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 ISS GmbH

- Zertifizierungsstelle -

Rabinstr.8, 53111 Bonn

bestätigt hiermit gemäß
§§ 15 Abs. 7 S. 1, 17 Abs. 2 SigG sowie §§ 15 Abs. 2 und 4, § 11 Abs. 3 SigV,
daß die

Signaturanwendungskomponente
„Sign@tor Version 2.0“

den nachstehend genannten Anforderungen des SigG und der SigV entspricht.

Die Dokumentation zu dieser Bestätigung ist registriert unter:

T-Systems. 02081.TE.04.2002

Bonn, den 30.04.2002

(gez. Dr. Heinrich Kersten)

T-Systems ISS GmbH - 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)

Die Bestätigung zur Registrierungsnummer T-Systems. 02081.TE.04.2002 besteht aus 6 Seiten.

Beschreibung der technischen Komponente:

1. Handelsbezeichnung der technischen Komponente und Lieferumfang

Handelsbezeichnung:
„Sign@tor Version 2.0“

Auslieferung:
Das Produkt ist über Zertifizierungsdiensteanbieter oder im Handel erhältlich; die Verpackung ist versiegelt; das Sign@tor Terminal (Hardware) ist zusätzlich durch inspizierbare Schweißpunkte gesichert

Lieferumfang:

Art	Name	Version	Lieferform
SW Dokumentation	SIGN@TOR PC (inkl. Installations- und Update-Programm) sowie Online Dokumentation für die Administration und Benutzerhandbuch	2.0	CD
HW und SW	SIGN@TOR Terminal	2.0	Gerät
SW	*Externe Applikation - Secure Viewer-Software eines Drittunternehmens (Optional)* *****	-	-

** Diese Komponente ist **kein** geprüfter Bestandteil des Produktes.*

Hersteller:
Siemens AG Österreich
Siemensstrasse 92
A-1211 Wien
Österreich

2. Funktionsbeschreibung

Der Sign@tor Version 2.0 ist ein Produkt vom Typ „Signaturanwendungskomponente“ und besteht aus den folgenden 2 Komponenten:

- dem externen, an den PC angeschlossenen Sign@tor Terminal und
- dem Sign@tor PC (der auf dem PC laufenden Software).

Das Sign@tor Terminal besteht aus einem Chipkartenleser mit integrierter Tastatur (PIN Eingabe) und einem Display (u.a. zur Hashwert-Anzeige). Die Software für das Sign@tor Terminal besteht aus folgenden Komponenten:

- Signatur-API,
- Update Software für das Sign@tor Terminal

Die ausgelieferte CD enthält im wesentlichen die

- Software für den Sign@tor PC

- Signatur-API
- Update Software für Sign@tor PC
- Funktion „Signatur Prüfen“
- Benutzeroberfläche (High Level) und
- Optional: Externe Applikation (Secure Viewer-Software eines Drittunternehmen)

Der Sign@tor unterstützt die Auswahl und Anzeige der zu signierenden Datei sowie die Berechnung des Hash-Wertes, den er dann an die Signaturkarte schickt.

Die Signaturkarte gibt die in ihr erzeugte Signatur an das Sign@tor Terminal zurück. Der Sign@tor erstellt eine signierte Datei im Format PKCS#7 (optional), nachdem er die Signatur der Datei (die in der Signaturkarte gebildet wurde) und das Zertifikat der Signaturkarte übernommen hat.

Im Rahmen dieser Nutzung dient das Sign@tor Terminal als Kartenleser für die Signaturkarte des Benutzers und als Eingabegerät für die PIN. Es stellt die Vertraulichkeit der PIN gegenüber dem (Sign@tor und restlichen) PC sicher.

Der Sign@tor gewährleistet sichere Software-Updates[3] für den Sign@tor PC, indem er die Integrität der heruntergeladenen Software anhand der Signatur überprüft.

Der Sign@tor gewährleistet sichere Software-Updates[3] für das Sign@tor Terminal, indem die Integrität der heruntergeladenen Software anhand der Signatur überprüft wird.

Der Sign@tor unterstützt die Auswahl und Anzeige in einem Viewer von Dateien, deren Signatur zu prüfen ist.

Bei der Signaturprüfung wird überprüft, ob die Signatur mit einem Signaturschlüssel erzeugt wurde, der zum öffentlichen Schlüssel korrespondiert. Dieser öffentliche Schlüssel ist im Zertifikat der signierten Datei enthalten.

3. Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Der „Sign@tor Version 2.0“ erfüllt die folgenden Anforderungen:

- §15 Abs. 2 Nr. 1 a) SigV
- §15 Abs. 2 Nr. 1 b) SigV
- §15 Abs. 2 Nr. 1 c) SigV
- §15 Abs. 4 SigV

Das Produkt stellt im Sinne des Gesetzes **einen Teil der Funktionen** einer Signaturanwendungskomponente bereit:

- Das Erzeugen einer Signatur wird vorher eindeutig angezeigt,
- es ist erkennbar, auf welche Daten sich die Signatur bezieht,
- eine Signatur erfolgt nur durch die berechtigt signierende Person,
- Identifikationsdaten werden nicht preisgegeben.

[3] Die geladenen Updates fallen **nicht** automatisch unter diese Sicherheitsbestätigung; über ggf. erteilte Sicherheitsbestätigungen für die Updates kann sich der Nutzer beim Hersteller, bei der Regulierungsbehörde oder bei der Bestätigungsstelle informieren.

Das Produkt besitzt **nicht** die Funktion einer sicheren Anzeige (§17 Abs. 2 S. 3 SigG) des zu signierenden Dateiinhaltes am PC. Insbesondere ist eine optionale Viewer Software eines Drittanbieters nicht Gegenstand dieser Sicherheitsbestätigung.

Die im Produkt enthaltene (Offline) Signatur-Prüfung durch die Benutzeroberfläche war nicht Gegenstand der Evaluierung und fällt somit **nicht** unter diese Sicherheitsbestätigung.

3.2 Einsatzbedingungen

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

a) Einrichtung der Signaturarbeitsstation

Grundsätzliches:

Sign@tor Version 2.0 ist für den Einsatz in einem geschützten Einsatzbereich geeignet, bei dem potentielle Angriffe über
- das Internet,
- ein angeschlossenes Intranet,
- einen manuellen Zugriff Unbefugter und
- Datenaustausch per Datenträger

durch eine Kombination von Sicherheitsvorkehrungen in der Einsatzumgebung (Infrastruktur, Systemplattform und Netzwerk) mit hoher Sicherheit abgewehrt werden.

Sign@tor Version 2.0 trägt zu diesen Sicherheitsvorkehrungen zwar durch Verfahren der Transportsicherung bei, kann allerdings für die Komponente „Sign@tor PC“ nicht alle Anforderungen selbst erfüllen.

Die Komponente „Sign@tor Terminal“ leistet jedoch für sich den erforderlichen Schutz, sofern ein *physischer* Zugriff (mit dem Ziel der Manipulation) durch Unbefugte auf das „Sign@tor Terminal“ ausgeschlossen ist.

Mit Auslieferung von Sign@tor Version 2.0 ist der Anwender auf die Einhaltung der genannten Sicherheitsvorkehrungen hinzuweisen.

Produktauslieferung:

Sign@tor Version 2.0 wird vom Hersteller gemäß Abschnitt 1 ausgeliefert. Das spezifizierte Auslieferungsverfahren ist einzuhalten.

Der Benutzer muss nach dem Kauf und vor der ersten Inbetriebnahme den einwandfreien Auslieferungszustand durch Kontrolle der Versiegelung der Verpackung und durch Kontrolle der Schweißpunkte beim Sign@tor Terminal verifizieren.

Installationsvoraussetzungen:

Die Software des Sign@tor PC benötigt die Unterstützung durch eines der Betriebssysteme Windows 98 SE, Windows ME oder Windows 2000. An die Hardware des PC sind folgende Anforderungen zu stellen: CPU ab Pentium I, USB-Schnittstelle, Internet Anschluss (optional), Festplatte mindestens 10 MB, Hauptspeicher mindestens 32 MB, CD-Laufwerk.

Als Signaturerstellungseinheiten können folgende Smartcards[4] eingesetzt werden:

- CardOS/M4.0 auf Prozessorchip Infineon
- TCOS auf Prozessorchip Infineon
- CardOS/M4.01 auf Prozessorchip Infineon
- Starcos SPK 2.2 + mod auf Prozessorchip Philipps
- Starcos 2.3 auf Prozessorchip Philipps

Sign@tor Version 2.0 darf ausschließlich mit der oben beschriebenen Hard- und Softwareausstattung eingesetzt werden.

