swissbit®

PU-50n DP
SECURE USB3.1 FLASH DRIVE
INDUSTRIAL DATA PROTECTION

The PU-50n DP USB stick provides highest performance, robustness and security in a USB Type-A device. Its built-in Data Protection (DP) function with AES256 encryption enables multiple use cases.

The memory of the USB stick can be partitioned into different logical sections. Each of them presents itself as a separate mass storage device with a freely configurable data protection policy.

Following access policies are available:

CD-ROM Partition can provide read-only data such as boot code, SW installers or any data, that must not be overwritten.

Private Partition encrypts and protects data. After secure PIN login, this partition is unlocked and available for unrestricted read-write access.

Public Partition is read-write accessible without any restrictions equal to a standard USB stick.

Hidden Storage serves to store WORM data (Write Once, Read Multiple) or random accessible data that can be controlled in every detail.

New Data Protection laws like EU-DSGVO or GDPR put sensitive data under special protection. In case of data loss, severe fines may apply. The PU-50n DP makes it trivial for solution providers to protect sensitive data and prevents such risks.

In case the USB device is lost, PIN protection combined with the built in HW retry counter prevents data abuse. Additionally, Read-Only data is efficiently protected from injection, i.e. the integrity of media is guaranteed.
The PU-50n DP is the ideal response to highest industrial data protection security requirements.

Advantages by Modularity

Applications very often suffer one or more of the following facts that may lead to risky compromises, e.g.

- Spread security between host hardware, OS and application
- Complex maintenance
- Inflexibility of logistical flows

Coming in a robust USB Type-A device the PU-50n DP clearly empowers solution providers to control all relevant solution parts by precise enforcement of policies. The security as such is self-contained and independent of the host system.

Due to the flexibility and standards compliance of the USB stick, it works off the shelf on most host platforms.

Typical Use Cases

The USB stick is used to securely store applications, SW updates and sensitive user data.

Audit trails saved in the WORM store serve to document the complete life cycle of host systems in manipulation proof manner.

SW updates for offline systems can be rolled out by PU-50n DP in various flavors by read-only protection or even more secure by protected SW update forcing strong mutual authentication between target system and PU-50n DP.

The possibility for Device Integrity Checks and an Authenticity Check help to prove the PU-50n DP is in exactly the intended functional state and has neither undergone manipulation nor counterfeit of device and stored data.
PU-50n DP is able to form one unit with the host as if the storage device were soldered onto the host PCB. The removable USB concept however keeps usage highly flexible and intuitive.
SW and security maintenance cannot be easier.

Existing systems can greatly benefit from upgraded security just by plugging in the PU-50n DP USB stick.

Data Protection Functions

Multitudes of data protection combinations can be configured by issuers of the USB stick and remain under their full control.

The data protection can be reconfigured and the partitioning of the memory space can be modified at any time.

A random, device internal AES key can be recreated to securely wipe the drive.

PIN protection combined with a HW based retry counter and the option to use a replay-safe login scheme shift limits to fulfill even the highest requirements of industrial data protection.

The CCID Interface and a proprietary mass storage communication interface allow integration into every platform. CCID is the de facto standard and natively supported by Windows and Linux without the need to install a proprietary driver.

None of the security features slows down the processing or has any disadvantage on data endurance as security is built in the DNA of the product during development.

Key features

Flash Memory

- 8/16/32/64 GB (MLC)
- 4/8/16/32 GB (pSLC)

Specification

- USB 3.1 Full- / High- / Super-Speed 5 Gbps
- USB mass storage device class
- Connector Type-A
- 4 LUN
- -40°C to 85°C range optional

Housing

- 24 mm x 12 mm x 4,5 mm (preliminary)
- Metal
- Dust and waterproof

Flash memory protection

- Full internal flash memory encryption
- CD-ROM
- Public partition
- Private partition
- Hidden/WORM storage

Security features

- AES 256 bit encryption
- User PIN and administrator login
- CCID standard
- Implicit and replay safe secure authentication
- Configurable retry counter
- Unique ID
- Counterfeit protection by authenticity and integrity check
- Fast crypto wipe

Supported platforms

- Windows, Linux
- Any USB capable host on request

Please ask for further Swissbit security products with integrated smart cards in USB, microSD, SD and eMMC form factors.
SDK available for solution providers and system integrators.

EMEA / APAC
SWISSBIT AG
Headquarters,
Industriestrasse 4,
9552 Bronschhofen, Switzerland
security@swissbit.com

JAPAN
SWISSBIT JAPAN
2-1-24 Koenji-Kita,
Suginami-Ku Tokyo 166-0002,
Japan
industrial@swissbit.co.jp

NORTH & SOUTH AMERICA
SWISSBIT NA PORT CHESTER, NY
18 Willett Ave #202,
Port Chester, NY 10573, USA
sales@swissbitna.com

GREATER CHINA
SWISSBIT CHINA
No. 149 QinghuiRd,
LongangDist., Shenzhen, China
salesasia@swissbit.com

WWW.SWISSBIT.COM