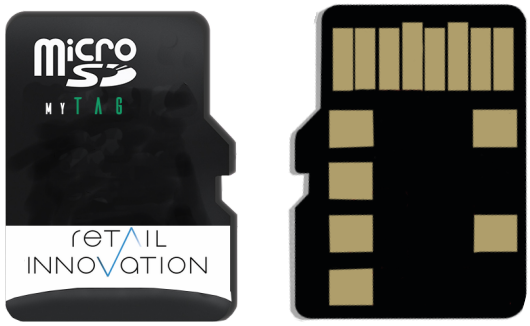


retAIL INNOVATION

CLEANCASH-TSE-8
TSE SECURITY MODULE
TECHNISCHE SICHERHEITSEINRICHTUNG FÜR ELEKTRONISCHE AUFZEICHNUNGSSYSTEME

Retail Innovation HTT AB
Kung Hans Väg 12
S-192 68 Sollentuna, Sweden

Phone: + 46 8 506 655 40
Fax: + 46 8 551 187 88
Mobile: + 46 709 27 77 02
www.retailinnovation.se

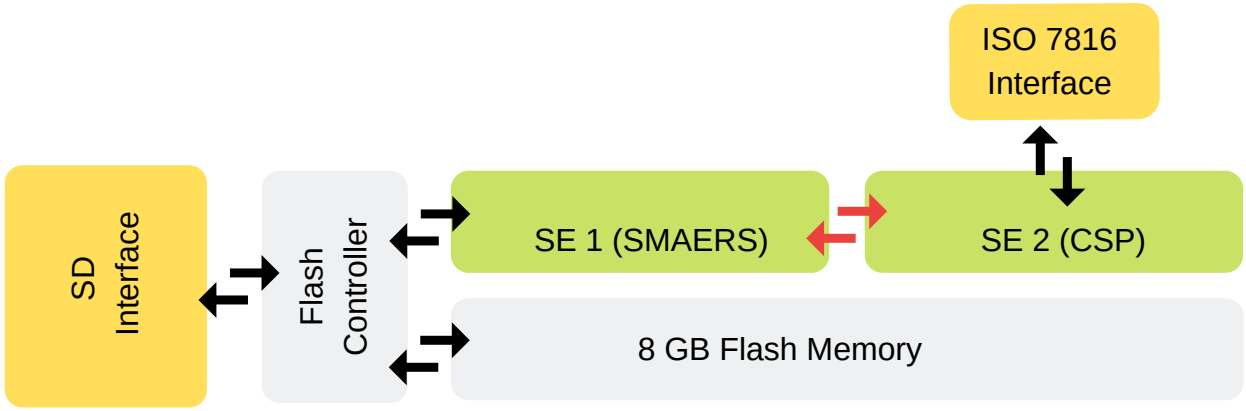
Retail Technology & Innovation

TSE SECURITY MODULE

TECHNISCHE SICHERHEITSEINRICHTUNG FÜR ELEKTRONISCHE AUFZEICHNUNGSSYSTEME

Brief Product Description

The CleanCash-TSE-8 is a high-security device which combines a standard UHS-I class microSD card with 8GB of NAND flash memory for long term storage with a unique combination of two independent highly secure high-performance dual-core 32bit security chips with Common Criteria EAL 5+ hardware security and dedicated secure hardware accelerators for all cryptographic operations. The secure chips can be accessed via the SD card interface or directly through standard ISO 7816 compatible interface.



Security Subsystem with Two Secure Elements

The device contains two physically separate secure elements (of the same type), where each of the secure elements can run different firmware. The secure elements can communicate directly with each other, without any involvement of the host system. Host access to the secure elements is either through the SD interface using the standard SD card command set (using a special systems folder) or through the external 7816 contacts. To access the secure elements in both modes, no special hardware drivers are required on the host.

Security Evaluated Firmware *

For the German “Kassensicherungsverordnung” use, the two secure elements are loaded with Common Criteria evaluated firmware covering the client-server configuration of the Security Module Application for Electronic Record-keeping Systems (SMAERS) according to BSI TR-03153 and Cryptographic Service Provider (CSP) according to TR-03151.

Versatile

The product can optionally be delivered on ISO 7810 ID-1 compliant plastic carrier and the secure chips can be personalised as a ISO 7816 contact smart card in any smart card personalisation equipment or card printer. The microSD card can then be removed from the plastic carrier and placed into the target host device for operational use. For hosts with SD card rather than microSD slot, a standard microSD to SD adapter can be used. For hosts with USB 2.0 or 3.0 interface and no (micro)SD card interface, a suitable (micro)SD card reader can be used. Alternatively the device can also be used in standard desktop ISO 7816 contact smart card readers.

Disclaimer: *
1. Firmware Common Criteria EAL2 (SMAERS) and Common Criteria EAL4+ certification in progress.
2. Specifications subject to change without notice based on updates from Specifications body actions.

