Sicherheitsbestätigung und Bericht

T-Systems.02192.TE.08.2007

SLE66CX322P oder SLE66CX642P / CardOS V4.2B FIPS 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, CardOS V4.2B FIPS 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.02192.TE.08.2007

Bonn, den 13.08.2007

(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 Signaturgesetz vom 16. Mai 2001 (BGBl. I S. 876), zuletzt geändert durch Artikel 4 des Gesetzes vom 26. Februar 2007 (BGBl. Jahrgang 2007, Teil I S. 179)

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 oder SLE66CX642P, CardOS V4.2B FIPS with Application for Digital Signature“

1.2 Auslieferung

Die verschiedenen Stufen und Wege der Auslieferung der technischen Komponente und die Abläufe der Initialisierung und Personalisierung sind im Dokument "CardOS® V4.2B FIPS, Delivery and Operation, Edition 06/2007", Version 1.00, 06.06.2007, in englischer Sprache detailliert beschrieben. Die Darstellung beschreibt die Auslieferung an den Chip-Hersteller, den ZDA, den Endnutzer und an Terminal-Entwickler sowie die Schritte der Initialisierung, Schlüsselerzeugung, Personalisierung und Zertifikatsinstallation.

1.3 Lieferumfang

Neben dem im Abschnitt 1.2 erwähnten Dokument "CardOS® V4.2B FIPS, Delivery and Operation, Edition 06/2007", Version 1.00, 06.06.2007, gehören folgende Komponenten zum Lieferumfang:

Anmerkung: In der folgenden Tabelle fehlt in der Spalte "Nr." die Zahl 8: Dies ist kein Fehler, sondern aus Gründen der Vergleichbarkeit mit Hersteller-Dokumenten (insbesondere dem Security Target) so übernommen worden.

Nr.	Art	Bezeichnung	Version	Datum	Übergabeform
1	Software (Operating System)	CardOS V4.2B	C809	05.07.05	in ROM / EEPROM geladen
2	Software Application Digital Signature	***Pre-loaded Variante:*** V42B_FIPS_InitScript.py	1.1	24.05.2007	Personalisierungsskripte im Python Format, nach deren Ausführung das ADS^3 in das in EEPROM geladen wird
		V42B_FIPS_InitScript_DF_DS_x.py	1.0	15.05.2007	
		V42B_FIPS_PersScript.py	1.1	24.05.2007	

Nr.	Art	Bezeichnung	Version	Datum	Übergabeform
	(Anwendung / Datenstrukturen)	V42B_FIPS_PersScript_DF_DS_x .py	1.1	24.05.2007	
		V42B_FIPS_CAScript.py	1.1	24.05.2007	
		V42B_FIPS_CAScript_DF_DS_x.py	1.0	15.05.2007	
		V42B_FIPS_RAScript.py	1.1	24.05.2007	
		V42B_FIPS_RAScript_DF_DS_x.py	1.2	04.06.2007	
		Post-loaded Variante: V42B_FIPS_InitScript_Post.py	1.1	24.05.2007	
		V42B_FIPS_LRAScript_Post.py	1.1	24.05.2007	
		V42B_FIPS_LRAScript_Post_DF_DS_x.py	1.1	24.05.2007	
		Alle Varianten: 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	21.05.2007	
		cardlib.py	1.0	22.06.2007	Cardlib Script Files im Python Format (erforderlich für die Ausführung der Personalisierungsskripte)
		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		

[3] ADS = Application Digital Signature

Nr.	Art	Bezeichnung	Version	Datum	Übergabeform
		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		
		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	Konfigurationsdatei
		M3_Crypto.dll	1.2	02.05.2006	Komponenten der Crypto Library
		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 Programmiersprache
		Python Cryptography Toolkit	2.0.1		Python Crypto Library

