



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: Sign@tor Terminal V1.0

Antragsteller:
Siemens Aktiengesellschaft Österreich
Postfach 83
A-1211 Wien

1. Beschreibung der zu bescheinigenden Komponente

Der Gegenstand der Bescheinigung ist Sign@tor Terminal Version 1.0 (nachstehend auch das Terminal genannt) mit folgender SW:

- Signatur API 1.0,
- Betriebssystem CoreOS 1.0, und
- BasicOS 1.0

Das Terminal ist ein Teil einer sicheren Signaturerstellungseinheit und dient als

- Kartenleser für die Signaturkarte des Signators
- Eingabegerät für die PIN (Personal Identification Number), und
- Gerät für die Berechnung des Hashwertes der zu signierenden Datei.

Der Sign@tor PC ist mit den Betriebssystemen Windows98 SE, Windows ME, und Windows2000 getestet.

Die zu signierende Datei wird vom PC an das Sign@tor Terminal gesendet. Der Hashwert der zu signierenden Datei wird auf dem PC und auf dem Terminal berechnet und gleichzeitig angezeigt, so dass der Benutzer beide Werte vergleichen kann. Falls beide Werte identisch sind, startet der Signator den Signierprozess, bei dem der Hashwert vom Terminal auf die Karte geschickt wird.

Um den Signierprozess zu starten, muss der Signator nach positiver Verifizierung des Hashwertes seine PIN am Terminal eingegeben. Die PIN wird nur an die Karte weiter gegeben und wird sofort nach der Übertragung im Terminal gelöscht. Die Signatur und das Zertifikat werden von der Karte an den PC gesendet. Auf dem PC werden die Signatur, das Zertifikat, und die Originaldatei nach PKCS#7 kodiert.

Das Terminal schickt den (auf dem Terminal berechneten) Hashwert an die Signaturkarte. Die Signatur wird durch die Signaturkarte erzeugt und an das Sign@tor Terminal zurückgegeben.

Die Sign@tor Terminal HW besteht aus

- einer CPU der 8051-Familie,
- 64KB Flash-EEPROM (Programmspeicher),
- 1 KByte statisches RAM,
- 2KB EEPROM (persistenter Datenspeicher),
- einer Tastatur Matrix 3x4,
- einem Display 16x1 ohne Beleuchtung, und
- einer USB-Schnittstelle

Es werden Standardbausteine verwendet, die am Markt frei erhältlich sind. Das Terminal ist mit dem USB-Kabel an einen Sign@tor PC angeschlossen. Das Terminal kommuniziert mit der Signaturkarte via ISO 7816-3 T=1 Protokoll.

2. Erfüllung der Anforderungen des SigG und der SigV

Das Sign@tor Terminal V1.0 erfüllt

- die Anforderung nach §18(2) SigG an technische Komponenten und Verfahren, dass die zu signierenden Daten nicht verändert werden,
- die Anforderung nach §7(1) SigV an zulässige Hashverfahren (Anhang 2 Punkt 2 SigV),
- die Anforderungen nach §7(3) SigV an Systemelemente, dass die eingegebenen Autorisierungs-codes von den verwendeten Systemelementen nicht gespeichert werden dürfen, und dass Eingabeerleichterungen bei wiederholter Eingabe von Autorisierungs-codes ausgeschlossen sein müssen, und
- die Anforderung nach §9(2) SigV an die Prüfung der übrigen (d.h. weder für die Erzeugung und Speicherung von Signaturerstellungsdaten noch für die Erstellung sicherer elektronischer Signaturen noch für die sichere Signaturprüfung eingesetzten) technischen Komponenten und Verfahren, dass die Evaluationsstufe ITSEC E2 mit der Mindeststärke der Sicherheitsmechanismen "hoch" eingehalten sein muss.

Das Sign@tor Terminal V1.0 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

Die Bescheinigung ist zwei Jahre nach der Ausstellung gültig. Die Gültigkeit dieser Bescheinigung ist an die unter Einsatzbedingungen genannten Auflagen gebunden.

4. Einsatzbedingungen

Die behaupteten und geprüften Sicherheitsfunktionen, die insbesondere den Einsatz im Zusammenspiel in einer nicht durch den Benutzer gänzlich kontrollierten Umgebung erleichtern können, gehen über die Basisanforderung der Signaturverordnung hinaus und sind insbesondere an die nachfolgenden Einsatzbedingungen gekoppelt:

- (1) Der Benutzer muss den Zustand des Terminals (anhand der Schweißpunkte) nach dem Kauf und vor der ersten Inbetriebnahme kontrollieren.
- (2) Das Sign@tor Terminal V1.0 muss im EVG-Betriebsmodus sein, der an der Anzeige des Sign@tor Terminals mit „Betriebsbereit“ zu erkennen ist.
- (3) Das Sign@tor Terminal V1.0 muss sich bei der Benutzung in demselben Raum wie der Sign@tor PC befinden und direkt vor dem Benutzer stehen.
- (4) Der Benutzer muss den physischen Zugang zum Sign@tor Terminal V1.0 ständig unter Kontrolle halten, um Manipulationen von HW zu verhindern.

- (5) Wird ein SW- oder HW-Update des Sign@tor Terminals V1.0 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 V1.0 ebenfalls einer Evaluierung/Bescheinigung zu unterziehen.

5. Algorithmen und zugehörige Parameter

Zum Erzeugen des Hashwertes aus dem Dokument wird vom Sign@tor Terminal V1.0 das SHA-1 Hashverfahren mit 160 Bit bereit gestellt. Dadurch sind die Anforderungen gemäß Anhang 2 Punkt 2 SigV erfüllt.

6. Prüfstufe und Mechanismenstärke

Das Produkt Siemens Sign@tor Version 1.0 bestehend aus dem Sign@tor PC (SW) und dem Sign@tor Terminal (SW und HW) ist ITSEC E2 hoch evaluiert. Folgende Sicherheitsziele sind erfüllt:

SZ1: Die Vertraulichkeit der PIN gegenüber den Prozessen auf dem PC soll gewährleistet werden.

SZ2: Die Integrität der vom Sign@tor PC an das Sign@tor Terminal gesendeten Datei soll vom Benutzer überprüfbar sein.

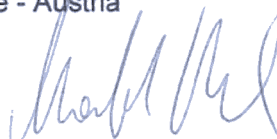
SZ3: Die Authentizität der Dateien, die für das Update des Sign@tor PCs bzw. des Sign@tor Terminals vorgesehen sind, soll überprüfbar sein.

In Wien, am 23.05.2001

A-SIT Zentrum für sichere Informationstechnologie - Austria



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



Manfred Holzbach
Geschäftsführender Vorstand