T Systems

Sicherheitsbestätigung und Bericht

T-Systems. 02122.TE.05.2005

SLE66CX322P / CardOS V4.3B / Applikation für digitale Signatur

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, Betriebssystem CardOS V4.3B mit Applikation für digitale Signatur“

den nachstehend genannten Anforderungen des SigG und der SigV entspricht.

Die Dokumentation zu dieser Bestätigung ist registriert unter:

T-Systems. 02122.TE.05.2005

Bonn, den 27.05.2005

_____
(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. 1 des Ersten Gesetzes zur Änderung des Signaturgesetzes (1. SigÄndG) vom 04. Januar 2005 (BGBl. Jahrgang 2005, Teil I, Nr. 1)

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

Die Bestätigung zur Registrierungsnummer T-Systems. 02122.TE.05.2005 besteht aus 10 Seiten.

Beschreibung des Produktes für qualifizierte elektronische Signaturen:

1. Handelsbezeichnung des Produktes für qualifizierte elektronische Signaturen

Handelsbezeichnung:

Signaturerstellungseinheit „Chipkarte mit Prozessor SLE66CX322P, Betriebssystem CardOS V4.3B mit Applikation für digitale Signatur“

Auslieferung:

Die Chipkarte wird vom Kartenhersteller an den ZDA per Kurier ausgeliefert. Alternativ kann der ZDA die Chipkarten beim Kartenhersteller abholen.

Lieferumfang:

Nr.	Typ	Bezeichnung	Version	Datum	Art der Auslieferung
0	Hardware	Prozessor Infineon SLE66CX322P, m1484b14 und m1484f18	Production Line Numbers: 2 für m1484b14 5 für m1484f18	-	Chipkarte
1	Software: Betriebssystem	CardOS V4.3B	C808	-	In ROM / EEPROM geladen
2	Software: Applikation/ Datenstruktur	SigG application	vgl. Tabelle 2 und Fußnote[3]	vgl. Tabelle 2 und Fußnote[3]	Script Files zur Personalisierung (.CSF)
3	Software	Service Pack	1.11	22.04.2005	Package enthalten in Skripts
4	Software	CERT Package	1.4	28.04.2005	Package enthalten in Skripts
5	Dokumentation	CardOS V4.3 User’s Manual	1.0	06/2004	Papierform oder PDF-File

[3] Sequences for centralised and decentralised personalisation, PersAppSigG(_withoutPUK).csf (Rev. 1.5), Pre-PersAppSigG(_withoutPUK).csf (Rev. 1.5) und Post-PersAppSigG(_withoutPUK).csf (Rev. 1.3) with five Defines_XXXX.csf (XXXX=1024, 1280, 1536, 1792 and 2048) (Rev. 1.2), Siemens AG, 09.05.2005

6	Dokumentation	User's Manual CardOS V4.3, Correction Sheet	0.1	05/2005	Papierform oder PDF-File
7	Dokumentation	CardOS V4.3B Administrator Guidance	0.7	10.05.2005	Papierform oder PDF-File
8	Dokumentation	Application SigG, CardOS V4.3B	0.2	08.04.2005	Papierform oder PDF-File
9	Dokumentation	CardOS V4.3B User Guidance	0.7	09.05.2005	Papierform oder PDF-File

Tabelle 1: Auslieferungsumfang

Nr.	Bezeichnung	Revision	Datum
a	PersAppSigG_withoutPUK.csf	1.5	09.05.2005
b	PersAppSigG.csf	1.5	09.05.2005
c	Pre-PersAppSigG.csf	1.5	09.05.2005
d	Pre-PersAppSigG_withoutPUK.csf	1.5	09.05.2005
e	Post-PersAppSigG.csf	1.3	09.05.2005
f	Post-PersAppSigG_withoutPUK.csf	1.3	09.05.2005
g	Defines_1024.csf	1.2	09.05.2005
h	Defines_1280.csf	1.2	09.05.2005
i	Defines_1536.csf	1.2	09.05.2005
j	Defines_1792.csf	1.2	09.05.2005
k	Defines_2048.csf	1.2	09.05.2005

Tabelle 2: Skript-Komponenten

Hersteller:

Siemens AG, Com ESY SEC DS1

Charles-de-Gaulle Straße 2, 81737 München

2. Funktionsbeschreibung[4]

Das Produkt ist eine Signaturerstellungseinheit bestehend aus dem Prozessorchip Infineon SLE66CX322P und der Software „CardOS V4.3B mit Applikation für digitale Signatur".