Aufstellung der Signaturarbeitsstation:

Das Sign@tor Terminal und der Sign@tor PC müssen sich in *einem* Raum sowie bei der Nutzung *direkt vor* dem Benutzer befinden, damit die Validierung der Daten sowie der Hash-Werte möglich ist.

Installation:

Der Benutzer muss die Erstinstallation der Software mit der ausgelieferten CD durchführen. Diese CD ist sicher aufzubewahren, da sie für ein späteres Software-Update benötigt wird.

Betriebsmodi:

Das Produkt verfügt über zwei Betriebsmodi. Die sicherheitsbestätigte Funktionalität ist nur im „EVG Betriebsmodus“ gegeben. Dieser ist an der Anzeige „Betriebsbereit“ auf dem Display des Sign@tor Terminals zu erkennen.

Sonstiges:

Andere Anwendungen, die Sign@tor Version 2.0 oder eines seiner Teile nutzen, sind **nicht** Gegenstand dieser Bestätigung.

b) Maßnahmen in der Einsatzumgebung

Aus den Auflagen an die Einsatzumgebung unter a) ergeben sich insbesondere die Forderungen,

- den physischen Zugang Unbefugter zur Signaturarbeitsstation auszuschließen, um damit eine Manipulation der Komponenten von Sign@tor Version 2.0 auszuschließen,
- durch eine Kontrolle einzuspielender Daten (Netzwerk, Datenträger) die Manipulation von Sign@tor PC durch maliziöse Programme zu verhindern.

c) Betrieb und Nutzung des Produktes

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

Die Vorgaben aus der Benutzerdokumentation zu Sign@tor Version 2.0 für die Sicherheitsadministration und den Schutz vor Fehlern sind einzuhalten, insbesondere:

---

[4] Die Aufzählung beinhaltet Karten, die kompatibel zu Sign@tor Version 2.0 sind, gibt aber keine Auskunft über deren Gesetzeskonformität. Hierzu vgl. man die Listen unter www.regtp.de.

- Der Benutzer muss darauf achten, dass nur Dokumente ohne Makros signiert werden. Ggf. in Dokumenten enthaltene Makros, die sonst mitsigniert würden, müssen vor dem Signieren entfernt werden.
- Dokumente, die durch Hyperlinks eingezogen werden, werden nicht signiert.
- Der Benutzer muss seine PIN direkt am Sign@tor Terminal eingeben, unmittelbar bevor eine Signatur gebildet wird.

d) Wartung und Reparatur des Produktes

Hinsichtlich der Wartung sind die Update-Verfahren für die Software von Sign@tor PC und Sign@tor Terminal einzuhalten (s. Benutzerdokumentation). Der Benutzer muß insbesondere bei einem Update der Software für den Sign@tor PC die Signatur der neuen Software mit der Hilfe der Original-CD überprüfen. Hinsichtlich der Sicherheitsbestätigung für die Updates ist die Fußnote 3 zu beachten.

Sonstige Wartung und Reparatur ist ausschließlich durch fachkundiges autorisiertes Personal durchzuführen.

Der zu Sign@tor Version 2.0 gehörende Datenträger (CD) ist so aufzubewahren, daß er vor unbemerktem Zugriff Unbefugter geschützt ist.

3.3 Algorithmen und zugehörige Parameter

Die Signaturanwendungskomponente Sign@tor Version 2.0 verwendet die Hashfunktion SHA-1. Die gemäß § 11 Abs. 3 in Verbindung mit Anlage I Nr. 2 SigV festgestellte Eignung reicht mindestens bis zum 31.12. 2006 (s. Bundesanzeiger Nr. 158 – Seite 18 562 vom 24. August 2001).

Diese Sicherheitsbestätigung ist somit **gültig bis zum 31.12.2006**; 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 Signaturanwendungskomponente „Sign@tor Version 2.0“ wurde unter der Registriernummer T-Systems-DSZ-ITSEC-04080-2002 von der Prüfstelle für IT-Sicherheit der T-Systems ISS GmbH gegen die Prüfstufe **E2** der **ITSEC** evaluiert. Die Evaluierung wurde am 30.04.2002 beendet. Die eingesetzten Sicherheitsmechanismen erreichten die Stärke **hoch**.

Ende der Bestätigung