Bestätigung
für technische Komponenten
gemäß § 14 (4) Gesetz zur digitalen Signatur und §§ 16 und 17 Signaturverordnung

debis Systemhaus Information Security Services GmbH
- Zertifizierungsstelle debisZERT -

Rabinstraße 8
53111 Bonn

bestätigt hiermit gemäß §14 Abs. 4 Signaturgesetz[1] und §17 Abs. 3 Signaturverordnung[2], daß

Siemens Sign@tor Version 1.0

den nachfolgend beschriebenen Anforderungen des Artikel 3 des Gesetzes zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Gesetz zur digitalen Signatur) vom 01. August 1997 bzw. der Signaturverordnung vom 01. November 1997 entsprechen und bei sachgemäßen Einsatz im Wirkungsbereich der genannten Rechtsvorschriften eingesetzt werden kann.

Die Dokumentation zu dieser Bestätigung ist unter

debisZERT.02065.TE.03.2001

registriert.

Bonn, den 06.04.2001 **gez. Dr. Heinrich Kersten**
Zertifizierungsstelle

debis Systemhaus Information Security Services GmbH – Zertifizierungsstelle debisZERT - ist gemäß der Veröffentlichung im Bundesanzeiger Nr. 31 vom 14. Februar 1998, Seite 1787, zur Erteilung von Bestätigungen für technische Komponenten gemäß § 14 Abs. 4 des Gesetzes zur digitalen Signatur ermächtigt.

---

1 Gesetz zur digitalen Signatur (Signaturgesetz – SigG) vom 22.07.1997 (BGBl. I., S. 1870, 1872)

2 Verordnung zur digitalen Signatur (Signaturverordnung – SigV) vom 08.10.1997 (BGBl. I., S. 2498 ff.)

Die Bestätigung zur Registriernummer debisZERT.02065.TE.03.2001 besteht aus 7 Seiten.

Beschreibung der technischen Komponente:

1 Handelsbezeichnung der technischen Komponente und Lieferumfang

Handelsbezeichnung:

- Siemens Sign@tor Version 1.0

Hersteller:

- Siemens AG Österreich
  Siemensstr. 82, A-1210 Wien

Technische Voraussetzungen:

Installation auf einem PC des Industrie-Standards (CPU: ab Pentium I, USB-Schnittstelle, Internet Anschluss (optional), Speicherbedarf/Festplatte: mindestens 10 MB, Hauptspeicher: mindestens 32 MB) mit dem Betriebssystem Windows 98 SE, Windows ME oder Windows 2000.

Lieferumfang:

- " Sign@tor Terminal" (Version 1.0, intelligenter Chipkartenleser mit Tastatur und Display und vorinstallierter Software),

- "Sign@tor PC" (Version 1.0, Software inkl. Installations- und Update-Programm sowie Online-Hilfe; Auslieferung auf einer CD)

  Auf der ausgelieferten CD befinden sich die folgenden Dateien:

Dateiname	Größe / Bytes	Datum
Hauptverzeichnis		
autorun.inf	63	21.12.00
Verzeichnis Autorun		
ct_signator.dll	45056	21.12.00
Installation.txt	2675	21.12.00
setup.exe	708608	21.12.00
setupcd.ico	766	21.12.00
signator.dll	327680	21.12.00
signator.sig	128	21.12.00
signator.tlb	2724	21.12.00

Dateiname	Größe / Bytes	Datum
Verzeichnis PC		
instmsia.exe	1511680	12.12.00
instmsiw.exe	1509632	12.12.00
setup.exe	83717	12.12.00
setup.ini	39	22.03.01
signator.msi	1071616	22.03.01
Verzeichnis Treiber		
signator2000.inf	6492	21.12.00
signator98.inf	972	21.12.00
Verzeichnis Update		
updatepc.exe	40960	21.12.00
Updateterminal.exe	24576	21.12.00

Bei den Dateien instmsia.exe und instmsiw.exe handelt es sich um Installationspakete, die in komprimierter Form vorliegen. Sie enthalten auch die für den Benutzer wichtige Online-Hilfe. Diese befindet sich nach der Installation, im Unterverzeichnis help und hat die folgenden Eigenschaften:

Name: sign@tor.hlp, Größe: 649444, Datum: 19.03.01,
Name: signieren.hlp, Größe: 286632, Datum: 16.03.01.

