swissbit®

User Manual

Swissbit Secure Boot SDK for Raspberry Pi

Doc. Version: 2.6.2

Table of Contents

1.1 Glossary and SDK Contents

1.1.1 Glossary

Abbreviation	Description
API	Application Programming Interface
DP	Data Protection
SDK	Software Development Kit
GUI	Graphical User Interface
CLI	Command Line Interface
SO	Security Officer
SHA	Secure Hash Algorithm
PIN	Personal Identification Number Note: In this document, PIN is synonym for password as any binary value can be defined. In practice the password will most probably be a ASCII PIN
NVRAM	Non-Volatile Random Access Memory

ⓘ Information / hints are denoted with this icon: ⓘ

1.1.2 Contents of the SDK

The Swissbit Secure Boot for Raspberry Pi solution provides an SDK with U-Boot binaries and configuration files for Raspberry 0, 2, 3 and 4 boards, and managing applications tools to configure a Swissbit DP products. Prebuilt U-Boot binaries are available for Raspberry Pi 0, 2, 3 and 4 boards, configuration tools for Microsoft Windows (Windows 7 and higher). This chapter describes where to find the particular components.
The Swissbit Secure Boot SDK is packed in the file Swissbit_SecureBoot_SDK_RPi.zip. After unpacking in a directory, the SDK has the following directory structure:

├── Apps	Management tools for Swissbit DP devices
│ └── uSDcard	Device manager location of (micro)SD-card DP card
│ └── Windows	Windows specific QT binary
│ └── USB	Device manager for location for USB DP stick
│ └── Windows	Windows specific QT binary
├── Document	Location of this document
├── Raspberry	
│ └── RPI0	U-Boot binaries for RPI 0
│ └── RPI2	U-Boot binaries for RPI 2
│ └── RPI3Bplus_CM3plus	U-Boot binaries for RPI 3 B Plus & CM3+ lite
│ └── RPI4	U-Boot binaries for RPI 4

1.1.3 U-Boot Binary Files

The U-Boot Binary can be found in the respective folders for the Raspberry Pi.

RPI 0

U-Boot binary:	<sdkroot>\Raspberry\ RPI0\u-bootRPI0.bin
Binary U-Boot boot script:	<sdkroot>\Raspberry\ RPI0\boot.scr.uimg

RPI 2

U-Boot binary:	<sdkroot>\Raspberry\ RPI2\u-bootRPI2.bin
Binary U-Boot boot script:	<sdkroot>\Raspberry\ RPI2\boot.scr.uimg

RPI 3 B Plus & CM3+ lite

U-Boot binary:	<sdkroot>\Raspberry\ RPI3Bplus_CM3plus\u-bootRPI3.bin
Binary U-Boot boot script:	<sdkroot>\Raspberry\ RPI3Bplus_CM3plus \boot.scr

RPI 4

U-Boot binary:	<sdkroot>\Raspberry\ RPI4\kernel7l
Binary U-Boot boot script:	<sdkroot>\Raspberry\ RPI4\boot.scr
Kernel image	<sdkroot>\Raspberry\ RPI4\uImage

1.1.4 Applications for Managing DP-Devices

Swissbit Security DP devices can be configured using the Device Manager applications for (micro)SD and USB, located <sdkroot>\Apps\uSDcard and <sdkroot>\Apps\USB, respectively.

2. Swissbit Secure Boot Solution for Protecting the System Integrity of a Raspberry PI Boot Media

A Raspberry Pi board boots from micro SD (RPI 0, 2, 3, CM3+ lite & 4) card inserted into the board. A default Raspbian installation installs the kernel on the boot partition and the root files system on a separate second partition. If standard storage cards are used, typically all data and files in both partitions can be read, modified and deleted by anybody.
The Swissbit Data Protection (DP) micro SD card PS-45u DP Raspberry Edition allows restricting access to data on the card by various configurable policies. The boot image can be set read-only to prevent from unauthorized modification. Authorization is performed in the Swissbit customized pre-boot phase to unlock access for a user or further boot.

Following security policy methods are available:
- PIN policy: PIN input by the user
- USB policy: an authorization dongle is plugged into the Raspberry Pi (requiring a Swissbit USB PU-50n DP "Raspberry Edition")
- NET policy: authorization through a network server

In the herein described setup, all files and data in the boot partition are read only and cannot be modified. The root file system of the Operating System can be read and writen after authentication. Thus, an authentication failure during boot will prevent the kernel from reading the OS root file system resulting in a boot failure.
Please check www.swissbit.com/secure-boot-rpi (➔ Downloads) for the latest version of the Secure Boot SDK and documentation.

Note: After a successfull authentication (unlocked access for a user) to raspberry-pi, raspberry-pi will remain in authenticated/unlocked state until a power supply occurs in the raspberry pi/swissbit DP card. That means on a soft reboot of raspberry-pi, it will remain in unlocked state with the only exception of RPi4, where a power cycle triggered to swissbit DP card during soft reboot.

3. Quickstart Guide

The Swissbit Secure Boot Solution for Raspberry Pi allows encryption and access protection of data stored on the card. The DP card safeguards a data policy that is enforced with minimum interaction of the host system with the Raspberry Pi.
Swissbit provides a Secure Boot SDK to integrate a Swissbit Data Protection (DP) micro SD card into a U-Boot boot environment.

Step 1: Check Prerequisites

In order to use Swissbit Secure Boot Solution for Raspberry Pi you first need:
- A Raspberry PI 0, 2, 3 B Plus, CM3+ lite or 4 and its peripherals
- A Windows-based computer for configuring the Swissbit DP products

Step 2: Get Swissbit Secure Boot Solution for Raspberry Pi

The Swissbit Secure Boot Solution for Raspberry Pi consists of:
- A Swissbit Secure microSD card PS-45u DP "Raspberry Edition"
- The Swissbit Secure Boot SDK for Raspberry Pi

In case you choose to pursue an USB policy (see chapter 4.5.2),
- An additional Swissbit Secure USB stick PU-50n DP „Raspberry Edition" is needed

In case you pursue a NET policy (see chapter 4.5.3),
- A linux based system is needed with docker installation to act as a NET policy server.

You can get the Swissbit Secure Boot Solution for Raspberry Pi from our Distribution partners. Please visit https://www.swissbit.com/en/products/product-finder/products/

Note: Currently, USB policy is not supported by the RPI4 because CCID is not supported by the current U-Boot for RPI4 and Net policy is not supported in RP0 because there is no Ethernet port in RP0.

Step 3: Configure the Swissbit micro SD Card by choosing your security policy (cf. Chapter 4)

Authorization is performed in the Swissbit customized pre-boot phase to unlock access for further boot.
Swissbit offers the following security policy methods:

1. PIN policy (cf. chapter 4.5.1): PIN input by the user
2. USB policy (cf. chapter 4.5.2): an authorization dongle is plugged into the Raspberry Pi (requiring a separate Swissbit DP device: PU-50n DP „Raspberry Edition“)
3. NET policy (cf. chapter 4.5.3): authorization through a network server (require a linux based system is needed with docker installation to act as a NET policy server)

Step 4: Install U-Boot (cf. Chapter 5)

Step 5: Activate DP Card Data Protection (cf. Chapter 6)

Step 6: Securely boot the Raspberry Pi (cf. Chapter 7)

4. Swissbit micro SD Card Configuration

4.1 Insert microSD card into your Windows-based system

You can use an adapter to insert the Swissbit microSD card into your Windows-based system, e.g. PC or Notebook.

4.2 Run Swissbit Device Manager

The Swissbit Device Manager can be found at <sdkroot>\Apps\uSDcard\Windows\bin\cardManager.exe. It can be started from that location or optionally be installed permanently using the install script at <sdkroot>\Apps\Windows\install.bat.
NOTE: The Swissbit Device Manager tool only works with Swissbit DP memory cards. If such a card is inserted and the Device Manager still reports "No secure device found", please make sure that the card is formatted (e.g. FAT32) and got assigned a drive letter (e.g. F:) by Windows. Furthermore, the card must be writeable – the write protect switch of micro-SD/SD adapters must be inactive.

