SECURED BY swissbit

Create trust in your embedded system

Enhance data protection and ensure secure access, perfectly suited for retrofit solutions.

Store. Secure. Trust.

swissbit®

Cybersecurity threats lead to

- Financial Damage
- Reputational Damage
- Loss of Customer trust

Embedded systems need to comply with Global cybersecurity regulations & standards

EU Regulations

- Radio Equipment Directive (RED)
- Cyber Resilience Act (CRA)
- Network & Information Security (NIS2)
- Data Act

US & Global Regulations

- For medical devices (FDA Act)
- For financial services (PCI-DSS)
- California IoT law (SB-327)
- Japan: IoT Security and Safety Framework (IoT-SSF)

Industry Standards

- Cyber Security Standard for IoT devices (EN 303 645)
- Security Framework for industrial automation and control systems (IEC 62443-4-2)
- NIST Cybersecurity for IoT Program (NISTIR 8259A)

How to meet unique requirements for security embedded systems

Embedded systems security issues

- Long Product Lifecycle
- Difficult to update
- Limited flexibility

›

Requirements

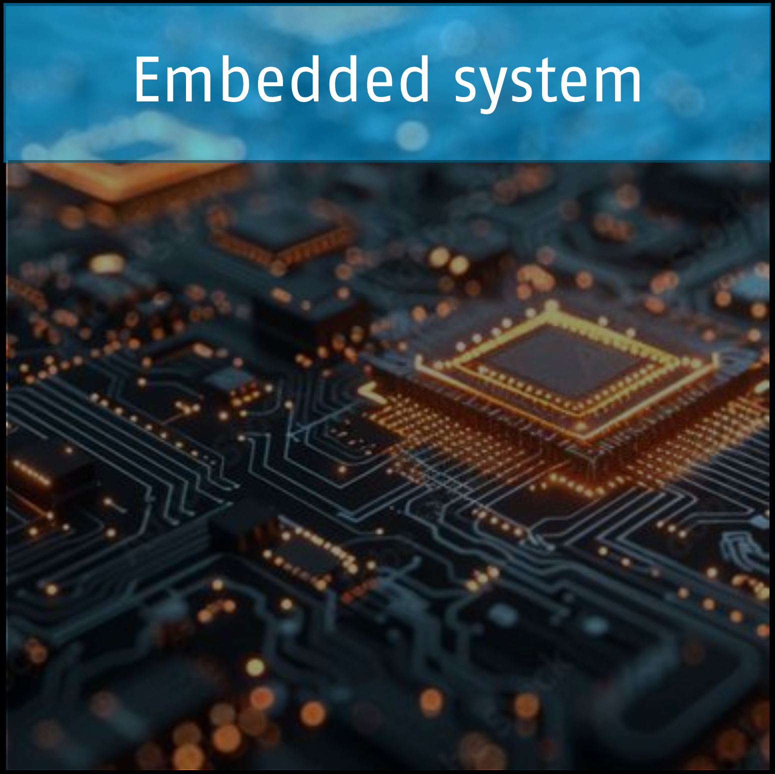
- Data confidentiality
- System integrity
- Data availability

›

Security Upgrade Kit

- Encryption
- Trusted platform
- Access control

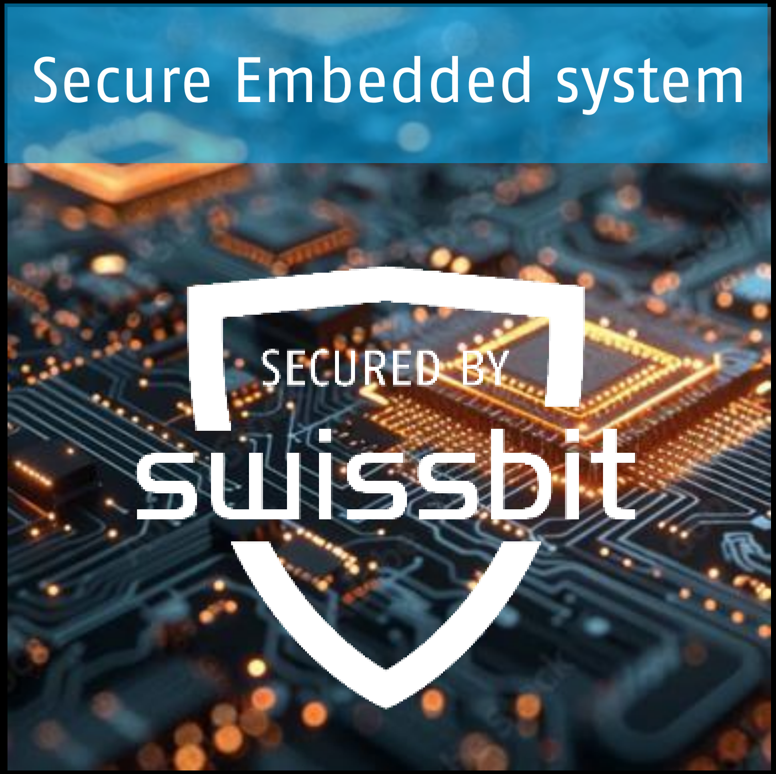
Swissbit Security Upgrade Kit: Ensuring secure embedded systems



