

Leistungsbeschreibung TeleSec TCOS 3.0 Signature Card V2.0



Kurzbeschreibung TCOS 3.0 Signature Card V2.0

Die TCOS 3.0 Signature Card V2.0 verfügt über einen NICHT personalisierten Kryptochip mit dem T-Systems-eigenen Betriebssystem TCOS 3.0 Signature Card V2.0 Release 1 (TeleSec Chipcard Operating System).

Die TCOS 3.0 Signature Card V2.0 kann zur Integritätssicherung eingesetzt werden und ermöglicht die Ver- und Entschlüsselung beliebiger Daten. Ebenso ist eine Verwendung als sichere Signaturerstellungseinheit für qualifizierte Signaturen im Umfeld des Deutschen Signaturgesetzes, auf Anfrage auch als Multisignaturvariante möglich.

Leistungsmerkmale

- Intelligente Prozessorchipkarte mit dem eigens hierfür von der T-Systems International GmbH entwickelten Chipkarten-Betriebssystem TCOS (TeleSec Chipcard Operating System)
- Netkey Applikation (NKS) für
 - Fortgeschrittene Signatur
 - Entschlüsselung
- Zugangsschutz für Firewalls, Router, Webserver, Internet-Service-Provider, sicheres lokales Login und/oder „Remote-Login“
- X.509V3-Zertifikate für fortgeschrittene Signatur, Entschlüsselung und Client-Server-Authentifikation
- Qualifizierte Signatur (SigG)
- Ein Siegelzertifikat zur Verwendung der Karte im SigG-Umfeld, sowohl als Einzel- als auch als Multisignaturvariante
- Verfügbarkeit umfassender Dokumentationen
- Verfügbarkeit von Schnittstellen-Software
 - ReadOnly TCOS-Cardmodul zum MS SmartCard BaseCSP
 - PKCS#11-Modul für Windows und Linux

Ihr Vorteil

Die TCOS 3.0 Signature Card V2.0 enthält bei Auslieferung verschiedene asymmetrische Schlüsselpaare. Die krypto-graphischen Schlüssel sind in Verbindung mit physikalischen Kartennummern eindeutig.

Die Qualität der asymmetrischen Schlüssel wird durch ein Erzeuger-siegel des Trust Centers der Deutschen Telekom AG nachgewiesen.

Die TCOS 3.0 Signature Card V2.0 ist evaluiert durch die Security Research & Consulting GmbH nach Common Criteria EAL4+.

Die TCOS 3.0 Signature Card V2.0 ist als sichere Signaturerstellungseinheit nach dem Deutschen Signaturgesetz (SigG) bestätigt.

Die TCOS 3.0 Signature Card V2.0 wird mit einer Transport-PIN ausgeliefert. Die Transport-PIN sichert die Unversehrtheit der Karte und erspart den Versand eines PIN-Briefes. Vor einer Nutzung der Karte wird die Transport-PIN durch eine persönliche PIN ersetzt.

Zusätzlich existiert auf der TCOS 3.0 Signature Card V2.0 eine weitere PIN, die auch zum Entsperren einiger Kartenfunktionalitäten genutzt werden kann.

Die kontaktlos-Schnittstelle der TCOS 3.0 Signature Card V2.0 ist kompatibel zum **neuen Personalausweis (nPA)**

Die TCOS 3.0 Signature Card V2.0 enthält bei der Auslieferung die folgenden Standardapplikationen:

<u>NetKey (NKS):</u>	Entschlüsselung, fortgeschrittene Signatur, Authentifikation.
<u>eSign:</u>	Erzeugung qualifizierter Signaturen .

Kontakt.

