Sicherheitsbestätigung und Bericht
T-Systems.02182.TE.11.2006

SLE66CX322P bzw. SLE66CX642P / CardOS V4.3B Re_Cert with Application for Digital Signature

Siemens AG

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 SLE66CX322P (oder SLE66CX642P), Software CardOS V4.3B Re_Cert with Application for Digital Signature“

den nachstehend genannten Anforderungen des SigG und der SigV entspricht.

Die Dokumentation zu dieser Bestätigung ist registriert unter:

T-Systems.02182.TE.11.2006

Bonn, den 30.11.2006

(Dr. Heinrich Kersten)

Die 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 Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften (Signaturgesetz – SigG), zuletzt geändert durch Art. 3 (9) des Zweiten Gesetzes zur Neuregelung des Energiewirtschaftsgesetzes (EnWG) vom 07. Juli 2005 (BGBl. Jahrgang 2005, Teil I, Nr. 42)

2 Verordnung zur elektronischen Signatur (Signaturverordnung – SigV), zuletzt geändert durch Art. 2 des Ersten Gesetzes zur Änderung des Signaturgesetzes (1. SigGÄndG) vom 04. Januar 2005 (BGBl. Jahrgang 2005, Teil I, Nr. 1)

Beschreibung der technischen Komponente:

1. Handelsbezeichnung der technischen Komponente und Lieferumfang

1.1 Handelsbezeichnung

Signaturerstellungseinheit

„Chipkarte mit Prozessor SLE66CX322P, Software CardOS V4.3B Re_Cert with Application for Digital Signature“.

„Chipkarte mit Prozessor SLE66CX642P, Software CardOS V4.3B Re_Cert with Application for Digital Signature“.

1.2 Auslieferung

Die verschiedenen Stufen und Wege der Auslieferung des EVG und die Abläufe der Initialisierung und Personalisierung sind im Dokument "Delivery and Operation, CardOS V4.3B Re_Cert, Version 0.2, 26.10.2006 (Siemens AG)" in englischer Sprache detailliert beschrieben.

Die Darstellung umfasst folgende Abschnitte: Delivery to the Chip Manufacturer, Delivery to the Trust Center, Procedure of Initialisation and Personalisation, Delivery of the signature card to the Card Holder by the Trust Center, Delivery of pre-personalised signature card to the Registration Authority by the Trust Center, Delivery to the Terminal Developer, Delivery of signature card to the Card Holder by the Registration Authority.

1.3 Lieferumfang

Nr.	Art	Bezeichnung	Version	Datum	Übergabeform
0	Hardware	Prozessor Infineon SLE66CX322P: m1484b14 und m1484f18 oder SLE66CX642P: m1485b16	Production Line Numbers: 2 - Dresden 5 – Altis Dresden	-	Chipkarte

Nr.	Art	Bezeichnung	Version	Datum	Übergabeform
1	Software: Betriebssystem (ROM-Teil)	CardOS V4.3B	**C808** - ATR: 0xC8 0x08 - GET DATA, P2=80h: 'CardOS V4.3B (C) Siemens…' - GET DATA, P2=82h: 0c8 008	-	in ROM geladen
2	Software	Service Pack	**3** - GET DATA, P2=88, Byte 27 + 28 : 013 **003**	-	Package[3] in EEPROM geladen durch Kartenhersteller[4]
3	Software	CERT Package	**3** - GET DATA, P2=88, Byte 16 + 17 : 01f **003**	-	Package[3] in EEPROM geladen durch Kartenhersteller[4]
4	Software	VRC Package	**1** - GET DATA, P2=88, Byte 5 + 6 : 007 **001**	-	Package[3] in EEPROM geladen durch Kartenhersteller[4]
5	Software: Applica-tion / Daten-Struktur	SigG application	s. Tabelle 2 und Fußnote[3]		Personalisierungsskript-Files (.CSF)
6	Dokumentation	User's Manual CardOS V4.3	-	06/2004	Papier / PDF-Datei
7	Dokumentation	Package & Release Notes CardOS V4.3 / 4.3B	-	11/2006	Papier / PDF-Datei
8	Dokumentation	CERT Package & Release Notes CardOS 4.3B	-	11/2006	Papier / PDF-Datei
9	Dokumentation	Administrator Guidance, CardOS V4.3B Re_Cert	1.2	27.11.06	Papier / PDF-Datei
10	Dokumentation	Application SigG, CardOS V4.3B Re_Cert	1.1	17.11.06	Papier / PDF-Datei

[3] enthalten in: Sequences for centralised and decentralised personalization, directory: V43B_Pers_2006_11_20, Siemens AG, 20.11.2006

[4] PackageLoad Key erforderlich.

