T · · Systems ·

Security Confirmation and Report
T-Systems.02182.TE.11.2006

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

Siemens AG

Confirmation

concerning Products for Qualified Electronic Signatures

according to §§ 15 Sec. 7 S. 1, 17 Sec. 4 German Electronic Signature Act[1] and §§ 11 Sec. 2 and 15 German Electronic Signature Ordinance[2]

T-Systems GEI GmbH
- Certification Body -

Rabinstr.8, D-53111 Bonn, Germany

hereby certifies according to §§ 15 Sec. 7 S. 1, 17 Sec. 1 SigG as well as §§ 15 Sec. 1 and 4 , § 11 Sec. 3 SigV that the

Signature Creation Device „Smartcard with Controller SLE66CX322P or SLE66CX642P, Software CardOS V4.3B Re_Cert with Application for Digital Signature“

complies with the requirements of SigG and SigV described in this document.

The documentation for this confirmation is registered under:

T-Systems.02182.TE.11.2006

Bonn: Nov 30, 2006

(Dr. Heinrich Kersten)

As published in the Bundesanzeiger (Federal Gazette) No. 31 dated February 14, 1998, p. 1787, T-Systems GEI GmbH – Certification Body - is entitled to issue confirmations for products according to §§ 15 Sec.7 S. 1 (or § 17 Sec.4) SigG.

---

[1] Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften (Signaturgesetz – SigG) [Law Governing Framework Conditions for Electronic Signatures and Amending Other Regulations], recently revised by Article 3 (9) of the second act changing the EnWG as of July 07, 2005 (BGBl. Year 2005, Part I, No. 42)

[2] Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) [Ordinance on Electronic Signatures (Signature Ordinance– SigV)], recently revised by Article 2 of the first act to adapt the Signature Act (1. SigGÄndG) as of January 04, 2005 (BGBl. Year 2005, Part I, No. 1)

Description of Technical Component:

1. Identification and Delivery of the Technical Component

1.1 Identification

Signature Creation Device

„Smartcard with Controller SLE66CX322P, Software CardOS V4.3B Re_Cert with Application for Digital Signature“

„Smartcard with Controller SLE66CX642P, Software CardOS V4.3B Re_Cert with Application for Digital Signature“

1.2 Delivery

The different steps and ways of delivering the TOE and the procedures for initialisation and personalisation have been described in detail in "Delivery and Operation, CardOS V4.3B Re_Cert, Version 0.2, 26.10.2006 (Siemens AG)".

The description refers to: 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 Scope of Delivery

No.	Type	Term	Version	Date	Form of Delivery
0	Hardware	Controller Infineon SLE66CX322P: m1484b14 and m1484f18 or SLE66CX642P: m1485b16	Production Line Numbers: 2 - Dresden 5 – Altis Dresden	-	Smartcard

No.	Type	Term	Version	Date	Form of Delivery
1	Software: (ROM part of the operating system)	CardOS V4.3B	**C808** - ATR: 0xC8 0x08 - GET DATA, P2=80h: 'CardOS V4.3B (C) Siemens…' - GET DATA, P2=82h: 0c8 008	-	Loaded in ROM
2	Software	Service Pack	**3** - GET DATA, P2=88, Byte 27 + 28 : 013 **003**	-	Package[3] finally loaded in EEPROM by card manufacturer [4]
3	Software	CERT Package	**3** - GET DATA, P2=88, Byte 16 + 17 : 01f **003**	-	Package[3] finally loaded in EEPROM by card manufacturer[4]
4	Software	VRC Package	**1** - GET DATA, P2=88, Byte 5 + 6 : 007 **001**	-	Package[3] finally loaded in EEPROM by card manufacturer[4]
5	Software: Application / Data Structure	SigG application	cf. Table 2 and footnote[3]		Personalization Script Files (.CSF)
6	Documentation	User's Manual CardOS V4.3	-	06/2004	Paper / PDF-File
7	Documentation	Package & Release Notes CardOS V4.3 / 4.3B	-	11/2006	Paper / PDF-File
8	Documentation	CERT Package & Release Notes CardOS 4.3B	-	11/2006	Paper / PDF-File
9	Documentation	Administrator Guidance, CardOS V4.3B Re_Cert	1.2	27.11.06	Paper / PDF-File
10	Documentation	Application SigG, CardOS V4.3B Re_Cert	1.1	17.11.06	Paper / PDF-File

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

[4] PackageLoad Key required.

