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 ISS GmbH
- Zertifizierungsstelle -

Rabinstr. 8, 53111 Bonn

bestätigt hiermit gemäß
§§ 15 Abs. 7 S. 1, 17 Abs. 1 SigG sowie §§ 15 Abs. 1 und 4, § 11 Abs. 3 SigV,
dass die

Signaturerstellungseinheit „Chipkarte mit Prozessor SLE66CX322P, Betriebssystem CardOS/M4.01A mit Applikation für digitale Signatur“

den nachstehend genannten Anforderungen des SigG und der SigV entspricht.

Die Dokumentation zu dieser Bestätigung ist registriert unter:

T-Systems.02085.TE.09.2002

Bonn, den 01.10.2002

(Dr. Heinrich Kersten)

T-Systems ISS 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)

Die Bestätigung zur Registrierungsnummer T-Systems. 02085.TE.09.2002 besteht aus 9 Seiten.

Beschreibung der technischen Komponente:

1 Handelsbezeichnung der technischen Komponente und Lieferumfang:

Handelsbezeichnung: Signaturerstellungseinheit „Chipkarte mit Prozessor SLE66CX322P, Betriebssystem CardOS/M4.01A mit Applikation für digitale Signatur“

Auslieferung: Auslieferung an Zertifizierungsdiensteanbieter (ZDA) durch Kurier mit folgendem Lieferumfang:

Art	**Gegenstand**	**Version**	**Datum**	**Art der Auslieferung**
Hardware	Prozessor Infineon SLE66CX322P (Chip Identifier 6C, Production Line Number 2)	-	-	Chipkarte
Software (Operating System)	CardOS M4.01A	C804	17.05.2002	Geladen in ROM / EEPROM
Software Personalisierungs-sequenzen: (Application / Data Structure)	PersAppSigG.csf VorPersAppSigG.csf NachPersAppSigG.csf	2.10 2.10 2.10	29.07.2002 29.07.2002 29.07.2002	auf Diskette
Software Personalisierungs-sequenz	StartKey_0 to StartKey_1.csf	Wird mit ZDA jeweils individuell vereinbart		auf Diskette
Software Personalisierungs-sequenz (Service Pack)	M401a_Service Pack_SigG.csf	5.0	26.07.2002	auf Diskette
Dokumentation	Applikation SigG	1.0	04.10.2001	Papier oder PDF-Datei
Dokumentation	Applikation SigG	2.0	19.06.2002	Papier oder PDF-Datei
Dokumentation	CardOS/M4 User’s Manual	1.0	10/2001	Papier oder PDF-Datei
Dokumentation	CardOS/M4 User’s Manual - correction sheet	2.0	06/2002	Papier oder PDF-Datei
Dokumentation	CardOS/M4.01 Benutzerdokumentation für Kartenhalter	1.02	27.02.2002	Papier oder PDF-Datei
Dokumentation	CardOS/M4.01A Benutzerdokumentation für Kartenhalter	2.1	08.07.2002	Papier oder PDF-Datei
Dokumentation	CardOS/M4.01 Benutzerdokumentation für Terminalentwickler	1.12	27.02.2002	Papier oder PDF-Datei

Art	Gegenstand	Version	Datum	Art der Auslieferung
Dokumentation	CardOS/M4.01A Benutzerdokumentation für Terminalentwickler	2.0	17.06.2002	Papier oder PDF-Datei
Dokumentation	CardOS/M4.01 Dokumentation für Trust Center	1.02	27.02.2002	Papier oder PDF-Datei
Dokumentation	CardOS/M4.01A Dokumentation für Trust Center	2.0	17.06.2002	Papier oder PDF-Datei
Dokumentation	CardOS/M4.01 Auslieferung, Generierung und Konfiguration	1.1	18.12.2001	Papier oder PDF-Datei
Dokumentation	CardOS/M4.01A Auslieferung, Generierung und Konfiguration	2.0	17.06.2002	Papier oder PDF-Datei

Hersteller:
Siemens AG
ICN EN TNA
Charles de Gaulle-Straße 2-4
81737 München

2 Funktionsbeschreibung[3]

Die Komponente ist eine Signaturerstellungseinheit bestehend aus dem Prozessorchip Infineon SLE66CX322P und der Software „CardOS/M4.01A mit Applikation für digitale Signatur“.

CardOS/M4.01A ist ein multifunktionales Smart Card Betriebssystem, das aktiven und passiven Datenschutz unterstützt und entwickelt wurde, um höchsten Sicherheitsanforderungen zu genügen.