Nr.	Art	Bezeichnung	Version	Datum	Übergabeform
11	Dokumentation	User Guidance, CardOS V4.3B Re_Cert	1.2	21.11.06	Papier / PDF-Datei

Tabelle 1: Auslieferungsumfang

Nr.	Bezeichnung	Version	Datum
a	PersAppSigG_ReCert.CSF	1.0	30.10.2006
b	PersAppSigG_ReCert_withoutPUK.CSF	1.0	30.10.2006
c	Pre-PersAppSigG_ReCert.CSF	1.0	30.10.2006
d	Pre-PersAppSigG_ReCert_withoutPUK.CSF	1.0	30.10.2006
e	Post-PersAppSigG_ReCert.CSF	1.0	30.10.2006
f	Post-PersAppSigG_ReCert_withoutPUK.CSF	1.0	30.10.2006
g	Mass_Pre-PersAppSigG_ReCert.CSF	1.2	22.11.2006
h	Mass_Post-PersAppSigG_ReCert.CSF	1.0	30.10.2006
i	Defines_2048.csf	1.0	30.10.2006
j	Defines_1024.csf	1.0	30.10.2006
k	Defines_1280.csf	1.0	30.10.2006
l	Defines_1536.csf	1.0	30.10.2006
m	Defines_1792.csf	1.0	30.10.2006

Tabelle 2: Skript-Komponenten

1.4 Hersteller

Siemens AG, MED GS SEC

Charles-de-Gaulle-Str. 2, 81737 München

2. Funktionsbeschreibung[5]

Das Produkt ist eine Signaturerstellungseinheit bestehend aus dem Prozessorchip Infineon SLE66CX322P oder SLE66CX642P und der Software „CardOS V4.3B Re_Cert with Application for digital Signature“.

CardOS V4.3B Re_Cert ist ein multifunktionales Smart Card Betriebssystem, das aktiven und passiven Datenschutz unterstützt und entwickelt wurde, um höchsten Sicherheitsanforderungen zu genügen. CardOS V4.3B Re_Cert ist konform zu ISO 7816-3, -4, -5, -8 und -9.

"CardOS V4.3B Re_Cert with Application for digital Signature" wurde entwickelt, um den Anforderungen des deutschen Signaturgesetzes zu genügen.

Ein patentiertes Schema zur Initialisierung / Personalisierung sorgt für eine kostengünstige Massenproduktion durch Kartenhersteller.

Generelle Eigenschaften von CardOS V4.3B Re_Cert:

- Läuft auf der Infineon SLE66 Chip-Familie. Die SLE66CX322P und SLE66CX642P Chips mit integriertem Security Controller für asymmetrische Kryptografie und echtem Zufallszahlengenerator wurden erfolgreich gegen die Anforderungen der Stufe EAL5+ der Common Criteria zertifiziert.
- Schutz gegen alle derzeit bekannten Sicherheitsattacken.
- Alle Kommandos entsprechen den ISO 7816-4, -8 und -9 Standards.
- PC/SC- und CT-API fähig.
- Sicherheitsarchitektur und Schlüsselmanagement sind klar strukturiert.
- Kunden- und anwendungsabhängige Konfigurierbarkeit der Kartendienste und -kommandos.
- Erweiterbarkeit des Betriebssystems durch ladbare Software-Komponenten/ -Packages.

Das Dateisystem:

CardOS V4.3B Re_Cert bietet ein dynamisches und flexibles Dateisystem, das durch Chip-spezifische kryptografische Mechanismen geschützt wird:

- Beliebige Anzahl von Dateien (EFs, DFs).
- Schachtelungstiefe von DFs nur durch die Speichergröße begrenzt.

