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. 1 SigG sowie §§ 15 Abs. 1 und 4, § 11 Abs. 3 SigV,
dass die

Signaturerstellungseinheit
Chipkarte mit Prozessor SLE 66CX320P,
Betriebssystem SetCOS 4.4.1 mit Signaturapplikation
„SetEID v1.0“ in SigG-Konfiguration A, B und C[3]

den nachstehend genannten Anforderungen des SigG und der SigV entspricht.

Die Dokumentation zu dieser Bestätigung ist registriert unter:

T-Systems.02017.TE.07.2003

Bonn, den 25.07.2003 _____
(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)

3 Die SigG-Konfigurationen A, B und C sind im Text erläutert.

Die Bestätigung zur Registrierungsnummer T-Systems.02017.TE.07.2003 besteht aus 7 Seiten

Beschreibung der technischen Komponente:

1. Handelsbezeichnung der technischen Komponente und Lieferumfang

Handelsbezeichnung:
Signaturerstellungseinheit Chipkarte mit Prozessor SLE 66CX320P, Betriebssystem SetCOS 4.4.1 mit Signaturapplikation „SetEID v1.0“, nachfolgend Signaturerstellungseinheit (SEE) genannt

Auslieferung:
Die Auslieferung erfolgt vom Kartenhersteller (Setec Oy) an den Zertifizierungsdiensteanbieter durch persönliche Übergabe.

Lieferumfang:

Bezeichnung	Art	Version	Datum
Hardware	Prozessor Infineon SLE 66CX320P	-	-
SetCOS 4.4.1	SW (im ICC ROM)	1.1	3.12.2002
rev A.2 extension for SetCOS 4.4.1	SW (im ICC EEPROM)	A2	12.11.2002
SigG signature application	ICC Anwendungs-daten (im ICC EEPROM)	1.1	24.6.2003
Infineon RMS+ Resource management system	Firmware	0.6	04/2000
Setec Signature Card SetEID v1.0, Signature application	Dokument	1.1	24.6.2003
SetCOS 4.4.1, Initialisation details	Dokument	1.0	8.4.2003
Setec Signature Card SetEID v1.0, Personalisation of the signature application	Dokument	1.2	1.7.2003
Setec Signature Card SetEID v1.0, Guidance documentation	Dokument	0.35	1.7.2003
SetCOS User's Guide Part 1, Overview	Dokument	1.2	15.10.1999
SetCOS User's Guide Part 2, SetCOS 4.x series	Dokument	1.3	28.4.2003
SetCOS User's Guide Part 3, SetCOS 4.4.1	Dokument	1.5	11.11.2002

Hersteller:
Setec Oy
Suometsäntie 1, FIN-01740 Vantaa, Finnland

2. Funktionsbeschreibung

Die Komponente Chipkarte mit Prozessor SLE 66CX320P, Betriebssystem SetCOS 4.4.1 mit Signaturapplikation „SetEID v1.0“ in Sig-Konfiguration A, B und C (nachfolgend sichere

Signaturerstellungseinheit oder SSEE genannt) ist ein bestätigtes Produkt nach §2 Nr. 10 SigG mit Erzeugung des Signaturschlüsselpaares auf der Karte.

Die SEE ist eine Kombination aus einem Prozessor SLE 66CX320P, dem Betriebssystem SetCOS 4.4.1 und der Signaturapplikation „SetEID v1.0“, die in dem Prozessorchip ausgeführt werden bzw. gespeichert sind. Diese Kombination stellt eine Anwendung zur Erzeugung elektronischer Signaturen nach dem Gesetz über die Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG) zur Verfügung.
Die Software der Komponente (SetCOS 4.4.1 rev A.2) ist ein multifunktionales Betriebssystem mit hierarchischem Dateisystem. Sie unterstützt dynamisches Dateisystemmanagement, symmetrische und asymmetrische kryptographische Operationen, Benutzerauthentisierung und eine flexible Zugriffskontrolle für die Dateien. Die Schnittstelle zum Prozessorchip unterstützt die ISO Standards 7816-3, 7816-4, 7816-5, 7816-6, 7816-8 und DIN 66391-1.
SetCOS 4.4.1 rev A.2 ist vorgesehen für die Nutzung durch Applikationen, die Public Key Kryptographie anwenden. Insbesondere kann es als Basis für eine Signaturerstellungseinheit entsprechend dem oben genannten SigG verwendet werden. Es unterstützt den asymmetrischen RSA-Kryptoalgorithmus mit Schlüssellängen bis zu 1024 Bit und den symmetrischen DES-3 (triple-DES) Kryptoalgorithmus mit 128 Bit langen Schlüsseln (112 Bit effektiv).
Die auf SetCOS 4.4.1 rev A.2 aufsetzende Applikation (SigG-Signaturanwendung) folgt der im Standard DIN 66391-1 beschriebenen Dateistruktur. Sie stellt dem Kartenhalter einen PIN-Wert und einen privaten Signaturschlüssel zur Verfügung. Gegenseitige Authentisierung mit einem Terminal wird nicht unterstützt.

3. Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Die SSEE 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**

Die oben genannten Anforderungen werden durch die SSEE in der im Abschnitt 3.2 beschriebenen Einsatzumgebung erfüllt. Zusätzlich gelten die folgenden Bestimmungen:

1. Ohne Reevaluierung und erneute Sicherheitsbestätigung ist es nicht erlaubt,
   - die SigG-Signaturanwendung zu ändern oder zu erweitern,
   - zusätzliche packages/patches, die das Betriebssystem SetCOS 4.4.1 ändern oder erweitern, in die SSEE zu laden.
2. Der symmetrische Kryptoalgorithmus DES-3 (triple-DES) wird zur Erzeugung elektronischer Signaturen nicht angewendet und ist deshalb nicht Gegenstand dieser Sicherheitsbestätigung.

3.2 Einsatzbedingungen

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

a) Technische Einsatzumgebung

Die SSEE wurde evaluiert auf der Basis der folgenden Hard- und Softwarekonfiguration:
Die durchgeführte Evaluierung der SSEE basiert auf dem Prozessorchip SLE 66CX320P der Infineon Technolohies AG. Diese Sicherheitsbestätigung ist **nur für diesen Prozessorchip** gültig. Bevor diese Sicherheitsbestätigung auf einen anderen Prozessorchip erweitert werden kann, ist eine Reevaluierung notwendig.

Die SSEE basiert auf den Images COS441.hex für die ROM-Maske und EEPRM441.hex für den EEPROM. Diese Masken sind identisch für alle Konfigurationen der SSEE.

Die Personalisierung der SSEE kann zentral oder dezentral erfolgen.

- Die zentrale Personalisierung erfolgt beim Kartenhersteller, der dabei als Teil des Zertifizierungsdiensteanbieters agiert und daher allen zutreffenden Regularien des entsprechenden Sicherheitskonzeptes folgen muss.
- Im Fall der dezentralen Personalisierung liefert der Kartenhersteller eine initialisierte Signaturerstellungseinheit an den Zertifizierungsdiensteanbieter, der für die Auswahl der Konfigurationen A, B oder C verantwortlich ist. In seinem Sicherheitskonzept muss der Zertifizierungsdiensteanbieter alle relevanten Sicherheitsaspekte der Personalisierung beschreiben.

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

b) Einbindung in die Softwareumgebung, Konfiguration

Die SSEE ist durch folgende Parameterwerte charakterisiert:

Konfiguration	Parameter	Wert
A	PUK-Benutzungszähler	Conf_GerLaw
	WearCycle	WearCycle_single (WearCycle=1)
	Authenticated_by_unblocking	Authenticated_by_unblocking_no
	Authenticated_by_changing	Authenticated_by_changing_no
B	PUK-Benutzungszähler	Conf_GerLaw
	WearCycle	WearCycle_policy (2£ WearCycle£ 6)
	Authenticated_by_unblocking	Authenticated_by_unblocking_no
	Authenticated_by_changing	Authenticated_by_changing_no
C	PUK-Benutzungszähler	Conf_GerLaw
	WearCycle	WearCycle_policy (WearCycle=0)
	Authenticated_by_unblocking	Authenticated_by_unblocking_no
	Authenticated_by_changing	Authenticated_by_changing_no

Tabelle 1: Die drei sicherheitsbestätigten Konfigurationen der SEE

In der SSEE kann der PUK-Mechanismus **nicht** benutzt werden.