CardOS/M4.01A ist auf dem Infineon SLE66CX322P Chip implementiert. Dieser Chip besitzt einen eingebetteten Security Controller für asymmetrische Kryptographie und einen echten Zufallszahlengenerator.

CardOS/M4.01A mit **Applikation für Digitale Signatur** wurde entwickelt, um den Anforderungen des Signaturgesetzes zu genügen.

Das für die elektronische Signatur erforderliche Schlüsselpaar wird bei der **Personalisierung** bei einem beliebigen autorisierten Zertifizierungsdiensteanbieter auf der Smart Card im DF SigG generiert. Der **öffentliche** Schlüssel wird beim Zertifizierungsdiensteanbieter ausgelesen und zur Erstellung des Kartenhalterzertifikats verwendet. Der **private** Signaturschlüssel kann **nicht** ausgelesen werden. Er kann nur

[3] Die nachfolgende Beschreibung ist vom Hersteller bereitgestellt und von der Bestätigungsstelle nur geringfügig an die Nomenklatur des Signaturgesetzes angepaßt worden.

nach Authentisierung mit der Signatur-PIN vom **Kartenhalter** zur Erstellung jeweils **einer qualifizierten elektronischen Signatur** verwendet werden.
Die Applikation **Digitale Signatur** ist **nur** für die Erzeugung digitaler Signaturen entwickelt worden.

Neben der vorgegebenen Applikation „SigG“ können jedoch beliebige weitere Applikationen auf die Karte personalisiert werden, die alle Eigenschaften des Betriebssystems nützen können.

Generelle Eigenschaften von CardOS/M4.01A:
- Schutz gegen alle derzeit bekannten Sicherheitsattacken,
- alle Kommandos entsprechen den ISO 7816-4, -8 und -9 Standards,
- PC/SC- und CT-API fähig,
- klar strukturierte Sicherheitsarchitektur und einwandfreies Schlüsselmanagement.
- Kunden- und anwendungsabhängige Konfigurierbarkeit der Kartendienste und -kommandos
- Erweiterbarkeit des Betriebssystems durch ladbare Software-Komponenten

Das Dateisystem:
CardOS/M4.01A bietet ein dynamisches und flexibles Dateisystem, das durch Chip-spezifische kryptographische Mechanismen geschützt wird:
- beliebige Anzahl von Dateien (EFs, DFs),
- Schachtelungstiefe von DFs nur durch Speichergröße begrenzt,
- dynamisches Speicher Management für optimale Ausnutzung des verfügbaren EEPROMs,
- Schutz gegen EEPROM Defekte und Spannungsverlust.

Zugriffskontrolle:
- bis zu 126 verschiedene vom Programmierer definierbare Zugriffsrechte,
- Zugriffsrechte können mit beliebigen Booleschen Ausdrücken kombiniert werden,
- jedes Kommando oder Daten-Objekt kann mit eigenen Zugriffsschemata geschützt werden,
- alle sogenannten Schlüsselobjekte sind im zugehörigen DF gespeichert,
- die Sicherheitsstruktur kann ohne Datenverlust nach dem Anlegen von Dateien noch inkrementell verfeinert werden.

Kryptographische Dienste:
- Algorithmen: RSA 1024 Bit (PKCS#1), SHA-1, Triple-DES (CBC), DES (ECB, CBC), MAC, Retail-MAC,
- Schutz gegen Differential Fault Analysis (”Bellcore-Attack”),
- Schutz von DES und RSA gegen Simple Power Analysis and Differential Power Analysis,
- Unterstützung von ”Command Chaining” nach ISO 7816-8,
- Generierung asymmetrischer Schlüssel unter Verwendung des echten “onboard” Zufallszahlengenerators,
- digitale Signaturfunktionen “on chip”,
- Anschlussfähigkeit an externe Public Key Zertifizierungsdienste.

Secure Messaging:
- kompatibel mit ISO 7816-4,
- kann für jedes Kommando und jedes Datenobjekt unabhängig definiert werden.

3 Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Die Signaturerstellungseinheit „Chipkarte mit Prozessor SLE66CX322P, Betriebssystem CardOS/M4.01A mit Applikation für digitale Signatur“ erfüllt die folgenden Anforderungen:

- §15 Abs. 1 S. 1 SigV
- §15 Abs. 1 S. 2 SigV
- §15 Abs. 1 S. 4 SigV
- §15 Abs. 4 SigV

Diese Anforderungen werden durch die Signaturerstellungseinheit unter den angegebenen Einsatzbedingungen 3.2 und unter Beachtung der nachfolgenden Restriktionen erfüllt.