Embedded system

+

=



Secure Embedded system

Creating trust in your embedded system

The Security Upgrade Kit with microSD card Security Level 2 creates trust in your embedded systems.

The kit enhances data protection and ensures secure access control with ease allowing users to keep their embedded system always secure by upgrading existing microSD/ SD cards. It is perfectly suited for retrofit solutions providing exceptional embedded security.

Data Protection

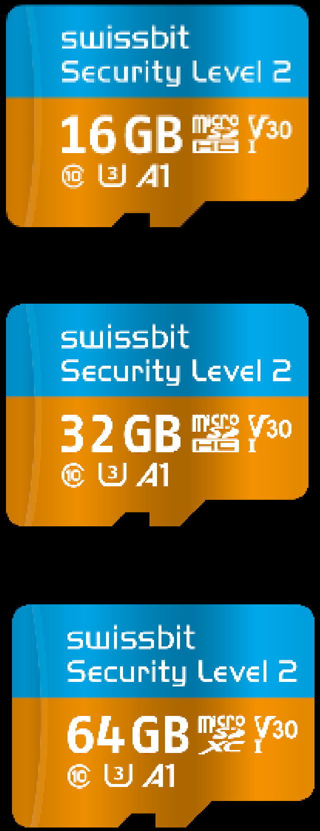
Access Control

Perfect for Retrofit

Product overview: Swissbit Security Level 2

Key Facts

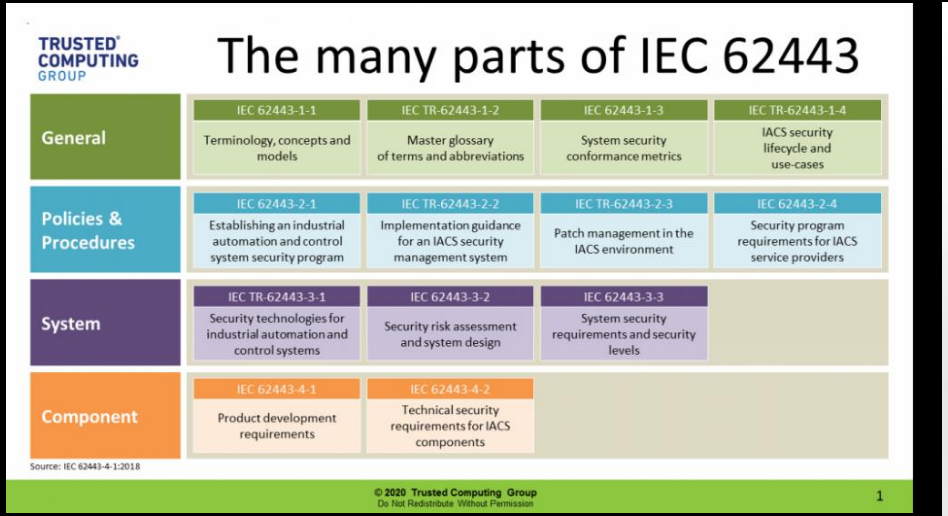
- Hardware-based Access Control
- Easy to use access control
- Self encrypting drive using real-time AES 256
- Individual configuration of protection profiles
- Industrial grade memory (pSLC) for high endurance



Use Cases

- Copy & Cloning protection Configurations, Privacy Data and AI models
- System Integrity protection as Retrofit Secure boot
- Data Protection for Removable media
- License Protection as hardware dongle

Swissbit Security Level 2 microSD card corresponds to Industrial Security Standards