Die SSEE stellt einen Initial-PIN-Mechanismus zur Verfügung. Im Auslieferungszustand berechtigt die Initial-PIN nicht zur Erzeugung einer elektronischen Signatur. Der Signaturschlüsselinhaber ist gehalten, sich einen neuen PIN-Wert zu erzeugen. Authentisierung mit dieser neuen PIN erlaubt dann die Erzeugung von elektronischen Signaturen.

Anwendungen, die die SSEE nutzen, sind **nicht** Gegenstand dieser Bestätigung.

Insgesamt gibt es 24 Konfigurationen der SEE, die durch die Werte von vier Parametern wie folgt charakterisiert sind:

1. Parameter: PUK-Benutzungszähler (2 Konfigurationen)

Symbolischer Name	Anfangswert des PUK-Benutzungszählers
Conf_GerLaw	0
Conf_CERT	≤ 14

Tabelle 2: Konfigurationen der SEE für die PUK-Benutzung

Der Personal Unblocking Key (PUK) kann nicht benutzt werden, wenn die Konfiguration **Conf_GerLaw** gewählt wird. Diese Sicherheitsbestätigung gilt nur für SEE, für die Conf_GerLaw gewählt wurde.

2. Parameter: WearCycle (3 Konfigurationen)

Symbolischer Name	Anzahl der Signaturen, die nach einmaliger Authentisierung mittels PIN erzeugt werden kann (WearCycle Value)
WearCycle_single	1
WearCycle_policy	≥ 2 und ≤ 6 oder unbegrenzt (=0)

Tabelle 3: Konfigurationen der SEE für die Aufhebung der Authentisierung nach Signaturerzeugung

Wenn die SEE für den normalen Gebrauch als Signaturerstellungseinheit für einen Signaturschlüsselinhaber personalisiert werden soll, darf nur die Konfiguration **WearCycle_single** benutzt werden. Die Konfiguration **WearCycle_policy** darf nur benutzt werden, wenn die SEE im Rahmen einer geeigneten externen Sicherheitspolitik genutzt werden soll (z. B. für einen Zeitstempeldienst als Signaturerstellungseinheit innerhalb eines Zertifizierungsdiensteanbieters).

3. Parameter: Authenticated_by_unblocking (2 Konfigurationen)

Symbolischer Name	Authenticated_by_unblocking Wert
Authenticated_by_unblocking_no	0 (no)
Authenticated_by_unblocking_yes	1 (yes)

Tabelle 4: Konfigurationen der SEE für die Aufhebung der Authentisierung nach Entsperren der PIN

Der Parameter Authenticated_by_unblocking beschreibt, ob die Authentisierung erhalten bleibt, nachdem die PIN entsperrt wurde. Im Falle **Authenticated_by_unblocking_no** bleibt die Authentisierung nicht erhalten. Im Falle Authenticated_by_unblocking_yes bleibt die Authentisierung nach Entsperren der PIN weiterhin erhalten. Diese Sicherheitsbestätigung gilt nur für SEE, für die Authenticated_by_unblocking_no gewählt wurde.

4. Parameter: Authenticated_by_changing (2 Konfigurationen)

Symbolischer Name	Authenticated_by_changing Wert
Authenticated_by_changing_no	0 (no)
Authenticated_by_changing_yes	1 (yes)

Tabelle 5: Konfigurationen der SEE für die Aufhebung der Authentisierung nach Ändern der PIN

Der Parameter Authenticated_by_changing beschreibt, ob die Authentisierung erhalten bleibt, nachdem die PIN geändert wurde. Im Falle **Authenticated_by_changing_no** bleibt die Authentisierung nicht erhalten. Im Falle Authenticated_by_changing_yes bleibt die Authentisierung nach Ändern der PIN weiterhin erhalten. Diese Sicherheitsbestätigung gilt nur für SEE, für die Authenticated_by_changing_no gewählt wurde.