Nr.	Art		Bezeichnung	Version	Datum	Übergabeform
3	Software CommandSet_ Extension Package		V42B_CommandSet_Ext_Package.csf	1.2	15.06.2007	Personalisierungsskripte in CSF Format, nach deren Ausführung der entspr. Code in das EEPROM geladen und aktiviert wird.
4	Software CAT Package		V42B_CAT_Package.csf	1.2	15.06.2007	
5	Software DRNG Package		V42B_DRNG_Package.csf	1.3	15.06.2007	
6	Software WIPE Package		V42B_WIPE Package.csf	1.1	06.06.2007	
7	Software HMAC Package (optional)		V42B_HMAC_Package.csf	1.2	15.06.2007	
9	Dokumentation		CardOS V4.2B User's Manual	1.0	09/2005	Papier / pdf Datei
10	Dokumentation		CardOS V4.2B Packages & Release Notes	1.0	05/2007	Papier / pdf Datei
11	Dokumentation		CardOS V4.2B CAT_DRNG_WIPE Packages & Release Notes	1.0	05/2007	Papier / pdf Datei
12	Dokumentation		Administrator Guidance CardOS V4.2B FIPS	1.4	07/2007	Papier / pdf Datei
13	Dokumentation		User Guidance CardOS V4.2B FIPS	1.4	06/2007	Papier / pdf Datei
14	Dokumentation		ADS_Description CardOS V4.2B FIPS	1.0	05/2007	Papier / pdf Datei
15						
16	Hard-ware (Chip)	32K	Infineon SLE66CX322P[4]	m1484b14 und m1484f18		Module
		64K	Infineon SLE66CX642P[5]	m1485b16		
	Firmware RMS		RMS	Version 1.5		In reservierten Bereich des User ROM geladen
	Software crypto library		RSA2048 crypto library	Version 1.30		in ROM geladen
17	Software STS		STS Self Test Software	V53.10.13		Im Test ROM auf dem IC gespeichert

[4] Production Line Indicator 2 or 5.

[5] Production Line Indicator 5.

1.4 Hersteller

Siemens AG, Medical Solutions, MED GS SEC DS 1

Charles-de-Gaulle-Str. 2-3, 81737 München

2. Funktionsbeschreibung[6]

Das Produkt ist eine Signaturerstellungseinheit bestehend aus dem Prozessorchip Infineon SLE66CX322P oder SLE66CX642P und der Software „CardOS V4.2B FIPS with Application for Digital Signature“.

CardOS V4.2B FIPS ist ein multifunktionales Smart Card Betriebssystem, das aktiven und passiven Datenschutz unterstützt. Das Betriebssystem wurde entwickelt, um höchsten Sicherheitsanforderungen zu genügen. CardOS V4.2B FIPS ist konform zu ISO 7816-3, -4, -5, -8 und -9.

"CardOS V4.2B FIPS with Application for Digital Signature" wurde entwickelt, um den Anforderungen des deutschen Signaturgesetzes zu genügen.

Das CardOS V4.2B DRNG Package implementiert die Functionalität eines Deterministischen Zufallszahlen-Generators hoher Qualität.

Das CardOS V4.2B CAT Package implementiert die Funktionalität eines ‘Cryptographic Algorithm Tests’ mit ‘Known Answer Tests’ für die Algorithmen RSA, RSA_SIG, RSA2_SIG, 3DES, MAC3, SHA-1 und für den DRNG.

Das CardOS V4.2B WIPE Package implementiert die Möglichkeit, nach Erhalt der entsprechenden Zugriffsrechte einen vollständigen DF-Baum zu löschen, ohne vorherige Löschung von Sub-Elementen.

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

<u>Generelle Eigenschaften von CardOS V4.2B FIPS</u>:

- Läuft auf der Infineon SLE66 Chip-Familie. Die SLE66CX322P und SLE66CX642P Chips mit integriertem Security Controller für asymmetrische

---

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

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 V4.2B FIPS 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.
- 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[7]: RSA mit bis zu 2048 Bit Schlüssellänge[8] (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:

- Kompatibel mit ISO 7816-4
- für jedes Kommando und jedes Datenobjekt (Datei, Schlüssel) unabhängig definierbar.

3. Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Die Signaturerstellungseinheit „Chipkarte mit Prozessor SLE66CX322P oder SLE66CX642P, CardOS V4.2B FIPS 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.

---

7 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.

8 Die bestätigte SSEE verwendet für RSA-Schlüssel nur die Schlüssellängen von 1024 bis zu 1752 Bit bzw. 1880 Bit (Letzteres mit ext. APDU mode).

3.2 Einsatzbedingungen

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

a) Grundsätzliches

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

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

3. Die Zertifizierungsdiensteanbieter (ZDA) und die beteiligten Rollen (Software- und Kartenhersteller) sind dafür verantwortlich, die missbräuchliche Nutzung der Funktionalität zum Laden von ausführbarem Code zu verhindern und somit dafür zu sorgen, dass genau die unter "Lieferumfang" genannten Code-Komponenten geladen werden, wobei das HMAC Package (Nr. 7) optional ist.

