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 GEI 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
„AVA-Sign Paket“

den nachstehend genannten Anforderungen des SigG und der SigV entspricht.

Die Dokumentation zu dieser Bestätigung ist registriert unter:

T-Systems.02098.TE.10.2003

Bonn, den 20.10.2003

_____
(Dr. Heinrich Kersten)

T-Systems GEI 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)

Beschreibung der technischen Komponente:

1. Handelsbezeichnung der technischen Komponente und Lieferumfang

Handelsbezeichnung:
Signaturanwendungskomponente (SAK) „AVA-Sign Paket“

Auslieferung:
Das „AVA-Sign Paket“ wird direkt vom Hersteller an den Kunden ausgeliefert.
Der Software-Bestandteil „AVA-Sign Version 2.1“ einschl. des Online-Handbuchs (s. Lieferumfang) kann darüber hinaus auch von der Web-Site des Herstellers geladen werden.

Lieferumfang bei Direktauslieferung:
Das AVA-Sign Paket besteht aus
(1) der Software AVA-Sign Version 2.1,
(2) einem Chipkartenterminal,
(3) dem sog. Bietermodul,
(4) einer Chipkarte,
(5) der Nutzerdokumentation

Gegenstand dieser Sicherheitsbestätigung sind die Bestandteile **(1)** und **(2)** in Verbindung mit **(5)**, die zusammen die Funktionalität einer SAK bereitstellen:

Bezeichnung	**Version**	**Datum**	**Auslieferungs-name**	**Übergabeform**
AVA-Sign	2.1	12.10.2003	AVA-Sign	CD Download möglich
Benutzerhandbuch	1.18	12.10.2003	avasign_help.pdf	Papier, Datei Download möglich

Chipkartenterminal, alternativ (s. auch Abschnitt 3.2 c)):	
Hersteller	**Typbezeichnung**
Cherry	G83-6700LPZxx/00 G83-6700LQZxx/00
Kobil	Kobil Kaan Standard Plus, FW-Version 02121852 Kobil Kaan Professional, Hardware KCT100, Firmware 2.08 GK 1.04
Orga	HML 5010 und 5020, jeweils Version 1.0
Reiner	SCT CyberJack e-com, Version 2.0 SCT CyberJack pinpad, Version 2.0 SCT CyberJack, Version 3.0
SCM Microsystems	SPR532, Firmware Version 4.15

Hersteller von AVA-Sign:
ventasoft GmbH
Prenzlauer Allee 36, 10405 Berlin

2. Funktionsbeschreibung

a) Überblick

Das AVA-Sign Paket, in dem die SAK enthalten ist, ermöglicht bei öffentlichen Ausschreibungen nach VOB/A, VOL/A und VOF eine digitale Bearbeitung der Vergabeunterlagen und eine rechtsverbindliche Abgabe von Angeboten in digitaler Form einschließlich qualifizierter elektronischer Signatur und Verschlüsselung.

Das AVA-Sign Paket arbeitet mit der Plattform AVA-Online auf einem Server in der Vergabestelle und AVA-Sign Paketen anderer Bieter zusammen.

Der Bieter kann die Ausschreibungsunterlagen (Datencontainer) auf seinen lokalen Computerarbeitsplatz laden. Die Signaturanwendungskomponente ermöglicht die Entschlüsselung und die Signaturprüfung der Ausschreibungsunterlagen sowie deren Bearbeitung.

Die erstellten Angebotsunterlagen können für die Übermittlung an den AVA-Online-Server mit AVA-Sign signiert und verschlüsselt werden.

Die SAK (Bestandteile (1), (2) und (5) des AVA-Sign Pakets) hat die Aufgabe

(a) die Ausschreibungsunterlagen und die Angebotsunterlagen darzustellen,
(b) als Signaturanwendung für die Erstellung und die Prüfung qualifizierter elektronischer Unterschriften zu dienen,
(c) eine verschlüsselte Kommunikation mit der Vergabestelle zu ermöglichen, mindestens die Ausschreibungsunterlagen zu entschlüsseln und die Angebotsunterlagen zu verschlüsseln.

Darüber hinaus stellt die SAK die Bearbeitungswerkzeuge für die Angebotsunterlagen bereit.