TSE SECURITY MODULE

TECHNISCHE SICHERHEITSEINRICHTUNG FÜR ELEKTRONISCHE AUFZEICHNUNGSSYSTEME

Storage Subsystem with 8GB Memory

- 32bit RISC flash controller.
- 8 GB of 15 nm MLC flash (SDHC class).
- Physical capacity of 8 006 926 346 bytes.
- User available memory size is 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 (note: the card MUST NOT be formatted using a different file system than FAT32).
- 512 byte blocks.
- SD Speed Class 10 / UHS Speed Class U1 (sequential write speed > 10 MB/s).
- Special folder in the root directory for communication with the secure elements. This folder is 125 894 656 bytes and the folder and files in this folder cannot be modified. This folder is pre-created during card formatting.
- Communication using SPI Mode or SD Mode: Standard Mode up to 25 MHz (12.5 MB/s), High Performance Mode up to 50 MHz (25 MB/s), UHS-I modes: SDR50, DDR50, SDR104 (up to 104 MB/s).

Common Properties for SE 1 (SMAERS) And SE 2 (CSP)

- Common Criteria EAL5+ certified product according to BSI CC-PP-0084-2014 (with augmentations).
- Two instances of ARM SecurCore SC300 32bit CPU at 60 MHz, connected in Lockstep mode.
- Elliptic Curve Cryptography hardware security accelerator running at 155 MHz.
- Hardware security AES accelerator.
- 2048 Kbytes of Flash memory for firmware and persistent data, 50 Kbytes of SRAM.
- Flash data retention minimum of 10 years, 200 000 erase cycles per page.
- Die integrity (active shield).
- Monitoring of environmental parameters.
- Highly efficient protection mechanisms against faults.
- Permanent timer, 3x 16-bit timers, watchdog timer.
- AIS20/AIS31 class PTG.2 compliant True Random Number Generator.
- Memory Management Unit.
- Flexible communication interface selection.
- Certified cryptographic library.
- Certified flash loader for initial and post-issuance code update.

SE 1 (SMAERS) Firmware: BSI TR-03153

Security Module Application for Electronic Record-keeping Systems

- Common Criteria EAL2 evaluated firmware.
- Protection Profile BSI CC-PP-0105-2018 (currently version 0.7.1 from 2018-11-21).
- Functionality according to BSI TR-03153 (currently version 1.0.1 from 2018-12-20).
- Secure Functionality:
  - Client-server architecture (separate device from CSP).
  - Secure channel communication with CSP using the PACE protocol according to BSI TR-03110-2 and -3.
  - Cryptographic algorithm support according to BSI TR-03116 Part 5 and BSI TR-02102 version 2018-02.
  - Uniform Digital Interface.
  - Internal storage for transaction logs.
  - Data export functionality.
  - Requires installation of a digital certificate according to BSI TR-03145.
  - After each power-on requires initialisation of current time and date from the host.

TSE SECURITY MODULE

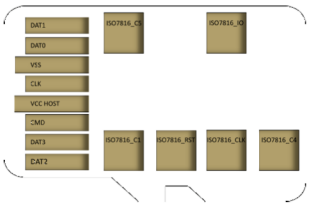
TECHNISCHE SICHERHEITSEINRICHTUNG FÜR ELEKTRONISCHE AUFZEICHNUNGSSYSTEME

SE 2 (CSP) Firmware: BSI TR-03151 Cryptographic Service Provider

- Common Criteria EAL4+ (augmented with ALC_DVS.2 and AVA_VAN.5) evaluated firmware.
- Protection Profile BSI-CC-PP-0104-2018 (currently version 0.9.2 from 2018-12-10).
- Functionality according to BSI TR-03151 (currently version 1.0.1 from 2018-12-20).
- Supported cryptographic protocols according to BSI TR-03116 Part 5 (currently version 2019-02-01):
  - ECDSA with BrainpoolP256r1, BrainpoolP384r1, BrainpoolP512r1, NIST P-256, NIST P-384, NIST P-521.
  - SHA-2 with 256, 384 bits.
  - Password Authenticated Connection Establishment (PACE), according to BSI TR-03110-2 and -3 version 2.20.
- Recommended Key Lenghts according to BSI TR-02102-1, Version 2018-02 from 2018-05-29: AES-128, AES-192, AES-256, CBC mode with ISO padding, CMAC.
- Client-server architecture: The CSP and the application component are physically separated components interacting through a trusted channel. The application component (in client role) uses the security services of the CSP (in server role).
- Secure functionality:
  - 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 with protection of their confidentiality and integrity.
  - Generation of random bits which may be used for security services outside the CSP.
  - Secure signature counter (32 bit counter limited to 16 million operations).
  - Time and timestamp services.

Electrical Specifications

SD Card 3.01, UHS-I mode + ISO/IEC 7816 contact interface (for optional personalisation).



- Supply voltage: 2.7 to 3.6 V, max current 400 mA.
- Electrostatic discharge: Contact up to 4kV, air up to 15 kV, up to 5 times/position.
- RoHS and EMI (CE, FCC) compliant.
- 8 standard microSD UHS-I pins for SD Card 3.01 communication.
- 6 standard ISO/IEC 7816 contact pads for contact personalisation of the secure chips.

Mechanical Specifications

microSD card with additional ISO 7816 contacts.

- Temperature range (operational): 0°C to 70°C, up to 95% relative humidity (at 25°C).
- Weight: ~1 gram.
- Up to 10,000 mating cycles with reader.
- Shock resistance up to 1500 g at 0.5 ms, 150 cm free fall.
- Bending with 10N, hold for 1 min, 5 times.
- Torsion 0.15 N/m or ±2.5 deg, hold for 30 seconds/direction, 5 times.