TRUSTED® COMPUTING GROUP

The many parts of IEC 62443

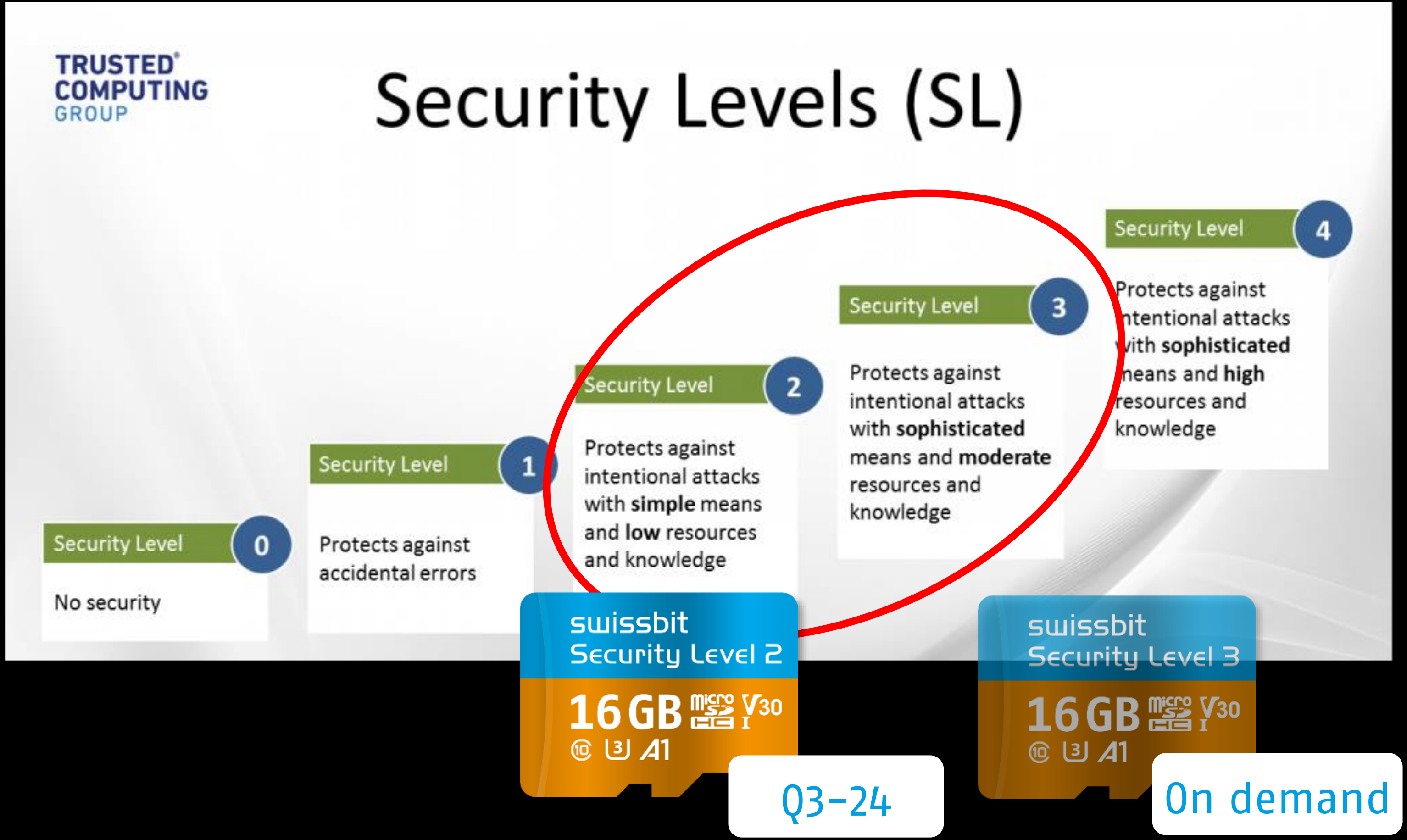
General	IEC 62443-1-1 Terminology, concepts and models	IEC TR-62443-1-2 Master glossary of terms and abbreviations	IEC 62443-1-3 System security conformance metrics	IEC TR-62443-1-4 IACS security lifecycle and use-cases
Policies & Procedures	IEC 62443-2-1 Establishing an industrial automation and control system security program	IEC TR-62443-2-2 Implementation guidance for an IACS security management system	IEC TR-62443-2-3 Patch management in the IACS environment	IEC 62443-2-4 Security program requirements for IACS service providers
System	IEC TR-62443-3-1 Security technologies for industrial automation and control systems	IEC 62443-3-2 Security risk assessment and system design	IEC 62443-3-3 System security requirements and security levels	
Component	IEC 62443-4-1 Product development requirements	IEC 62443-4-2 Technical security requirements for IACS components		

