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

http://www.a-sit.at
E-Mail: office@a-sit.at

STELLUNGNAHME
SICHERE SIGNATUR UND KARTENLESER

Das österreichische SigG[1] und die SigV[2] sehen - wie auch die EU-Signaturrichtline[3] - nur eine Prüfpflicht für sichere Signaturerstellungseinheiten nicht aber für Komponenten und Verfahren, die der Systemumgebung zuzurechnen sind, vor. Kartenleser, die bei sicheren Signaturen eingesetzt werden, sind der Systemumgebung der Signaturerstellungseinheit zuzuordnen und es bestehen daher keine gesetzlichen Anforderungen, dass diese nach bestimmten Kriterien geprüft sein müssen.

Bei sicheren Signaturen müssen die in § 4 SigV („Technische Sicherheitserfordernisse für die Systemumgebung der Signaturerstellungseinheit bei sicheren Signaturen“) genannten Sicherheitsanforderungen, die auf das betreffende in der Signaturumgebung verwendete Gerät anwendbar sind, erfüllt sein. Wesentliche i. A. auf Kartenleser zutreffende Anforderungen sind dabei *„Die eingegebenen Autorisierungscodes dürfen von den verwendeten Systemelementen nicht über den Signaturvorgang hinaus im Speicher verbleiben.“* (§ 4 Abs. 2 vierter Satz) und *„Eingabeerleichterungen bei wiederholter Eingabe von Autorisierungscodes müssen ausgeschlossen sein.“* (§ 4 Abs. 2 fünfter Satz)

§ 4 Abs. 2 vierter Satz erlaubt auch die sog. „Stapelsignatur“, d.h. dass der Signaturvorgang für einen Stapel von einzelnen und unabhängigen sicheren elektronischen Signaturen mit dem gleichen Schlüsselpaar durch die einmalige Eingabe des Autorisierungscodes ausgelöst werden kann. Dabei muss jedoch die Möglichkeit zur Darstellung der zu signierenden Daten (SigG § 18 Abs. 2) gewahrt bleiben. Alle Daten, die mit der Eingabe des Autorisierungscodes signiert werden, müssen daher zum Zeitpunkt der Eingabe bereits vorliegen. Das „Freischalten“ des Autorisierungscodes für eine Anzahl von Signaturen oder für ein bestimmtes Zeitfenster, bevor die zu signierenden Daten überhaupt vorliegen (d.h. eine „Blankounterschrift“), ist damit nicht zulässig. Das Verbot von Eingabeerleichterungen (§ 4 Abs. 2 fünfter Satz) ist in erster Linie als Sicherheitsanforderung zu sehen, um unbewusste oder nicht gewollte Signaturen auszuschließen. Im Zusammenhang mit einer Stapelsignatur ist dieses Verbot bei der Abarbeitung mehrerer Stapel (d.h. es werden mehrere Signaturvorgänge ausgelöst), anwendbar, nicht aber innerhalb der Abarbeitung eines Stapels (d.h. innerhalb eines Signaturvorgangs).

Die Erfüllung der o.g. Anforderungen ist allerdings von der Gesamtheit der Signaturumgebung (d.h. Kartenleser, Software, …) zu gewährleisten. Die SigV macht keine Vorschriften, ob eine bestimmte Sicherheitsanforderung für die Signaturumgebung durch ein spezifisches Gerät zu erfüllen ist. Insbesondere ist aus den Anforderungen des § 4 SigV nicht ableitbar, dass eine Eingabe von Autorisierungscodes nur über Kartenleser mit PIN-Pad zulässig wäre.

Auf Wunsch kann A-SIT Produkte, die der Systemumgebung der Signaturerstellungseinheit zuzuordnen sind, gegen Kostenersatz prüfen und dafür Gutachten auf privatrechtlicher Basis

---

[1] Bundesgesetz über elektronische Signaturen (Signaturgesetz – SigG, BGBl I Nr. 190/1999 vom 19.August 1999) in der Fassung des Bundesgesetzes BGBl. I Nr. 164/2005 vom 30. Dezember 2005.
[2] Verordnung des Bundeskanzlers über elektronische Signaturen (Signaturverordnung – SigV, BGBl. II Nr. 30/2000 vom 2. Februar 2000) in der Fassung BGBl. II Nr. 527/2004 vom 30. Dezember 2004.
[3] Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen.

ausstellen, die die Eignung für sichere Signaturen feststellen. Derartige Gutachten sind Aussagen von A-SIT und keine notwendige Voraussetzung für den Einsatz dieser Produkte, die von der zuständigen Aufsichtsstelle (Telekom-Control-Kommission) auch nicht verlangt werden. Ein Gutachten könnte z.B. von einem Zertifizierungsdiensteanbieter bei der Beurteilung, ob er den Signatoren ein Produkt gem. § 20 Abs. 3 SigG als zur Anwendung bei sicheren Signaturen geeignet empfiehlt, als Absicherung herangezogen werden.

Wien, April 2006

A-SIT Zentrum für sichere Informationstechnologie – Austria