Security Confirmation and Report

T-Systems.02192.TE.08.2007

SLE66CX322P or SLE66CX642P / CardOS V4.2B FIPS 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
„Smart Card with Controller SLE66CX322P or SLE66CX642P, CardOS V4.2B FIPS 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.02192.TE.08.2007

Bonn: August 13, 2007

(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 Signaturgesetz vom 16. Mai 2001 (BGBl. I S. 876) [Signature Act as of May 16, 2001 (BGBl. I p. 876)], recently revised by Article 4 of the act as of February 26, 2007 (BGBl. Year 2007, Part I p. 179)

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 „Smart Card with Controller SLE66CX322P or SLE66CX642P, CardOS V4.2B FIPS with Application for Digital Signature“

1.2 Delivery

The different steps and ways of delivering the technical component and the procedures for initialisation and personalisation have been described in detail in “CardOS® V4.2B FIPS, Delivery and Operation, Edition 06/2007", version 1.00, June 06, 2007, in English language. The description refers to: Delivery to the Chip Manufacturer, Delivery to the CSP, to the Card Holder and to the Terminal Developer as well as the steps of Initialisation, Key Generation, Personalisation and Certificate Installation.

1.3 Scope of Delivery

In addition to the document “CardOS® V4.2B FIPS, Delivery and Operation, Edition 06/2007", version 1.00, June 06, 2007, referenced in 1.2, the following components belong to the scope of delivery:

Remark: In the table below (column marked by „No.“) there is no entry „8“. This omission has not been corrected in order to align with the numbering in the vendor documentation, in particular the security target.

No.	Type	Term	Version	Date	Form of delivery
1	Software (Operating System)	CardOS V4.2B	C809	05.07.05	loaded in ROM / EEPROM
2	Software Application Digital Signature (Application / Data Structure)	*Pre-loaded variant* V42B_FIPS_InitScript.py	1.1	May 24 2007	Personalization Script Files in Python format, after whose execution the ADS will be loaded in EEPROM
		V42B_FIPS_InitScript_DF_DS_x.py	1.0	May 15 2007	
		V42B_FIPS_PersScript.py	1.1	May 24 2007	
		V42B_FIPS_PersScript_DF_DS_x .py	1.1	May 24 2007	
		V42B_FIPS_CAScript.py	1.1	May 24 2007	
		V42B_FIPS_CAScript_DF_DS_x.py	1.0	May 15 2007	
		V42B_FIPS_RAScript.py	1.1	May 24 2007	
		V42B_FIPS_RAScript_DF_DS_x.py	1.2	Jun 04 2007	

No.	Type	Term	Version	Date	Form of delivery
		Post-loaded variant:			
		V42B_FIPS_InitScript_Post.py	1.1	May 24 2007	
		V42B_FIPS_LRAScript_Post.py	1.1	May 24 2007	
		V42B_FIPS_LRAScript_Post_DF_DS_x.py	1.1	May 24 2007	
		All variants: V42B_FIPS_Default_1024.py V42B_FIPS_Default_1280.py V42B_FIPS_Default_1536.py V42B_FIPS_Default_1752.py V42B_FIPS_Default_1880.py	1.0	May 21 2007	
		cardlib.py	1.0	22.06.2007	Cardlib Script Files in Python format (necessary for execution of the Personalization Scripts)
		Apdu.py	1.14		
		Chips.py	1.2		
		codeLen.py	1.6		
		Constants.py	1.33		
		CsfParser.py	1.9		
		DevInifile.py	1.10		
		DirectInterface.py	1.16		
		EchoAPDU.py	1.9		
		EchoInterface.py	1.7		
		Exceptions.py	1.4		
		__init__.py	1.0		
		ExpandedRules.py	1.2		
		Interface.py	1.13		
		InterfaceToCard.py	1.16		
		Iso.py	1.26		
		locate.py	1.39		
		m_classes.py	1.29		
		m_functions.py	1.17		
		m3constants.py	1.1		
		m4lib.py	1.0		
		MAC.py	1.0		
		MAC3.py	1.0		
		makeOptions.py	1.2		
		OsVersionCNS.py	1.5		
		OsVersionHPC1.py	1.15		
		OsVersionM3.py	1.3		
		OsVersionM4.py	1.33		
		OsVersionM401.py	1.2		
		OsVersionM401a.py	1.2		
		OsVersionM401x.py	1.2		
		OsVersionM401y.py	1.3		
		OsVersionM403.py	1.25		
		OsVersionM410.py	1.15		
		OsVersionM420.py	1.4		