Note: The configuration steps can also be performed by CLI tool which can be found in location <sdkroot>\Apps\uSDcard\Windows\bin\cardManagerCLI.exe. In this manual, we have also provided the **CLI Commands** to setup the card. Customer can setup card either by our cardManager tool or by CLI Command.

4.3 Set Security Flags

Set the security flags with following steps:

1. Start the Swissbit Device Manager
2. Go to menu "Manage > Security Settings" and choose these settings:
   - Support Fast Wipe: not checked
   - Reset Requires SO PIN: checked
   - Multiple Partition Protection: checked
   - Secure PIN Entry: checked
   - Login Status Survives Soft Reset: checked

   Multiple Partition Protection has to be checked for the OS integrity (Raspberry) use case.

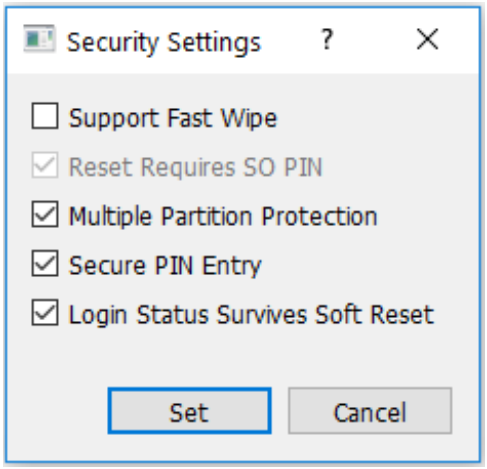


Fig. 1 Security Settings

3. Click "Set" to confirm your choices.
4. Close the Swissbit Device Manager
5. Remove the Swissbit micro SD card from your computer, insert it again and restart Swissbit Device manager.

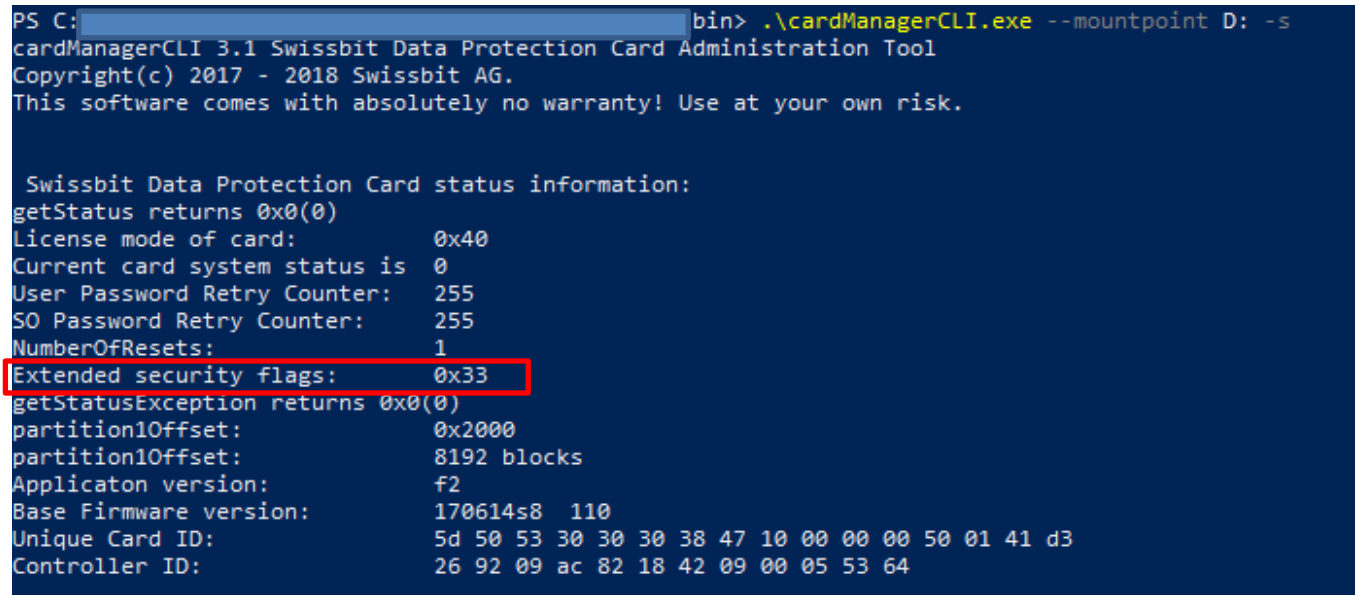
CLI Command:

$.\cardManagerCLI.exe --mountpoint D: -A 0x33

After this command, please ignore the error.

After setting the extended security flag please remove the SD card, insert it again, and then verify the extended security flag status 0x33 by checking the card status with below command

$.\cardManagerCLI.exe --mountpoint D: -s



4.4 Prepare a Security Policy

Swissbit Secure Boot for Raspberry Pi requires setting a security policy used by U-Boot.
Policies are written to the first block of the random access NVRAM. Therefore, the policy must contain at least one block and have correct access rights.

Prepare a security policy with following steps:

1. Start the Swissbit Device Manager
2. Go to menu "NVRAM > Configure"
3. Select for booth "Size" fields the value "1" and check the column for Read and Write access rights as shown below in Fig. 2.
4. Click "Configure" to confirm your choices.

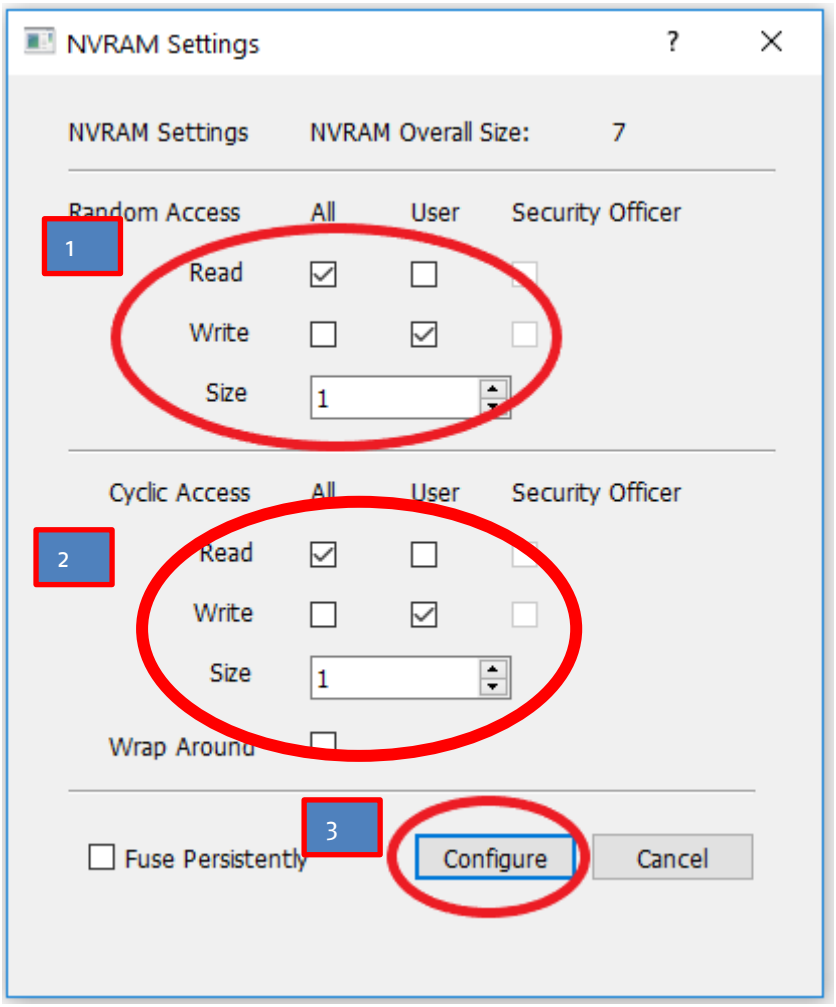


Fig. 2 Configuring the NVRAM

CLI Command:

```
$.\cardManagerCLI.exe --mountpoint D: --configNvram 0x909 --rsectors 1 --csectors 1
```