Source: IEC 62443-4-1:2018

© 2020 Trusted Computing Group
Do Not Redistribute Without Permission

1

https://www.iotglobalnetwork.com/iotdir/2020/04/16/iec-62443-how-to-achieve-the-highest-levels-of-industrial-security-24420/



TRUSTED® COMPUTING GROUP

Security Levels (SL)

Security Level 0
No security

Security Level 1
Protects against accidental errors

Security Level 2
Protects against intentional attacks with **simple** means and **low** resources and knowledge

Security Level 3
Protects against intentional attacks with **sophisticated** means and **moderate** resources and knowledge

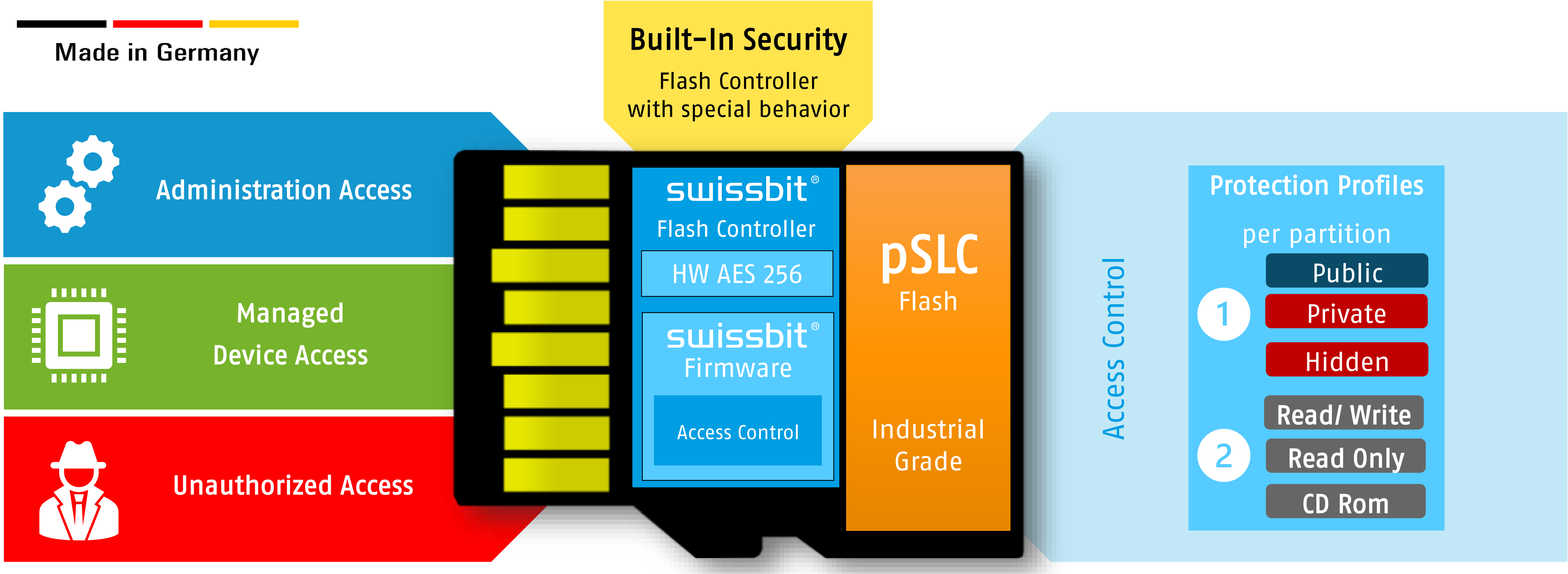
Security Level 4
Protects against intentional attacks with **sophisticated** means and **high** resources and knowledge