Das Chipkartenterminal hat die Aufgabe,

(a) die Kommunikationsschnittstelle zwischen dem PC und der Chipkarte bereitzustellen, insbesondere zur Übergabe der zu signierenden Daten vom PC an die Chipkarte und der digitalen Signatur von der Chipkarte an den PC,
(b) als Eingabeschnittstelle des Benutzers die Authentisierungsdaten (PIN) entgegenzunehmen und an die Chipkarte weiterzuleiten.

Das Bietermodul ist ein selbständiges Programm zur Darstellung und Bearbeitung von Leistungsverzeichnissen und Angeboten in den durch den *Gemeinsamen Ausschuss Elektronik im Bauwesen* (GAEB) definierten Formaten GAEB-D83 und GAEB-D84. Das Bietermodul stellt **keine** Sicherheitsfunktionen zur Verfügung.

Die Chipkarte hat als sichere Signaturerstellungseinheit die Aufgabe
(1) die Signaturerstellungsdaten (privater Schlüssel) zu speichern,
(2) digitale Signaturen zu den vom Chipkartenterminal übergebenen Daten zu erzeugen und an das Chipkartenterminal zu übergeben,
(3) die Authentisierungsdaten des Kartenhalters zu prüfen und die dafür benötigten Referenzdaten zu speichern und zu wechseln.

AVA-Sign Software kann mit folgenden nach SigG bestätigten Signaturerstellungseinheiten zusammenarbeiten:

- DATEV e:secure-Card V1.0,
- D-TRUST-CARD, Version 1.0,

- Signtrust SEA – Karte, Version 2.0
- STARCOS SPK2.3 with Digital Signature Application StarCert
- T-Telesec PKS – Card, Version 2.0, 3.0,
- T-Telesec E4Netkey – Karte, Version 3.0

b) Funktionalität nach SigG

Die SAK prüft qualifizierte elektronische Signaturen und zeigt nach jeder Prüfung an,

- auf welche Dateien innerhalb des Datencontainers sich die Signatur bezieht,
- ob die Dateien insgesamt unverändert sind,
- welchem Signaturschlüssel-Inhaber die Signatur zuzuordnen ist,
- welchen Inhalt das qualifizierte Zertifikat und ggf. zugehörige qualifizierte Attribut-Zertifikate besitzen,
- ob die nachgeprüften qualifizierten Zertifikate im jeweiligen Zertifikatverzeichnis zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren,
- ob die Signaturprüfung korrekt durchgeführt werden konnte.

Eine Online-Prüfung der Zertifikate in den Verzeichnisdiensten erfolgt auf Anforderung des Benutzers. Der öffentliche Schlüssel der RegTP ist in der SAK fest kodiert.

Die SAK unterstützt die Erstellung qualifizierter elektronischer Signaturen und leistet dabei

- die Zusammenstellung der Dateien des Datencontainers
- die Anzeige, auf welche Dateien sich die zu erstellende Signatur bezieht,
- bei Bedarf die sichere Anzeige der zu signierenden Datei,
- die Berechnung des Hashwerts und Übertragung an das Terminal,
- die Aufforderung zur Authentisierung am Chipkartenterminal,
- die eindeutige Anzeige der Erzeugung der Signatur durch die Chipkarte,
- nach Erhalt der Signatur die Überprüfung, ob der Hashwert ggf. manipuliert wurde,
- die geeignete Speicherung der signierten Datei bzw. des Datencontainers.

Im Lieferumfang ist ein Prüfprogramm enthalten, mit dem die Integrität der AVA-Sign Software Module bei der Installation und im späteren Betrieb verifiziert werden kann. Das Programm (ausgeliefert auf CD bzw. per Download mit Signatur) „kennt“ die Signaturen aller Module und vergleicht sie mit den jeweils berechneten Signaturen.

3. Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Die Signaturanwendungskomponente „AVA-Sign Paket“ erfüllt in Verbindung mit den Einsatzbedingungen die folgenden Anforderungen:

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

Das Bietermodul, die Chipkarten und die Vergabeplattform AVA-Online sind **nicht** Gegenstand dieser Sicherheitsbestätigung.