No.	Type	Term	Version	Date	Form of Delivery
11	Documentation	User Guidance, CardOS V4.3B Re_Cert	1.2	21.11.06	Paper / PDF-File

Tabelle 1: Scope of Delivery

No.	File Name	Version	Date
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

Table 2: Script Components

1.4 Vendor

Siemens AG, MED GS SEC

Charles-de-Gaulle-Str. 2, D-81737 Munich, Germany

2. Functional Description[5]

The component is a Signature Creation Device consisting of the controller chip Infineon SLE66CX322P or SLE66CX642P and the software „CardOS V4.3B Re_Cert with Application for digital Signature“.

CardOS V4.3B Re_Cert is a multifunctional smart card operating system supporting active and passive data protection; it was developed to meet highest security requirements. CardOS V4.3B Re_Cert is compliant to ISO 7816-3, -4, -5, -8 and -9.

"CardOS V4.3B Re_Cert with Application for digital Signature" is designed to meet the requirements of the German Electronic Signature Act.

A patented scheme for initialisation / personalisation provides for cost efficient mass production by card manufacturers.

General features of CardOS V4.3B Re_Cert:

- Runs on the Infineon SLE66 chip family. The SLE66CX322P and SLE66CX642P chips with embedded security controller for asymmetric cryptography and true random number generator have successfully been certified against the Common Criteria EAL5+ security requirements.
- Shielded against all presently known security attacks.
- All commands are compliant with ISO 7816-4, -8 and -9 standards.
- PC/SC- compliance and CT-API.
- Cleanly structured security architecture and key management.
- Customer and application dependent configurability of card services and commands.
- Extensibility of the operating system using loadable software components (packages).

File system:

CardOS V4.3B Re_Cert offers a dynamic and flexible file system, protected by chip specific cryptographic mechanisms:

- Arbitrary number of files (EFs, DFs).
- Nesting of DFs limited by memory only.

---

[5] The subsequent description was provided by the vendor; minor changes have been applied by the certification body to comply with the terminology of the German Electronic Signature Act.

- Dynamic memory management aids in optimum usage of the available EEPROM.
- Protection against EEPROM defects and power failures.

Access control:

- Up to 126 distinct programmer definable access rights.
- Access rights may be combined with arbitrary Boolean expressions.
- Any command or data object may be protected with an access condition scheme of its own.
- All security tests and keys are stored as so-called basic security objects in the DF bodies (no reserved file Ids for key- or PIN files).
- Security structure may be refined incrementally after file creation without data loss.

Cryptographic Services:

- Implemented algorithms[6]: RSA with 1024 up to 2048 bit key length (PKCS#1 padding), SHA-1, Triple-DES (CBC), DES (ECB, CBC), MAC, Retail-MAC.
- Protection against Differential Fault Analysis (”Bellcore-Attack”).
- Protection of DES and RSA against SPA and DPA.
- Support of ”Command Chaining” following ISO 7816-8.
- Asymmetric key generation “on chip” using the onboard true random number generator.
- Digital Signature functions “on chip”.
- Connectivity to external Public Key certification services.

Secure Messaging[7]:

- Compatible with ISO 7816-4.
- May be defined for every command and every data object (files, keys) independently.

---

6 The algorithms Triple-DES (CBC), DES (ECB, CBC), MAC, Retail-MAC are not used in the context of electronic signatures and, thus, are not subject to this security confirmation.

7 The "Application for Digital Signature" does not use secure messaging. Thus, secure messaging is not subject to this security confirmation.

3. Compliance with the Signature Act and the Signature Ordinance

3.1 Compliance

The Signature Creation Device „Smartcard with Controller SLE66CX322P or SLE66CX642P, Software CardOS V4.3B Re_Cert with Application for Digital Signature“ (in the sequel abbreviated as "SSCD") meets the following requirements:

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

These requirements are met by the SSCD provided that the following conditions (in sec. 3.2) on the operational environment are fulfilled.

