

PS-45 AND PS-46 DP DATA PROTECTION

INDUSTRIAL DATA PROTECTION MADE EASY



The Data Protection (DP) card provides highest performance and security in the shape of a microSD or SD card. Its built-in data protection function with AES256 encryption enables multiple security use cases.

The memory of the DP card can be partitioned into different logical areas, each of them with a configurable data protection policy which can be flexibly controlled. Following access policies are available:

CD-ROM function protects read-only data such as boot media, SW installers or any data, that must not be overwritten.

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

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

Of course the card can also be configured to act like a standard unprotected SD memory card.

Long life cycles of industrial systems of up to 15 years need flexible security solutions. The DP card offers such flexibility for new designs as well as for legacy systems.

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

In case the card is lost or stolen, PIN protection combined with the built in HW retry counter prevents data abuse. Additionally, read-only data is efficiently protected from malware injection, i.e. the integrity of such media is guaranteed.

A DP card 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 tasks between host hardware, OS and application
- Inflexible maintenance e.g. SW updates
- Inflexibility of logistical flows

Coming in popular form factors like SD and microSD, DP cards clearly empower 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 SD interface, it can be used on many different platforms.

Typical Use Cases

DP cards are used to securely store applications, SW updates and sensitive user data as well as valuable Know-How. DSGVO / EU-GDPR compliance can easily be achieved by protection of sensitive user data at rest or in transit.

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

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

The possibility for Device Integrity Checks and an Authenticity Check help to prove that the DP card is in exactly the intended functional state and has neither undergone manipu-

lation nor counterfeit of device and stored data.

Although the card is removable, DP cards are able to form one unit with the host by cryptographic pairing as if the storage device were soldered onto the host PCB. The removable card concept however keeps usage highly intuitive while increasing memory demand in the future will never be a problem. SW and security maintenance cannot be easier.

Existing systems can greatly benefit from upgraded security just by plugging in the DP card.

Data Protection Functions

Multitudes of data protection combinations can be configured by issuers of the DP card 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 provides the possibility to securely wipe the card.

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.

Support for the fully standardized ASSD interface as well as a proprietary mass storage communication interface allow integration into every platform. The ASSD interface is the de-facto standard for security use cases on microSD and SD cards.

The DP card's security features come with high speed while data endurance and data retention is best in class.

Key features

Flash Memory

- microSD 8 – 128 GB (MLC)
- microSD 4 – 64 GB (pSLC)
- microSD 512MB– 2GB (SLC)
- SD 8–128 GB (MLC)
- SD 4–64 GB (pSLC)

Interface specifications

- SD 3.0 / Class 10 / UHS-I
- ASSD / proprietary security Interface
- –40°C to 85°C range optional

Flash memory protection

- Full internal flash memory encryption
- CD-ROM Emulation
- Private Partition
- Hidden/WORM Storage

Security features

- AES 256 bit flash memory encryption
- Encrypted security activation
- User PIN and administrator login
- Implicit and replay safe secure authentication against password theft
- Configurable retry counter
- Unique ID
- Counterfeit protection by authenticity and integrity check
- Fast crypto wipe

Supported platforms

- Windows, Linux
- RaspBerry Pi, Arduino
- More on request

The DP functionality can be provided also in different form factors.

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

WWW.SWISSBIT.COM

EMEA / APAC

SWISSBIT AG
Headquarters, R&D, FAE support, Sales
Industriestrasse 4,
9552 Bronschhofen, Switzerland
security@swissbit.com

NORTH & SOUTH AMERICA

SWISSBIT NA PORT CHESTER, NY
HQ SBNA, Sales
18 Willett Ave #202,
Port Chester, NY 10573, USA
sales@swissbitna.com

JAPAN

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

GREATER CHINA

SWISSBIT CHINA
FAE support
No. 149 Qinghui Rd,
Longgang Dist., Shenzhen, China
salesasia@swissbit.com