3.2 Einsatzbedingungen

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

a) Technische Einsatzbedingungen

Die SAK wird in einem geschützten Einsatzbereich eingesetzt, an den folgende Anforderungen zu stellen sind:

- Der PC, auf dem das AVA-Sign Paket eingesetzt wird, läuft unter Microsoft Windows 2000 oder Windows XP.
- Der PC ist vor unbefugten Zugriffen (Internet/ Intranet) durch geeignete Maßnahmen (Personal Firewall, Virenscanner mit aktuellen Virensignaturen) zu schützen.
- Der PC ist vor manuellen Zugriffen Unbefugter und Manipulationen über Datenaustausch per Datenträger zu schützen.

Anmerkungen:

AVA-Sign läuft auf allen Microsoft Windows Betriebssystemen ab Windows 98; jedoch fällt **nur** der Betrieb mit Windows 2000 und Windows XP unter diese Sicherheitsbestätigung.

b) Installation und Nutzung der SAK

Die Installation der Software hat durch einen System-Administrator zu erfolgen, der das im Handbuch detailliert beschriebene Verfahren einhält – insbesondere:

- Die Integrität der Software-Komponenten ist nach der Auslieferung bzw. bei der Installation sowie regelmäßig im Betrieb zu prüfen.
- Für die Nutzung der SAK bzw. des gesamten AVA-Sign Pakets ist unter den zulässigen Betriebssystemen ein normaler User Account (ohne Administratorrechte) mit Passwort einzurichten.

Für die Nutzung gilt:

- Während des Signaturvorganges sollte der PC nicht mit dem Internet / Intranet verbunden sein.
- Alle in der Benutzerdokumentation des AVA-Sign Pakets beschriebenen Sicherheitshinweise sind zu beachten und die entsprechenden Vorgaben einzuhalten.

c) Sonstiges

AVA-Sign Version 2.1 unterstützt funktional auch Terminals ohne sichere PIN-Eingabe. Es wird darauf hingewiesen, dass der Betrieb mit solchen Terminals **nicht** als „sicherheitsbestätigt“ gilt.

Bezieht der Nutzer den Kartenleser nicht über den Hersteller ventasoft als Teil des AVA-Sign Pakets, muss sichergestellt werden, dass der Kartenleser entsprechend SigG sicherheitsbestätigt ist; in Zweifelsfällen ist der Hersteller zu kontaktieren; beim verschiedentlich angebotenen Firmware-Update für Kartenleser ist darauf zu achten, dass nur auf solche Firmware-Versionen aktualisiert wird, die unter die entsprechende Sicherheitsbestätigung fallen.

Laut Herstellerangaben konnten die D-TRUST und STARCOS Signaturkarten mit dem „Kobil Kaan Standard Plus“ Kartenleser nicht unter Windows 2000 getestet werden. Daher fallen diese Kombinationen **nicht** unter diese Sicherheitsbestätigung.

3.3 Algorithmen und zugehörige Parameter

Im Rahmen der Signaturprüfung und –erstellung werden die Hashverfahren SHA-1 und RIPEMD-160 bereitgestellt. Die gemäß § 11 Abs. 3 in Verbindung mit Anlage I Nr. 2 SigV festgestellte Eignung reicht mindestens bis Ende des Jahres 2008.

Die Signaturprüfung verwendet RSA-1024. Die gemäß § 11 Abs. 3 in Verbindung mit Anlage I Nr. 2 SigV festgestellte Eignung reicht mindestens bis Ende des Jahres 2007.

Diese Sicherheitsbestätigung ist somit gültig bis zum 31.12.2007; 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 Software „AVA-Sign Version 2.1“ wurde erfolgreich nach der Prüfstufe **E2** der ITSEC evaluiert. Die eingesetzten Sicherheitsmechanismen erreichen die Stärke **hoch**. Hierfür liegt das „Deutsche IT-Sicherheitszertifikat“ T-Systems-DSZ-ITSEC-04097-2003 vom 20.10.2003 vor.

Bei allen im Lieferumfang des AVA-Sign Pakets (alternativ) enthaltenen Chipkartenterminals handelt es sich um nach SigG **sicherheitsbestätigte** Systeme, die (mindestens) nach E2, hoch (ITSEC) bzw. EAL3+, SOF-hoch (Common Criteria) evaluiert worden sind: s. Angaben unter www.regtp.de.

Die sicherheitstechnisch korrekte Integration von AVA-Sign Version 2.1 mit den im Lieferumfang genannten Chipkartenterminals (s. 2 Ausnahmen unter 3.2 c)) wurde durch entsprechende Tests verifiziert.

Ende der Bestätigung