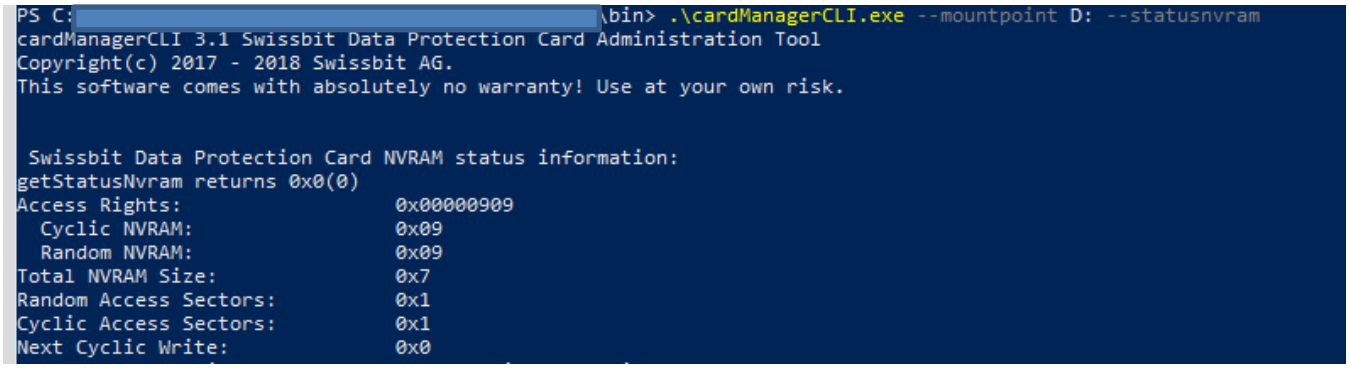
```
PS C:                                    bin> .\cardManagerCLI.exe --mountpoint D: --configNvram 0x909 --rsectors 1 --csectors 1
cardManagerCLI 3.1 Swissbit Data Protection Card Administration Tool
Copyright(c) 2017 - 2018 Swissbit AG.
This software comes with absolutely no warranty! Use at your own risk.

configureNvram returns 0x0(0)
```

After configuring the nvram it can be verified using statusnvram command

```
$.\cardManagerCLI.exe --mountpoint D: --statusnvram
```

It should look like below snapshot:



4.5 Set a Security Policy

There are three policies available:

- PIN policy: PIN input by the user
- USB policy: an authorization dongle is plugged into the Raspberry Pi (requiring a Swissbit USB PU-50n DP „Raspberry Edition“)
- NET policy: authorization through a network server (require a linux based system is needed with docker installation to act as a NET policy server)

4.5.1 Set a “PIN” policy

PIN policy means the user has to enter a PIN to unlock the card for further boot process.
Set the PIN policy with the following steps:

1. Start the Swissbit Device Manager
2. Go to menu “NVRAM > Read/Write Random Access Memory”
3. Enter “0” as the value for the block and click on “Select”
4. Write “PIN” into the text field
5. Click “Commit”
6. Click “Quit” to leave dialog

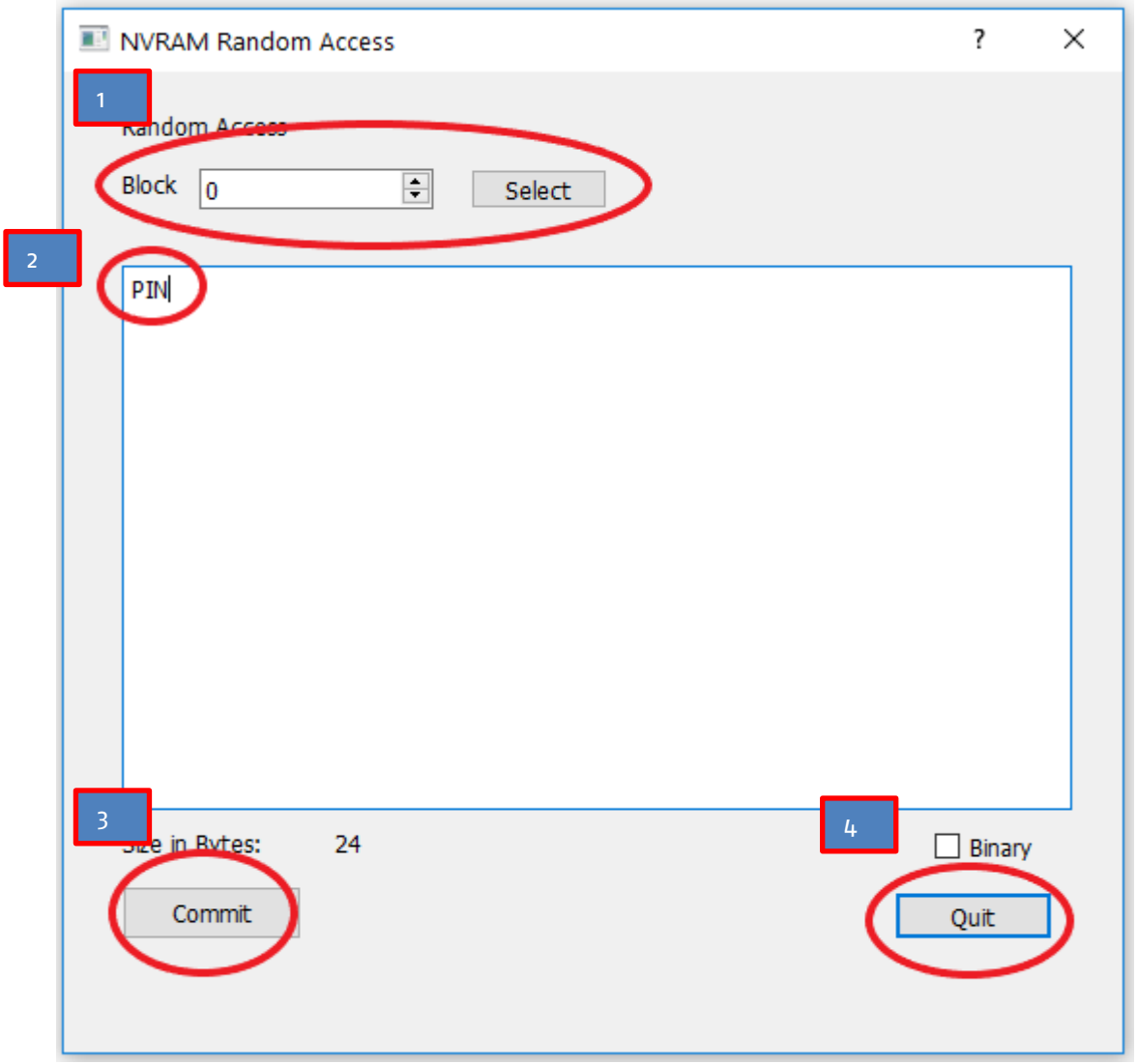


Fig. 3 Setting a PIN policy

4.5.2 Set a "USB" policy

USB policy means that there is an additional Swissbit Secure USB stick PU-50n DP „Raspberry Edition" with CCID capabilities inserted in a USB slot of the Raspberry Pi board that is booted. This CCID device holds the unlock PIN in an encrypted format and provides it at boot time to the U-Boot authentication function.

Note: Currently, USB policy is not supported by the RPI4 because CCID is not supported by the current U-Boot for RPI4.