3.2 Operational Environment

The compliance indicated above is based on meeting the following requirements for the operational environment:

a) Basics

1. It is not allowed to change or extend the „Application for digital Signature“ without a re-evaluation and re-confirmation of the SSCD.
2. The software developer (Siemens AG) and the chip manufacturer (Infineon Technologies AG) are responsible to prevent misuse of the PackageLoadKey; especially they have to ensure the confidentiality of this key.
3. The number of TOE devices (i.e. smart cards) in operational use must not exceed 83 million.

b) Personalisation

Personalisation may take place either centralised or decentralised:

- In centralised mode, personalisation is performed completely by the CSP[8]; the personalisation script for centralised personalisation is used.
- In decentralised mode, a so-called pre-personalisation is performed at the CSP using the pre-personalisation script.
  Then, a decentralised registration authority (as an outsourced unit of the CSP)

[8] CSP = Certification Service Provider (Trust Center)

completes the personalisation process; this so-called post-personalisation is performed by using the post-personalisation script.

The personalisation scripts may be modified only in the sense and at places indicated by the corresponding comments.

All security measures required for a secure personalisation have to be documented by the CSP in his security concept. The procedures documented in "Administrator Guidance" and "Application SigG" must not be altered.

c) Configuration and Delivery of the SSCD

The SSCD has the following different configurations chosen during personalisation:

A) Configuration 'Personal Signature Card' + 'Single Signature Module':

i) using *one* PIN object with associated n=1: user authentication with one PIN entry expires after generating exactly one signature. In this configuration a PUK letter concept[9] is avalaible.

B) Configuration 'Personal Signature Card' + 'Mass Signature Module':

ii) using *one* PIN object with associated n between 2 and 254: user authentication expires after generating exactly n signatures.

iii) using *one* PIN object with associated n∈{0, 255}: user authentication never expires (limited by the external application[10] only).

In both sub-configurations ii) and iii) a PUK letter concept[9] is avalaible.

C) Configuration 'Two PIN Module' (this configuration automatically implies 'Mass Signature Module'):

iv) using *two* PIN objects PIN1, PIN2. In this case, user authentication requires correct entry of both PINs. User authentication never expires[11] (limited by the external application[10] only). In this configuration a PUK letter concept[9] is <u>not</u> avalaible.

The (sub-)configurations ii), iii) and iv) are to be used exclusively in an environment (e.g. in an office, a Trust Center or a registration facility) operating under an appropriate external security policy that is considered trustworthy by the card issuer. The environment in which the corresponding TOE is employed has to prevent malpractice, i.e. it has to ensure that the TOE is not used for purposes other than

---

9 PUK letter concept: The card holder is sent a PUK letter, the included PUK allows for unblocking the transport PIN_T in case where PIN_T was blocked due to a number of failed PIN_T entries.

10 e.g. through time control or a signature counter

11 The value of the associated n (in the range 0…255) is ignored.

intended.

For the usage of the SSCD the following parameters can be chosen during personalisation (but cannot be altered afterwards):

- module length of RSA key pair from 1024 to 2048 (in steps of 8 bits), and
- usage of a PUK object (yes/no); if the option PUK object = yes has been chosen, a PUK (Personal Unblocking Key) can be used to reset a retry counter for PIN entry to its initial value. After correct entry of the PUK, a new value for the PUK can be set as well. A retry count for PUK usage is configured during personalisation. The correct entry of a PUK does not allow for creating an electronic signature.

The CSP is responsible for the secure delivery of the SSCD and, thus, has to document the delivery procedure in his security concept in accordance with the requirements laid down in "Delivery and Operation, CardOS V4.3B Re_Cert, Version 0.2, 26.10.2006 (Siemens AG)".

It is the responsibility of the CSP to guarantee that SSCDs in configurations under B) and C) are not delivered to end users (card holders).

The SSCD uses a transport PIN_T for secure delivery. PIN_T can successfully be used only once and has to be used to unblock PIN and PUK and set new values for PIN and PUK.
In case of the 'PUK letter concept' being applicable only to the configuration 'Personal Signature Card', PIN_T can be unblocked by PUK, as long as PIN_T has not successfully been used yet.
The transport PIN_T does not allow for creating electronic signatures.

d) Usage

With delivery of the Signature Creation Device „Smartcard with Controller SLE66CX322P or SLE66CX642P, Software CardOS V4.3B Re_Cert with Application for Digital Signature“ to the CSP, the CSP has to be advised to strictly follow the operational requirements specified above under a), b) and c).

