



Zentrum für sichere Informationstechnologie – Austria Secure Information Technology Center - Austria

A-1040 Wien, Weyringergasse 35
Tel.: ++43 1 - 503 19 63 - 0
Fax: ++43 1 - 503 19 63 - 66

A-8010 Graz, Inffeldgasse 16a
Tel.: ++43 316 - 873 5514
Fax: ++43 316 - 873 5520

Homepage: www.a-sit.at
E-Mail: office@a-sit.at

Bescheinigung nach §18(5) SigG: Chipkartenterminal mit Tastatur und Display Sign@tor Terminal Version 2.0

Antragsteller:
Siemens AG Österreich
Siemensstrasse 92
A-1211 Wien

1. Beschreibung der bescheinigten Komponente

Die bescheinigte Komponente ist das Chipkartenterminal Sign@tor Terminal Version 2.0 (nachstehend Terminal genannt) bestehend aus

- Hardware:
 - einer CPU der 8051-Familie,
 - 64KB Flash-EEPROM (Programmspeicher),
 - mind. 1 KByte statisches RAM,
 - 32 KByte RAM (zusätzlicher Speicherbaustein),
 - mind. 2KB EEPROM (persistenter Datenspeicher),
 - einer Tastatur Matrix 3x4,
 - einem Display 16x1 ohne Beleuchtung, und
 - einer USB-Schnittstelle.
- Software (bei Erwerb des Terminals bereits installiert):
 - Signatur API 2.0,
 - Betriebssystem CoreOS 1.0, und
 - BasicOS 1.0.

Die Benutzerdokumentation ist generell online verfügbar. Die Hinweise für den Benutzer zum Verhalten bei fehlerhafter Installation/Funktion sind der Benutzerdokumentation zu entnehmen.

Das Terminal dient als

- Chipkartenleser für die Signaturkarte des Signators¹,
- Eingabegerät für die Signatur-PIN², und
- Gerät für die Berechnung des Hashwertes der zu signierenden Datei (optional):
 - Um den Signierprozess zu starten, muss der Signator nach positiver optischen Verifizierung des Hashwertes auf dem Display seine Signatur-PIN am Terminal eingeben.

Das Protokoll T=1 nach ISO 7816 wird vom Terminal für die Kommunikation mit der Signaturkarte unterstützt.

¹ d.h. der signierenden Person
² Personal Identification Number

Die Signatur-PIN wird nur an die Signaturkarte weiter gegeben und sofort nach der Übertragung im Terminal gelöscht. Die Signatur und das Zertifikat werden von der Karte an den Computer (d.h. PC) gesendet. Das Terminal schickt den (optional auf dem Terminal berechneten) Hashwert an die Signaturkarte. Die Signatur wird durch die Signaturkarte erzeugt und an das Terminal zurückgegeben.

Das Terminal nimmt alle Mitteilungen der Signaturkarte entgegen. Wenn die Mitteilung der Signaturkarte die Signatur darstellt (und kein Fehler aufgetreten ist), wird sie unverändert an den PC gesendet. Wenn die Mitteilung eine Fehlermeldung der Signaturkarte darstellt, wird sie vom Terminal wie folgt interpretiert:

- Entweder wird eine neue Fehlermeldung gebildet, die an den PC weitergeschickt wird; dabei kann zwischen drei folgenden Fällen unterschieden werden: keine Karte vorhanden bzw. Signatur-PIN gesperrt bzw. Fehlermeldung der Signaturkarte (außer Signatur-PIN gesperrt);
- oder es wird eine neue Fehlermeldung gebildet, die auf dem Display des Terminals dem Signator gezeigt wird, und zwar „PIN falsch!“, falls die Signatur-PIN falsch aber noch nicht gesperrt ist.

Eine Änderung der Signatur-PIN ist auf dem Terminal nicht möglich.