Q3-24

On demand

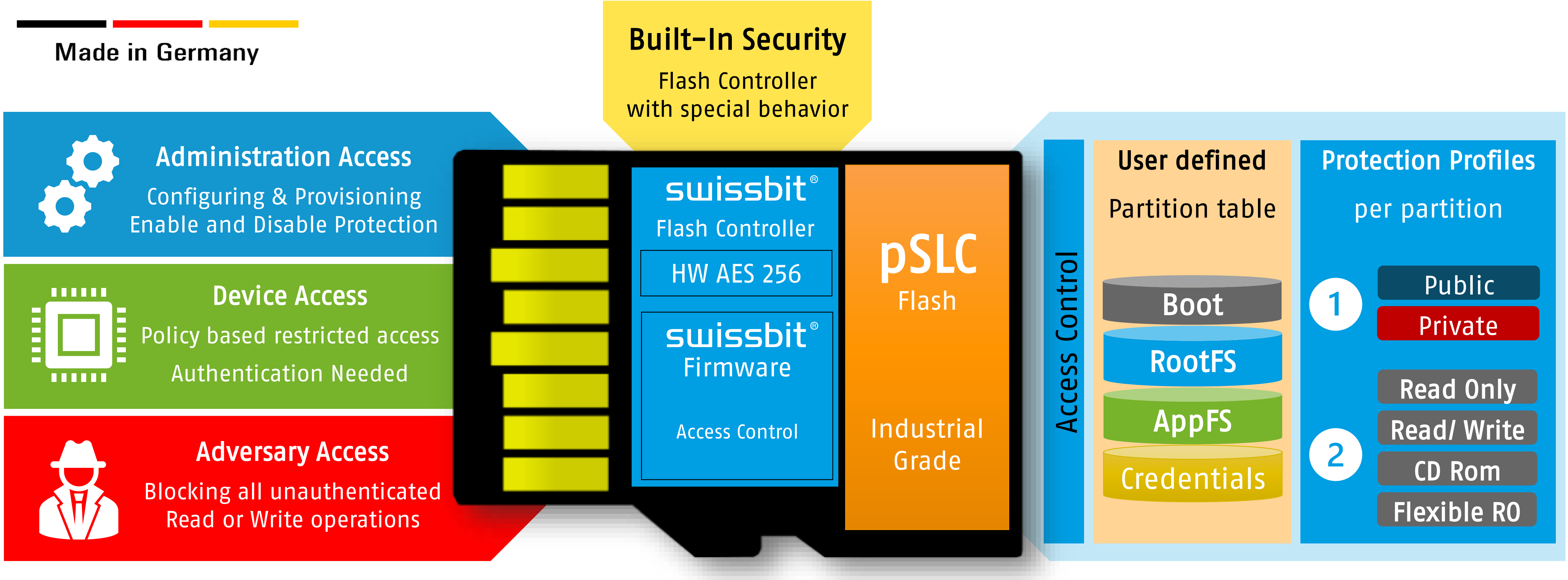
How does it work

Made in Germany



How does it work

Made in Germany



Built-In Security

Flash Controller
with special behavior

Administration Access

Configuring & Provisioning
Enable and Disable Protection

Device Access

Policy based restricted access
Authentication Needed

Adversary Access

Blocking all unauthenticated
Read or Write operations

swissbit®
Flash Controller

HW AES 256

swissbit®
Firmware

Access Control

pSLC
Flash

Industrial
Grade

Access Control

User defined

Partition table

Boot
RootFS
AppFS
Credentials

Protection Profiles

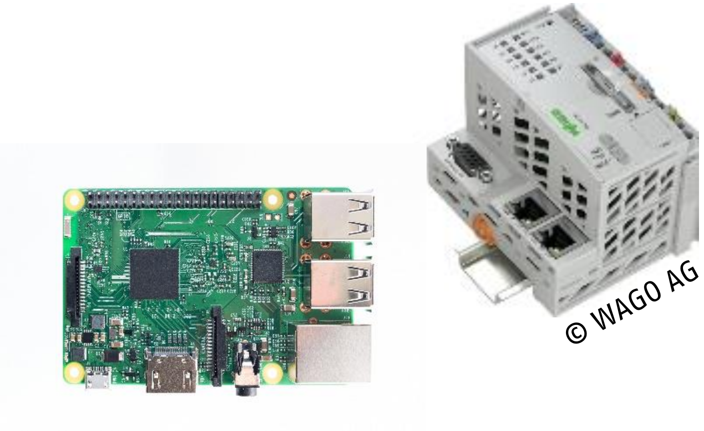
per partition

1
Public
Private

2
Read Only
Read/ Write
CD Rom
Flexible RO

Ensuring secure embedded Linux systems

Protecting data e.g. IP, configurations and credentials from being stolen, copied or manipulated on any embedded Linux system



