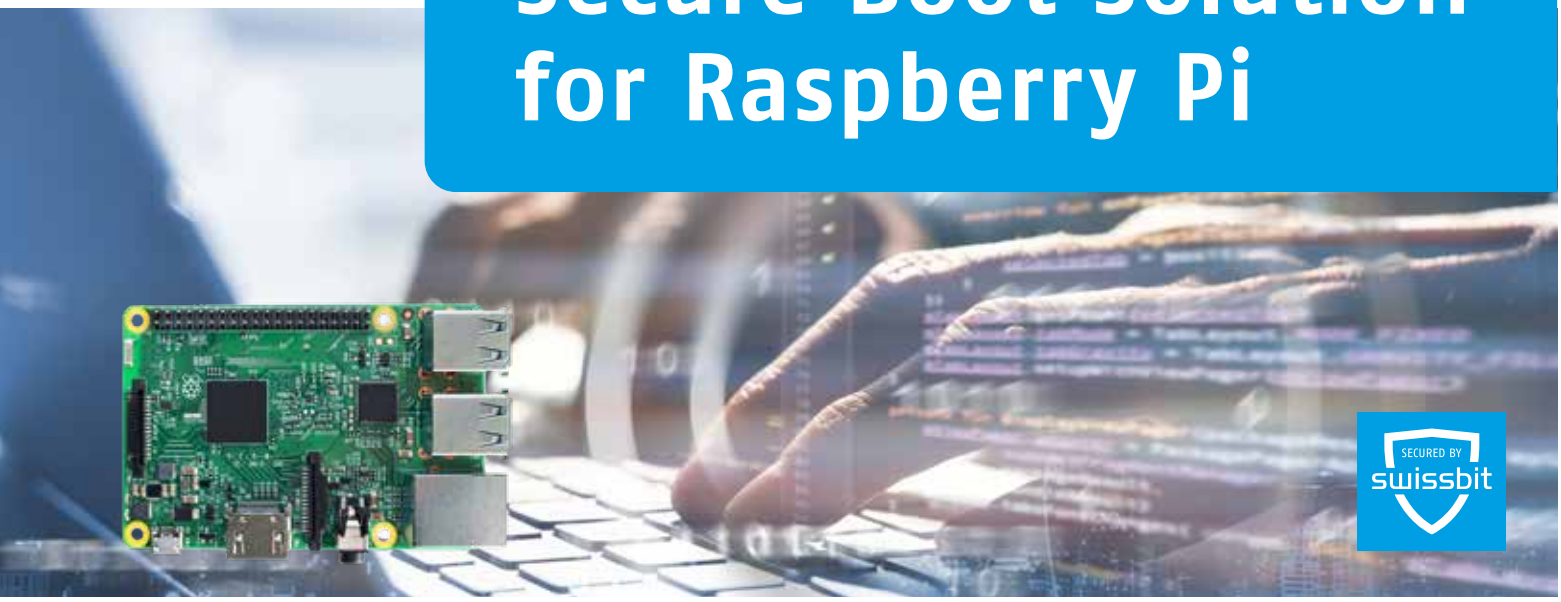
swissbit®

Secure Boot Solution for Raspberry Pi



Protecting the System Integrity of a Raspberry Pi Boot Media

Swissbit Secure Boot Solution for Raspberry Pi

The Swissbit Secure Boot Solution for Rasberry Pi allows encryption and access protection of data stored on the microSD card by various configurable security policies.

It protects the boot image and software installation against manipulation, unwanted copying, or removal of a system from a defined network.

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

Getting started

Step 1: Check Prerequisites

Step 2: Get Swissbit Secure Boot Solution for Raspberry Pi:

a) Swissbit microSD card "Raspberry Edition"
b) Swissbit Secure Boot Solution SDK for Raspberry Pi

Step 3: Configure the Swissbit microSD card "Raspberry Edition" with Swissbit Secure Boot SDK by choosing your preferred security policy:

- PIN policy: PIN entry
- USB policy: USB as authentication dongle
- NET policy: Authentication through a network server

Step 4: Install U-Boot

Step 5: Activate protection

SECURED BY swissbit

Swissbit PS-45u DP microSD card "Raspberry Edition"

www.swissbit.com

Swissbit microSD card PS-45u DP "Raspberry Edition"