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

CardOS V4.3B ist auf dem **Infineon SLE66CX322P Chip** implementiert. Dieser Chip besitzt einen eingebetteten Security Controller für asymmetrische Kryptographie und einen echten Zufallszahlengenerator.

CardOS V4.3B mit **Applikation für Digitale Signatur** wurde entwickelt, um den Anforderungen des Signaturgesetzes zu genügen.

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

Generelle Eigenschaften von CardOS V4.3B:

- CardOS V4.3B läuft auf der Infineon SLE66 Chip-Familie. Der SLE66CX322P Chip mit integriertem Security Controller für asymmetrische Kryptografie und echtem Zufallszahlengenerator wurde 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.

---

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

Das Dateisystem:

CardOS V4.3B 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[5]: 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.

---

[5] 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.

Secure Messaging[6]:

- Kompatibel mit ISO 7816-4.
- Kann für jedes Kommando und jedes Datenobjekt unabhängig definiert werden.

3. Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

Die Signaturerstellungseinheit „Chipkarte mit Prozessor SLE66CX322P, Betriebssystem CardOS V4.3B mit Applikation für digitale Signatur“ 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 Signaturerstellungseinheit unter den angegebenen Einsatzbedingungen (Abschnitt 3.2) und unter Beachtung der nachfolgenden Restriktionen erfüllt.

1. Ohne Re-Evaluierung und erneute Sicherheitsbestätigung ist es nicht zulässig, eine Änderung oder Erweiterung der sicherheitsbestätigten Applikation „Digitale Signatur“ vorzunehmen.

2. ZDAs müssen sicherstellen, dass – mit Ausnahme der definierten Software in Tabelle 1 (s. Lieferumfang) – kein anderer ausführbarer Code auf die Smartcard geladen wird. Es ist insbesondere nicht zulässig, andere Packages außer dem Service Pack und dem CERT Package zu laden. ZDAs müssen sicherstellen, dass ein Missbrauch der Funktionalität zum Laden von Packages wirksam verhindert wird.

3.2 Einsatzbedingungen

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

---

[6] Die Applikation für digitale Signatur nutzt das secure messaging nicht. Deshalb ist secure messaging nicht Gegenstand dieser Sicherheitsbestätigung.

a) Personalisierung und technische Einsatzumgebung

Die Personalisierung kann zentral oder dezentral erfolgen.

- Im zentralen Fall erfolgt die Personalisierung vollständig beim Zertifizierungsdiensteanbieter; dabei kommt das Personalisierungsscript für die zentrale Personalisierung zum Einsatz.
- Im dezentralen Fall erfolgt eine sogenannte Vorpersonalisierung zentral beim Zertifizierungsdiensteanbieter mit Hilfe des Vorpersonalisierungsscripts.
  Anschließend vollendet eine dezentrale Registrierungsstelle (als ausgelagerte Einheit des ZDA) die Personalisierung; diese sogenannte Nachpersonalisierung wird mit Hilfe des Nachpersonalisierungsscripts ausgeführt.

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

Der Zertifizierungsdiensteanbieter (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 in Abschnitt 1: Nr. 7 und Nr. 8) beschriebenen Abläufen darf nicht abgewichen werden.

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

b) Auslieferung und Konfigurationen der Signaturerstellungseinheit

Die Auslieferung der personalisierten oder vorpersonalisierten Chipkarte durch den ZDA liegt in der Verantwortung des ZDA und ist in dessen Sicherheitskonzept zu beschreiben.