Nicht zum Lieferumfang des Produktes gehören ein geeigneter **Viewer** und eine geeignete **Signaturchipkarte**.

Folgende Chipkarten[3] sind aus technischer Sicht für die Verwendung mit dem Produkt freigegeben:

- Signaturchipkarte der Firma Datakom Austria (A-Sign) mit Prozessorchip Infineon und Chipkartenbetriebssystem CardOS / M4.0,

- Signaturchipkarte der Firma A-Trust mit Prozessorchip Philips und Chipkartenbetriebssystem Starcos SPK 2.2 + mod.

2 Funktionsbeschreibung

Siemens Sign@tor Version 1.0 besteht aus den Teilen Sign@tor PC (der auf einem PC laufenden Software) und dem externen, an den PC per USB angeschlossenen Sign@tor Terminal.

Siemens Sign@tor Version 1.0 dient der

---

[3] Diese Sicherheitsbestätigung macht keine Aussage über den gesetzeskonformen Status der angegebenen Chipkarten.

- sicheren Erfassung der Identifikationsdaten (PIN) des Benutzers und Weitergabe derselben an eine (nicht zum Produkt gehörende) Chipkarte über den im Sign@tor Terminal eingebauten Chipkartenleser,

- Auswahl der zu signierenden Datei, Unterstützung eines externen (nicht zum Produkt gehörenden) Viewers zur Anzeige der zu signierenden Datei, Berechnung des Hashwertes über die ausgewählte Datei zur Transportsicherung, Übertragung dieser Datei vom PC zum Terminal,

- Berechnung des Hashwertes über die ausgewählte Datei im Sign@tor Terminal, Hashwert-Vergleich durch den Benutzer (Anzeige am PC und am Display des Terminals), im positiven Fall Weiterleitung des Hashwertes an die Chipkarte zur Signaturerzeugung,

- Veranlassung des Signaturvorganges bei der eingesetzten Chipkarte,

- Übernahme der Signatur und des Benutzerzertifikats, Speicherung der Datei einschließlich Signatur und Benutzer-Zertifikat in einer PKCS#7 konformen Datenstruktur auf dem PC,

- Offline-Prüfung anderer Signaturen,

- sicheren Aktualisierung (Update) der Software von Sign@tor PC und Sign@tor Terminal.

Hinweis: Die Offline-Signaturprüfung und die Software-Aktualisierung sind nicht Gegenstand der Sicherheitsbestätigung.

3 Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllung der Anforderungen

Siemens Sign@tor Version 1.0 erfüllt im Zusammenhang mit den vorgegebenen technischen und organisatorischen Einsatzbedingungen folgende Anforderungen aus SigV in dem jeweils angegebenen Umfang:

§16 (2) Satz 4: **Die zum Erfassen von Identifikationsdaten erforderlichen technischen Komponenten müssen so beschaffen sein, daß sie die Identifikationsdaten nicht preisgeben und diese nur auf dem Datenträger mit dem privaten Signaturschlüssel gespeichert werden.**

§16 (2) Satz 5: **Sicherheitstechnische Veränderungen an den technischen Komponenten müssen für den Nutzer erkennbar werden.**

Die Anforderung nach §16 (2) Satz 4 erfüllt das Produkt in der betrachteten Einsatzumgebung mit dem vom PC getrennten, zur PIN-Eingabe verwendeten Terminal mit separater Tastatur, Display, Chipkartenleser und integrierter Software. Die Identifikationsdaten sind dauerhaft nur auf der genutzten Chipkarte gespeichert, eine Preisgabe durch das Terminal ist in der betrachteten Einsatzumgebung ausgeschlossen.

Die Anforderung nach §16 (2) Satz 5 erfüllt das Produkt insofern, als in der betrachteten Einsatzumgebung keine sicherheitstechnischen Veränderungen möglich sind.