4.5.2.1 Set a "USB" policy in Swissbit microSD

Set the USB policy in the **Swissbit microSD** card with the following steps:

1. Start the Swissbit Device Manager
2. Go to menu "NVRAM > Read/Write Random Access Memory"
3. Enter "0" as the value for the block and click on "Select"
4. Write "USB" into the text field
5. Click "Commit"
6. Click "Quit" to leave dialog

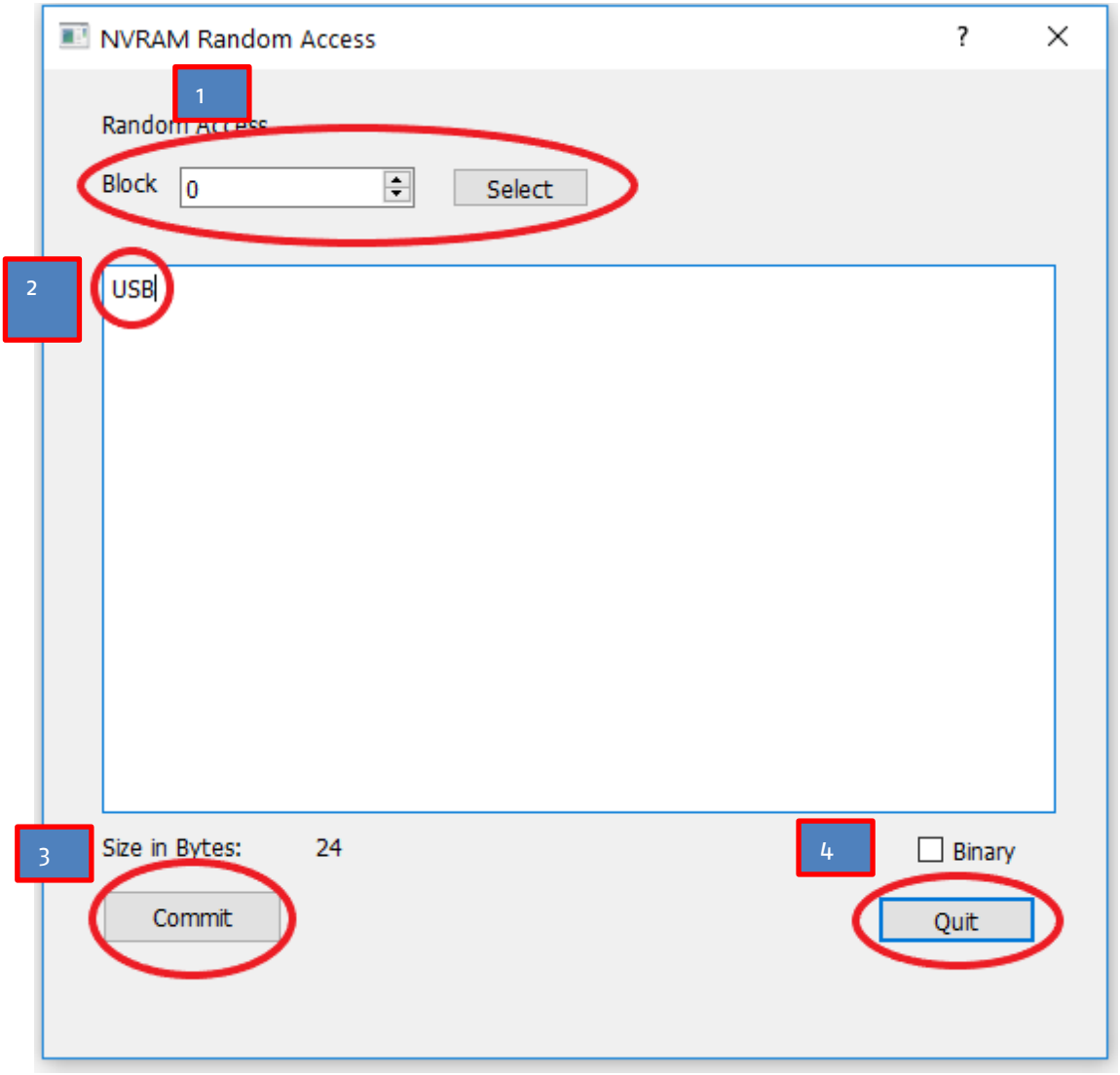


Fig. 4 Setting a USB policy

4.5.2.2 Set a "USB" policy in authentication dongle

Set the USB policy in the authentication dongle (= additional **Swissbit USB stick PU-50n DP „Raspberry Edition"**) with the following steps:

1. Unplug the microSD card
2. Insert the additional Swissbit USB stick PU-50n Raspberry Pi Edition
3. Start the **Swissbit Device Manager for USB** at <sdkroot>\Apps**USB**\Windows\bin\cardManager.exe
4. Go to menu "Manage > Set Authenticity Secret"
5. Enter a PIN as an Authenticity Secret, re-type the Authenticity Secret
6. Click on "Set Authenticity Secret"

Note: Please remember the entered PIN (= Authenticity Secret) as you need to set the same value as the Authenticity Secret later on in the microSD card DP Activation Dialog.

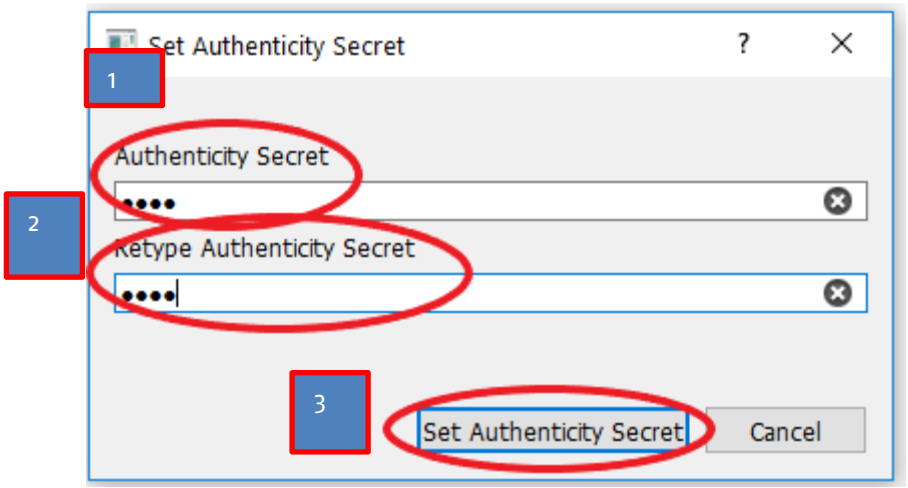


Fig. 5 Configuring the additional USB device as an authentication dongle when using an USB policy

CLI Command:

Create new file (e.g. secret.txt) and add secret as the content to the file. After that run the below command.
Note: Use USB card manager CLI from location Swissbit_SecureBoot_SDK_RPi_v1.0.4\Apps\USB\Windows\bin
$.\cardManagerCLI.exe --mountpoint E: --setSecret secret.txt

```
PS C                                    2\bin> .\cardManagerCLI.exe --mountpoint E: --setSecret secret.txt
cardManagerCLI 3.1 Swissbit Data Protection Card Administration Tool
Copyright(c) 2017 - 2018 Swissbit AG.
This software comes with absolutely no warranty! Use at your own risk.

setAuthenticityCheckSecret returns 0x0(0)
```

4.5.3 Set a NET policy

NET policy means that during the boot process, U-Boot will retrieve authentication information from an authentication server in the network. The corresponding document "Swissbit NetPolicyServer User Manual" describes how to set up an authentication server.

In General:
The NET policy has this format: NET#<ipaddr>#<port>.
<ipaddr>: the IPv4 address or the name of the authentication server (Net policy server).
<port>: the UDP port on which the Net policy server is listening. Default port is 12375.
Thus a properly formatted NET policy string would look like this:

Example: NET#192.168.178.75#12375

➔ indicating an authentication server with the IP address 192.168.178.75 listening on port 12375.

In case server is hosted over internet and can be access using DNS name then NET policy has format:
NET#<DNS name>#<port>.

Example: NET#netpolicy.ishield.cloud#12375

➔ indicating an authentication server with the DNS name netpolicy.ishield.cloud listening on port 12375.

