Leistungsbeschreibung & zusätzliche Bedingungen TeleSec NetKey 3.0

Version: 1.01

Stand: 01.07.2019

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

Bei NetKey 3.0 handelt es sich um einen NICHT personifizierten Kryptochip mit dem T-Systems eigenem Betriebssystem TCOS 3.0 (TeleSec Chipcard Operating System).

NetKey 3.0 kann für Zugangsberechtigungen zu Personal Computern, Servern und Netzen, sowie für Gleitzeiterfassung und Zutrittssystemen, sowie als OneTimePass für sicheren Zugang zu Internet- bzw. Intranet-Servern eingesetzt werden. Außerdem dient NetKey 3.0 der Integritätssicherung und ermöglicht die Ver- und Entschlüsselung beliebiger Dateien. Weitere Applikationen können zusätzlich auf den Chip implementiert werden.

1 LEISTUNGEN DER TELEKOM

1.1 Bereitstellung

Die Telekom erbringt folgende Leistung:

1. Lieferung der produktrelevanten Dokumentation
2. Lieferung der TeleSec NetKey 3.0

System-Voraussetzungen

- Kartenlesegerät
- PC mit Software zur Ansteuerung der verfügbaren Applikationen
- Bei Einsatz von Einmal-Passwörtern Teilnahme an der Dienstleistung OTP

Typbezeichnung

Kartenkörper weiß	Blaues TeleSec-Layout	Mit Schriftzug	Aufdruck Kartennummer	Typbezeichnung
	x	x	x	733/072 b mSZ mK
	x		x	733/072 b oSZ mK
x		x	x	733/072 w mSZ mK
x			x	733/072 w oSZ mK

1.2 Funktionen

NetKey 3.0 enthält bei Auslieferung verschiedene asymmetrische Schlüsselpaare und symmetrische Schlüssel. 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.

NetKey 3.0 ist evaluiert durch die TÜV Informationstechnik GmbH nach Common Criteria EAL4+.

NetKey 3.0 wird im sogenannten NullPIN-Status ausgeliefert. Die NullPIN sichert die Unversehrtheit der Karte und erspart den Versand eines PIN-Briefes. Vor einer Nutzung der Karte wird die NullPIN durch eine persönliche PIN ersetzt.

Zusätzlich existiert auf NetKey 3.0 eine weitere PIN, die auch zum Entsperren einiger Karten funktionalitäten genutzt werden kann.

NetKey 3.0 enthält bei der Auslieferung die folgenden Standardapplikationen:

NetKey (NKS):	Entschlüsselung, fortgeschrittene Signatur, Authentifikation.
OneTimePass (OTP):	Erzeugung von Einmalpasswörtern.
Gleitzeit (GLAZ) :	Gleitzeiterfassung
Zutritt (ZTRT):	Sicherung von Gebäudeteilen

Leistungsmerkmale der TeleSec NetKey 3.0

- Intelligente Prozessorchipkarte mit dem eigens hierfür von der T-Systems entwickelten Chipkarten-Betriebssystem TCOS (TeleSec Chipcard Operating System), RSA2048 Bit Schlüssellänge, DES, 3-DES und IDEA
- Netkey Applikation (NKS)
- Fortgeschrittene Signatur
- Entschlüsselung
- Zugangsschutz für Firewalls, Router, Webserver, Internet-Service-Provider, sicheres lokales Login und/oder „Remote-Login“, sowie Authentifizierung der Endkunden durch das Trustcenter der DTAG bei Nutzung der Dienstleistung OTP
- Vier X.503V3-Zertifikate für fortgeschrittene Signatur, Entschlüsselung und Client-Server-Authentifikation
- Ein Prüfzertifikat zur Verwendung der Lösung im SigG-Umfeld, sowohl als Einzel- als auch als Multisignaturlösung
- Zutritt (ZTRT) – Sicherung von Gebäudeteilen
- Gleitzeit (GLAZ)
- OneTimePass (OTP) – Erzeugung von Einmal-Passwörtern
- Verfügbarkeit umfassender Dokumentationen
- Verfügbarkeit von Schnittstellen-Software
- TCOS-Cardmodul zum Microsoft SmartCard BaseCSP
- PKCS#11-Modul für Windows und Linux

Bauformen

ID-1:	Karte im Scheckkarten-Format
ID-000:	Plug-In-Karte
Chipmodul:	auf Rolle

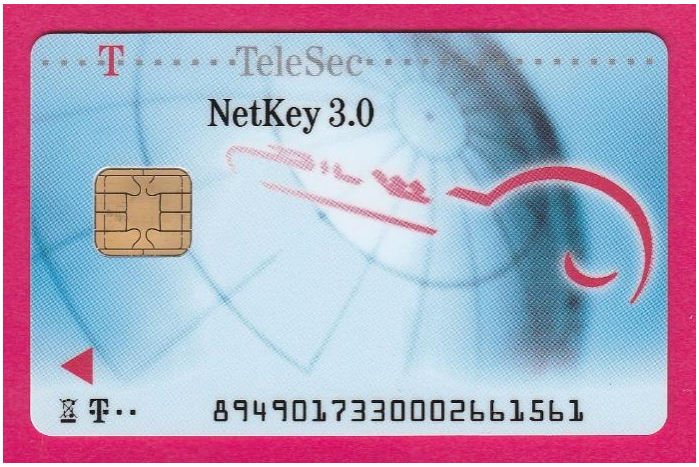

Abb.: 733/072 b mSZ mK

Technische Daten

Betriebssystem:	TCOS 3.0
Befehlssatz:	gemäß ISO 7816
Evaluierung:	Common Criteria EAL4+
Kartenkörper:	TeleSec-Layout, weiß oder Kundenlayout
Typbezeichnung:	733
Kartennummer:	89 49 01733 xxxxxxxxx x
Protokoll:	T=1 nach ISO 7816-3
Chiptyp:	NXP P5CT072, Evaluierung CC EAL 5+
Speichergröße:	insgesamt: 72 kByte (EEPROM)
Schlüssellänge:	RSA bis max. 2048 bit
Algorithmen:	DES, 3DES, IDEA, RSA
Chaining:	ECB, CBC

1.3 Optionale Leistungen

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