

# Konformitätsbestätigung für die Umsetzung von Sicherheitskonzepten

gemäß § 15 Abs. 2 Gesetz über Rahmenbedingungen  
für elektronische Signaturen  
und § 11 Abs. 2 Signaturverordnung

**TÜV Informationstechnik GmbH**  
Unternehmensgruppe TÜV NORD  
**Zertifizierungsstelle**  
**Langemarckstraße 20**  
**45141 Essen**

bestätigt hiermit gemäß  
§ 15 Abs. 2 Satz 1 Signaturgesetz<sup>1</sup> und § 11 Abs. 2 Signaturverordnung<sup>2</sup>,  
dass die

**Personalisierung für STARCOS 3.x Chipkarten**  
**der Giesecke & Devrient GmbH**

den nachstehend genannten Anforderungen des SigG und der SigV entspricht.

Die Dokumentation zu dieser Bestätigung ist registriert unter

**TUVIT.09491.SE.11.2008.**

**Essen, 07.11.2008**

\_\_\_\_\_  
Dr. Christoph Sutter  
Leiter Zertifizierungsstelle



TÜV Informationstechnik GmbH ist, gemäß der Veröffentlichung im Bundesanzeiger Nr. 126 vom 10.07.1999, Seite 11181, und gemäß § 25 Abs. 3 SigG zur Erteilung von Bestätigungen für die Umsetzung von Sicherheitskonzepten gemäß § 15 Abs. 2 Satz 1 SigG ermächtigt.

<sup>1</sup> Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG) vom 16.05.2001 (BGBl. I S. 876) zuletzt geändert durch Artikel 4 des Gesetzes vom 26.02.2007 (BGBl. I S. 179)

<sup>2</sup> Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16.11.2001 (BGBl. I S. 3074) zuletzt geändert durch Artikel 9 Abs. 18 des Gesetzes vom 23. November 2007 (BGBl. I S. 2631)

Die Bestätigung zur Registrierungsnummer TUVIT.09491.SE.11.2008 besteht aus 4 Seiten.

## Beschreibung zum Sicherheitskonzept:

### 1 Bezeichnung des Betreibers

Giesecke & Devrient GmbH  
Prinzregentenstraße 159  
81607 München

### 2 Funktionsbeschreibung

Die Giesecke & Devrient GmbH betreibt für Zertifizierungsdiensteanbieter gemäß § 2 Nr. 8 und § 15 SigG die Dienstleistung Personalisierung der sicheren Signaturerstellungseinheiten (SSEE – gemäß § 2 Nr. 10 SigG) einschließlich Versand der SSEE und nachfolgend der diesen zugeordneten PIN-Briefe mit einer Initial-PIN zur Festlegung eines individuellen Wissensdatums durch den Signaturschlüssel-Inhaber zu seiner Identifikation gegenüber der SSEE.

Das Sicherheitskonzept beschreibt die folgenden für diese Bestätigung relevanten Phasen zur Personalisierung von SSEE:

- A Komplettierung und Initialisierung: In dieser Phase wird die SSEE gemäß Produktbestätigung fertiggestellt. Dazu gehören die Vervollständigung des Betriebssystems und die Aufbringung des sicherheitsrelevanten Anteils des Filesystems.
- B Vorpersonalisierung: In dieser Phase wird das Signaturschlüsselpaar auf der SSEE generiert und sicher in dem in der vorigen Phase angelegten Filesystem abgelegt. Die Sicherheit des Schlüsselgenerierungsprozess ist Gegenstand der Bestätigung der SSEE.
- C Personalisierungsphase 1.1: In dieser Phase werden weitere für die Personalisierung benötigte Daten aus dem durch den ZDA gelieferten Personalisierungsdatensatz in die SSEE eingebracht. Ferner wird der Kartenkörper der SSEE optisch personalisiert (z. B. bedruckt oder gelasert).
- D Personalisierungsphase 1.2: In dieser Phase erfolgen das gesicherte Auslesen des Signaturprüfsschlüssels und die Übermittlung an den ZDA.
- E Personalisierungsphase 2: In dieser Phase wird das vom ZDA gelieferte qualifizierte Zertifikat in die SSEE eingebracht.