---

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

- 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 Sicherheitstests und Schlüssel sind in so genannten "basic security objects" in den DFs gespeichert (keine reservierten File-IDs für Schlüssel- oder PIN-Files).
- Die Sicherheitsstruktur kann ohne Datenverlust nach dem Anlegen von Dateien noch inkrementell verfeinert werden.

Kryptografische Dienste:

- Implementierte Algorithmen[6]: RSA mit 1024 Bit bis 2048 Bit Schlüssellänge (PKCS#1 Padding), 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[7]:

- Kompatibel mit ISO 7816-4.
- Kann für jedes Kommando und jedes Datenobjekt (Files, Keys) unabhängig definiert werden.

---

6 Die Algorithmen Triple-DES (CBC), DES (ECB, CBC), MAC, Retail-MAC kommen bei der elektronischen Signatur nicht zur Anwendung und sind deshalb auch nicht Gegenstand dieser Sicherheitsbestätigung.

7 Die "Application for Digital Signature" nutzt das secure messaging nicht. Deshalb ist secure messaging nicht Gegenstand dieser Sicherheitsbestätigung.

3. Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Die Signaturerstellungseinheit „Chipkarte mit Prozessor SLE66CX322P oder SLE66CX642P, Software CardOS V4.3B Re_Cert with Application for Digital Signature“ (im Folgenden kurz als "SSEE" bezeichnet) 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 SSEE unter den angegebenen Einsatzbedingungen (Abschnitt 3.2) erfüllt.

3.2 Einsatzbedingungen

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

a) Grundsätzliches

1. Ohne Re-Evaluierung und erneute Sicherheitsbestätigung ist es nicht zulässig, eine Änderung oder Erweiterung der sicherheitsbestätigten „Application for digital Signature“ vorzunehmen.

2. Der Software-Entwickler (Siemens AG) und der Chip-Hersteller (Infineon Technologies AG) sind verantwortlich dafür, die missbräuchliche Nutzung des PackageLoadKey zu verhindern; insbesondere ist seine Vertraulichkeit sicherzustellen.

3. Die Anzahl der im Gebrauch befindlichen SSEE darf 83 Millionen nicht überschreiten.

b) Personalisierung

Die Personalisierung kann zentral oder dezentral erfolgen.

- Im zentralen Fall erfolgt die Personalisierung vollständig beim ZDA[8]; dabei kommt das Personalisierungsscript für die zentrale Personalisierung zum Einsatz.
- Im dezentralen Fall erfolgt eine sogenannte Pre-Personalisierung beim ZDA mit Hilfe des Pre-Personalisierungsscripts. Anschließend vollendet eine dezentrale Registrierungsstelle (als ausgelagerte Einheit des ZDA) die Personalisierung; diese sogenannte Post-Personalisierung wird mit Hilfe des Post-Personalisierungsscripts ausgeführt.

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

Der ZDA muss in seinem Sicherheitskonzept alle Maßnahmen beschreiben, die für eine sichere Personalisierung erforderlich sind. Von den in den Dokumenten "Administrator Guidance" und "Application SigG" (siehe Tabelle 1) beschriebenen Abläufen darf nicht abgewichen werden.

c) Konfigurationen und Auslieferung der SSEE

Die SSEE besitzt folgende Konfigurationen, die im Rahmen der Personalisierung festgelegt werden:

A) Konfiguration ‘Personal Signature Card’ + ‘Single Signature Module'':

i) Es wird *ein* PIN Objekt verwendet und es gilt n=1: Die Benutzer-Authentisierung nach PIN-Eingabe verfällt nach Erzeugen genau einer Signatur.
In dieser Konfiguration ist das 'PUK letter concept[9]' verfügbar.

B) Konfiguration ‘Personal Signature Card’ + ‘Mass Signature Module’:

ii) Es wird *ein* PIN Objekt verwendet und n liegt zwischen 2 und 254: Die Benutzer-Authentisierung verfällt nach Erzeugen von genau n Signaturen.

iii) Es wird *ein* PIN Objekt verwendet und $n \in \{0, 255\}$: Die Benutzer-Authentisierung verfällt nie, solange nicht die externe Applikation die Anzahl erzeugter Signaturen begrenzt[10].

