorithm using the CBC mode of operation. The 256 bit AES key is derived from the user entered password by the PBKDF2 key derivation algorithm using the SHA-512 hash algorithm, with 100,000 iterations, and using a 256 bit random salt value generated by the Windows CAPI.

The password derived AES key is set on creation of the container and changed on the user initiated password change operation. A new AES IV is generated on each save of the container, generated by the Windows CAPI.

The password length does not have an arbitrary upper limit, and can contain any characters representable in UTF-8. The lower limit of the password length is 1 character, but a message is displayed when setting the password to a value that is under 16 characters, encouraging the user to select a stronger password – however this is only a suggestion.

Menu Items

Container -> New

Creates a new container. Prompts user to set a password. Opens the container for use.

Note: The current container must be closed before performing this operation.

Note: The container is not automatically saved – you must use Container -> Save or Container -> Save As to save the container to disk.

Container -> Open

Opens an existing container from disk. Prompts user to enter a password to decrypt the container.

Note: The current container must be closed before performing this operation.

Container -> Edit

Opens the Edit Container window to modify the container's contents.

Note: The current container must already be open before performing this operation.

Container -> Change Password

Prompts user to change the container's password. Displays the

Note: The current container must already be open before performing this operation.

Container -> Save

Saves the current container to disk. If the container was opened from disk, it will overwrite that container on disk. If the container was created, the user will be prompted to select a location to save the container.

Note: The current container must already be open before performing this operation.

Container -> Save As

Saves the current container to disk. Prompts the user to select a location to save the container.

Note: The current container must already be open before performing this operation.

Container -> Close

Closes the current container. If the container has been modified, prompts the user to choose whether to save the container or not.

Note: The current container must already be open before performing this operation.

Windows

Edit Container

Keys

Options are the same as in P25 KFD -> Keyload, with the exception of the text box **Name** and button **Save**.

Name

The name text box defines a name for the key.

Note: The key name is required.

Note: The key name must be unique.

Save

The save button saves the key parameters.

Groups

Name

The name text box defines a name for the group.

Note: The group name is required.

Note: The group name must be unique.

Available

The available list displays the available keys from the key container.

Selected

The selected list displays the available keys from the key container.

Add

When a key is selected in the available column, moves the key to the selected column.

Remove

When a key is selected in the selected column, moves the key to the available column.

Save

The save button saves the group parameters.

New

Creates a new key or group depending on the tab selected.

Up

Moves the selected key or group up in the list.

Down

Moves the selected key or group down in the list.

Delete

Deletes the selected key or group.

Type

Overview

The type menu allows for the selection of the device type used to communicate with the target. The **Type** menu's selection influences the options available in the Device menu.

Menu Items

TWI (KFDtool)

Selects the TWI protocol with a connection to the target device via the KFDtool USB adapter.

DLI (IP)

Selects the DLI (IP) protocol with a connection to the target device via the internal Windows IP stack. The target device can be over any interface that is reachable by a route in the Windows IP routing table – for example, RNDIS over USB or PPP over serial.

Device

Overview

The device menu allows for the selection of the device used to communicate with the target. It displays different options depending on the Type menu's selection.

Menu Items

When Type is TWI (KFDtool)

Contains a list of connected KFDtool USB adapters by COM port. When no adapters are connected, displays 'No devices found'.

When Type is DLI (IP)

Contains only the option *[Edit]*. Opens the DLI (IP) Connection Settings window. Only one configuration is supported at this time.

Windows

DLI (IP) Connection Settings

Protocol

The protocol selection is used as the transport layer on the IP network layer. At this time, the only selection is *UDP*.

Note: This selection is set by default to UDP, the protocol used by Motorola devices.

Hostname

The hostname field is used to determine the IP address of the target device. It can either be set to a host name and be resolved, or set to the IP address directly. Both IPv4 and IPv6 addresses are supported.

Note: This field is required.

Note: This field is set by default to 192.168.128.1, the default IP address used by Motorola devices.

Port

The port field is used as the protocol's destination port.

Note: This field is required.

Note: The valid port range is 1-65535.

Note: This field is set by default to 49644, the default port used by Motorola devices.

Variant

The variant selection is used to change the behavior of the DLI protocol, as some vendor's devices do not follow the P25 standard, and require non-standard behavior to operate properly.