No.	Type	Term	Version	Date	Form of delivery
		OsVersions.py	1.11		
		OsVersionV42B.py	1.7		
		OsVersionV42BCNS.py	1.2		
		OsVersionV42CNS.py	1.2		
		OsVersionV43.py	1.4		
		OsVersionV43B.py	1.4		
		OsVersionV43BCNS.py	1.3		
		OsVersionV43CNS.py	1.2		
		Pcsc.py	1.13		
		setBaudRate.py	1.1		
		SM.py	1.24		
		tracer.py	1.4		
		translateAddr.py	1.2		
		xd.py	1.3		
		romkeys.py (Default keys)	1.26.1.0		
		reader.ini (Card Reader configuration file)	1.0	23.11.2006	Config File
		M3_Crypto.dll	1.2	02.05.2006	Crypto Library components (used for SM calculation)
		Des_crypt.dll	1.2	02.05.2006	
		rsa_crypt.dll	1.1	25.02.2003	
		m3lib.pyd	1.5	27.08.2003	
		Python-2.3.4.exe	2.3.4		Python Programming Language
		Python Cryptography Toolkit	2.0.1		Python CryptoLibrary (used for SM calculation)
3	Software CommandSet_ Extension Package	V42B_CommandSet_Ext_Package.csf	1.2	Jun 15 2007	Personalization Script Files in CSF format, after whose execution the resp. code will be loaded and activated in EEPROM
4	Software CAT Package	V42B_CAT_Package.csf	1.2	Jun 15 2007	
5	Software DRNG Package	V42B_DRNG_Package.csf	1.3	Jun 15 2007	
6	Software WIPE Package	V42B_WIPE Package.csf	1.1	Jun 06 2007	
7	Software HMAC Package (optional)	V42B_HMAC_Package.csf	1.2	Jun 15 2007	
9	Documentation	CardOS V4.2B User's Manual	1.0	09/2005	Paper form or PDF-File
10	Documentation	CardOS V4.2B Packages & Release Notes	1.0	05/2007	Paper form or PDF-File
11	Documentation	CardOS V4.2B CAT_DRNG_WIPE	1.0	05/2007	Paper form or PDF-File

No.	Type	Term		Version	Date	Form of delivery
		Packages & Release Notes				
12	Documentation	Administrator Guidance CardOS V4.2B FIPS		1.4	07/2007	Paper form or PDF-File
13	Documentation	User Guidance CardOS V4.2B FIPS		1.4	06/2007	Paper form or PDF-File
14	Documentation	ADS_Description CardOS V4.2B FIPS		1.0	05/2007	Paper form or PDF-File
15		(intentionally left blank)				
16	Hardware (Chip)	32K	Infineon SLE66CX322P	m1484b14 and m1484f18		Module
		64K	Infineon SLE66CX642P	m1485b16		
	Firmware RMS	RMS		Version 1.5		loaded in reserved area of User ROM
	Software crypto library	RSA2048 crypto library		Version 1.30		loaded in ROM
17	Software STS	STS Self Test Software		V53.10.13		Stored in Test ROM on the IC

1.4 Vendor

Siemens AG, Medical Solutions, MED GS SEC DS 1

Charles-de-Gaulle-Str. 2-3, D-81737 Munich, Germany

2. Functional Description[3]

The component is a Signature Creation Device consisting of the controller chip Infineon SLE66CX322P or SLE66CX642P and the software „CardOS V4.2B FIPS with Application for Digital Signature“.

CardOS V4.2B is a multifunctional smart card operating system (OS) supporting active and passive data protection. The operating system is designed to meet the

[3] 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.

most advanced security demands. CardOS V4.2B complies with the ISO standard family ISO 7816 part 3, 4, 5, 8 and 9.

“CardOS V4.2B FIPS with application Digital Signature” is designed to meet the requirements of the German Digital Signature Act.

The CardOS V4.2B DRNG Package implements the functionality of a high quality ‘Deterministic Random Number Generator’.

The CardOS V4.2B CAT Package implements the functionality of ‘Cryptographic Algorithm Tests’ via ‘Known Answer Tests’ for the algorithms RSA, RSA_SIG, RSA2_SIG, 3DES, MAC3, SHA-1 and for the DRNG.

The CardOS V4.2B WIPE Package implements the possibility to delete a complete DF-tree, without prior deletion of sub-elements, after aquisition of the corresponding access right.

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

General features:

- CardOS V4.2B runs on the Infineon SLE66 chip family. The SLE66CX322P and SLE66CX642P chips with embedded security controller for asymmetric cryptography and with a 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 V4.2B FIPS 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.
- 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[4]: RSA with up to 2048 bit key length[5] (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 Simple Power Analysis and Differential Power Analysis.
- Support of ”Command Chaining” following ISO 7816-8.
- Asymmetric key generation “on chip” using a deterministic random number generator.
- Digital Signature functions “on chip”.
- Connectivity to external Public Key certification services.

Secure Messaging:

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

---

[4] 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.

