Leistungsbeschreibung & zusätzliche Bedingungen TeleSec TCOS 3.0 Signature Card V2.0

Version: 1.0

Stand: 01.09.2018

Impressum

Herausgeber

T-Systems International GmbH

Hahnstraße 43d

60528 Frankfurt am Main

WEEE-Reg.-Nr. DE50335567

nachfolgend – Telekom – genannt

www.t-systems.de/pflichtangaben

INHALT

EINLEITUNG

Die TCOS 3.0 Signature Card V2.0 verfügt über einen NICHT personifizierten Kryptochip mit dem T-Systems eigenem Betriebssystem TCOS 3.0 (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.

1 LEISTUNGEN DER TELEKOM

1.1 Bereitstellung

Die Telekom erbringt folgende Leistung:

1. Lieferung der produktrelevanten Dokumentation
2. Lieferung der TeleSec TCOS 3.0 Signature Card V2.0

System-Voraussetzungen

- Kartenlesegerät
- PC mit Software zur Ansteuerung der verfügbaren Applikationen

Typbezeichnung

Kartenkörper weiß	Blaues TeleSec-Layout	Dual Interface	Aufdruck Schrift-zug	Aufdruck Karten-nummer	Aufdruck CAN	Typbezeichnung
	x	x	x	x	x	715/1440 DI b mSZ mK
	x	x		x	x	715/1440 DI b oSZ mK
x		x	x	x	x	715/1440 DI w mSZ mK
x		x		x	x	715/1440 DI w oSZ mK

Weitere Varianten z.B. Plug-In-Stanzung auf Anfrage

1.2 Funktionen

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

Die Qualität der asymmetrischen Schlüssel wird durch ein Erzeugersiegel des Trust Centers der T-Systems nachgewiesen.

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:

NetKey (NKS):	Entschlüsselung, fortgeschrittene Signatur, Authentifikation.
eSign:	Erzeugung qualifizierter Signaturen.

Leistungsmerkmale

- Intelligente Prozessorchipkarte mit dem eigens hierfür von der T-Systems 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 Microsoft SmartCard BaseCSP
    - PKCS#11-Modul für Windows und Linux

Bauform

ID-1: Karte im Scheckkarten-Format

ID-1 (DI): Karte im Scheckkarten-Format

weitere Bauformen auf Anfrage

TCOS 3.0 Signature Card V2.0: Blaues TeleSec-Layout mit mSZ mK und CAN

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
Kartennummer:	89 49 01715 xxxxxxxxx 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

1.3 Optionale Leistungen

- Weitere Varianten des Produkts auf Anfrage
- Bedruckung kundenindividuelles Layout auf Anfrage