Das Terminal unterstützt folgende in Österreich bescheinigte Signaturkarten (d.h. sichere Signaturerstellungseinheiten):

- mit Prozessorchip Infineon SLE 66CX320P und Betriebssystem TCOS V2.0 Rel.3 („E4 KeyCard V3.0“);
- mit Prozessorchip Infineon SLE 66CX320P und Betriebssystem CardOS/M4.01 und Applikation für Digitale Signatur Version 0.20;
- mit Prozessorchip Philips P8WE5032V0G und Betriebssystem STARCOS SPK 2.3 mit Digital Signature Application StarCert;
- mit Prozessorchip Philips P8WE5032V0G und Betriebssystem STARCOS SPK 2.3 v 7.0 mit Digital Signature Application StarCert v 2.2; und
- mit Prozessorchip Philips P8WE5032V0G und Betriebssystem STARCOS SPK 2.3 mit Digital Signature Application TrustSign;

2. Erfüllung der Anforderungen des SigG und der SigV

Das Terminal erfüllt unter nachstehenden Einsatzbedingungen:

- Anforderungen nach §18(1) SigG³;
- Anforderungen nach §18(2) SigG⁴;
- Anforderungen nach §7(1) SigV^{5 6};
- Anforderungen nach §7(3) SigV⁷;
- Anforderungen nach §7(3) SigV⁸; und
- Anforderungen nach §9(2) SigV⁹.

³ Für die Erzeugung und Speicherung von Signaturerstellungsdaten sowie für die Erstellung sicherer Signaturen sind solche technische Komponenten und Verfahren einzusetzen, die die Fälschung von Signaturen sowie die Verfälschung signierter Daten zuverlässig erkennbar machen (...).

⁴ Die bei der Erstellung einer sicheren Signatur verwendeten technischen Komponenten und Verfahren müssen zudem sicherstellen, dass die zu signierenden Daten nicht verändert werden; (...)

⁵ Die Signatoren dürfen für die Erstellung sicherer elektronischer Signaturen nur solche Hashverfahren (...) einsetzen, die im Anhang 2 Punkt 2. (...) genannt sind.

⁶ Folgende Hashverfahren werden als sicher anerkannt (...) b) Funktion SHA-1. Diese Hashverfahren sind bis 31.12.2005 für den Einsatz bei elektronischen Signaturen als sicher anzusehen. (...)

⁷ (...) Das unbefugte Erfahren der Autorisierungs-codes muss (...) praktisch ausgeschlossen sein. (...)

⁸ (...) Die eingegebenen Autorisierungs-codes dürfen von den verwendeten Systemelementen nicht gespeichert werden.

Eingabeerleichterungen bei wiederholter Eingabe von Autorisierungs-codes müssen ausgeschlossen sein. (...)

⁹ Die Prüfung der technischen Komponenten und Verfahren nach § 7 Abs. 2, § 10 und § 18 SigG kann auch nach den Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC), (...), erfolgen. Bei der Anwendung von ITSEC muss für die Erzeugung und Speicherung von Signaturerstellungsdaten sowie für die Erstellung sicherer elektronischer Signaturen und gegebenenfalls für die sichere Signaturprüfung die Evaluationsstufe E 3 mit der Mindeststärke der Sicherheitsmechanismen "hoch" eingehalten sein; bei den übrigen technischen Komponenten und Verfahren muss die Evaluationsstufe E 2 mit der Mindeststärke der Sicherheitsmechanismen "hoch" eingehalten sein.

Das Terminal ist daher in folgenden Kategorien bescheinigt:

- Komponenten und Verfahren zum Erzeugen des Hashwertes aus dem Dokument; und
- Komponenten und Verfahren zur Sicherstellung des autorisierten Zuganges.

3. Gültigkeitsdauer der Bescheinigung

Diese Bescheinigung ist zwei Jahre nach der Ausstellung gültig.