For an appropriate usage of the SSCD the following requirements have to be met:

Requirements to the CSP

According to §6 Abs. 1 und 3 SigG, the CSP has to advise the card holder on the correct usage of the transport PIN_T, PIN and PUK as well as on using an appropriate signature application component.

General requirements to the end user / signature key holder:

- The signature key holder has to use and keep the SSCD in such a way as to prevent misuse and manipulation.
- The signature key holder applies the signature creation function only to data for which he intends to guarantee integrity and authenticity.
- The signature key holder keeps his identification data for the SSCD confidential.
- The signature key holder changes his identification data for the SSCD in regular intervals.
- The signature key holder uses the SSCD only in connection with a signature application component compliant to the German Electronic Signature Act.

Applications

Applications using the SSCD are **not** objective of this confirmation.

3.3 Algorithms and corresponding Parameters

The SSCD uses the following algorithms: SHA-1 and RSA (module length 1024 to 2048 Bit).

- In Accordance with § 11 Sec. 3 in connection with Annex I No. 2 SigV, **SHA-1** is approved for usage with qualified certificates (at least) until end of 2010 (cf. Bundesanzeiger [Federal Gazette] No. 58 – page 1913-1915 as of March 23, 2006).
- In Accordance with § 11 Sec. 3 in connection with Annex I No. 2 SigV, approval of **RSA** depends on the module length. Details on the approval period are given by the following table (cf. Bundesanzeiger [Federal Gazette] No. 58 – page 1913-1915 as of March 23, 2006).

Module Length	1024	1280	1536	1728
Approved until	End of 2007	End of 2008	End of 2009	End of 2010

This confirmation is therefore valid until

- Dec 31, 2007 (for usage of RSA-1024),
- Dec 31, 2008 (for usage of RSA-1280),
- Dec 31, 2009 (for usage of RSA-1536),
- Dec 31, 2010 (for usage of RSA-1728 and RSA-2048).

It may be prolonged if at that time there are no findings invalidating either the security of the technical component or its algorithms.

3.4 Assurance Level and Strength of Mechanism

The Software "CardOS V4.3B Re_Cert with Application for Digital Signature“ was successfully evaluated against the Common Criteria level EAL4+ augmented in compliance to Annex 1, Sec. I, No. 1.2 SigV. The required security mechanisms were rated to have a "**high**" strength of function (SOF). This result is confirmed by the "Deutsches IT-Sicherheitszertifikat" [German IT Security Certificate] T-Systems-DSZ-CC-04181-2006 as of Nov 30, 2006.

The controller SLE66CX322P was successfully evaluated against the Common Criteria level EAL5+ augmented in compliance to Annex 1, Sec. I, No. 1.2 SigV. The required security mechanisms were rated to have a "**high**" strength of function (SOF). This result is confirmed by the "Deutsches IT-Sicherheitszertifikat" [German IT Security Certificate] BSI-DSZ-CC-0266-2005 as of April 22, 2005.

The controller SLE66CX642P was successfully evaluated against the Common Criteria level EAL5+ augmented in compliance to Annex 1, Sec. I, No. 1.2 SigV. The required security mechanisms were rated to have a "**high**" strength of function (SOF). This result is confirmed by the "Deutsches IT-Sicherheitszertifikat" [German IT Security Certificate] BSI-DSZ-CC-0315-2005 as of Aug 12, 2005.

The correct integration of „CardOS V4.3B Re_Cert with Application for Digital Signature“ and the controller SLE66CX322P resp. SLE66CX642P with respect to IT security aspects was assessed.

Thus, the assurance level (with the required augmentation) and strength of mechanism / function rating required by the German Electronic Signature Ordinance for a SSCD was achieved (and partially exceeded).

End of Confirmation

Disclaimer (added to English version only):
In cases of doubt the original German version of this Security Confirmation shall prevail.

Security Confirmation:
T-Systems.02182.TE.11.2006

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