Zurzeit sind ausschließlich die Phasen A-C umgesetzt. Damit sind lediglich die Phasen A-C einschließlich des Versands der SSEE Gegenstand dieser Bestätigung und nicht die Phasen D und E.

Optional bietet die Giesecke & Devrient GmbH im Rahmen des Sicherheitskonzeptes noch die folgenden Dienstleistungen an:

- Generierung der Transport-PIN und der PUK zum Rücksetzen des Fehlbedienungs Zählers und Speicherung in der SSEE,
- Druck von PIN- und PUK-Briefen sowie
- Versand von PIN- und PUK-Briefen.

Diese Optionen sind zurzeit noch nicht umgesetzt und sind damit auch nicht Gegenstand dieser Bestätigung.

### **3 Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung**

#### **3.1 Erfüllte Anforderungen**

Das Sicherheitskonzept der Giesecke & Devrient GmbH für die Dienstleistung Chipkartenpersonalisierung erfüllt für die oben genannten Funktionen die Anforderungen nach § 2 SigV.

#### **3.2 Einsatzbedingungen**

Dies gilt unter der Voraussetzung, dass folgende Einsatzbedingungen gewährleistet sind:

##### **a) Technische Einsatzumgebung**

Die Giesecke & Devrient GmbH führt die genannte Dienstleistung innerhalb einer abgesicherten Infrastruktur durch. Die Datensätze, die mit dem Zertifizierungsdiensteanbieter ausgetauscht werden, sind verschlüsselt und integritätsgesichert.

Jeder Austausch oder jede Veränderung im Gesamtkonzept und in den System- oder Sicherheitskomponenten ist einer Bestätigungsstelle anzuzeigen und erfordert ggf. eine Überprüfung und eine Erweiterung der Bestätigung. Die hiernach gültigen Änderungen im Sicherheitskonzept sind den Zertifizierungsdiensteanbietern zur Ermöglichung einer Überprüfung auch ihrer Sicherheitskonzepte unverzüglich zur Kenntnis zu bringen.

##### **b) Inbetriebnahme**

Der Betriebsablauf der Chipkartenpersonalisierungsprozesse wurde der Bestätigungsstelle im Rahmen der Umsetzungsprüfung gemäß § 15 Abs. 2 SigG demonstriert. Die Inbetriebnahme im Zusammenspiel mit einem Zertifizierungsdiensteanbieter muss unter Aufsicht der Bestätigungsstelle erfolgen, sobald auch dieser die Umsetzung der Anbindung seiner Schnittstellenprozesse an die Giesecke & Devrient GmbH gegenüber einer Bestätigungsstelle nachgewiesen hat und eine Bestätigung für die bei der Chipkartenpersonalisierung verwendete SSEE vorliegt.

### **c) Betrieb der Dienstleistungen für Zertifizierungsdiensteanbieter**

Während des Betriebes sind die folgenden Bedingungen zu beachten:

- Beim Zertifizierungsdiensteanbieter müssen die im Dokument „SigG konformes Sicherheitskonzept für die externe Personalisierung von STARCOS 3.x Signaturkarten durch Giesecke & Devrient GmbH: Schnittstellen und Anforderungen an einen Zertifizierungsdiensteanbieter“, Version 1.2, 25.04.2007 der Giesecke & Devrient GmbH beschriebenen Aufgaben umgesetzt und Anforderungen an die Schnittstellen eingehalten werden. Dann kann das Sicherheitskonzept der Giesecke & Devrient GmbH für die Dienstleistung Chipkartenpersonalisierung als Modul des Sicherheitskonzeptes eines Zertifizierungsdiensteanbieters referenziert werden.
- Alle Betriebsauflagen aus den Bestätigungen für die eingesetzten SSEE sind sorgfältig zu beachten.

Alle an den Chipkartenpersonalisierungsprozessen beteiligten Mitarbeiter der Giesecke & Devrient GmbH sind nachdrücklich auf die sorgfältige Einhaltung aller Arbeits- und Sicherheitsanweisungen hinzuweisen.

Jede sicherheitserhebliche Veränderung ist der zuständigen Behörde unverzüglich anzuzeigen.

**Ende der Bestätigung**