4. Einsatzbedingungen

- (1) Der Benutzer muss den Zustand des Terminals nach dem Kauf (versiegelte Verpackung) und vor der ersten Inbetriebnahme (Schweißpunkte des Terminals) kontrollieren.
- (2) Das Sign@tor Terminal V2.0 muss im EVG-Betriebsmodus sein, der an der Anzeige des Sign@tor Terminals mit „Betriebsbereit“ zu erkennen ist.
- (3) Das Sign@tor Terminal V2.0 muss sich bei der Benutzung in demselben Raum wie der Rechner mit der Signaturanwendungs-Software befinden und direkt vor dem Benutzer stehen. Der physische Zugang Unbefugter muss ausgeschlossen sein.
- (4) Der Benutzer muss den physischen Zugang zum Sign@tor Terminal V2.0 ständig unter Kontrolle halten, um Manipulationen von Hardware zu verhindern.
- (5) Wird ein Software- oder Hardware-Update des Sign@tor Terminals V2.0 durchgeführt, erlischt die Gültigkeit der aktuellen Bescheinigung. Um die Bescheinigung des Sign@tor Terminals aufrecht zu erhalten, ist es daher erforderlich, alle weiteren Aktualisierungen des Sign@tor Terminals V2.0 ebenfalls einer Evaluierung/Bescheinigung zu unterziehen.
- (6) Alle Annahmen über die Einsatzumgebung aus Kapitel 2 des Zertifizierungsberichtes T-Systems-ITSEC-04080-2001 vom 30.04.2002, die sich auf das Sign@tor Terminal V2.0 beziehen (mit Ausnahme von Software-Updates), müssen erfüllt werden.

Folgende **Empfehlung** soll den Signator auf zusätzliche Maßnahmen aufmerksam machen, welche die Sicherheit des Signiervorgangs erhöhen können:

- Es wäre von Vorteil, wenn der Benutzer die von der Signaturanwendung und vom Terminal berechneten Hashwerte optisch vergleichen würde, um die Integrität der Übertragung sicherzustellen, bevor der Signierprozess gestartet wird (entspricht Optionen 1.1 und 1.2 im Zertifizierungsbericht T-Systems-ITSEC-04080-200110).

5. Algorithmen und zugehörige Parameter

Zum Erzeugen des Hashwertes aus dem Dokument wird vom Sign@tor Terminal V2.0 das SHA-1 Hashverfahren mit 160 Bit bereitgestellt. Dadurch sind die Anforderungen gemäß Anhang 2 Punkt 2 SigV erfüllt.

6. Prüfstufe und Mechanismenstärke

Es liegt das Deutsche IT-Sicherheitszertifikat T-Systems-DSZ-ITSEC-04080-2002 für „Sign@tor Version 2.0“ (bestehend aus Sign@tor PC und Sign@tor Terminal) vor, ausgestellt durch die Zertifizierungsstelle der T-Systems ISS GmbH¹¹ am 30.04.2002. Dieses Zertifikat weist der Komponente die Evaluierungsstufe **E2** mit der Mindeststärke der Mechanismen „**hoch**“ nach ITSEC V1.2 aus. Die materiellen Prüfungen sind im Zertifizierungsbericht T-Systems-ITSEC-04080-2001¹² vom 30.04.2002 beschrieben.

Es liegt die Bestätigung von Produkten für qualifizierte elektronische Signaturen gemäß §§ 15 Abs. 7 S. 1, 17 Abs. 4 Gesetz über Rahmenbedingungen für elektronische Signaturen (Fassung vom 16.05.2001) und §§ 11 Abs. 2 und 15 Signaturverordnung T-Systems.02081.TE.04.2002 für die Signaturanwendungskomponente „Sign@tor Version 2.0“ vor, ausgestellt durch die T-Systems ISS GmbH – Zertifizierungsstelle am 30.04.2002.

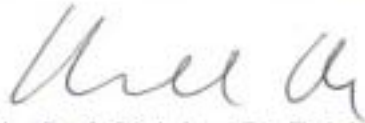
¹⁰ http://www.t-systems-zert.com/pdf/ein_01_zer_itsec_cc/zr_04080_d.pdf

¹¹ Rabinstr. 8, D-53111 Bonn

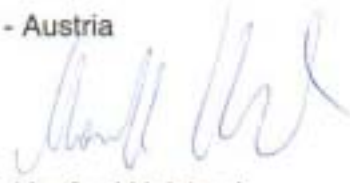
¹² http://www.t-systems-zert.com/pdf/ein_01_zer_itsec_cc/zr_04080_d.pdf

Wien, 04.11.2002

A-SIT Zentrum für sichere Informationstechnologie - Austria



o. Univ.-Prof. Dipl.-Ing. Dr. Reinhard Posch
Wissenschaftlicher Gesamtleiter



Manfred Holzbach
Geschäftsführender Vorstand