Bei Fragen zu Preisen, Lieferzeiten, individuellen Kunden-Layouts, Bestellmodalitäten sowie Auslieferungs- und Versandwegen wenden Sie sich bitte an die Funktionsmailbox : telesec-auftrag@t-systems.com

Ihre technischen Fragen senden Sie bitte an: telesec-smartcard@t-systems.com

Herausgeber:

T-Systems International GmbH
Hahnstraße 43d
D-60528 Frankfurt am Main

Leistungsbeschreibung TeleSec TCOS 3.0 Signature Card V2.0



System-Voraussetzungen:

- Kartenlesegerät
- PC mit Software zur Ansteuerung der verfügbaren Applikationen

Bauform:

- ID-1: Karte im Scheckkarten-Format
- weitere Bauformen auf Anfrage

Typbezeichnung:

Kartenkörper weiß	Blaues TeleSec-Layout	Dual Interface	Aufdruck Schriftzug	Aufdruck Kartennummer	Aufdruck CAN	Typbezeichnung
	x	x	x	x	x	715/1440 DI bl mSZ mK
	x	x		x	x	715/1440 DI bl oSZ mK
x		x	x	x	x	715/1440 DI ws mSZ mK
x		x		x	x	715/1440 DI ws oSZ mK

Weitere Varianten auf Anfrage

Technische Daten

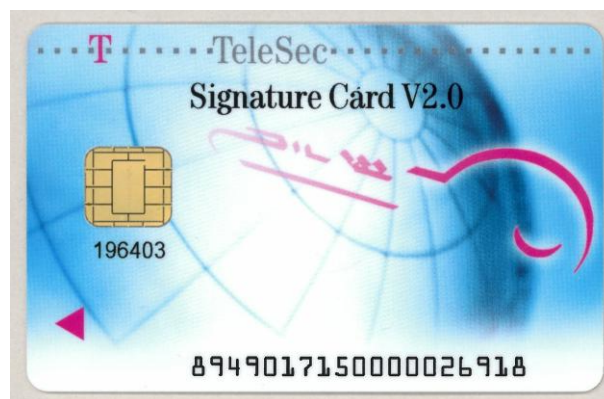
Betriebssystem: TCOS 3.0 Signature Card V2.0 Release 1
Befehlssatz: gemäß ISO 7816
Evaluierung: Common Criteria EAL4+
Kartenkörper: TeleSec-Layout, weiß oder Kundenlayout
Typbezeichnung: **715**
Kartenummer: 89 49 01**715** xxxxxxxx x
Protokoll: T=1 nach ISO 7816-3
 T=CL nach ISO 14443 Typ B
Chiptyp: Infineon SLE78CLX1440P
Chip-Evaluierung: CC EAL 5+
Speichergröße: insgesamt: 144 kBytes (EEPROM)

Kryptographie:

Signatur: ECDSA mit 256 Bit
Entschlüsselung: Gem. CEN-14890, Teil 2 auf Basis Elliptischer Kurven (NIST P-256)
Authentikation: ECDH mit 256 Bit, NIST P-256 (für Windows-LogOn), PACE gem. TR-03110
Zufalls-Zahlengenerator: Hardware-basiert, P2 Klassifizierung (SOF „hoch“) gem. AIS-31

AGB:

Grundlage für die Auslieferung der TCOS 3.0 Signature Card V2.0 sind die Allgemeinen Geschäftsbedingungen (AGB) Kauf Hardware, welche unter dem folgenden Link abrufbar sind:
<http://www.t-home.de/allgemein/agb?id=1562>



TCOS 3.0 Signature Card V2.0:
Blaues TeleSec-Layout mit Schriftzug und Aufdruck von Kartennummer und CAN

Kontakt.

Bei Fragen zu Preisen, Lieferzeiten, individuellen Kunden-Layouts, Bestellmodalitäten sowie Auslieferungs- und Versandwegen wenden Sie sich bitte an die Funktionsmailbox : telesec-auftrag@t-systems.com

Ihre technischen Fragen senden Sie bitte an: telesec-smartcard@t-systems.com

Herausgeber:

T-Systems International GmbH
 Hahnstraße 43d
 D-60528 Frankfurt am Main