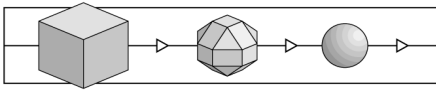




Zertifizierungsregeln

Zertifizierungsstelle der T-Systems



Vorwort

Ziel dieses Dokumentes ist es, Interessenten über

- die Regeln der Zertifizierung,
- den Ablauf von Zertifizierungsverfahren und
- die zu beachtenden Rahmenbedingungen

zu informieren.

Dieses Dokument wird laufend nach den Erfordernissen aktualisiert und auf dem Web unter www.t-systems-zert.com („Service-Bereich“) zum Download bereit gestellt.

Für Durchführung eines Verfahrens ist stets die zum Zeitpunkt des Vertragsabschlusses gültige Fassung anzuwenden.

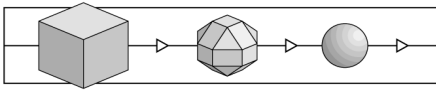
Eine Beschreibung der Zertifizierungsprogramme der T-Systems findet man im „Certification Practice Statement“ (CPS), das an gleicher Stelle publiziert wird.

© T-Systems GEI GmbH, 2000-2008

Verteiler: öffentlich

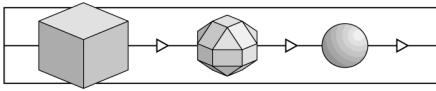
Für weitere Auskünfte ist die Zertifizierungsstelle wie folgt erreichbar:

- ✉ Zertifizierungsstelle der T-Systems
c/o T-Systems GEI GmbH, Rabinstr.8, 53111 Bonn
- ☎ +49-(0)228-9841-0, FAX -60
- 🌐 www.t-systems-zert.com



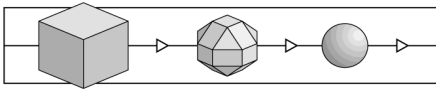
Inhaltsverzeichnis

1	Verfahrensablauf	5
1.1	Vorgespräche	5
1.2	Antrag auf Zertifizierung	5
1.3	Start des Verfahrens	6
1.4	Prüfaktivitäten	6
1.5	Abschluss des Verfahrens	6
1.6	Aufrechterhaltung nach Änderungen	7
2	Zertifizierungsregeln	8
2.1	Pflichten der Zertifizierungsstelle	8
2.2	Pflichten des Auftraggebers	8
2.2.1	Alle Zertifizierungsprogramme	8
2.2.2	Zertifizierungsprogramme 01, 02, 04, 09	9
2.2.3	Zertifizierungsprogramme 03, 05, 06, 07, 08	10
3	Sonstiges	12
3.1	Vertraulichkeit	12
3.2	Auskünfte und Veröffentlichungen	12
3.3	Verfahrenskosten und Haftung	12
3.4	Beschwerdeverfahren	13



Revisionsliste

Version	Datum	Aktivität
0.9	08.09.2000	Erst-Erstellung
1.0	28.02.2001	Aktualisierung
1.1	04.07.2001	Aktualisierung
1.2	01.08.2001	Aktualisierung aufgrund neuer Services
1.3	09.01.2002	Umbenennungen
1.4	01.06.2002	Aktualisierung der Services, kleine Korrekturen
1.5	02.01.2003	Namensänderungen, entspr. Anpassungen; Aufnahme von s4b
1.6	07.08.2003	Ergänzungen in Abschnitt 4.3 und 5.6
1.7	27.10.2003	Änderungen: © und Adressangaben
1.8	22.07.2004	Abgleich mit Web
1.9	04.03.2005	Aktualisierung der Prüfgrundlagen und Verfahrensnamen
2.0	04.04.2005	Aufnahme von ETSI 101.456
2.1	25.07.2005	Aktualisierung wg. BNetzA
2.2	31.10.2005	Kleinere Reparaturen
2.3	23.02.2006	Update Standards
2.4	18.01.2007	Programm-Anpassungen, verschiedene Aktualisierungen
2.5	06.06.2007	Anpassungen für das Verfahren 08
2.6	19.07.2007	Aktualisierung der AGB
3.0	18.03.2008	Aufteilung in CPS und Richtlinien



1 Verfahrensablauf

In den folgenden Abschnitten wird der typische Ablauf eines Zertifizierungsverfahrens beschrieben.