Features

- Security policies with flexible and configurable authentication
- Access protection with configurable retry counter
- Authentication is performed during the Swissbit customized pre-boot phase to unlock access
- Works with Rasperry Pi 2 and 3B+

Key Applications

- IP Protection by locking microSD card
- Theft protection by locking microSD card
- License control by providing unique ID (with NET policy)

Benefits

- Easy-to-integrate CPU independent hardware security
- Cost effective data protection and encryption
- Easy-to-retrofit and future proof security solution

Function

- Protecting Raspberry Pi boot loader
- Encrypting user and boot code to protect license, know-how and IP
- The boot image can be set as read-only to prevent unauthorized modification
- Restricting the access to data on the card by various configurable security policies: PIN or USB or NET policy

Security Function	PIN Policy	USB Policy	NET Policy
Know-how protection	✓	✓	✓
IP & license protection	✓	✓	✓
Remote attestation	✓	✓	✓
Data protection	✓	✓	✓
Theft protection	✓		✓
Tamper protection			✓
Lock device			✓
Secure unattended boot		✓	✓

Security Policies and Requirements

PIN

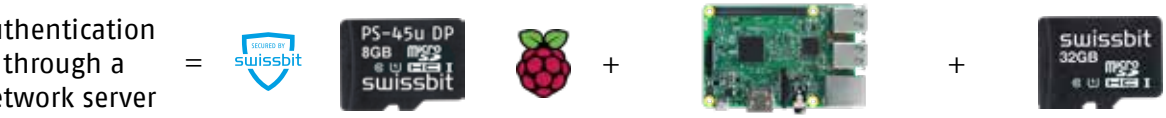
PIN input = Swissbit microSD card PS-45u DP „Raspberry Edition"

USB

Authentication Dongle = Swissbit microSD card PS-45u DP „Raspberry Edition" + Additional: Swissbit USB stick PU-50n DP „Raspberry Edition"

NET

Authentication through a network server = Swissbit microSD card PS-45u DP „Raspberry Edition" + Additional: Raspberry Pi + Additional: microSD card min. 8 GB e.g. Swissbit S-45u



Distribution Partners

www.digikey.com

www.farnell.com

www.mouser.com

Use Cases

Robust Boot Media with IP and Copy Protection

Problem

- Boot device must provide high retention
- Boot partition needs to be protected against manipulation
- System image needs to be protected against IP theft

Requirement

- Boot partition readable on each host & write protected
- Read / write storage partition accessible after authentication
- Private partition

Solution

- Swissbit Data Protection card with full encryption and protection profile
- Fine-grained access policy with user pin and administrator login
- IP Data can be protected against theft, manipulation and reverse engineering

Data Protection of Control System

Problem

- Risk of unauthorized Data access or data manipulation
- Device unprotected against manipulation and license fraud

Requirement

- Secure license provider to unlock access
- Secure storage extension for control system
- Private partition

Solution

- Swissbit microSD card with full encryption and customizable data protection profile
- USB as authentication dongle
- Fine-grained access policy with user pin and administrator login
- Device protection with USB authentication dongle

Protecting Loss or Theft of Data captured by Cameras

Problem

- MicroSD slot provides access to data
- Risk of unauthorized data access, data manipulation, deletion and data loss

Requirement

- Data protection and encryption
- Role-based access control
- Private partition for recorded data

Solution

- Swissbit microSD card with full encryption and customizable data protection profile
- Hardware access protection will only show the protected data if the right authentication has been applied
- Data is protected against reading

Use Cases

Device Integrity by Secure Storage

Problem

- Weak protection against unauthorized access

Requirement

- Access control
- Securing unattended boot
- Preventing insertion of unauthorized hardware (microSD) by pairing client and server

Solution

- Removable Swissbit microSD card with full encryption and access profiles
- (Automated) Pairing ensures that secure storage works only in combination with specific device hardware
- Net-policy-server for access control

Privacy Data Protection

Problem

- Risk of unauthorized data access, data manipulation and data loss
- GDPR (DSGVO) legislation requires that customer data must be protected against theft, unauthorized viewing or manipulation

Requirement

- Read / write storage partition access only granted after authentication
- Outside of the Raspberry Pi or without proper authentication the data is fully protected
- Only after applying the right authentication the private partition is visible

Solution

- Swissbit data protection microSD card with full encryption and protection profile
- Fine-grained access policy
- Private data is protected against theft, unauthorized viewing and manipulation