Secure microSD card
- a tool in combating tax frauds

The success of modern tax administration is increasingly becoming dependent on access to data flows, including in real-time. The aim is to secure recorded sales data in a tamper proof way, to retrieve data offline on site and transmit it online to a tax authority.

We answer these trends with secure microSD cards - designed, developed and produced based on customer's requirements. Secure microSD cards can be used in sales recording systems like cash registers, taximeters, vending machines, parking meters etc.

Hardware

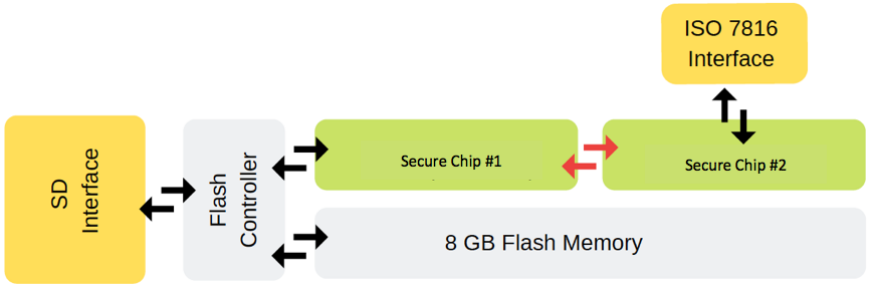
Our secure microSD cards are a standard memory cards with 8GB and higher NAND flash memory with unique features:

- combining two independent high-performance security chips
- with standard ISO 7816 compatible contacts placed on the surface

Specifications

Form Factor	SDHC microSD card 3.01, UHS-I, ISO7816 contact interface Outline dimensions 15 x 11 x 1 mm
Flash Controller	Phison PS8036
Flash Memory	Toshiba NAND 15nm MLC, 8GB or 16GB flash memory
Secure chip(s)	One or two secure chips, based on customer's requirements
Electrical features	Supply voltage 2,7 to 3,6V, max current 400mA Electrostatic discharge: contact up to 4kV, air up to 15kV, up to 5 times/position RoHS ad EMI (CE, FCC) compliant 8 standard microSD UHS-I pins for SD Card 3.01 communication 5 standard ISO/IEC 7816 contact pads for contact personalization of the secure chips
Mechanical features	Operational temperature range: 0°C – 70°C, up to 95% relative humidity (at 25°C) Weight: ~ 1 g

Basic Schematic Example



Unique Features

- Each of the secure chips can run a different firmware while the chips can communicate directly with each other, without any involvement of the host system. **Thus each can underlie particular certification that enables you to use two separate subsystems for different certification levels** e.g. a tax authority record-keeping system and a cryptographic system
- One secure chip can be used for pre-processing of data sending it to the second secure chip which can **securely archive signed data and off-load this data based on a remote command.** The command will export data out of the secure chip and send it to the Host. This will enable control devices staying not-connected
- Some **devices do not have enough memory or mostly work offline**. In this case the secure chip can pre-process the data, signed it and store it encrypted on a Flash memory
- Host access to the secure chips is either through the SD interface or through the external ISO/IEC 7816 contacts. No special hardware drivers are required to access the secure chips in both modes. Such access to secure chips allows **complaint testing, in-field off-line uploads, firmware secure upload etc.**

- The microSD card can **optionally be delivered on ISO 7810 ID-1 compliant carrier and the secure chips can be personalized as an ISO 7816 contact smart card in any smart card personalization equipment or card printer.** After the personalization, the microSD card is removed from the plastic carrier and placed into the target host device
- **Versatile usage** – the secure microSD card can be used in host device with microSD slot, SD slot (via microSD to SD adapter), USB 2.0 or 3.0 interface (via a suitable microSD card reader). Alternatively, the secure microSD card can be used in a standard desktop ISO 7816 contact smart card readers.
- We implement **fast communication for convenient use-cases also with big data flowing**:
  - up to 13Mbit/s using SPI mode between NAND and Flash controller
  - up to 625Mbit/s between secure chip#1 and Flash Controller
  - up to 1Mbit/s between secure chips
- We use a standard flash controller (Phison PS8036) with a proprietary firmware supporting communication with secure chips that can be customized according to your needs

A Security Module

The secure microSD card is a physical platform on which you can develop a particular security module. Two secure chips and external ISO 7816 interface of the secure microSD card can empower security and functionality of the security module and end-to-end solution. Your solution features, functionalities and compliance with various certification schemas will depend on the choice of the secure chips, common properties of these secure chips, storage subsystem utilization and certified firmware of the secure chips.

- **Storage Subsystem**
  - 32bit RISC flash controller (Phison PS8036), 8 GB of 15 nm MLC flash (SDHC)

- Physical capacity of 8 006 926 346 bytes
- User available memory size 7 880 966 134 bytes
- Defect and error management using BCH Error Correction Code
- Static and Dynamic Wear Levelling, Bad Block Management
- FAT32 file system
- 512 byte blocs
- SD speed class 10/ UHS Speed Class U1 (sequential write speed > 10MB/s
- Special folder in the root directory for communication with the secure chips
- Communication using SPI Mode or SD Mode

- **Common properties of Secure chips (SE#1 and SE#2)**
  - Common Criteria EAL5+ certified product
  - Two instances of ARM SecurCore SC300 32bit CPU at 60MHz
  - Elliptic Curve Cryptography hardware security accelerator running at 155MHz
  - Hardware security AES accelerator
  - 2014 Kbytes of Flash memory for firmware and persistent data, 50 Kbytes of SRAM. Flash data retention minimum 10 years
  - AIS20/AIS31 class PTG.2 compliant True Random Number Generator
  - Certified cryptographic library
  - Certified flash loader of initial and post-issuance code update

Example of Implementation

- **SE#1 firmware - Security Module Application for electronic record-keeping systems**
  - Common Criteria EAL2 evaluated firmware
  - Protection profile BSI CC-PP-0105-2018
  - Functionality according to BSI TR-03153
  - Secure channel communication with CSP using the PACE protocol according to BSI TR-03110-2 and 3
  - Cryptographic algorithm support according to BSI TR-0316 and BSI TR-02102
  - Uniform digital interface, internal storage for transaction logs, data export functionality
  - Enabled installation of a digital certificate according to BSI TR-03145
  - After each power-on requires initialization of current tie and date from the host

- **SE#2 firmware – Cryptographic Service Provider (CSP)**
  - Common Criteria EAL4+ evaluated firmware
  - Protection Profile BSI-CC-PP-0104-2018
  - Functionality according to BSI TR-03151

- Supported cryptographic protocols according to BSI TR-03116 Part 5
- Recommended Key Lengths according to BSI TR-02102-1: AES-128, AES-192, AES-256, CBC mode with ISO padding, CMAC
- Client-server architecture: The CSP and the application component are physically separated
- Authentication of users, authentication and attestation of the CSP to entities, data authentication and non-repudiation including timestamps, encryption and decryption of user data, trusted channel including mutual authentication of the communicating entities, encryption and message authentication proof for the sent data, decryption and message authentication verification for received data
- Management of cryptographic keys with security attributes including key generation, key derivation and key agreement, internal storage of keys, import and export of keys
- Generation of random bits, secure signature counter, time and timestamp services

Applications and industries

- **Fiscal compliance -** cash registers, vending machines, taximeters, ticket kiosks, parking meters
- **Industry security** - industry automation, smart grid, energy distribution, energy consumption control, electro mobile charging
- **Industries** – retail, government, automotive, IoT, transport ticketing, parking