In beiden Unter-Konfiguration ii) und iii) ist das 'PUK letter concept[9]' verfügbar.

---

8 ZDA = Zertifizierungsdiensteanbieter (Trust Center)

9 PUK letter concept: Der Kartenhalter erhält einen PUK-Brief; die PUK erlaubt es, die PIN_T (Transport-PIN) zu entsperren, wenn diese durch mehrfache fehlerhafte Eingabe gesperrt worden ist.

10 z. B. durch Überwachung eines Zeitfensters oder eines Signaturzählers

C) Konfiguration ‘Two PIN Module’ (Diese Konfiguration impliziert automatisch ‘Mass Signature Module’):

iv) Es werden *zwei* PIN Objekte PIN1, PIN2 verwendet. Hierbei ist zur Benutzer-Authentisierung die korrekte Eingabe beider PINs erforderlich. Die Benutzer-Authentisierung verfällt nie, solange nicht eine externe Applikation die Anzahl erzeugter Signaturen begrenzt[10].
In dieser Konfiguration ist das 'PUK letter concept[9]' nicht verfügbar.

Die (Unter-)Konfigurationen ii), iii) und iv) dürfen ausschließlich in einer Umgebung (z. B. in einem Büro, einem Trust Center oder einer Registrierungsstelle) angewendet werden, die im Rahmen einer geeigneten externen Sicherheitspolitik betrieben wird, welche vom Kartenherausgeber als vertrauenswürdig angesehen wird. Diese Einsatzumgebung des EVG muss jede unbeabsichtigte und jede missbräuchliche Verwendung des EVG ausschließen.

Für die Nutzung der SSEE sind im Rahmen der Personalisierung unter anderem folgende Parameter einstellbar und nach ihrer einmaligen Einstellung nicht mehr änderbar:

- die Modullänge des RSA-Schlüsselpaares von 1024 bis 2048 mit Schrittweite 8, sowie
- die Nutzung des PUK-Objektes (ja/nein); wird die Option PUK-Objekt = ja gewählt, kann ein PUK (Personal Unblocking Key) verwendet werden, um den Fehlbedienungszähler für die Eingabe der PIN auf den Initialwert zurückzusetzen. Bei richtiger Eingabe des PUK kann außerdem ein neuer Wert des PUK gesetzt werden. Die Anzahl der Benutzungen der PUK-Funktionalität ist begrenzt (wird während der Personalisierung geeignet festgelegt). Die richtige Eingabe des PUK ermöglicht keine Signaturerzeugung.

Die Auslieferung der SSEE durch den ZDA liegt in der Verantwortung des ZDA und ist in dessen Sicherheitskonzept in Übereinstimmung mit den Anforderungen in "Delivery and Operation, CardOS V4.3B Re_Cert, Version 0.2, 26.10.2006 (Siemens AG)"zu beschreiben.

Es ist die Aufgabe des jeweiligen ZDAs sicherzustellen, dass SSEE in den Konfigurationen unter B) und C) nicht als Signaturerstellungseinheiten an Endkunden (Kartenhalter) ausgeliefert werden.

Die SSEE verfügt über eine Transport-PIN für die sichere Auslieferung. Die Transport-PIN kann nur einmal korrekt eingegeben werden und dient der Entsperrung von PIN und PUK sowie der Eingabe neuer Werte für PIN und PUK.
Bei Verwendung des 'PUK letter concept' – nur möglich in Verbindung mit der Konfiguration ‘Personal Signature Card’ - kann PIN_T durch den PUK entsperrt werden, solange PIN_T nicht korrekt eingegeben wurde.
Mit der Transport-PIN kann keine Signaturerstellung erfolgen.

d) Nutzung des Produktes

Mit Auslieferung der Signaturerstellungseinheit „Chipkarte mit Prozessor SLE66CX322P oder SLE66CX642P, Software CardOS V4.3B Re_Cert with Application for Digital Signature“ an den ZDA ist dieser auf die Einhaltung der unter a), b) und c) genannten Einsatzbedingungen hinzuweisen.

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

Anforderungen an den ZDA

Der ZDA muss die Kartenhalter gemäß §6 Abs. 1 und 3 SigG über die sachgerechte Benutzung von Transport-PIN, PIN und PUK sowie den Einsatz einer geeigneten Signaturanwendungskomponente unterrichten.