The selections are either *Standard* or *Motorola*. The *Standard* variant conforms to the P25 standard. The *Motorola* variant deviates from the P25 standard to operate correctly with Motorola devices.

Note: This selection is set by default to *Motorola*, the variant used by Motorola devices.

P25 KFD

Overview

TODO

Menu Items

P25 KFD -> Multiple Keyload

Keys

Available

The available list displays the available keys from the key container.

Selected

The selected list displays the available keys from the key container.

Add

When a key is selected in the available column, moves the key to the selected column.

Remove

When a key is selected in the selected column, moves the key to the available column.

Groups

Available

The available list displays the available groups from the key container.

Selected

The selected list displays the available groups from the key container.

Add

When a group is selected in the available column, moves the group to the selected column.

Remove

When a group is selected in the selected column, moves the group to the available column.

Load

The load button loads the selected keys/groups into the target device.

P25 KFD -> Keyload

Keyset ID

The Keyset ID text box is used to specify the keyset to use.

Note: The Keyset ID is required if Active Keyset is not checked.

Note: When Active Keyset is checked, this field is disabled as the keyset is automatically determined during the keyload operation.

Active Keyset

The Active Keyset check box is used to specify whether to use the target device's current keyset (checked), or to use the keyset specified in the Keyset ID field (unchecked).

SLN/CKR

The SLN/CKR text box is used to specify the SLN or CKR to use.

Note: The SLN/CKR is required.

Key Type

The Key Type combo box is used to specify what type of key is to be loaded. The selection Auto automatically selects the key type based on the SLN/CKR specified. The selection TEK forces the key type to a KEK, and the selection KEK forces the key type to a KEK.

Note: The Key Type is required.

Note: When the Auto option is selected, the label besides the combo box displays the key type in real time based on the current SLN/CKR value.

Key ID

The Key ID text box is used to specify the key ID to use.

Note: The Key ID is required.

Algorithm

The Algorithm text box is used to specify the algorithm to use. The combo box to the right of the text boxes contains commonly used algorithm options.

Note: The Algorithm is required.

Note: If the algorithm combo box has a selection other than Other, the algorithm text boxes are disabled, and the currently selected algorithm preset value is shown in them.

Key

The key text box is used to specify the encryption key to load into the target. It may only contain hex characters (0-9, A-F, a-f), with a length divisible by 2.

Note: The Key is required.

Hide

The hide check box is used to hide the entered key from view. When checked (default), the key is hidden. When unchecked, the key is visible.

Generate

The generate button is used to generate an encryption key. The parameters of the generated key is based on the Algorithm selection.

Note: The generate function only works with the algorithms AES-256, DES-OFB, DES-XL, ADP/RC4.

Load

The load button loads the key into the target device.

P25 KFD -> Key Erase

TODO

P25 KFD -> Erase All Keys

TODO

P25 KFD -> View Key Info

TODO

P25 KFD -> View Keyset Info

TODO

P25 KFD -> RSI Configuration

TODO

P25 KFD -> KMF Configuration

TODO

P25 MR

Overview

TODO

Menu Items

P25 MR-> Emulator

TODO

Utility

Overview

TODO

Menu Items

Utility -> Fix DES Key Parity

TODO

Utility -> Update Adapter Firmware

TODO

Utility -> Initialize Adapter

TODO

Utility -> Adapter Self Test

TODO

Glossary

ADP – Advanced Digital Privacy

AES – Advanced Encryption Standard

CAPI – Cryptographic Application Programming Interface

CBC – Cipher block chaining

CKR – Common Key Reference

DES – Data Encryption Standard

DLI – Data Link Independent

IP – Internet Protocol

IPv4 – Internet Protocol Version 4

IPv6 – Internet Protocol Version 6

IV – Initialization Vector

KEK – Key Encryption Key

KFD – Key Fill Device

P25 – Project 25

PBKDF2 – Password-Based Key Derivation Function 2

PDF – Portable Document Format

PPP – Point-to-Point Protocol

RC4 – Rivest Cipher 4

RNDIS – Remote Network Driver Interface Specification

SLN – Storage Location Number

TEK – Traffic Encryption Key

TWI – Three-Wire Interface

UDP – User Datagram Protocol

USB – Universal Serial Bus

UTF-8 – 8-bit Unicode Transformation Format