

PS-100u PE SECURE MICRO SD MEMORY CARD

SMART CARD SECURITY BY MICRO SD



The PS-100u PE microSD card is a standard flash memory mass storage card supplemented with an additional secure element providing high security for enterprises and organizations. This card offers pre-integrated features for improved usability, performance and security.

The product provides next to smart card security additional 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.

In combination with flash memory the microSD smart card allows to fulfill the need for security and flash memory storage in one device.

The PS-100u PE card provides highest possible smart card security without the need of a smart card reader. 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 card is used to secure emails, voice and video data, network access, company information, firmware images, TPM like boot processes, SW licenses,

health data, tax data, cash register journals, M2M telemetry data, BYOD data, data of body-worn-video cameras etc.

For portable devices like mobile phones, smart phones, tablets and embedded devices the microSD mass storage form factor is the de facto standard for flash memory extensions.

FLEXIBILITY BY JAVA CARD TECHNOLOGY

The smart card inside the PS-100u PE is running a state of the art Java Card OS in version 3.0 allowing highest flexibility for solution providers to implement their own cryptographic API.

The security certification of the chip and the Java Card VM define this microSD as the trusted anchor in mobile and embedded security.

Multiple security domains compliant to Global Platform enable the card issuer to manage the smart card runtime environment securely and provide tailored security solutions to the market.

Solution providers choose the PS-100u because it offers flexibility by

- Java Card with high security
- open business model
- multi platform support for mobile / tablet / PC / Laptop / embedded

TYPICAL USE CASES

Typical use cases occur in the strong combination of the smart card security and the long list of preconfigured extra functions of the Premium Edition card.

Advantages lie in the hybrid approach to use the high security of the smart card and the possibility to delegate high speed encryption to the premium functions. The solution provider is empowered to define the work share and thus the balance of security versus speed.

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

The high speed **on-the-fly data at rest**

encryption(*) function of the microSD protects the data 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 read/write storage media. The **CD ROM(*)** partition function of the card enables malware and virus free PC and Laptops for mobile and home office in parallel to read/write secure storage for the user.

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

Relevant security market segments are Government, Enterprise, Banking, M2M, Industry 4.0 and Multimedia.

(*) ask for separate information

KEY FEATURES

Smart Card Chip

- Infineon SLE 78
- 80 kB free EEPROM
- Common Criteria EAL 5+

Smart Card Chip OS

- jTOP ID
- Java Card 3.0
- Global Platform 2.2.1
- Common Criteria EAL 5+

Flash Memory

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

SD specifications

- SD 3.0
- Micro SD add. 3.0
- ASSD V 1.1

Security functions

- RSA up to 2048 bits
- TDES and AES up to 256 bits
- MD5 and SHA2 up to 512 bits

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

Compatible Middleware

- AET SafeSign
- Charismathics
- Certgate

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,
Zhubel City, Hsinchu County 302
Taiwan (R.O.C.)

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

WWW.SWISSBIT.COM