Allgemeine Anforderungen an den Endanwender / Signaturschlüsselinhaber :

- 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.

Anwendungen

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

3.3 Algorithmen und zugehörige Parameter

Die SSEE verwendet folgende Algorithmen: SHA-1 sowie RSA (Schlüssellängen 1024 bis 2048 Bit).

Die gemäß § 11 Abs. 3 in Verbindung mit Anlage I Nr. 2 SigV festgestellte Eignung von **SHA-1** (bei Anwendung für qualifizierte Zertifikate) reicht mindestens bis Ende des Jahres 2010 (Bundesanzeiger Nr. 58, S. 1913-1915 vom 23. März 2006).

Die gemäß § 11 Abs. 3 in Verbindung mit Anlage I Nr. 2 SigV festgestellte Eignung von **RSA** ist abhängig von der Schlüssellänge. Die Eignungsdauer ist der folgenden Tabelle (Bundesanzeiger Nr. 58, S. 1913-1915 vom 23. März 2006) zu entnehmen:

Schlüssellänge	1024	1280	1536	1728
Geeignet bis	Ende 2007	Ende 2008	Ende 2009	Ende 2010

Diese Sicherheitsbestätigung ist somit gültig bis

- 31.12.2007 (bei Nutzung von RSA-1024),
- 31.12.2008 (bei Nutzung von RSA-1280),
- 31.12.2009 (bei Nutzung von RSA-1536),
- 31.12.2010 (bei Nutzung von RSA-1728 und RSA-2048).

Sie kann verlängert werden, wenn zu diesem Zeitpunkt keine Hinderungsgründe hinsichtlich der Sicherheit des Produktes oder der Algorithmen vorliegen.

3.4 Prüfstufe und Mechanismenstärke

Die Software „CardOS V4.3B Re_Cert with Application for Digital Signature“ wurde erfolgreich nach der Prüfstufe EAL4+ der Common Criteria mit Zusatz in Übereinstimmung mit Anlage 1, Abschnitt I, Nr. 1.2 SigV evaluiert. Die erforderlichen Sicherheitsfunktionen erreichten dabei die Stärke „hoch“. Hierfür liegt das Deutsche IT-Sicherheitszertifikat T-Systems-DSZ-CC-04181-2006 vom 30.11.2006 vor.

Der Prozessor SLE66CX322P wurde erfolgreich gemäß der Stufe EAL5+ der Common Criteria mit Zusatz in Übereinstimmung mit Anlage 1, Abschnitt I, Nr. 1.2 SigV evaluiert. Die erforderlichen Sicherheitsfunktionen erreichten dabei die Stärke „hoch“. Hierfür liegt das Deutsche IT-Sicherheitszertifikat BSI-DSZ-CC-0266-2005 vom 22.04.2005 vor.

Der Prozessor SLE66CX642P wurde erfolgreich gemäß der Stufe EAL5+ der Common Criteria mit Zusatz in Übereinstimmung mit Anlage 1, Abschnitt I, Nr. 1.2 SigV evaluiert. Die erforderlichen Sicherheitsfunktionen erreichten dabei die Stärke „hoch“. Hierfür liegt das Deutsche IT-Sicherheitszertifikat BSI-DSZ-CC-0315-2005 vom 12.08.2005 vor.

Die sicherheitstechnisch korrekte Integration von „CardOS V4.3B Re_Cert with Application for Digital Signature“ und des Prozessors SLE66CX322P bzw. SLE66CX642P wurde überprüft.

Die für eine Signaturerstellungseinheit nach SigV maßgebende Evaluierungsstufe (mit den erforderlichen Erweiterungen) und die Funktions-/ Mechanismenstärke sind damit erreicht (und in Teilen übertroffen).

Ende der Bestätigung

Sicherheitsbestätigung:
T-Systems.02182.TE.11.2006

Hrsg.: T-Systems GEI GmbH
Adresse: Rabinstr.8, 53111 Bonn
Telefon: +49-(0)228-9841-0
Fax: +49-(0)228-9841-60
Web: www.t-systems-itc.de
www.t-systems-zert.com