1. Ohne Re-Evaluierung und erneute Sicherheitsbestätigung ist es nicht zulässig,
   - eine Änderung oder Erweiterung der sicherheitsbestätigten Applikation „Digitale Signatur“ vorzunehmen, oder
   - zusätzliche Packages zum Ändern oder Erweitern von CardOS/M4.01A auf der sicherheitsbestätigten Karte einzubringen.
2. Die in Kapitel 2 aufgeführten Algorithmen Triple-DES (CBC), DES (ECB, CBC), MAC, Retail-MAC kommen bei der elektronischen Signatur nicht zur Anwendung und sind deshalb auch nicht Gegenstand der Sicherheitsbestätigung.
3. In der Dokumentation „Applikation SigG 2.0“ vom 19.06.2002 werden die Personalisierungsskripte PersAppSigG.csf, VorPersAppSigG.csf und NachPersAppSigG.csf mit älteren Versionsnummern referenziert; maßgebend für die vorliegende Sicherheitsbestätigung sind jedoch die in der Tabelle in Kapitel 1 aufgeführten Skripte mit der Versionsnummer 2.10, die zum Lieferumfang der Signaturerstellungseinheit gehören.

3.2 Einsatzbedingungen

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

a) Personalisierung und technische Einsatzumgebung

Die dieser Bestätigung zugrunde liegende Prüfung von „CardOS/M4.01A mit Applikation für digitale Signatur“ ist in Verbindung mit dem Prozessor SLE66CX322P der Firma Infineon durchgeführt worden, und zwar für Prozessoren, deren Chip Type Identifier ‘6C’ (hexadezimal) ist und die in der Production Line Number “2” (für Dresden) hergestellt wurde: Die Bestätigung ist deshalb zunächst **nur für diese Prozessoren** gültig.
Bevor diese Sicherheitsbestätigung auf einen anderen Prozessorchip erweitert werden kann, ist eine Re-Evaluierung notwendig.

Die Signaturerstellungseinheit basiert auf der ROM-Maske Version C804 (CardOS/M4.01A); diese ist identisch für alle Konfigurationen (s. Abschnitt b) der Signaturerstellungseinheit. Ebenfalls identisch für alle Konfigurationen ist das Grundgerüst

der Signaturapplikation. Ferner wird während des Personalisierungsvorgangs ein Service Package auf die Signaturerstellungseinheit geladen; auch dieses ist für alle Konfigurationen identisch.

Der Zertifizierungsdiensteanbieter (ZDA) muss in seinem Sicherheitskonzept alle Maßnahmen beschreiben, die für eine sichere Personalisierung erforderlich sind.
Von den Abläufen der Komplettierung, Initialisierung und Personalisierung, beschrieben in den Dokumenten *CardOS/M4.01 Auslieferung, Generierung und Konfiguration*, *CardOS/M4.01**A** Auslieferung, Generierung und Konfiguration*, *CardOS/M4.01 Dokumentation für Trust Center* und *CardOS/M4.01**A** Dokumentation für Trust Center*, darf nicht abgewichen werden. Diese Abläufe schließen Bedienfehler aus und müssen Bestandteil des Sicherheitskonzepts der Zertifizierungsdiensteanbieter sein.

Die Personalisierung kann zentral oder dezentral erfolgen.

- Im zentralen Fall erfolgt die Personalisierung vollständig beim Zertifizierungsdiensteanbieter; dabei kommt das Personalisierungsscript für die zentrale Personalisierung zum Einsatz.
- Im dezentralen Fall erfolgt eine sogenannte Vorpersonalisierung zentral beim Zertifizierungsdiensteanbieter mit Hilfe des Vorpersonalisierungsscripts.
  Anschließend vollendet eine dezentrale Registrierungsstelle (als ausgelagerte Einheit des ZDA) die Personalisierung; diese sogenannte Nachpersonalisierung wird mit Hilfe des Nachpersonalisierungsscripts ausgeführt.

Die Personalisierungsscripte dürfen nur an den durch Kommentare kenntlich gemachten Stellen im Sinne der Kommentare angepasst werden.

Die Signaturerstellungseinheit verfügt nicht über eine benutzerlesbare Schnittstelle. Sie muss daher zusammen mit einer geeigneten gesetzeskonformen Signaturanwendungskomponente genutzt werden.

b) Auslieferung und Konfigurationen der Signaturerstellungseinheit

Die Signaturerstellungseinheit „Chipkarte mit Prozessor SLE66CX322P, Betriebssystem CardOS/M4.01A mit Applikation für digitale Signatur“ wird vom Hersteller gemäß Abschnitt 1 an Zertifizierungsdiensteanbieter ausgeliefert. Das spezifizierte Auslieferungsverfahren ist einzuhalten.