© WAGO AG

Ensure data confidentiality of externally stored data like security logs, privacy or configurations on any embedded Linux system

© WAGO AG

Ensure system integrity of the operating system and applications on many embedded Linux systems

Security Upgrade Kit ensures business continuity

Intellectual Property

Credentials

Identifiers
(Device and people)

Digital
Product-License

Algorithms /
Firmware

Logfiles /
Logdata

Location

Accounts

Process Data

Configuration
(Files/Flags)

Safety
Functions

Sensor Data

Privacy

Communication

Security Goal Description

Asset	Comment	Confident.	Integrity	Authenticity	Availability
Operating System	Basic system functionality, security settings	(X)	X	X	
Application Software	Protection from manipulation	(X)	X	X	
Communication Interface	LAN, IPconfig, MAC, WiFi, WAN, LoRa, ISM Radio, ...				X
Configuration Files	Hostname, Backend URLs, IPs	X	X		
Login Credentials	Root PW Hash, Public Keys	X			
License Files		(X)	X	X	
VPN Private Key		X			
Backend URLs		(X)	X	X	
Privacy Data		X			
Application Data	Sent to a backend	(X)	X	X	

Security upgrade kit for any organization

Enterprise OT & IT

The Security Upgrade Kit fortifies company networks, ensuring that operations remain secure and uninterrupted.

Public Sector

The Security Upgrade Kit ensures the resilience and reliability of the public sector's digital services.

Critical Infrastructures

Security Upgrade Kit ensures operational continuity and public trust.

swissbit®

How to get started: Security Upgrade Kit with software, tools and drivers

www.swissbit.com/security-upgrade-kit

Setup & Configuration

Linux Windows

Target System Integration

Linux Windows

Secure Boot Implementation

Available for Raspberry Pi
Portable to other systems

RaspberryPi Linux

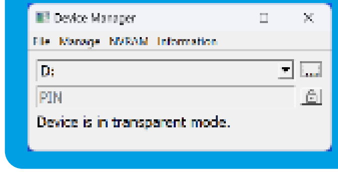
How to get started

Setup and Configuration

Tools available

Initial Configuration

Card Manager App



D:

PIN

Device is in transparent mode.

Card Manager CLI

DLL / Lib Support

1010 1010 1010
1010 1010 1010

Target System Integration

Designed for possible

Routine Lock and Unlock

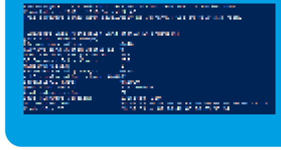
ASSD Protocol

1010 1010 1010
1010 1010 1010

U-Boot Integration

U-Boot

Card Manager CLI or Lib



1010
1010

Secure Boot Implementation

Available for Raspberry Pi

Portable to other systems

Reference Design

U-Boot based Integration

Source Code available

U-Boot

```
## Booting bootflow '[illegible]' with script
Loading boot script for RPi 4
327 bytes read in 21 ms ([illegible])
## Executing script at [illegible]
switch to partitions #0, OK
mmc0 is current device
[illegible] bytes read in [illegible] ms ([illegible])

Swissbit Data Protection Login (Protocol Version 3)

State: Card locked

Found PIN_POLICY

Please enter your PIN: ****
```

Tested with

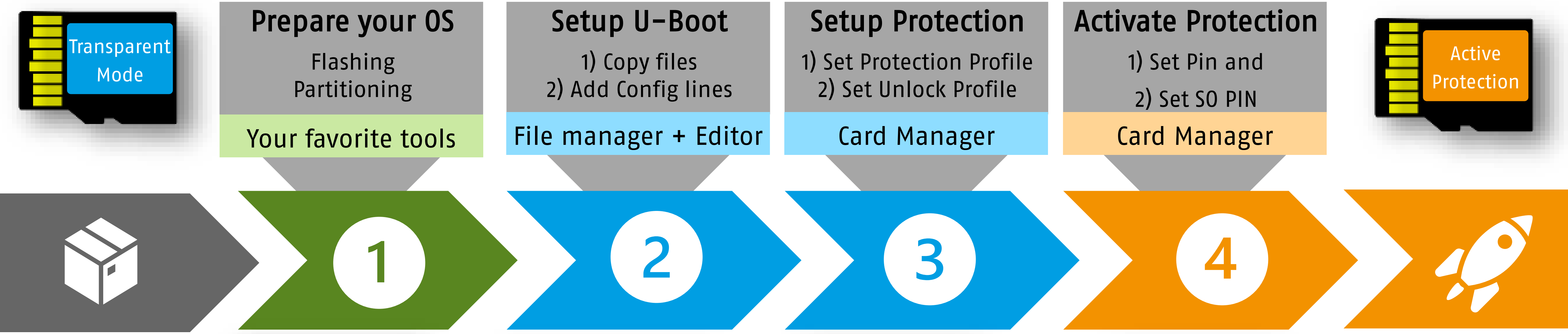
RPi Zero (2W)

