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 §§ 11 Abs. 3, 15 Abs. 3 und 4 SigV,
dass der

Zeitstempeldienst
„Zeitstempeldienst (TSS) des Trust Centers der DPAG
Version 1.4“

den nachstehend genannten Anforderungen des SigG und der SigV entspricht.

Die Dokumentation zu dieser Bestätigung ist registriert unter:

T-Systems.02093.TU.11.2003

Bonn, den 12.11.2003

(Dr. Heinrich Kersten)

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

Bezeichnung:
Zeitstempeldienst (TSS) des Trust Centers der DPAG Version 1.4

Auslieferung:
als System innerhalb des Zertifizierungsdienstes der
Deutschen Post Signtrust GmbH

Lieferumfang:
CD-ROM mit Zeitstempeldienst-Software Version 1.4 und Konfigurationsdaten

Hersteller:
Deutsche Post Signtrust GmbH
Tulpenfeld 9, 53113 Bonn

2. Funktionsbeschreibung

Der Zeitstempeldienst „Zeitstempeldienst (TSS) des Trust Centers der DPAG Version 1.4“ ist ein System, das als technische Komponente für Zertifizierungsdienste gemäß §2 Nr. 12c SigG innerhalb der gesicherten Umgebung des Trust Centers des Zertifizierungsdiensteanbieters Deutsche Post Signtrust GmbH betrieben wird. Er erzeugt qualifizierte Zeitstempel gemäß §2 Nr.14 SigG für Personen, die im Besitz eines vom Zertifizierungsdiensteanbieter Deutsche Post Signtrust GmbH verwalteten Signaturschlüssel-Zertifikates sind.

3. Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Der Zeitstempeldienst „Zeitstempeldienst (TSS) des Trust Centers der DPAG Version 1.4“ erfüllt die folgenden Anforderungen:

- §17 Abs. 3 Nr. 3 SigG
- §15 Abs. 3 S. 4 SigV
- §15 Abs. 4 SigV

3.2 Einsatzbedingungen

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

a) Technische Einsatzumgebung

Der Zeitstempeldienst „Zeitstempeldienst (TSS) des Trust Centers der DPAG Version 1.4“ wurde für die spezielle Einsatzumgebung des Trust Centers des Zertifizierungsdienste-anbieters Deutsche Post Signtrust GmbH als System evaluiert auf der Basis der folgenden Hard- und Softwarekonfiguration:

- Server 9000 K380 von Hewlett Packard mit Betriebssystem HP-UX Version 11.0,
- 2 Funkuhren DCF77-C51 der Firma Meinberg,
- Chipkartenleser nach der B1-Spezifikation,
- SigG-konform personalisierte Signaturkarte SEA-Card V1.0 mit dem Chipkarten-Betriebssystem TCOS V2.0 Rel. 2 der Telesec,
- SigG-konform personalisierte Signaturkarte SEA-Card V2.0 mit dem Chipkarten-Betriebssystem TCOS V2.0 Rel. 3 der Telesec und
- Signaturanwendungskomponente ArtSignComponent V1.0 der Deutschen Post Signtrust GmbH zur Erzeugung und Prüfung elektronischer Signaturen.

Jeder Austausch und jede Veränderung der Hard- und Softwarekonfiguration ist der Bestätigungsstelle anzuzeigen und erfordert gegebenenfalls eine Reevaluierung.

Für den sicheren Betrieb des Zeitstempeldienstes werden in der ergänzenden Einsatzumgebung weiterhin benötigt:

- Fehlerprotokollierungsrechner (Compaq Professional Workstation mit Windows NT 4.0 SP4),
- Zeitstempelprotokollierungsrechner (Compaq Professional Workstation mit Windows NT 4.0 SP4).

Der Zeitstempeldienst „Zeitstempeldienst (TSS) des Trust Centers der DPAG Version 1.4“ wurde als System innerhalb der gesicherten Umgebung des Trust Centers des Zertifizierungsdiensteanbieters Deutsche Post Signtrust GmbH evaluiert. Er darf deshalb ausschließlich innerhalb dieser Umgebung und mit der oben beschriebenen Hard- und Softwareausstattung betrieben werden.

b) Auslieferung und Inbetriebnahme

Der Zeitstempeldienst „Zeitstempeldienst (TSS) des Trust Centers der DPAG Version 1.4“ wurde vom Hersteller als IT-System implementiert. Die Inbetriebnahme von Instanzen des Zeitstempeldienstes muss im Rahmen der Umsetzungsprüfung des Sicherheitskonzeptes gemäß §4 Abs. 2 SigG geprüft und bestätigt werden.

c) Nutzung des Zeitstempeldienstes

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

- Der Zeitstempeldienst darf nur in der vertrauenswürdigen und zugangsbeschränkten Umgebung mit den oben genannten Hard- und Softwarekomponenten betrieben werden, in der er als IT-System evaluiert wurde.
- Es ist insbesondere vertrauenswürdiges Personal einzusetzen.
- Es ist sicherzustellen, dass auf der von der Signaturanwendungskomponente ArtSignComponent V1.0 benutzten Hardwareplattform keine Viren oder Trojanischen Pferde eingespielt werden.
- Vertraulicher Umgang mit Identifikationsmerkmalen, die an die Signaturanwendungskomponente ArtSignComponent V1.0 weitergereicht werden, insbesondere seitens handelnder Personen und der nutzenden Anwendung.
- Die Überwachungsreports des Überwachungstools Tripwire sind mindestens einmal wöchentlich durch den IT-Sicherheitsbeauftragten und den ZS-Administrator zu erzeugen und auszuwerten.
- Der Eingang neuer ITO-Meldungen auf der ITO-Benutzeroberfläche ist sorgfältig zu kontrollieren.

- Es ist zu beachten, dass die bekannten Schwachstellen in der Konstruktion und bei der operationellen Nutzung nicht durch Veränderungen der Einsatzumgebung ausnutzbar werden dürfen und keine neuen Schwachstellen entstehen.

Mit Auslieferung des Zeitstempeldienstes „Zeitstempeldienst (TSS) des Trust Centers der DPAG Version 1.4“ ist der Betreiber des Trust Centers auf die Einhaltung der oben genannten Einsatzbedingungen hinzuweisen.

3.3 Algorithmen und zugehörige Parameter

Der Zeitstempeldienst verwendet den RSA-Algorithmus mit 1024 bit. Die gemäß § 11 Abs. 3 in Verbindung mit Anlage I Nr. 2 SigV festgestellte Eignung reicht daher mindestens bis Ende des Jahres 2007 (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

Der Zeitstempeldienst „Zeitstempeldienst (TSS) des Trust Centers der DPAG Version 1.4“ wurde erfolgreich nach der Prüfstufe **E2** der ITSEC evaluiert. Die eingesetzten Sicherheitsmechanismen erreichen die Stärke **hoch**.

Ende der Bestätigung