Bestätigung
von Produkten für qualifizierte elektronische Signaturen

gemäß §§ 15 Abs. 7 S. 1, 17 Abs. 4 Gesetz über Rahmenbedingungen für elektronische Signaturen[1] und §§ 11 Abs. 2 und 15 Signaturverordnung[2]

T-Systems

- Zertifizierungsstelle -

Rabinstr.8, 53111 Bonn

bestätigt hiermit gemäß
§§ 15 Abs. 7 S. 1, 17 Abs. 3 SigG sowie §§ 15 Abs. 3 und 4, § 11 Abs. 3 SigV,
dass die

Funktionsbibliothek „ArtSignComponent V1.0“

den nachstehend genannten Anforderungen des SigG und der SigV entspricht.

Die Dokumentation zu dieser Bestätigung ist registriert unter:

T-Systems. 02091.TE.10.2003

Bonn, den 03.11.2003 _____
(Dr. Heinrich Kersten)

Die T-Systems – Zertifizierungsstelle - ist, gemäß der Veröffentlichung im Bundesanzeiger Nr. 31 vom 14. Februar 1998, Seite 1787, zur Erteilung von Bestätigungen für Produkte gemäß § 15 Abs. 7 S. 1 (oder § 17 Abs. 4) SigG ermächtigt.

---

1 Gesetz über die Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG) in der Fassung vom 16. Mai 2001 (BGBl. Jahrgang 2001 Teil I Nr. 22)

2 Verordnung zur elektronischen Signatur (Signaturverordnung - SigV) in der Fassung vom 16. November 2001 (BGBl. Jahrgang 2001 Teil I Nr. 59)

Beschreibung der technischen Komponente:

1. Handelsbezeichnung der technischen Komponente und Lieferumfang

Handelsbezeichnung:
Funktionsbibliothek „ArtSignComponent V1.0“

Auslieferung:
Auslieferung durch persönliche Übergabe.

Lieferumfang:

Bezeichnung	**Version**	**Datum**	**Übergabeform**
ArtSignComponent	1.0	- ohne -	CD
Betriebsdokumentation	2.0	19.05.2003	Papierform pdf-Datei auf CD

ArtSignComponent enthält die folgenden Bibliotheksmodule:

Modul	Größe/Bytes	Datum
libArtSignatureComponent.a	387.660	08.07.2003
libArtCrSmartCard.a	1.180.266	08.07.2003
libAsn1Lib.a	13.500.658	08.07.2003

Hersteller:
Deutsche Post Signtrust GmbH
Tulpenfeld 9, 53113 Bonn

2. Funktionsbeschreibung

Die Komponente ist eine Funktionsbibliothek zum Einsatz im Trust Center der Deutschen Post Signtrust GmbH. Sie besitzt folgende durch Anwendungen aufrufbare Funktionen:

- Sicherheitsfunktion SF1 – „digitales Signieren“
  Unter dieser Bezeichnung wird der Vorgang der Vorbereitung und Veranlassung einer elektronischen Signatur durch Aufruf der Funktionsbibliothek verstanden:
  Die Nutzer-PIN wird durch die die ArtSignComponent nutzende Applikation erfasst und an die ArtSignComponent übergeben.
  Die Inbetriebnahme und Initialisierung der Chipkarten (in einem Chipkartenleser) erfolgt durch die ArtSignComponent mittels Übergabe der PIN an die Chipkarte. Nach erfolgreicher Initialisierung der Chipkarten überschreibt die ArtSignComponent ihren eigenen Speicherbereich, in dem sich die PIN befindet, mit einem Muster, so dass dann kein unbefugter Zugriff auf die PIN möglich ist.
  Aus den zu signierenden Daten wird mittels einer Hash-Funktion ein Hash-Wert erzeugt und an die Chipkarte gesandt. Dieser wird anschließend mittels eines privaten Signatur-

schlüssels von Prozessorchipkarte signiert. Die ArtSignComponent übergibt die von der Chipkarte erhaltene Signatur zurück an die aufrufende Applikation.

- Sicherheitsfunktion SF2 - Verifikation einer digitalen Signatur
  Die Applikationen übergibt die signierten Daten und die zugehörige Signatur sowie das zugehörige Signaturschlüsselzertifikat oder alternativ den öffentlichen Schlüssel an die ArtSignComponent. Hier werden durch die üblichen Prozesse (Hashen der Daten, Entschlüsseln der übermittelten Signatur) zwei Vergleichswerte erzeugt. Das Ergebnis des Vergleichs (übereinstimmend oder nicht-übereinstimmend) übermittelt ArtSignComponent an die aufrufende Applikation.

3. Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Die Funktionsbibliothek „ArtSignComponent V1.0“ erfüllt die folgenden Anforderungen:

- §15 Abs. 2 Nr. 1 a) SigV (keine Preisgabe oder Speicherung von Identifikationsdaten)
- §15 Abs. 2 Nr. 2 a) SigV (Korrektheit der elektronischen Signatur)
- §15 Abs. 2 Nr. 4 (Erkennbarkeit sicherheitstechnischer Veränderungen)

3.2 Einsatzbedingungen

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

a) Technische Einsatzumgebung

Die Funktionsbibliothek „ArtSignComponent V1.0“ ist für den Einsatz unter dem Betriebssystem HP-UX Version 11.0 vorgesehen. Die Funktionsbibliothek stellt keine besonderen Anforderungen an die Hardware. Sie kann auf einer HP-Workstation mit Anschlussmöglichkeit für einen Chipkartenleser und CD-ROM (zur Installation) eingesetzt werden.

Die Funktionsbibliothek „ArtSignComponent V1.0“ wird vom Hersteller gemäß Abschnitt 1 ausgeliefert. Das spezifizierte Auslieferungsverfahren ist einzuhalten.

Als Chipkarten können die sicherheitsbestätigten Telesec-Signaturkarten mit dem Chipkartenbetriebssystemen TCOS 2.0 Release2 bzw. TCOS2.0 Release3 eingesetzt werden[3]. Die Chipkartenschnittstelle erfüllt den Standard ISO 7816.

Als Chipkartenterminal können sicherheitsbestätigte Kartenleser vom Typ B1, welche die universelle Schnittstelle CT-API unterstützen, eingesetzt werden, sofern die Chipkartenschnittstelle kompatibel zu den unterstützten Chipkarten ist.

b) Nutzung des Produktes

Während des Betriebes sind die folgenden Bedingungen für den sachgemäßen Einsatz zu beachten:

---

[3] Chipkartenseitig sollte das *Secure Messaging* verwendet werden, das ebenfalls von ArtSignComponent unterstützt wird. Das Secure Messaging sichert die Übertragung der PIN an die Chipkarte zusätzlich ab. Diese Funktion fällt jedoch **nicht** unter die Sicherheitsbestätigung. Hinsichtlich der Anwendung dieser Zusatzfunktion sind weitere Vorgaben zu beachten (s. Deutsches Sicherheitszertifikat T-Systems-DSZ-ITSEC-04090-2003, Anhang „Sicherheitsvorgaben“).

Die Funktionsbibliothek „ArtSignComponent V1.0“ ist für den Einsatz im Trust Center der Deutschen Post Signtrust GmbH vorgesehen. Für die Evaluierung wurden die dort vorhandene sichere Einsatzumgebung zugrunde gelegt.

Die aufrufende Applikation muss dafür Sorge tragen, dass die PIN-Eingabe unsichtbar erfolgt und alle Speicherbereiche, in denen sich die PIN befindet, nach Übergabe an die ArtSign-Component wiederaufbereitet oder anderweitig vor Zugriff geschützt werden.

Für den gesetzeskonformen Betrieb darf die Funktionsbibliothek „ArtSignComponent V1.0“ nur im Zusammenhang mit vertrauenswürdigen Anwendungen sowie entsprechend sicherheitsbestätigten Terminals und Chipkarten eingesetzt werden.

Zur Erkennung sicherheitstechnischer Veränderungen ist die eingespielte Software durch Binärvergleich mit den Daten auf der ausgelieferten CD zu überprüfen.

3.3 Algorithmen und zugehörige Parameter

Die Funktionsbibliothek verwendet die kryptographischen Algorithmen RSA-1024 bzw. SHA-1 und RIPEMD160.

Die gemäß § 11 Abs. 3 in Verbindung mit Anlage I Nr. 2 SigV festgestellte Eignung reicht mindestens bis Ende des Jahres 2007 für RSA-1024 sowie bis mindestens Ende 2008 für SHA-1 und RIPEMD160 (s. Bundesanzeiger Nr. 48, S. 4202-4203 vom 11. März 2003).

Diese Sicherheitsbestätigung ist somit gültig bis zum 31.12.2007; sie kann jedoch verlängert werden, wenn zu diesem Zeitpunkt keine Hinderungsgründe hinsichtlich der Sicherheit der technischen Komponente oder der Algorithmen vorliegen.

3.4 Prüfstufe und Mechanismenstärke

Die Funktionsbibliothek „ArtSignComponent V1.0“ wurde erfolgreich nach der Prüfstufe **E2** der ITSEC evaluiert. Die eingesetzten Sicherheitsmechanismen erreichen die Stärke **hoch**.

Ende der Bestätigung