Die SEE verfügt über einen PUK-Mechanismus mit folgender Funktionalität:
- Bei richtiger Eingabe des PUK kann der Wert der PIN gesetzt werden.
- Die richtige Eingabe des PUK berechtigt **nicht** zur Signaturerzeugung.

c) Nutzung des Produktes

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

Anforderungen an den Zertifizierungsdiensteanbieter

- Der Zertifizierungsdiensteanbieter muss alle Maßnahmen und Regelungen in seinem Sicherheitskonzept beschreiben, die eine sichere Personalisierung gewährleisten. Alle Vorgehensweisen und anderen Anforderungen, die in den jeweiligen Dokumenten beschrieben sind (siehe Lieferumfang oben), müssen befolgt werden. Sie vermeiden Fehler und sollen daher Teil des Sicherheitskonzeptes des Zertifizierungsdienste-anbieters sein.
- SSEE der Konfigurationen B, C (hier „Signaturmodule“ genannt) dürfen nur in besonders gesicherter Umgebung benutzt werden, in denen ein Missbrauch der Signaturfunktion ausgeschlossen werden kann.
- Bei Signaturmodulen der Konfiguration C, die nach einmaliger Authentisierung die Erzeugung einer unbegrenzten Anzahl von elektronischen Signaturen ohne erneute Authentisierung gestatten, 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.
- Ein Signaturmodul darf nicht an Signaturschlüsselinhaber ausgegeben werden, die es normalerweise nicht in einer besonders gesicherten Umgebung benutzen.
- An Signaturschlüsselinhaber, die eine Signaturerstellungseinheit normalerweise nicht in einer speziell gesicherten Umgebung benutzen, ist eine SSEE der Konfiguration A auszugeben.
- Die Einbringung der Identifikationsdaten in die SSEE während der Personalisierung hat so zu erfolgen, dass die Identifikationsdaten anschließend nicht außerhalb der SSEE gespeichert sind.
- In seinem Sicherheitskonzept hat der Zertifizierungsdiensteanbieter ein Verfahren zur Übergabe oder Nutzung der Identifikationsdaten an den bzw. durch den Signatur-schlüsselinhaber vorzusehen, das keine Speicherung der Identifikationsdaten außerhalb der SSEE vorsieht.

Bei der Auslieferung ist der ZDA auf die Einhaltung der oben genannten Einsatzbedingungen hinzuweisen.

Allgemeine Anforderungen an den Endanwender

- Der Signaturschlüsselinhaber muss die SSEE 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 SSEE geheim.
- Der Signaturschlüsselinhaber ändert seine Identifikationsdaten für die SSEE in regelmäßigen Abständen.
- Der Signaturschlüsselinhaber verwendet die SSEE nur in Verbindung mit einer gesetzeskonformen Signaturanwendungskomponente.

Mit Auslieferung der SSEE an den Endanwender ist dieser durch den ZDA auf die Einhaltung der oben genannten Anforderungen hinzuweisen.

3.3 Algorithmen und zugehörige Parameter

Von der SSEE werden die Hashfunktion SHA-1 und der Signaturalgorithmus RSA mit einer Schlüssellänge von 1024 bit bereitgestellt.

Die gemäß § 11 Abs. 3 in Verbindung mit Anlage I Nr. 2 SigV festgestellte Eignung reicht mindestens bis Ende des Jahres 2007 (s. Bundesanzeiger Nr. 48 – Seite 4202f vom 11. März 2003).

Diese Sicherheitsbestätigung ist somit gültig bis zum Ende des Jahres 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 Hardware SLE 66CX320P wurde nach den Sicherheitskriterien ITSEC der Stufe E4 mit der Mindeststärke der Mechanismen „hoch“ evaluiert, vgl. das Deutsche IT-Sicherheitszertifikat TUViT-DSZ-ITSEC-9115. Der zugehörige Zertifizierungsreport verlangt, dass die Mndeststärke der Mechanismen erneut bewertet wird, sobald neue Erkenntnisse zum reverse engineering oder zur DPA-Technologie vorliegen, spätestens jedoch nach einem Jahr (d.h. bis zum 04.08.2001). Im Rahmen der für diese Sicherheitsbestätigung durchgeführten Evaluierung wurde eine erneute Bewertung der Mindeststärke der Mechanismen vorgenommen und damit die Anforderung aus dem Zertifikat erfüllt. Die Evaluierung der SSEE zeigte, dass die Aussage zur Stärke der Mechanismen des Prozessorchips SLE 66CX320P weiterhin gültig ist.

Die sicherheitstechnisch korrekte Integration des Betriebssystems SetCOS 4.4.1, der Signaturapplikation „SetEID v1.0“ und des Prozessors SLE 66CX320P wurde überprüft.

Die SSEE wurde erfolgreich nach der Prüfstufe **E3** der ITSEC evaluiert. Die eingesetzten Sicherheitsmechanismen erreichen die Stärke **hoch**.

Ende der Bestätigung