[5] The SSCD uses only 1024 up to 1752 bit RSA keys (with ext. APDU mode up to 1880 bit).

3. Compliance with the Signature Act and the Signature Ordinance

3.1 Compliance

The Signature Creation Device „Smart Card with Controller SLE66CX322P or SLE66CX642P, CardOS V4.2B FIPS with Application for Digital Signature“ (in the sequel abbreviated as "SSCD[6]") 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. The number of SSCDs in operational use must not exceed 83 million.
2. It is not allowed to change or extend the „Application for digital Signature“ without a re-evaluation and re-confirmation.
3. The certification service provider (CSP) and the involved parties (software develoiper and card manufacturer) are responsible to prevent misuse of the functionality to load executable code, and to guarantee that exactly the code components listed under “Scope of Delivery” are loaded, the HMAC Package (no. 7) being optional.
4. Cryptographically strong random number generators have to be used to generate keys e. g. for Secure Messaging and other purposes (like authentication with challenge-response).

In addition, it is recommended to choose the ICCSN (unique 16 bytes long Integrated Circuit Card Serial Number) so that the first and last 8 Bytes are different for different cards.

---

6 for “Secure Signature Creation Device”

b) Configuration

The SSCD has exactly one configuration implementing the policy "one successful authentication allows for exactly one signature".

The module length of the RSA key pair can be configured in the range from 1024 to 1880 bits by choosing the corresponding personalisation script (cf. "Scope of Delivery").

The SSCD provides for a transport PIN mechanism enabling a secure delivery. The transport PIN can be correctly entered only once. The transport PIN cannot be used to initiate a signature creation.

The usage of PIN and PUK complies with the requirements of the German Signature Act; in particular, a correct entry of the PUK does not allow for the creation of a signature.

Hashing of data to be signed has to be performed outside the SSCD, using SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 or RipeMD160 algorithm.

c) Delivery and Personalisation

The CSP is responsible for the delivery of the SSCD; the delivery process has to be described in the security concept of the CSP in accordance with "CardOS® V4.2B FIPS Delivery and Operation, Edition 06/2007", version 1.00, June 06, 2007.

Personalisation may take place in two variants described in detail in document no. 12 (cf. “Scope of delivery”):

- "pre-loaded" variant: After the card has been prepared (initialized, key pair generation, personalized), it is delivered to the LRA, where the card holder has to i) activate all applications, ii) set for each application the corresponding PIN and PUK objects, iii) sign the request for the certificate(s) and iv) have the certificate(s) generated by the CA installed on his card. Before these activities, the authenticity of the card holder has to be checked; by using the transport PIN (delivered in advance), it can be tested if the card has been used previously.
- "post-loaded" variant: The partially initialized card (without signature application) is delivered to the card holder who has to go to a LRA where the loading of the signature application is performed and the card is activated. These procedures are secured by authentication measures (card ↔ LRA) and by secure messaging.

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 described in document no. 12 must not be altered.

d) Usage of the Product

With delivery of the SSCD to the CSP, the CSP has to be advised to strictly follow the operational requirements specified above under a), b) and c).

In operatioonal phase, the following requirements have to be met for an appropriate usage of the SSCD :

Requirements to the CSP

According to §6 Abs. 1 und 3 SigG, the CSP has to advise the card holder on the adequate 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 / card holder:

- The card holder has to use and keep the SSCD in such a way as to prevent mis-use and manipulation.
- The card holder applies the signature creation function only to data for which he intends to guarantee integrity and authenticity.
- The card holder keeps his identification data for the SSCD confidential.
- The card holder changes his identification data for the SSCD in regular intervals.
- The card holder uses the SSCD only in connection with a signature application component compliant to the German Electronic Signature Act[7].

Applications

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

3.3 Algorithms and corresponding Parameters

The SSCD uses the following algorithms: RSA (module length 1024 to 1880 bits). 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. 69, page 3759 as of April 12, 2007).

[7] for compliance to German legislation only.

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-1880).

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

Remark: Depending on the algorithm used for external hashing, the compliance period for the combined functionality (hashing and signing) may be restricted further.

3.4 Assurance Level and Strength of Mechanism

"CardOS V4.2B FIPS 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-04191-2007 as of August 13, 2007.

The controller SLE66CX322P[8] 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[9] 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.

[8] Design levels m1484b14 and m1484f18, with RSA 2048 V1.30 and including RMS 1.5

[9] Design level m1485b16, with RSA 2048 V1.30 and including RMS 1.5

The correct integration of "CardOS V4.2B FIPS 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 mandatory (according to SigV) for a SSCD were achieved (and partially exceeded).

End of Confirmation

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

Security Confirmation:
T-Systems.02192.TE.08.2007

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.com/ict-security
www.t-systems-zert.com