4. Es sind kryptografisch starke Zufallszahlengeneratoren für die Generierung von Schlüsseln z. B. für das Secure Messaging und andere Zwecke (z. B. die Authentisierung über challenge-response) zu verwenden.

Zusätzlich wird empfohlen, die ICCSN (eindeutige 16 Byte lange Integrated Circuit Card Serial Number) so zu wählen, dass die ersten und letzten 8 Byte für verschiedene Karten unterschiedlich gewählt werden.

b) Konfiguration

Die SSEE besitzt nur eine Konfiguration, und zwar entsprechend der Vorgabe "Eine erfolgreiche Authentisierung erlaubt genau eine Signatur".

Durch die Auswahl der Personalisierungsskripte (s. "Lieferumfang") wird die Modullänge des RSA-Schlüsselpaares von 1024 bis 1880 gesteuert.

Die SSEE verfügt über eine Transport-PIN für die sichere Auslieferung. Die Transport-PIN kann nur einmal korrekt eingegeben werden. Mit der Transport-PIN kann keine Signaturerstellung erfolgen.

Die Verwendung von PIN und PUK entspricht den Vorgaben des Signaturgesetzes, insbesondere ermöglicht die richtige Eingabe eines PUK keine Signaturerzeugung.

Das Hashen zu signierender Daten muss außerhalb der SSEE erfolgen, und zwar nach den Verfahren SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 oder RipeMD160.

c) Auslieferung und Personalisierung

Die Auslieferung der SSEE durch den ZDA liegt in der Verantwortung des ZDA und ist in dessen Sicherheitskonzept in Übereinstimmung mit den Anforderungen in "CardOS® V4.2B FIPS Delivery and Operation, Edition 06/2007", Version 1.00, 06.06.2007 zu beschreiben.

Bei der Personalisierung werden zwei Varianten unterschieden, die im Dokument Nr. 12 (s. "Lieferumfang") detailliert beschrieben sind:

- Bei der Variante "pre-loaded" wird die Karte nach Initialisierung, Schlüsselgenerierung und Personalisierung an eine LRA ausgeliefert. Der Karteninhaber muss vor Ort in der LRA alle Anwendungen aktivieren, die PIN- und PUK-Objekte für jede Anwendung festlegen sowie den Zertifikatsrequest signieren und erhält danach die von der CA erzeugten Zertifikate auf seine Karte installiert. Vor diesen Aktivitäten wird die Authentizität des Antragstellers geprüft; mithilfe einer (vorher ausgelieferten) Transport-PIN wird geprüft, ob die entsprechende Karte bereits früher genutzt wurde.
- Bei der Variante "post-loaded" wird die teil-initialisierte Karte (noch ohne Signaturanwendung) vorher an den Antragsteller ausgeliefert, der seinerseits mit der Karte zur LRA gehen muss, um dort die Signaturanwendung auf seine Karte installiert zu bekommen und diese aktivieren zu können. Diese Vorgänge sind durch Authentisierungsmaßnahmen (Karte $\leftrightarrow$ LRA) und Secure Messaging gesichert.

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 im Dokument Nr. 12 beschriebenen Abläufen darf nicht abgewichen werden.

d) Nutzung des Produktes

Mit Auslieferung der SSEE 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:

<u>Anforderungen an den ZDA</u>

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: RSA (Schlüssellängen 1024 bis 1880 Bit). 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 (vgl. Bundesanzeiger Nr. 69, S. 3759 vom 12. April 2007) 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-1880).

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

Hinweis: Abhängig von dem beim externen Hashen verwendeten Algorithmus kann der Bestätigungsstatus der Gesamtfunktionalität (Hashen und Signieren) weiter zeitlich eingeschränkt sein.

3.4 Prüfstufe und Mechanismenstärke

"CardOS V4.2B FIPS 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-04191-2007 vom 13.08.2007 vor.

Der Prozessor SLE66CX322P[9] 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[10] 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 V4.2B FIPS 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

[9] Designstände m1484b14 und m1484f18, mit RSA 2048 V1.30 und einschließlich RMS 1.5

[10] Designstand m1485b16, mit RSA 2048 V1.30 und einschließlich RMS 1.5

Sicherheitsbestätigung:
T-Systems.02192.TE.08.2007

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