Die Signaturerstellungseinheit verfügt über eine fünfstellige Transport-PIN mit einem Fehlbedienungszähler von 3. Bei abgelaufenem Fehlbedienungszähler ist die Inbetriebnahme der Signaturfunktionalität permanent gesperrt. Die Transport-PIN kann genau einmal benutzt werden. Sie dient dem Signaturschlüsselinhaber dazu, eine PIN und einen PUK (sofern das PUK-Objekt angelegt ist) zu setzen. Mit der Transport-PIN kann keine Signaturerstellung erfolgen.

Die Bestandteile der Signaturerstellungseinheit sind in Tabelle 1 und Tabelle 2 (Abschnitt 1) aufgelistet. Die Signaturerstellungseinheit besitzt genau eine Konfiguration, verfügt aber über Parameter, die während der Personalisierung eingestellt und nach ihrer einmaligen Einstellung nicht mehr verändert werden können. Diese Parameter sind:

1. Modullänge des RSA-Schlüsselpaares: von 1024 bis 2048 mit Schrittweite 8

2. PUK-Objekt angelegt und verwendbar: ja / nein
   Wenn das PUK-Objekt angelegt und verwendbar ist, verfügt die Signaturerstellungseinheit über einen PUK (Personal Unblocking Key) mit folgender Funktionalität: Bei richtiger Eingabe des PUK kann der Fehlbedienungszähler der PIN auf seinen Initialwert gesetzt werden. Bei richtiger Eingabe des PUK kann ein neuer Wert des PUK gesetzt werden. Die Anzahl der Benutzungen der PUK-Funktionalität ist begrenzt. Die richtige Eingabe des PUK ermöglicht keine Signaturerzeugung. Die Länge des PUK kann 6 bis 12 Zeichen betragen. Dem PUK ist ein Fehlbedienungszähler zugeordnet. Der Wert des Fehlbedienungszählers richtet sich nach der minimalen Länge des PUK und wird während der Personalisierung geeignet festgelegt. Näheres enthält die in Tabelle 1 unter Nr. 7 genannte Dokumentation.
3. Anzahl N der elektronischen Signaturen, die nach einmaliger Authentisierung ohne erneute Authentisierung erzeugt werden können: N = 1 bis N = 254 mit Schrittweite 1 oder keine Beschränkung (N = 0 und N = 255).
   Bei den für Endkunden (Kartenhalter) bestimmten Signaturerstellungseinheiten ist stets N = 1 zu setzen: Hierdurch wird nach Authentisierung mittels PIN die Erzeugung genau einer elektronischen Signatur erlaubt. Die Erzeugung jeder weiteren elektronischen Signatur erfordert jeweils eine erneute Authentisierung.

   Unter diese Sicherheitsbestätigung fallen auch Signaturerstellungseinheiten, die zum Einsatz in besonders gesicherten Umgebungen (z.B. beim ZDA) bestimmt sind und die nach einmaliger PIN-Authentisierung die Generierung von mehreren oder unendlich vielen Signaturen erlauben ($N \neq 1$).

Die Länge der PIN kann 6 bis 12 Zeichen betragen. Der PIN ist ein Fehlbedienungszähler zugeordnet. Der Wert des Fehlbedienungszählers richtet sich nach der minimalen Länge der PIN und wird während der Personalisierung geeignet festgelegt. Näheres enthält die in Tabelle 1 unter Nr. 7 genannte Dokumentation.

Anwendungen, die die Signaturerstellungseinheit „Chipkarte mit Prozessor SLE66CX322P, Betriebssystem CardOS V4.3B mit Applikation für digitale Signatur“ nutzen, sind **nicht** Gegenstand dieser Bestätigung.

c) Nutzung des Produktes

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

Anforderungen an den Zertifizierungsdiensteanbieter

- Die Erzeugung des für die Signaturanwendung benötigten Schlüsselpaares auf einer für Endkunden (Kartenhalter) vorgesehenen Signaturerstellungseinheit („N = 1“) darf nur in einer besonders gesicherten Umgebung (z. B. bei einem akkreditierten ZDA) erfolgen.

