DATENBLATT

TSE-Modul

Technische Sicherheitseinrichtung (TSE)

Kennzahlen im Überblick

Kategorie	Spezifikation
Formfaktor	microSD (Größe 11,00 mm × 15,00 mm × 0,7 mm), gem. SD Card Association
Transaktionszeit	< 250 ms
Anzahl Schreibzugriffe	> 20 Mio.
Parallele Transaktions-verwaltung	bis zu 512 (SM_MULTI)
Unterstütztes Zeitformat	UnixTime
JAVA Laufzeitumgebungen	Getestet in JRE 8, 10, 11 (LTS)
Betriebstemperatur	0°C bis 70°C (unmittelbare Betriebsumgebung)
Lagertemperatur	–40°C bis 85°C
Luftfeuchtigkeit	Einsatzfähigkeit bei Betrieb: 25°C / 95 % rel. Luftfeuchtigkeit (1 h) Lagerung: 40°C / 93 % rel. Luftfeuchtigkeit (500 h)
Schock	schockresistent, microSD Mechanical Shock Test condition: 500G / 2 ms

Das TSE-Modul ist gem. TR-03153 vom BSI zertifiziert worden.
Zertifizierungsnummer: BSI-K-TR-0374-2020

Seriennummern

Auf der Rückseite der microSD-Karte befinden sich drei Seriennummern.

1) Token-Seriennummer:
- SD-Typ: Commercial Grade
- Produktionszeitpunkt: Jahr & Kalenderwoche, z. B. 1948 (2019, KW48)

2) Controller-Seriennummer:
- Flash-Speicher-Hersteller: Toshiba
- Flash-Speicher-Typ: R (MLC Flash)
- Controller-Typ: 4 (PS8210 SD controller)
- Work-Order-Nummer

3) Fortlaufende Logistik-Seriennummer

Hinweis: Die TSE-Seriennummer gem. BSI TR-03153 wird nach Initialisierung der TSE ausgelesen.

Teilkomponenten des TSE-Moduls

Sicherheitsmodul

Das Secure Element (SE) NXP SE050 stellt die Plattform für die kryptografischen Vorgänge der sicherheitskritischen Kommunikations- und Steuerungsfunktionen dar.

Spezifikationen:
- Java Card Betriebssystem Version 3.0.5
- Sicherheitszertifizierung: CC EAL6+ (HW+JCOP)
- Global Platform Spezifikation: Version GP 3.0
- Speicherzuverlässigkeit: bis zu 100 Mio Schreibzyklen
- Signaturzertifikatslaufzeit: 5 Jahre
- Zertifiziert gem. BSI TR-03153
- SE Applikationen:
  - CSP (BSI CC-Zertifizierung EAL.4+, PP-0104, PP-0107)
  - SMAERS (BSI CC-Zertifizierung EAL.2, PP-0105)

Speichermedium

Als Medium zur Speicherung aller Einzelaufzeichnungen wird ein Toshiba NAND Flash verwendet.

Einheitliche digitale Schnittstelle

Die Funktionen der Export- und Einbindungsschnittstellen gem. „Secure Element API" [BSI TR-03151] werden unterstützt.

Version 17.02.2022

D-Trust GmbH | Kommandantenstraße 15 | 10969 Berlin
Tel: +49 (0)30 25 93 91-0 | info@d-trust.net | www.d-trust.net