§16 (3) Satz 1: **Die zum Darstellen zu signierender Daten erforderlichen technischen Komponenten müssen so beschaffen sein, daß die signierende Person die Daten, auf die sich die Signatur erstrecken soll, eindeutig bestimmen kann, eine digitale Signatur nur auf ihre Veranlassung erfolgt und diese vorher eindeutig angezeigt wird.**

§16 (3) Satz 4: **Die technischen Komponenten müssen nach Bedarf den Inhalt der zu signierenden oder signierten Daten hinreichend erkennen lassen.**

§16 (3) Satz 6: **Sicherheitstechnische Veränderungen an den technischen Komponenten müssen für den Nutzer erkennbar werden.**

Da das Produkt keine eigene Anzeigekomponente (Viewer) besitzt, ist die Anforderung nach §16 (3) Satz 4 nur insoweit erfüllt, als in der betrachteten Einsatzumgebung (hier insbesondere die ausschließliche Verwendung vertrauenswürdiger Software auf dem PC) keine *manipulierte* Anzeige erfolgt; jedoch sind die Maßnahmen der hier betrachteten Einsatzumgebung allein nicht ausreichend, um eine *sichere* Anzeige nach SigV zu ermöglichen: Weitere Anforderungen sind an die Anzeigeoptionen des verwendeten Viewers zu stellen, um den Inhalt der zu signierenden Daten hinreichend erkennen zu können.

Die Anforderungen nach §16 (3) Satz 1 erfüllt das Produkt insoweit, als in der betrachteten Einsatzumgebung (hier insbesondere die ausschließliche Verwendung vertrauenswürdiger Software auf dem PC) eine präzise Dateiauswahl möglich ist, die Signatur nur durch den Benutzer veranlaßt werden kann und eine eindeutige Anzeige der Signatur gegeben ist.

Die Anforderung nach §16 (2) Satz 5 erfüllt das Produkt insofern, als in der betrachteten Einsatzumgebung keine sicherheitstechnischen Veränderungen möglich sind.

3.2 Einsatzbedingungen

Grundsätzliches

Die Benutzerdokumentation und die Angaben in dieser Sicherheitsbestätigung beinhalten wichtige Informationen für die sichere Benutzung des Produktes und sind daher strikt zu befolgen.

Auslieferung

Nach dem Erwerb (und vor jeder Installation) hat der Benutzer das Sign@tor Terminal daraufhin zu überprüfen, daß die Versiegelung (Schweißpunkte) des Gehäuses unverletzt ist.

Installation

Es muß durch geeignete Maßnahmen in der Einsatzumgebung verhindert werden, dass Unbefugte Zugang zum Arbeitsplatz mit installiertem Siemens Sign@tor Version 1.0 haben.

Das Sign@tor Terminal und der Sign@tor PC müssen im gleichen Raum und nebeneinander aufgestellt werden, so daß der Benutzer den PC-Bildschirm und das Display des Terminals im Blickfeld hat.

Es ist sicherzustellen, daß auf dem PC nur vertrauenswürdige Software installiert und eingesetzt wird. Die Installation von Siemens Sign@tor Version 1.0 und anderer (vertrauenswürdiger) Software auf dem betreffenden PC ist nur durch qualifiziertes Personal vorzunehmen.

Es ist sichzustellen, daß auf dem PC stets ein aktueller Virenscanner installiert ist und dieser in regelmäßigen Abständen aktiviert wird, insbesondere vor der Installation von Siemens Sign@tor Version1.0.

Die Software des Sign@tor Terminals ist bei Erwerb des Gerätes bereits installiert.

Der Benutzer muss die Erstinstallation der Software auf dem PC mit der CD, die in der Verpackung des Siemens Sign@tor Version1.0 mitgeliefert wird, durchführen.

Die Hinweise in der Benutzerdokumentation (Sign@tor Onlinehilfe) zum Verhalten bei fehlerhafter Installation sind zu befolgen.

Die CD ist sicher aufzubewahren, da sie für eine Neu-Installation und für ein Software-Update benötigt wird.

Betrieb

Der Siemens Sign@tor Version 1.0 verfügt über zwei Betriebsmodi, von denen nur einer den Anforderungen des Signaturgesetzes entspricht. Der sicherheitsbestätigte Betriebmodus ist nach dem Einschalten an der Anzeige „Betriebsbereit“ im Display des Sign@tor Terminals zu erkennen.