- Die Erzeugung des für die Signaturanwendung benötigten Schlüsselpaares in den Fällen „N ≠ 1“ darf nur unter Einhaltung besonderer Sicherheitsvorkehrungen (z.B. unter behördlicher Aufsicht) erfolgen.
- Signaturerstellungseinheiten mit einer Einstellung „N ≠ 1“ dürfen nur in besonders gesicherten Einsatzumgebungen betrieben werden, in denen ein Missbrauch der Signaturerstellungsfunktionen sicher auszuschließen ist. Eine solche Einsatzumgebung liegt typischerweise bei einem akkreditierten ZDA vor.
- Im Fall „N ≠ 1“ 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.
- Signaturerstellungseinheiten mit einer Einstellung „N ≠ 1“ dürfen nicht als Signaturerstellungseinheiten an Endkunden (Kartenhalter) ausgeliefert werden. Es ist die Aufgabe des jeweiligen ZDAs, dies sicherzustellen.

PIN, PUK und Transport-PIN:

i) Die Einbringung der Identifikationsdaten (PIN und ggf. PUK) in die Signaturerstellungseinheit wird vom Signaturschlüsselinhaber vorgenommen. Während der Personalisierung werden lediglich die entsprechenden Datenobjekte angelegt und mit nicht relevanten Daten gefüllt. Bezüglich dieser nicht relevanten Daten bestehen keine Anforderungen an den Zertifizierungsdiensteanbieter.

ii) Als Mittel zur Sicherung auf dem Transportweg gegen unerkannte unbefugte Benutzung der Signaturerstellungseinheit wird eine Transport-PIN genutzt. Der Zertifizierungsdiensteanbieter muss den Kartenhalter über den Transport-PIN-Mechanismus[7], seine relevanten Eigenschaften und seine sachgerechte Benutzung gemäß §6 Abs. 1 und 3 SigG unterrichten.

- Der Zertifizierungsdiensteanbieter darf von dem gemäß i) und ii) vorgesehenen Verfahren nicht abweichen. Jede Änderung bedarf der vorherigen Prüfung der Sicherheit und der Bestätigung, dass die Anforderungen des SigG und der SigV erfüllt sind.

Mit Auslieferung der Signaturerstellungseinheit „Chipkarte mit Prozessor SLE66CX322P, Betriebssystem CardOS V4.3B mit Applikation für digitale Signatur“ an den ZDA ist dieser auf die Einhaltung der oben genannten Einsatzbedingungen hinzuweisen.

---

[7] Der Transport-PIN-Mechanismus erfordert keine Speicherung der Identifikationsdaten (PIN und ggf. PUK) außerhalb der Signaturerstellungseinheit.

Allgemeine Anforderungen an den Endanwender

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

3.3 Algorithmen und zugehörige Parameter

Die Signaturerstellungseinheit „Chipkarte mit Prozessor SLE66CX322P, Betriebssystem CardOS V4.3B mit Applikation für digitale Signatur“ stellt die Algorithmen SHA-1 und RSA (Schlüssellängen 1024 bis 2048 Bit) bereit.

Die gemäß § 11 Abs. 3 in Verbindung mit Anlage I Nr. 2 SigV festgestellte Eignung von **SHA-1** reicht mindestens bis Ende des Jahres 2010 (s. Bundesanzeiger Nr. 59 - S. 4695-4696 vom 30. März 2005).

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 (s. Bundesanzeiger Nr. 59 - S. 4695-4696 vom 30. März 2005) 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 mit Applikation für digitale Signatur“ wurde auf dem Prozessor SLE66CX322P 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-04121-2005 vom 20. Mai 2005 vor.

Der Prozessor SLE66CX322P wurde erfolgreich nach den Common Criteria 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.

Die sicherheitstechnisch korrekte Integration von „CardOS V4.3B mit Applikation für digitale Signatur“ und des Prozessors SLE66CX322P 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. 02122.TE.05.2005

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