swissbit®

PS-100u DP
SECURE MICRO SD MEMORY CARD

DATA SECURITY BY MICRO SD

The PS-100u DP microSD card is a standard flash memory mass storage card improved by a multitude of security functions for increased usability, performance, security and privacy.

Data protection problems of various kinds are solved by security functions like

- On-the-fly Flash Memory encryption
- Hidden NVRAM storage
- CD-ROM function
- Message encryption
- Stream encryption
- Remote Management
- Unique identification

The card is a tangible crypto module in the form factor of microSD acting as a Hardware-Security-Module (HSM) as well as a secure mass storage device.

Thus technical, legal and commercial risks can be very efficiently reduced.

The combination of flash memory storage and security options in one device let standard applications reach new security levels.

The PS-100u card works in mobile devices based on Android and BlackBerry OS as well as PCs, Laptops, Tablets and embedded devices based on Windows 7 / 8 and Linux.

The microSD card factor itself with supportive USB readers or SD adaptors reaches nearly all mobile, desktop and embedded platforms.

ADVANTAGES OF MODULARITY

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

- Distributed ownership between host hardware, OS and application
- Complexity of maintenance processes
- Inflexibility of logistical flows

Coming in a standard hardware form factor the PS-100u DP clearly empowers the solution owner to control the relevant solution parts such as secure storage of SW or data, trusted execution of symmetric cryptographic functions and enforcement of data protection policies totally independent of the host system.

TYPICAL USE CASES

The card is used to securely store emails, voice and video data, sensitive company information, BYOD data, firmware images, health data, tax data, cash register journals and recordings of body-worn-cameras. It is also suitable for stream encryption of M2M telemetry data, video and voice data while the host system would not have to care about the security implementation.

Existing systems can easily be upgraded just by insertion of the PS-100u DP card and usage of the flexible interfaces.

Each of the following data protection functions can be separately activated on order of the card.

DATA PROTECTION FUNCTIONS

The high speed **on-the-fly data at rest encryption**(*) function of the microSD protects the data on the card with no speed limitation for the user. In case the card is lost all data are secured by PIN/PUK authentication.

A role separation lets the administrator keep full control over all keys and the cards flash memory content while the user is smoothly enabled to use the card.

Remote Management(*) provides the ability for the administrator to manage cards in the field via untrusted networks and potentially compromised devices, which is important especially in mobile scenarios. All relevant functions can be executed remotely by card individual encrypted commands.

Hidden NVRAM(*) stores in separate invisible data area telephone books, SW libraries, tax data, cash-register journals, health data, etc.

Each card is equipped with a **unique ID** for product traceability.

Very often a trusted boot process is not ensured due to usage of read/write storage media. The **CD ROM**(*) partition function of the card enables malware or virus free environments for mobile and home office scenarios.

The **message and stream encryption**(*) is ideal for secure data transfer such as secure messaging, remote control, home automation, secure chat, video and voice streaming or any M2M telemetry data encryption.

(*) ask for separate information

KEY FEATURES

Flash Memory
- 4 GB or more (MLC)
- speed class 10
- AES 256 bit encryption

SD specifications
- SD 3.0
- microSD addendum 3.0
- ASSD V 1.1

Flash Memory encryption
- Automatic file protection
- Data container protection
- Full flash memory encryption

Hidden NVRAM
- Random access storage
- Cyclic storage
- Write Once storage

CD-ROM
- Partial or full write protection
- Persistent lock/unlock
- Temporary unlock

Stream and message encryption
- AES CBC
- AES CTR

Remote Management
- Secure wipe
- De/Activation of policy
- PIN unlock

Supported platforms
- Windows 7 / 8 in 32 / 64 bit
- BlackBerry OS 5 or later
- Android 2.2.or later
- Linux kernel 2.2 or later
- Raspberry Pi
- More on request

SDK available for solution providers and system integrators

SWISSBIT SALES LOCATIONS WORLDWIDE

EMEA / APAC

Swissbit AG
Industriestrasse 4
CH-9552 Bronschhofen
Switzerland

Tel. +41 71 913 03 03
Fax +41 71 913 03 15
security@swissbit.com

North & South America

Swissbit NA
1117 E Plaza Drive Unit E Suite 105 / 205
Eagle, Idaho 83616
USA

Tel. +1 208 938 4525
Fax +1 914 935 9865
sales@swissbitna.com

Japan

Swissbit Japan Inc.
4F, 2-40-16 Umesato
Suginami-ku, Tokyo 166-0011
Japan

Tel. +81 3 33 17 12 11
Fax +81 3 33 17 12 22
industrial@swissbit.co.jp

Greater China

Swissbit Asia
2F., No. 125, Shengli 2nd Rd,
Zhubei City, Hsinchu County 302
Taiwan (R.O.C.)

Tel. +886 3 550 8166
Fax +886 3 550 8126
salesasia@swissbit.com

WWW.SWISSBIT.COM