2B | 3B(+) | 4

Not 5

Raspberry Pi OS
Bookwork 32/64 bit

Secure Boot for Raspberry Pi: How to get started



Prepare your OS

Flashing
Partitioning

Your favorite tools

Setup U-Boot

1) Copy files
2) Add Config lines

File manager + Editor

Setup Protection

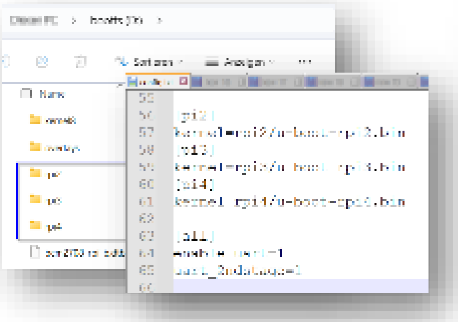
1) Set Protection Profile
2) Set Unlock Profile

Card Manager

Activate Protection

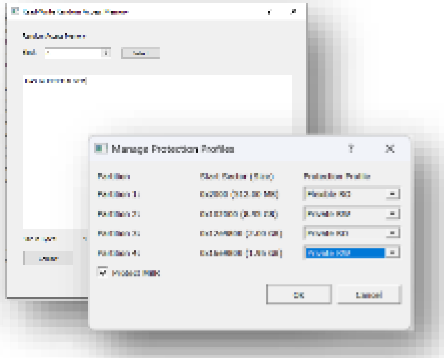
1) Set Pin and
2) Set SO PIN

Card Manager



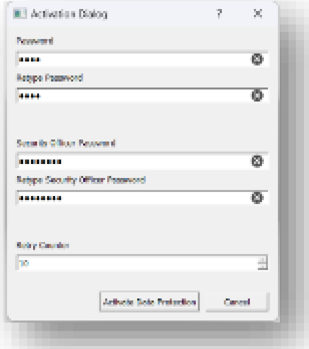
```
[pi2]
kernel=rpi2/u-boot-rpi2.bin
[pi3]
kernel=rpi3/u-boot-rpi3.bin
[pi4]
kernel=rpi4/u-boot-rpi4.bin

[all]
enable_uart=1
uart_2ndstage=1
```


Manage Protection Profiles

Partition	Start Sector (Size)	Protection Profile
Partition 1:	[illegible]	[illegible]
Partition 2:	[illegible]	Private RW
Partition 3:	[illegible]	Private RO
Partition 4:	[illegible]	Private RW

☑ Protect MBR


Activation Dialog

Password: ****
Retype Password: ****
Security Officer Password: ********
Retype Security Officer Password: ********
Retry Counter: 10

Get your security upgrade now

Contact us

swissbit®

swissbit.com/security-upgrade-kit/
sales@swissbit.com

Why Swissbit

Trusted Partner for 20 years

- Own production & products “Made in Germany”
- Worldwide leader of industrial storage and security solutions

Proven Security Competence

- Over 10 years of field proven security products and solutions to protect data and devices
- Trusted supply chain

Best Service & Support

- Custom form factor and custom branding possible
- Unique sales & worldwide technical support

Your Partner for Trusted Data & Identity

Swissbit Europe (HQ)

Tel. +41 71 913 03 00
sales@swissbit.com

Swissbit North America

Tel. +1 978 490 3252
salesna@swissbit.com

Swissbit Japan

Tel. +81 3 6258 0521
sales-japan@swissbit.com

Swissbit Asia

Tel. +886 912 059 197
salesasia@swissbit.com

Store. Secure. Trust.