Die Signaturerstellungseinheit hat zwei unterschiedliche Konfigurationen:

- Die personenbezogene Signaturerstellungseinheit, die für Endkunden (Kartenhalter) bestimmt ist, erlaubt nach Authentisierung mittels PIN die Erzeugung genau einer elektronischen Signatur. Diese Konfiguration wird kurz mit „**n = 1**“ bezeichnet.
- Gegenstand dieser Bestätigung sind auch „Signaturmodule“, die zum Einsatz in speziell gesicherten Umgebungen (z.B. beim ZDA) bestimmt sind und die nach einmaliger PIN-Authentisierung die Generierung von mehreren oder unendlich vielen Signaturen erlauben. Diese Konfigurationen werden kurz mit „**n** ^{1} **1**“ bezeichnet.

Die Bezeichnung lehnt sich an den technischen Parameter n an, über den dieses Verhalten gesteuert wird. In den Fällen n = 0 und n = 255 können nach einmaliger PIN-Authentisierung unendlich viele Signaturen erzeugt werden, in allen anderen

erlaubten Fällen ($1 \leq n \leq 254$) können genau n Signaturen erzeugt werden. Um ein Signaturmodul zu erstellen, ist eine Anpassung der Personalisierung erforderlich. Die Personalisierungsstellen werden über das anzuwendende Vorgehen informiert und zu besonderer Sorgfalt verpflichtet. Beide Konfigurationen „**n = 1**“ und „**n ¹ 1**“ fallen unter diese Sicherheitsbestätigung.

Die Signaturerstellungseinheit "Chipkarte mit Prozessor SLE66CX322P, Betriebssystem CardOS/M4.01A mit Applikation für digitale Signatur" verfügt über einen PUK (Personal Unblocking Key) mit folgender Funktionalität:

- Bei richtiger Eingabe des PUK kann der Wert der PIN neu gesetzt werden.
- Die richtige Eingabe des PUK ermöglicht keine Signaturerzeugung.

Der PUK darf nur dann verwendet werden, wenn der Zertifizierungsdiensteanbieter sicherstellt, dass die unter Abschnitt 3.2 c) genannten Voraussetzungen erfüllt sind.

Anwendungen, die die Signaturerstellungseinheit „Chipkarte mit Prozessor SLE66CX322P, Betriebssystem CardOS/M4.01A mit Applikation für digitale Signatur“ nutzen, sind **nicht** Gegenstand dieser Bestätigung.

c) Nutzung des Produktes

Während des Betriebes sind die folgenden Bedingungen für den sachgemäßen Einsatz zu beachten:

Anforderungen an den Zertifizierungsdiensteanbieter

- Die Erzeugung des für die Signaturanwendung benötigten Schlüsselpaares auf einer personenbezogenen Signaturerstellungseinheit („**n = 1**“) darf nur in einer besonders gesicherten Umgebung (z. B. bei einem akkreditierten ZDA) erfolgen.
- Die Erzeugung des für die Signaturanwendung benötigten Schlüsselpaares auf einem Signaturmodul („**n ¹ 1**“) darf nur unter Einhaltung besonderer Sicherheitsvorkehrungen (z.B. unter behördlicher Aufsicht) erfolgen.
- Die Konfiguration „**n ¹ 1**“ darf nur in besonders gesicherten Einsatzumgebungen betrieben werden, in denen ein Mißbrauch der Signaturerstellungsfunktion sicher auszuschließen ist. Eine solche Einsatzumgebung liegt typischerweise bei einem akkreditierten ZDA vor.
- Bei Signaturmodulen (Konfiguration „**n ¹ 1**“), die nach einmaliger Authentisierung die Erzeugung einer unbegrenzten Anzahl von elektronischen Signaturen ohne erneute Authentisierung gestatten (n = 0 oder n = 255), kann eine Begrenzung dieser Anzahl mittelbar über die Parameter "Zeit" oder "Anzahl" durch eine geeignete gesetzeskonforme Signaturanwendungskomponente erfolgen, sofern sichergestellt ist, daß eine erneute Authentisierung stets durch den Signaturschlüsselinhaber (und nicht automatisiert durch die Anwendung) erfolgt. Dabei muss eindeutig die willentliche Erklärung des Signaturschlüsselinhabers zur Signaturerzeugung erkennbar sein.
- Zum Einsatz in besonders gesicherter Umgebung bestimmte Signaturmodule (Konfiguration „**n ¹ 1**“) dürfen nicht als personenbezogene Signaturerstellungseinheiten an Endkunden (Kartenhalter) ausgeliefert werden. Es ist die Aufgabe der Zertifizierungsdiensteanbieter, dies sicherzustellen.
- i) Die Einbringung der Identifikationsdaten (PIN und PUK) in die Signaturerstellungseinheit während der Personalisierung hat so zu erfolgen, dass die Identifikationsdaten anschließend nicht außerhalb der Signaturerstellungseinheit gespeichert sind.