Set the NET policy in the Swissbit microSD card with following steps:

1. Start the Swissbit Device Manager
2. Go to menu "NVRAM > Read/Write Random Access Memory"
3. Enter "0" as the value for the block and click on "Select"
4. Write the "NET#<ipaddr>#<port>" string into the text field (example shown below in Fig. 6)
5. Click "Commit"
6. Click "Quit" to leave dialog

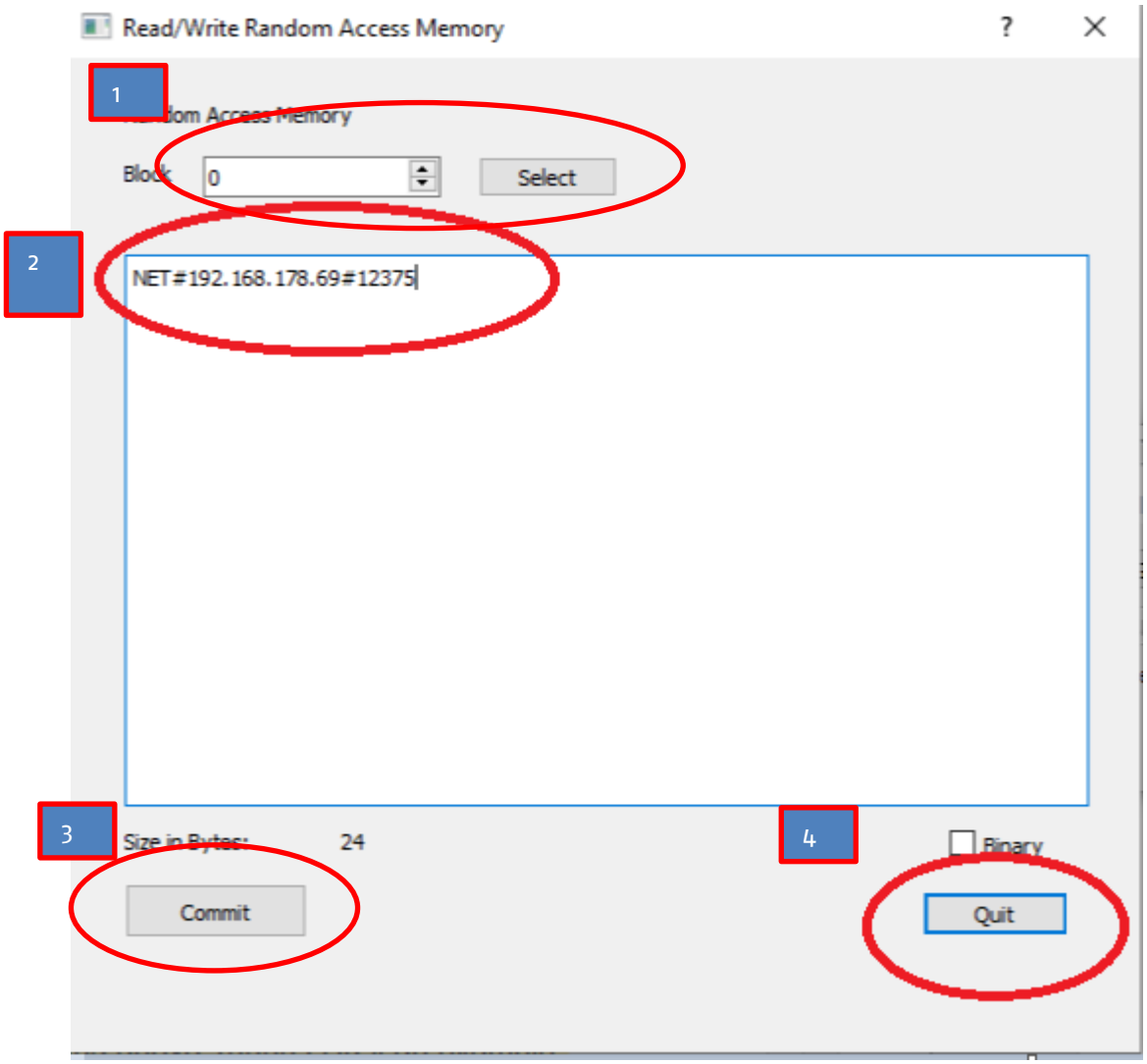


Fig. 6 Setting a NET policy

Next, it is required to get the Unique ID of the Swissbit microSD card for for the later configuration of the NET policy server:

1. Start the Swissbit Device Manager
2. Go to menu "Information > Device Status" or press "CTRL-S"
3. Write down the UniqueID of the Swissbit microSD card (or copy it to clipboard and save it digitally)

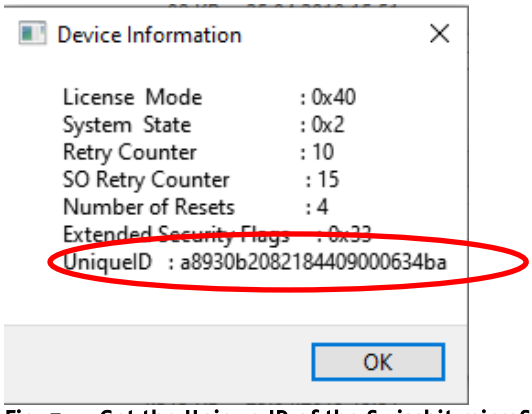


Fig. 7 Get the Unique ID of the Swissbit microSD card

CLI Command:

Create new file (e.g. newFile.txt) and add "PIN", "USB or "NET#192.168.178.69#12375" content to the file. After that run the below command.

```
$.\cardManagerCLI.exe --mountpoint D: --writenvram newFile.txt --addrnvram 0
```

```
PS C:                                \bin> .\cardManagerCLI.exe --mountpoint D: --writenvram nvram.txt --addrnvram 0
cardManagerCLI 3.1 Swissbit Data Protection Card Administration Tool
Copyright(c) 2017 - 2018 Swissbit AG.
This software comes with absolutely no warranty! Use at your own risk.

writeNvram returns 0x0(0)
```

4.6 Install the Raspberry Pi Operating System

Install the Raspberry Pi Operating System onto the Swissbit micro SD card with the following steps:

1. Download the latest Raspberry Pi OS image from:
   https://www.raspberrypi.com/software/

2. Follow the installation procedure using e.g. the balenaEtcher tool:
   https://www.raspberrypi.com/documentation/computers/getting-started.html

3. After you installed the Operating System onto the microSD card verify you can boot your Raspberry PI from this card and apply all OS updates.

4.7 Set a Protection Profile

Set a Protection Profile on the Swissbit micro SD card with following steps:

1. Re-Insert the microSD card into your Windows-based PC or notebook
2. Click on "Cancel" if your system requests to format the second partition on the micoSD card

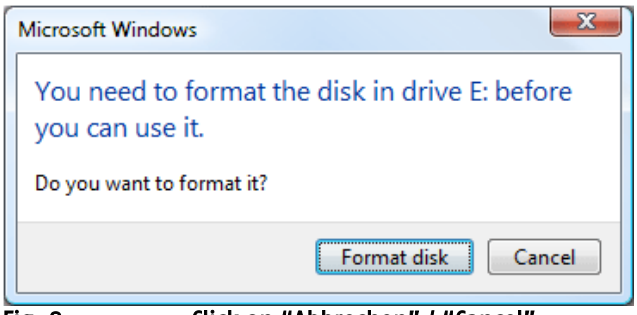


Fig. 8 Click on "Abbrechen" / "Cancel"

A Protection Profile has to be set only in case "Multiple Partition Protection" has been selected in step 4.3
Note: If Multiple Partition Support has not been activated, this step cannot be applied since the protection profile is applied implicitly.
The Protection Profile determines which kind of protection is in force after security has been activated on the card. Protection profiles are assigned to partitions. Each partition can have exactly one profile type assigned.
It is strongly recommended to check "Protect MBR". With this setting, the card's MBR can be read but not be modified. Even in unlocked state, the MBR is immutable and the card cannot be repartitioned.
Note: Repartitioning of the MBR is possible by the Admin and requires deactivation of the card's security first. See 8.1 .
The OS integrity use case (e.g. for the Raspberry Pi) assumes two partitions. A boot partition that shall be readable at any time and a root file system partition that shall be accessible only after authentication.
Set a protection profile with following steps:

1. Start the Swissbit Device Manager
2. Go to menu "Manage > Manage Protection Profiles"
3. If a popup window titled "Profiles not matching partitions" appears, asking whether you "want to reset all protection profiles?", click "Yes".
4. For Partition 1 choose value "Public CD-ROM"
5. For Partition 2 choose value "Private RW"
6. Check "Protect MBR"
7. Click "OK"

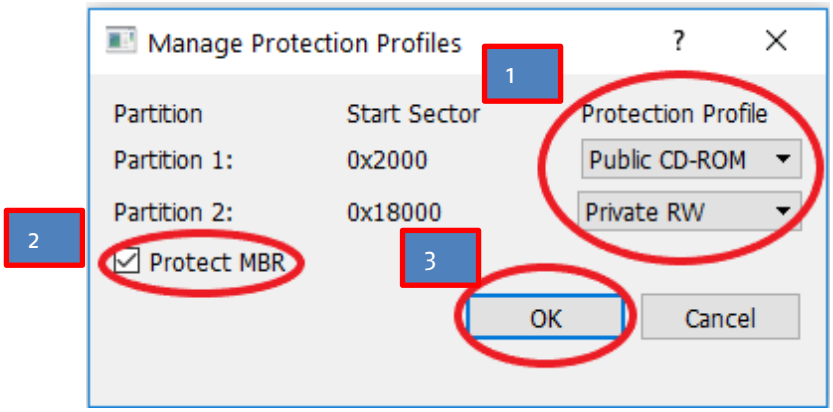


Fig. 9 Setting Protection Profiles for a Raspberry Pi installation.

