



Zentrum für sichere Informationstechnologie – Austria Secure Information Technology Center - Austria

A-1040 Wien, Weyringergasse 35
Tel.: ++43 1 – 503 19 63 – 0
Fax: ++43 1 – 503 19 63 – 66

A-8010 Graz, Inffeldgasse 16a
Tel.: ++43 316 – 873 5514
Fax: ++43 316 – 873 5520

Homepage: www.a-sit.at
E-Mail: office@a-sit.at

Bescheinigung nach §18(5) SigG: E4 KeyCard V3.0

Antragsteller:
Deutsche Telekom AG, T-TeleSec
Untere Industriestraße 20
57250 Netphen
Deutschland

1. Beschreibung der bescheinigten Komponente

E4 KeyCard V3.0 ist eine Prozessorchipkarte mit Betriebssystem bestehend aus

- Prozessorchipkarte SLE 66CX320P von Infineon Technologies, und
- Telesec Chipcard Operating System TCOS V2.0 Rel. 3 von Deutsche Telekom AG

Das Betriebssystem TCOS V2.0 Rel. 3 stellt für sicherheitsrelevante Anwendungen mit der Chipkarte Sicherheitsfunktionen zur Verfügung, die insbesondere die Authentisierung, die sichere Datenspeicherung (insbesondere von Signaturschlüsseln und Identifikationsdaten), die Sicherung der Kommunikation zwischen einer (externen) Hostanwendung und dem Betriebssystem, sowie Kryptofunktionen zur Erstellung sicherer elektronischer Signaturen umfassen.

E4 KeyCard V3.0 wird von einem externen Schlüsselgenerator (Typ1-Gerät) beschlüsselt.

2. Erfüllung der Anforderungen des SigG und der SigV

E4 KeyCard V3.0 erfüllt

- Anforderungen nach §18(1) und §18(2) SigG ausgenommen Anforderungen an die Erzeugung der Signaturerstellungsdaten, da diese Funktionalität auf E4 KeyCard V3.0 nicht implementiert ist, und
- Anforderungen nach §7(3) SigV ausgenommen Anforderungen an die Hostanwendung.

E4 KeyCard V3.0 ist daher in folgenden Kategorien bescheinigt:

- Komponenten und Verfahren zur Verwahrung der Signaturerstellungsdaten und zur Sicherstellung des autorisierten Zuganges, und
- Komponenten und Verfahren zur Anwendung der Signaturerstellungsdaten und zur Erzeugung der Signaturformate.

3. Gültigkeitsdauer der Bescheinigung

Diese Bescheinigung ist zwei Jahre nach der Ausstellung gültig. Die Gültigkeit dieser Bescheinigung ist an die unter Einsatzbedingungen genannten Auflagen gebunden.