- ii) In seinem Sicherheitskonzept hat der Zertifizierungsdiensteanbieter ein Verfahren zur Übergabe und Nutzung der Identifikationsdaten an den bzw. durch den Signaturschlüsselinhaber vorzusehen, das keine Speicherung der Identifikationsdaten außerhalb der Signaturerstellungseinheit vorsieht.
- Die vom Zertifizierungsdiensteanbieter für i) und ii) vorgesehenen Verfahren müssen auf ihre Sicherheit hin geprüft sein und es muss bestätigt sein, dass sie die Anforderungen des SigG und der SigV erfüllen. Die Verfahren sind vor ihrer erstmaligen Nutzung der Regulierungsbehörde für Telekommunikation und Post (RegTP) explizit zur Zustimmung vorzulegen.

Mit Auslieferung der Signaturerstellungseinheit „Chipkarte mit Prozessor SLE66CX322P, Betriebssystem CardOS/M4.01A mit Applikation für digitale Signatur“ an den ZDA ist dieser auf die Einhaltung der oben genannten Einsatzbedingungen hinzuweisen.

Allgemeine Anforderungen an den Endanwender

- Der Signaturschlüsselinhaber muss die Signaturerstellungseinheit so benutzen und aufbewahren, daß Mißbrauch und Manipulation vorgebeugt wird.
- Der Signaturschlüsselinhaber benutzt die Signaturerzeugungsfunktion nur für solche Daten, deren Integrität oder Authentizität er sicherstellen will.
- Der Signaturschlüsselinhaber hält seine Identifikationsdaten für die Signaturerstellungseinheit geheim.
- Der Signaturschlüsselinhaber ändert seine Identifikationsdaten für die Signaturerstellungseinheit in regelmäßigen Abständen.
- Der Signaturschlüsselinhaber verwendet die Signaturerstellungseinheit nur in Verbindung mit einer gesetzeskonformen Signaturanwendungskomponente.

3.3 Algorithmen und zugehörige Parameter

Von der Signaturerstellungseinheit werden der Hash-Algorithmus SHA-1 und der Algorithmus RSA bereitgestellt.

Die gemäß § 11 Abs. 3 in Verbindung mit Anlage I Nr. 2 SigV festgestellte Eignung reicht (mindestens) bis zum 31.12. 2006 (s. Bundesanzeiger Nr. 158 – Seite 18 562 vom 24. August 2001).

Diese Sicherheitsbestätigung ist somit **gültig bis zum 31.12.2006**; 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 „CardOS/M4.01A mit Applikation für digitale Signatur“ wurde auf dem Prozessor SLE66CX322P erfolgreich nach der Prüfstufe **E4** der ITSEC evaluiert. Die eingesetzten Sicherheitsmechanismen erreichten dabei die Mindeststärke „**hoch**“.

Der Prozessor SLE66CX322P wurde erfolgreich nach den Common Criteria gemäß der Stufe **EAL5+** (mit den Erweiterungen ALC_DVS.2, AVA_MSU.3 und AVA_VLA.4.) evaluiert. Die erforderlichen Sicherheitsfunktionen erreichten dabei die Stärke „**hoch**“.

Hierfür liegt das Deutsche IT-Sicherheitszertifikat BSI-DSZ-CC-0169-2002 vom 07. Mai 2002 vor.

Die sicherheitstechnisch korrekte Integration von „CardOS/M4.01A mit Applikation für digitale Signatur“ und des Prozessors SLE66CX322P wurde überprüft.

Die für die Signaturerstellungseinheit nach SigV maßgebende Evaluierungsstufe **E3** bzw. **EAL4+** (mit den erforderlichen Erweiterungen) und die Funktions-/ Mechanismenstärke „**hoch**“ sind damit erreicht (und in Teilen übertroffen).

Ende der Bestätigung