ⓘ If you see more than 2 partitions (e.g. 4 partitions) under "manage protection profiles", please make sure that this is what you want. More than 2 partitions also appear if the "installing Operating System" step has been skipped by mistake. If so, please go back to Chapter 4.6 .
ⓘ Please note that the "Public CD-ROM" partition becomes read-only after the DP Card protection has been activated (see Ch. 6). Even in read-only mode the partition appears to be writable, but all changes will be reverted after removing & re-inserting the memory card.

When the protection is not activated like described in Chapter 6. (Card is in "transparent mode"), regular read/write operation is possible on the partition.

CLI Command:

```
$.\cardManagerCLI.exe --mountpoint D: --setprofiles 0x00000000,3,0x000007D0,3,0x00014050,0
```

```
PS C:                                \bin> .\cardManagerCLI.exe --mountpoint D: --setprofiles 0x00000000,3,0x000007D0,3,0x00014050,0
cardManagerCLI 3.1 Swissbit Data Protection Card Administration Tool
Copyright(c) 2017 - 2018 Swissbit AG.
This software comes with absolutely no warranty! Use at your own risk.

Set protection profile
setProtectionProfiles returns 0x0(0)
```

Profiles can be verified with command

```
$.\cardManagerCLI.exe --mountpoint D: --getprofiles
```

```
PS C:                                bin> .\cardManagerCLI.exe --mountpoint D: --getprofiles
cardManagerCLI 3.1 Swissbit Data Protection Card Administration Tool
Copyright(c) 2017 - 2018 Swissbit AG.
This software comes with absolutely no warranty! Use at your own risk.


 Swissbit Data Protection Card profile information:
0x00000000 PUBLIC_CDROM
0x00002000 PUBLIC_CDROM
0x00082000 PRIVATE_RW
```

5. U-Boot Installation

The U-Boot files required for the Swissbit U-Boot implementation on Raspberry Pi consists of a U-Boot binary and a U-Boot configuration script.

1. Insert the microSD-Card into a Windows-based machine and depending on your Raspberry Pi model, please follow the according steps as stated below:
2. **If your Raspberry Pi model is a Raspberry PI 0:**
    a. Copy the file <sdkroot>\Raspberry\RPI0\u-bootRPI0.bin onto the first partition of your microSD card.
    b. Copy the file <sdkroot>\Raspberry\ RPI0\boot.scr.uimg to the first partition of your microSD card.
    c. On the first partition of your microSD card open the file "config.txt" and add the following line at the end:
        kernel=u-bootRPI0.bin
3. **If your Raspberry Pi model is a Raspberry PI 2:**
    a. Copy the file <sdkroot>\Raspberry\RPI2\u-bootRPI2.bin onto the first partition of your microSD card.
    b. Copy the file <sdkroot>\Raspberry\ RPI2\boot.scr.uimg to the first partition of your microSD card.
    c. On the first partition of your microSD card open the file "config.txt" and add the following line at the end:
        kernel=u-bootRPI2.bin
4. **If your Raspberry Pi model is a Raspberry PI 3 B Plus or CM3+ lite:**
    a. Copy the file <sdkroot>\Raspberry\RPI3Bplus_CM3plus\u-bootRPI3.bin onto the first partition of your microSD card.
    b. Copy the file <sdkroot>\Raspberry\RPI3Bplus_CM3plus\boot onto the first partition of your microSD card.

c. On the first partition of your microSD card please open the file "config.txt" and add the following line at the end:
kernel=u-bootRPI3.bin

5. **If your Raspberry Pi model is a Raspberry PI 4:**

a. Replace the file kernel7l onto the first partition of your microSD card with <sdkroot>\Raspberry\RPI4\kernel7l.
b. Copy the file <sdkroot>\Raspberry\RPI4\boot onto the first partition of your microSD card.
c. Copy the file <sdkroot>\Raspberry\RPI4\uImage onto the first partition of your microSD card
d. On the first partition of your microSD card please open the file "config.txt" and add the following line at the end:
enable_uart=1
e. On the first partition of your microSD card please open the file "config.txt" and comment the line "dtoverlay=vc4-fkms-v3d" (that means add # before "dtoverlay=vc4-fkms-v3d" e.g. "# dtoverlay=vc4-fkms-v3d")

6. Activation of Card Data Protection

In case the PIN or USB policy has been set before, please proceed with the activation of the DP card data protection.
In case the NET policy has been set before, please verify that the authentication server is up and running, then please proceed with the activation of the DP card data protection.
Insert the microSD-Card into a Windows-based machine and follow these steps:

1. Start the Swissbit Device Manager

2. Go to menu "Manage > Activate Data Protection"

3. Set a Password (min. 4 characters), which will be your user PIN, and set the Security Officer Password (min. 8 characters)
NOTE: If you have chosen "USB policy", the password must match the authenticity secret of the authentication dongle (USB stick PU-50n "Raspberry Pi Edition"), which has been set in Chapter 4.5.2 .

4. Click on "Activate Data Protection".
NOTE: The "Public CD-ROM" partition(s) (see Chapter 4.7) will become read-only after the micro SD card data protection has been activated. Even in read-only mode the partition(s) will appear to be writable, but all changes will be reverted after removing & re-inserting the memory card.