4. Einsatzbedingungen

- (1) Das Auslieferungsverfahren der E4 KeyCard an den Signator mit allen Zwischenschritten muss den durch den Zertifizierungsdiensteanbieter vorzugebenden Bedingungen und Prozeduren genügen, damit die Haftung des Zertifizierungsdiensteanbieters auch ermöglicht wird. Der Nachweis über diese Erfüllung der Bedingungen und Prozeduren muss in einem auf die einzelne Karte rückführbaren und nachvollziehbaren Protokoll inklusive der notwendigen Prüfschritte bei der Eingangskontrolle beim Zertifizierungsdiensteanbieter vorhanden sein. Die Qualität und die Schlüssellänge der Schlüssel, die die Authentizität kryptographisch schützen, müssen mindestens der Qualität und der Schlüssellänge von Schlüsseln, die zur sicheren elektronischen Signatur geeignet sind entsprechen.
- (2) Folgende Auflage aus dem Zertifizierungsbericht vom 4.8.2000 an die Firma Infineon Technologies AG zum Deutschen IT-Sicherheitszertifikat TUVIT-DSZ-ITSEC-9115-2000 vom 4.8.2000 für die Prozessorchipkarte SLE 66CX320P muss beachtet werden: „Die Analyse der Mechanismenstärke beruht auf einer Zeit- und Aufwandsabschätzung, wie sie sich nach dem heutigen Stand der Technik darstellt. Da zu erwarten ist, dass sich die Analysetechniken hinsichtlich des Reverse Engineerings bzw. der DPA-Technik in Zukunft rasch entwickeln werden, ist eine regelmäßige Überprüfung der Analysen unbedingt erforderlich. Nach Vorliegen neuer Erkenntnisse auf diesen Gebieten, **spätestens aber nach einem Jahr** (d.h. bis 4.8.2001), sollte daher die Mindeststärke der Mechanismen neu bewertet und gegenüber der Prüfstelle nachgewiesen werden.“ (Übersetzung aus dem englischen Original-Zertifizierungsbericht.) Der Hersteller ist gehalten, sich über die Ergebnisse dieser Überprüfungen unmittelbar zu informieren und der Bestätigungsstelle diese Ergebnisse ebenfalls unverzüglich zur Kenntnis zu bringen.
- (3) E4 KeyCard V3.0 darf nur mit einem Schlüsselgenerator beschlüsselt werden, der die Anforderungen des SigG und der SigV erfüllt. Dies gilt auch für die Schlüssel, die damit auf die E4 KeyCard V3.0 gebracht werden. Der Telesec Schlüsselgenerator TC-SG V1.11 ist ein aus technischer Sicht geeigneter Schlüsselgenerator.
- (4) Sofern die Beschlüsselung der Karte nicht im Aufsichtsbereich der österreichischen Aufsichtsstelle liegt, ist durch geeignete Maßnahmen sicherzustellen, dass jeder die Sicherheit bedrohende Umstand unverzüglich der österreichischen Aufsicht und der Bestätigungsstelle bekannt wird.
- (5) Auf die E4 KeyCard 3.0 darf kein ausführbarer Code geladen werden. Das Laden von Code nach der Beschlüsselung muss technisch nachweislich verhindert sein.
- (6) Bei der Entwicklung und Administration von Hostanwendungen für die Personalisierung und die Anwendung der E4 KeyCard V3.0 ist zu gewährleisten, dass diese die Sicherheitsfunktionen des Betriebssystems TCOS V2.0 Rel. 3 sachgerecht nutzen und selbst hinreichend geschützt sind.
- (7) Bei Erhalt einer E4 Key Card V3.0 ist die voreingestellte Null-PIN auf einen geheimen und individuellen Wert zu setzen. Vor dieser PIN-Aktivierung ist der Einsatz der Chipkarte nicht möglich.

5. Algorithmen und zugehörige Parameter

Zur Erstellung einer sicheren elektronischen Signatur wird vom Betriebssystem TCOS V2.0 Rel. 3 der RSA-Algorithmus unter Verwendung vom CRT mit einer Schlüssellänge von 1024 Bit bereit gestellt. Dadurch sind die Anforderungen gemäß Anhang 1 Punkt 2 SigV erfüllt.

6. Prüfstufe und Mechanismenstärke

Die Prozessorchipkarte SLE 66CX320P wurde erfolgreich nach der Prüfstufe E4 der ITSEC evaluiert, mit der Mechanismenstärke „hoch“ (siehe das Deutsche IT-Sicherheitszertifikat TUVIT-DSZ-ITSEC-9115-2000 vom 4.8.2000).

Das Telesec Chipcard Operating System TCOS V2.0 Rel. 3 wurde auf der Prozessorchipkarte SLE 66CX320P erfolgreich nach der Prüfstufe E4 der ITSEC evaluiert, mit der Mechanismenstärke „hoch“ (siehe Evaluierungsbericht TÜViT, Version 1.0, vom 6.12.2000, ITSEC E4 hoch, gültig für die Portierung dieses Betriebssystems auf die SLE66CxxxP Prozessoren).

Der Produkttyp E4 KeyCard V3.0 ist bezüglich der Bestätigung einer technischen Komponente identisch zum Produkttyp PKS-Card V3.0. PKS-Card V3.0 wurde als

- Komponente zum Speichern und Anwenden des privaten Signaturschlüssels, und
 - Komponente zum Speichern und Anwenden der Identifikationsdaten.
- nach dem deutschen SigG (1997) bestätigt (TUVIT.09339.TE.12.2000).

Wien 1.06.2001

A-SIT Zentrum für sichere Informationstechnologie - Austria



o. Univ.-Prof. Dipl.-Ing. Dr. Reinhard Posch
Wissenschaftlicher Gesamtleiter



Manfred Holzbach
Geschäftsführender Vorstand