Der Benutzer muss die für die Aktivierung der Chipkarte erforderliche PIN vertraulich halten. Die PIN ist nur am Sign@tor Terminal einzugeben.

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, auf die mit Hyperlinks verwiesen wird, werden nicht signiert.

Der Benutzer hat den Signiervorgang erst dann zu starten, wenn er sich davon überzeugt hat, daß die auf dem PC und dem Display des Terminals angezeigten Hashwerte identisch sind. Dazu müssen alle vier Zeilen des Hashwertes auf dem Terminal durchgeblättert werden, bevor mit OK der Signiervorgang gestartet werden kann.

Die Hinweise in der Benutzerdokumentation (Sign@tor Onlinehilfe) zum Verhalten bei nicht übereinstimmenden Hash-Werten sind zu befolgen.

Der Signiervorgang kann mit der C-Taste am Terminal abgebrochen werden.

Zur Sicherheit sollte die signierte Datei stets mittels der Funktion „Signatur prüfen Offline“ überprüft werden.

Diese von Siemens Sign@tor Version 1.0 angebotene Offline-Signaturprüfung wird aber ohne Überprüfung der Zertifikatsgültigkeit durchgeführt und deckt insofern die gesetzlichen Anforderungen nicht vollständig ab.

Es ist sicherzustellen, daß auch nachträglich nur vertrauenswürdige Software auf dem PC installiert wird.

Der jeweils auf dem Terminal angezeigte Dateiname, die Dateigrösse und das Erstellungsdatum sind nur als zusätzliche Information anzusehen, denen keine besondere Verlässlichkeit zukommt.

Update

Bei einem Update der Software "Sign@tor PC" muß der Benutzer die Signatur des Updates mit Hilfe der (alten) Original-CD überprüfen. Die Original-CD muß deshalb sicher verwahrt werden.

Die entsprechende Prüfung bei einem Update der Software des Sign@tor Terminals erfolgt automatisch durch das Terminal.

Die Hinweise in der Benutzerdokumentation (Sign@tor Onlinehilfe) zum Verhalten bei fehlerhaftem Update sind zu befolgen.

Wichtiger Hinweis: Mit einem Update des sicherheitsbestätigten Produktes Siemens Sign@tor Version 1.0 verliert dieses seinen gesetzeskonformen Status – es sei denn, daß das Update bzw. das aktualisierte Produkt eine erneute Sicherheitsbestätigung erhalten hat. Der Benutzer erhält hierzu Informationen auf den Web-Seiten der Regulierungsbehörde für Telekommunikation und Post unter www.regtp.de, von der Bestätigungsstelle unter www.debiszert.de oder direkt vom Hersteller.

3.3 Eingesetzte Algorithmen und Parameter mit Gültigkeit

Die folgenden Algorithmen und Parameter sind für Verwendung bei gesetzeskonformen digitalen Signaturen durch die Regulierungsbehörde für Telekommunikation und Post freigegeben:

- Hashwert-Berechnung nach SHA-1, freigegeben bis 31.12.2005.

Als weiterer Mechanismus wird RSA verwendet, und zwar im Rahmen der Offline-Signaturprüfung und der Software-Updates von Sign@tor PC und Sign@tor Terminal; da diese Funktionen nicht Gegenstand der Sicherheitsbestätigung sind, sind hinsichtlich der Freigabe durch die Regulierungsbehörde außer SHA-1 keine weiteren Mechanismen zu betrachten.

Diese Sicherheitsbestätigung gilt bis zum 31.12.2005; sie kann jedoch verlängert werden, wenn zu diesem Zeitpunkt keine neuen Erkenntnisse hinsichtlich der Sicherheit des Produktes oder seiner Algorithmen vorliegen.

3.4 Prüfstufe und Mechanismenstärke

Den gesetzlichen Vorgaben entsprechend sind die hier betrachteten technischen Komponenten erfolgreich gegen die Evaluationsstufe **E2** und die Mechanismenstärke **hoch** der ITSEC evaluiert worden.

Ende der Sicherheitsbestätigung zur Registrierungsnummer debisZERT.02065.TE.03.2001.