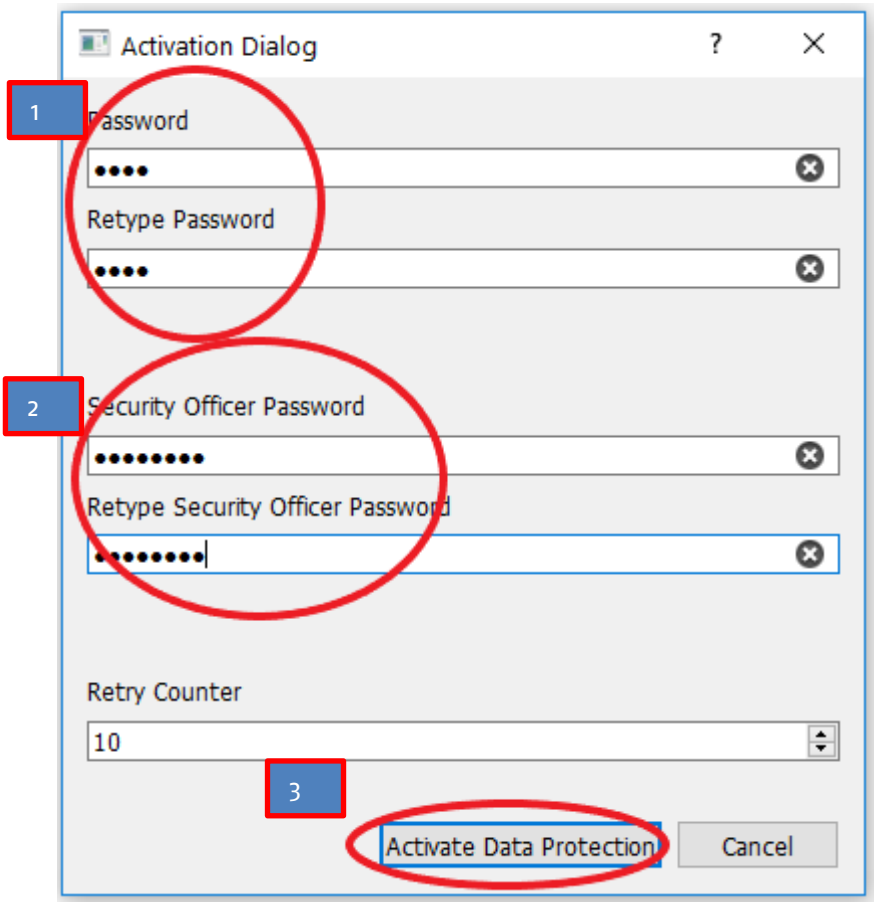


Fig. 10 Activating Data Protection

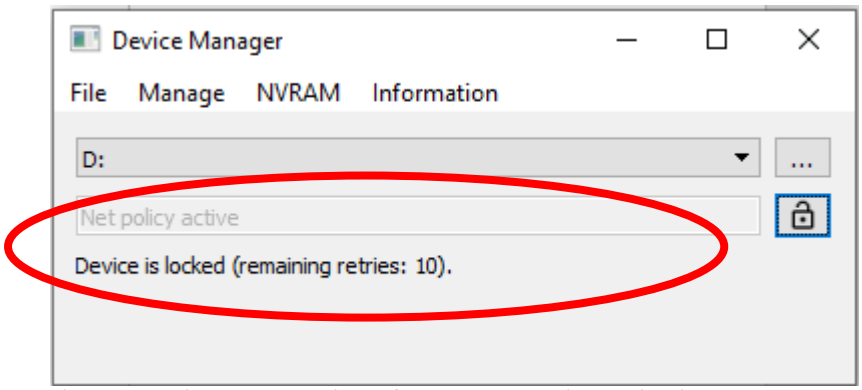


Fig. 11 Device Manager view after Data Protection activation

CLI Command:

```
$.\cardManagerCLI.exe --mountpoint D: --activate --pin 1234 --sopin 12345678
```

```
PS C                                          bin> .\cardManagerCLI.exe --mountpoint D: --activate --pin 1234 --sopin 12345678
cardManagerCLI 3.1 Swissbit Data Protection Card Administration Tool
Copyright(c) 2017 - 2018 Swissbit AG.
This software comes with absolutely no warranty! Use at your own risk.


 Activating card...
activate returns 0x0(0)
```

Status of the card if it is locked or not can be checked using below status command. "Current card system status is 2", means card is locked.

$.\cardManagerCLI.exe --mountpoint d: --status

```
PS C:                                         bin> .\cardManagerCLI.exe --mountpoint d: --status
cardManagerCLI 3.1 Swissbit Data Protection Card Administration Tool
Copyright(c) 2017 - 2018 Swissbit AG.
This software comes with absolutely no warranty! Use at your own risk.


 Swissbit Data Protection Card status information:
getStatus returns 0x0(0)
License mode of card:          0x40
Current card system status is  2
User Password Retry Counter:   10
SO Password Retry Counter:     15
NumberOfResets:                1
Extended security flags:       0x33
getStatusException returns 0x0(0)
partition1Offset:              0x0
partition1Offset:              0 blocks
Applicaton version:            167
Base Firmware version:         211028s9 X100
Unique Card ID:                10 53 44 30 30 34 47 42 01 00 00 03 9f 00 97 cb
Controller ID:                 00 00 00 00 00 00 00 00 00 00 00 00
```

7. Booting the Raspberry Pi with activated security

Now you can insert the prepared microSD Card Raspberry Pi Edition into your Raspberry Pi and securely boot up your Raspberry Pi.

When using ...

1. PIN policy: you will be asked to enter the Password in order to boot up the Raspberry PI

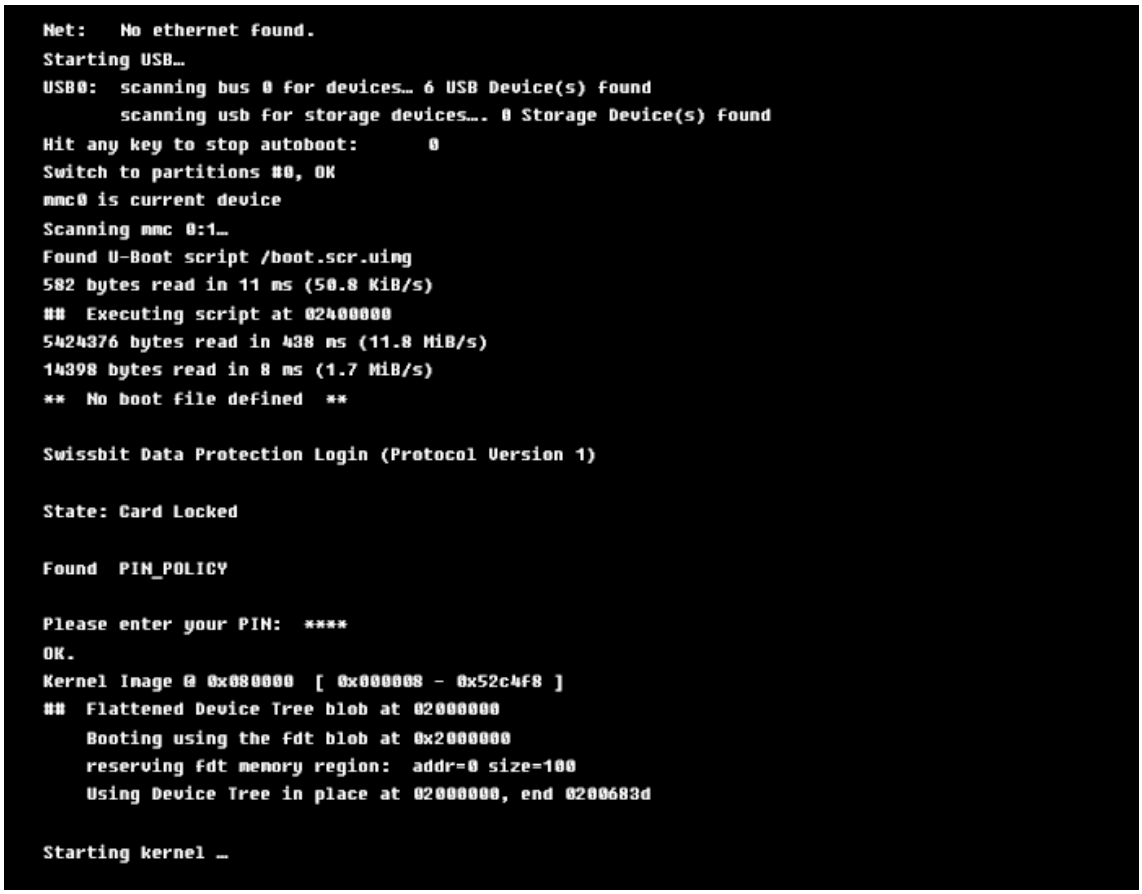


Fig. 12 Secure Boot of Raspberry PI with PIN policy

2. USB policy: please make sure that the Authenticity dongle (= USB stick PU-50n) is inserted into your Raspberry PI before you power up your Raspberry PI

The boot up of your Raspberry PI will look similar to the screenshot shown below:

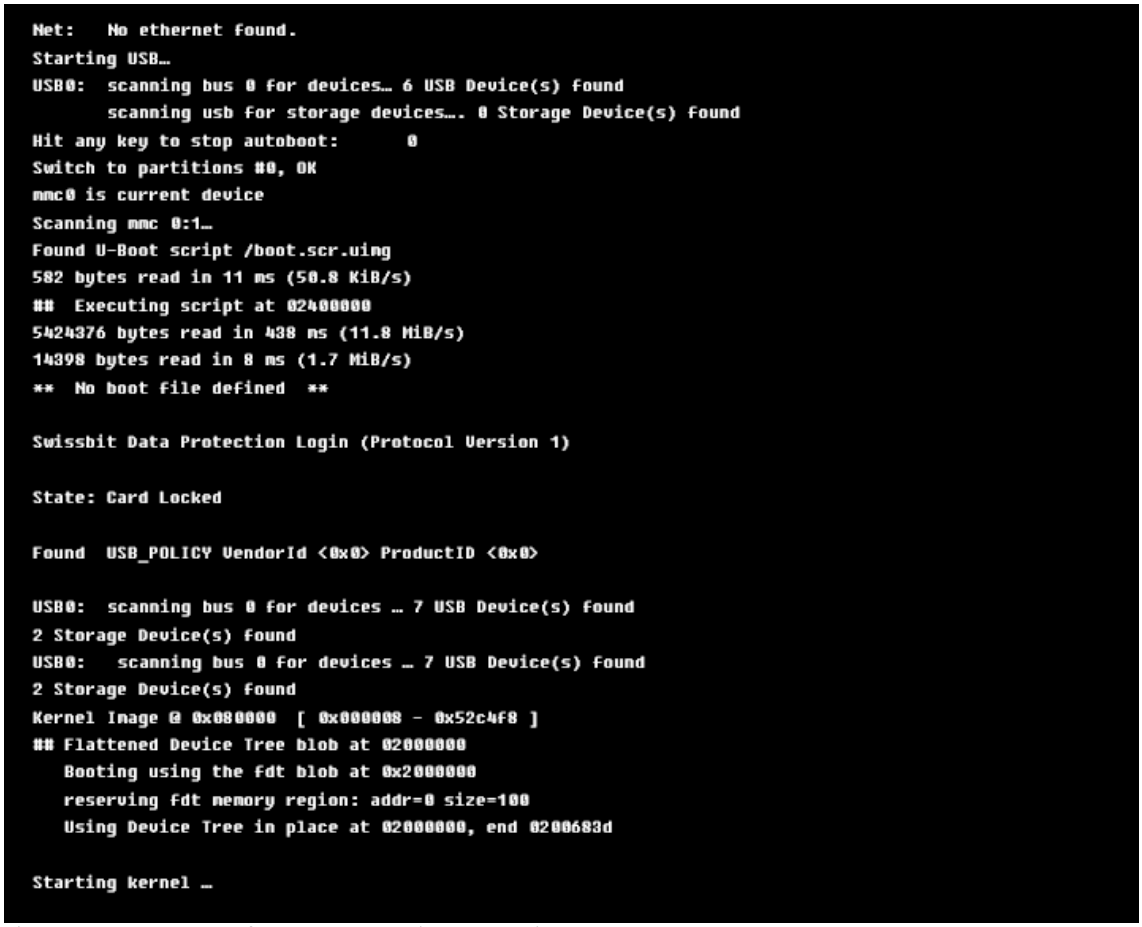


Fig. 13 Secure Boot of Raspberry PI with USB policy

3. NET Policy: Please make sure, that your Raspberry PI is connected to the network and the net policy server is up and running.
   The boot up of your Raspberry PI will look similar to shown below:

```
Net:   No ethernet found.
Starting USB…
USB0:  scanning bus 0 for devices… 6 USB Device(s) found
       scanning usb for storage devices…. 0 Storage Device(s) found
Hit any key to stop autoboot:      0
Switch to partitions #0, OK
mmc0 is current device
Scanning mmc 0:1…
Found U-Boot script /boot.scr.uimg
582 bytes read in 11 ms (50.8 KiB/s)
##  Executing script at 02400000
5424376 bytes read in 438 ms (11.8 MiB/s)
14398 bytes read in 8 ms (1.7 MiB/s)
**  No boot file defined  **

Swissbit Data Protection Login (Protocol Version 1)

State: Card Locked


Found  NET policy ███.███.███.███:12375

Lan78xx_eth Waiting for PHY auto negotation to complete, done
DHCP broadcast 1
net_dns_server: ███.███.███.███
net_netmask   : ███.███.███.███
net_gateway   : ███.███.███.███
Our IP address is ███.███.███.███

IP address for ███.███.███.███ is ███.███.███.███

Lan78xx_eth Waiting for PHY auto negotation to complete, done
Using lan78xx_eth device

DP login server ███.███.███.███ is active

Lan78xx_eth Waiting for PHY auto negotation to complete, done

Send Packet : Wait for reply from server

.Response from server received:
Kernel Image @ 0x080000  [ 0x000008 - 0x52c4f8 ]
## Flattened Device Tree blob at 02000000
   Booting using the fdt blob at 0x2000000
   reserving fdt memory region: addr=0 size=100
   Using Device Tree in place at 02000000, end 0200683d

Starting kernel …
```

Fig. 14 Secure Boot of Raspberry PI with NET policy

8. Appendix

8.1 Deactivating DP Card Data Protection

If you want to make changes to the boot partition of the Swissbit DP card (PS-45u Raspberry Pi Edition), you can do this only when the card has data protection deactivated (transparent mode).
Deactivate DP card following steps:

1. Start the Swissbit Device Manager
2. Go to menu "Manage > Deactivate Data Protection"
3. Enter the Security Officer Password
4. Click on "Deactivate Data Protection"

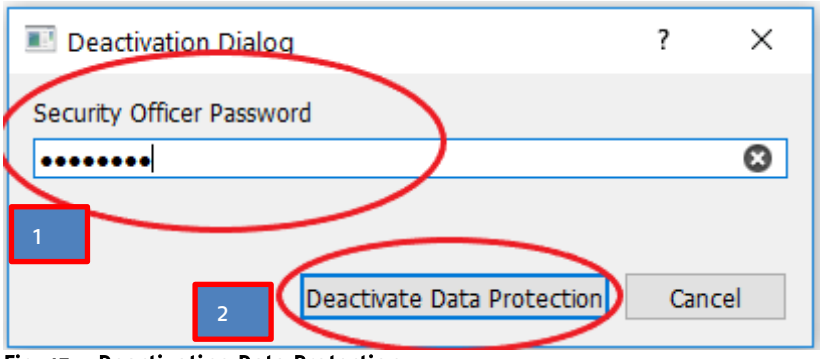


Fig. 15 Deactivating Data Protection

CLI Command:

```
$.\cardManagerCLI.exe --mountpoint E: --deactivate --sopin 12345678
```

8.2 DP-card Compatibility on Raspberry-Pi

Due to a violation of the SD specification by the host (Raspberry-Pi), power-on recognition problems can occur in seldom cases when Swissbit DP Cards are used on the Raspberry Pi. If the issue is triggered, the Raspberry Pi's LED does flash 4 times and it won't boot. This problem does not exist once the device has booted successfully.

Below are the status of Raspberry-PIs where there is a possibility that this problem can be occur:

Pi Model	Safe for use
2 Mod B	Very low probability for issue
3 Mod B+	Very low probability for issue
CM3 B+ lite	Yes
4 Mod B	Yes

Note: For Secure boot use case Swissbit recommends to use CM3 B+ lite model as it safe for use against power-on recognition problem with Swissbit DP Cards on the Raspberry Pi.

Remedies:

This very seldom power-on recognition problem with Swissbit DP card on the Raspberry Pi can be solved by adding ~100k Ω resistor between CLK and GND pin in SD card slot of Raspberry Pi as shown in the below picture.

Note: Apply remedy only if the problem occurs

Placement of 100k Pull-Down between CLK and GND pin in SD card slot of Raspberry Pi

8.3 Reference Material

8.3.1 Swissbit

Swissbit Net Policy Server User Manual

8.3.2 U-Boot

https://www.denx.de/wiki/view/DULG/UBoot
http://www.denx.de/wiki/DULG/Faq

8.3.3 Raspberry Pi

https://elinux.org/RPi_U-Boot

9. Document History

Version	Updated on	Updated by	Short description
2.0	April 20th, 2020	Swissbit AG	First public release
2.1	Nov. 18th, 2020	Swissbit AG	Update CM3+ support & DP card compatibility
2.2	May. 31st 2021	Swissbit AG	Update RPI4 support & netpolicy support for Ishield server.
2.5	July 21th 2021	Swissbit AG	Changes after review
2.6.1	March 03 2022	Swissbit AG	Update RPo support
2.6.2	July 12 2022	Swissbit AG	Add CLI commands