Leistungsbeschreibung & zusätzliche Bedingungen TeleSec IDKey Card

Version: 1.01

Stand: 01.06.2019

Impressum

Herausgeber

T-Systems International GmbH

Hahnstraße 43d

60528 Frankfurt am Main

WEEE-Reg.-Nr. DE50335567

nachfolgend – Telekom – genannt

www.t-systems.de/pflichtangaben

Copyright

© 2018 Alle Rechte, auch die des auszugweisen Nachdruckes, der elektronischen oder fotomechanischen Kopie sowie die Auswertung mittels Verfahren der elektronischen Datenverarbeitung, vorbehalten.

INHALT

Einleitung 4

1 Leistungen der Telekom 4

1.1 Bereitstellung 4

1.2 Funktionen 4

1.3 Optionale Leistungen 7

EINLEITUNG

Bei der TeleSec IDKey Card handelt es sich um eine NICHT personifizierte Kryptochipkarte mit dem T-Systems eigenem-Betriebssystem TCOS 3.0 (TeleSec Chipcard Operating System), optimiert für die Verwendung im Windows-Umfeld.

Die TeleSec IDKey Card unterstützt das Windows Identity Life Cycle Management (ILM) und kann hiermit für Zugangsberechtigungen zu Personal Computern, Servern und Netzen eingesetzt werden. Außerdem dient IDKey der Integritätssicherung und ermöglicht die Ver- und Entschlüsselung beliebiger Dateien. Weitere Applikationen können zusätzlich auf der TeleSec IDKey Card implementiert werden.

1 LEISTUNGEN DER TELEKOM

1.1 Bereitstellung

Die Telekom erbringt folgende Leistung:

1. Lieferung der produktrelevanten Dokumentation
2. Lieferung der TeleSec IDKey.TCOS 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 Karten-nummer	Dual Interface	Plug-In Stanzung	Typbezeichnung
	x		x			736/080 b oSZ mK
	x					736/080 b oSZ oK
x			x			736/080 w oSZ mK
x						736/080 w oSZ oK
x			x	x		736/080 DI w oSZ mK
x				x		736/080 DI w oSZ oK
	x		x	x		736/080 DI b oSZ mK C4/C8
	x		x		x	736/080 b p oSZ mK C4/C8

1.2 Funktionen

Bei IDKey handelt es sich um einen NICHT personifizierten Kryptochip mit dem Betriebssystem TCOS 3.0 (TeleSec Chipcard Operating System).

IDKey enthält bei Auslieferung verschiedene asymmetrische Schlüsselpaare und symmetrische Schlüssel. Die kryptographischen Schlüssel sind in Verbindung mit physikalischen Kartennummern eindeutig. Es existieren keine Kopien der privaten Schlüssel.

IDKey wird im sogenannten NullPIN-Status ausgeliefert. Die NullPIN sichert die Unversehrtheit des Produkts und erspart den Versand eines PIN-Briefes. Vor einer Nutzung von IDKey wird die NullPIN durch eine persönliche PIN ersetzt.

Eine Zuordnung zu bestimmten Personen oder Systemen (Personalisierung) wird nach Auslieferung im Kundenumfeld vorgenommen.

IDKey enthält bei der Auslieferung die folgenden Standardapplikationen:

ILM (Identity Life Cycle Management):
Entschlüsselung,
fortgeschrittene Signatur,
Authentikation.

Diese Applikation kann z.B. mit dem TCOS 3.0 Card Module über den Microsoft BaseCSP in das Microsoft ILM (Identity Life Cycle Management) integriert werden. Eine Nutzung vergleichbar zur NetKey-Applikation der NetKey 3.0 ist ebenfalls möglich.

OneTimePass (OTP): Erzeugung von Einmalpasswörtern.

Gleitzeit (GLAZ): Gleitzeiterfassung

Zutritt (ZTRT): Sicherung von Gebäudeteilen

Leistungsmerkmale der IDKey-Card

- Intelligente Prozessorchipkarte mit dem eigens hierfür von der T-Systems entwickelten Chipkarten-Betriebssystem TCOS, RSA2048 Bit Schlüssellänge, DES, 3-DES und IDEA
- Mit sechs 2048 Bit-RSA-Schlüsselpaaren aus T-Systems-Trustcenter vorpersonalisiert
- Vorbereitet für Key-Recovery
- Unterstützung des Challenge-Response-Verfahrens (CR-Key)
- Authentifizierung der Endkunden durch das Trustcenter der DTAG bei Nutzung der Dienstleistung OTP.
- Zutritt (ZTRT) – Sicherung von Gebäudeteilen
- Gleitzeit (GLAZ)
- OneTimePass (OTP) – Erzeugung von Einmal-Passwörtern
- Verfügbarkeit umfassender Dokumentationen
- HICO-Magnetstreifen 4000 Oerstedt (uncodiert) auf der Kartenrückseite oben

Die zur Verfügung gestellten Schnittstellen ermöglichen

- Einfache Integration in Microsoft Standard-Anwendungen über das TCOS Cardmodul zum Microsoft Smartcard BaseCSP (z.B. Outlook, Internet Explorer, Word) über Microsoft-Crypto-API bzw. Microsoft Crypto Next Generation.
- Einfache Integration der IDKey in das Microsoft Betriebssystem Windows (2000 bis einschließlich Win 10 und unterschiedliche Windows Server).
- Einfache Integration ins Microsoft Identity Life Cycle Management (ILM)
- Einfache Integration in unterschiedliche Cardmanagement Systeme über die TCOS-Software Schnittstellen
- Einfache Integration in Mozilla über PKCS#11
- Verwendbar unter Linux über PKCS#11 oder JCE
- Fortgeschrittene Signatur
- Entschlüsselung und Authentifikation
- TCOS-Cardmanager.net zur einfachen PIN/PUK/CR-Key- und Zertifikatsverwaltung
- Einfach integrierbar in Zugangsschutz für Firewalls, Router, Webserver, Internet-Service-Provider, sicheres Domain-Login
- Für berührungslose Nutzung kann die Antenne geeigneter Adapter über die Kontakte C4 und C8 (untere Kontaktreihe) zum Chipmodul kontaktiert werden
- Verfügbarkeit von Schnittstellen-Software
    - TCOS-Cardmodul zum Microsoft SmartCard BaseCSP
    - PKCS#11-Modul für Windows, MacOS, Linux, Android, Raspberry und Cubietruck
    - TCOS JCE (Java Cryptography Extension)
    - TCOS Cardmanager.net für Windows, Linux und MacOS

Bauformen

ID-1:	Karte im Scheckkarten-Format
ID-1 (DI):	Karte im Scheckkarten-Format (Dual Interface)
ID-000:	Plug-In-Karte
Chipmodul:	auf Rolle

Abb.: 736/080 w oSZ m K

Technische Daten

Betriebssystem:	TCOS 3.02
Befehlssatz:	gemäß ISO 7816
Kartenkörper:	TeleSec-Layout, weiß oder Kundenlayout
	teilweise mit Magnetstreifen
Typbezeichnung:	736
Kartennummer:	89 49 01736 xxxxxxxxx x
Protokoll:	T=1 nach ISO 7816-3
	T=CL nach ISO 14443 (bei DI-Karten)
Chiptyp:	NXP P5CD080,
	evaluiert nach CC EAL 5+
Speichergröße:	insgesamt: 80 kByte (EEPROM)
Schlüssellänge:	RSA bis max. 2048 bit
Algorithmen:	DES, 3DES, RSA
Chaining:	ECB, CBC

1.3 Optionale Leistungen

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