1.1 Vorgespräche

Bei diesem Verfahrensabschnitt wird der Interessent mit allen notwendigen Informationen versorgt, bevor eine Entscheidung zur Durchführung einer Zertifizierung getroffen wird.

Themen sind:

- Gegenstand der Zertifizierung
- Vertraulichkeit der Informationen
- anzuwendendes Zertifizierungsprogramm
- Rechte und Pflichten der Beteiligten
- Sicherheitskriterien
- vorhandene / zu erstellende Dokumente
- Verfahrensablauf
- Meilensteinplan, Zeit und Kosten

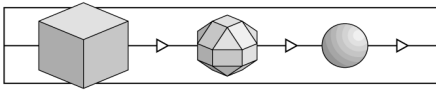
1.2 Antrag auf Zertifizierung

Die Zertifizierungsstelle erstellt auf Anfrage und unter Berücksichtigung der Vorgespräche ein Angebot über die gewünschte Zertifizierung.

Das Angebot benennt den Zertifizierungsgegenstand, das anzuwendende Zertifizierungsprogramm, die technischen und administrativen Vorgaben an den Auftraggeber zur Erlangung des Zertifikats, beinhaltet eine grobe Terminplanung sowie die weiteren kommerziellen Bedingungen.

Der Antrag auf Erteilung eines Zertifikats kommt durch die formelle Annahme des Angebots zustande. Das Auftragsschreiben muss von einem zur Unterschrift Bevollmächtigten des Auftraggebers unterzeichnet sein, und insbesondere den Unternehmensnamen, seine Rechtsform sowie die Anschrift laut Handelsregister enthalten.

Das vorliegende Dokument „Zertifizierungsregeln“ ist stets Angebots- und Vertragsbestandteil.



1.3 Start des Verfahrens

Ein Verfahren wird nach Stellung des Zertifizierungsantrags gestartet.

Die Zertifizierungsstelle teilt dem Verfahren anschließend eine Verfahrenskennung zu, die vom Auftraggeber zu Referenzzwecken (bei Kunden etc.) verwendet werden kann. Sofern der Auftraggeber einverstanden ist, kann das Zertifizierungsverfahren unter www.t-systems-zert.com angekündigt werden

Es findet bei Bedarf ein gemeinsames Kick-Off Meeting aller Beteiligten statt. Der Terminplan für das Verfahren wird einvernehmlich festgelegt.

Arbeitsort für die Durchführung des Verfahrens sind die Geschäftsräume der Zertifizierungsstelle - mit Ausnahme ggf. verfahrensbedingt durchzuführender Audits und Inspektionen in den Geschäftsräumen des Auftraggebers.

Die am Projekt beteiligten Parteien entscheiden gemeinsam über ggf. notwendige Änderungen am Zertifizierungsauftrag, z. B. den Zertifizierungsgegenstand und die Abwicklung der Prüfung betreffend.

1.4 Prüftaktivitäten

Je nach Art des Prüfverfahrens werden Prüfschritte von der beauftragten Prüfstelle (unter Begleitung durch die Zertifizierungsstelle), von Auditoren oder von der Zertifizierungsstelle selbst durchgeführt.

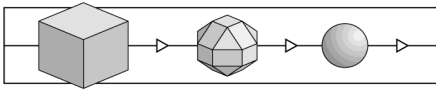
Über den Ablauf und das Ergebnis der Prüfungen werden Prüf-, Audit- oder Inspektionsberichte erstellt, die dem Auftraggeber jeweils zur inhaltlichen Prüfung vorgelegt werden. Hat er keine Einwände, gilt der Bericht als formell abgenommen. Bestehen Einwände, wird die Zertifizierungsstelle darüber nach pflichtgemäßem Ermessen entscheiden und die Entscheidung dem Auftraggeber mitteilen.

1.5 Abschluss des Verfahrens

Nach erfolgreicher Prüfung wird ein Zertifikat bzw. eine Bestätigung ausgestellt. Bei bestimmten Verfahrenstypen wird zusätzlich ein Zertifizierungsreport oder ein Anhang zum Zertifikat erstellt. Diese Unterlagen werden dem Auftraggeber in elektronischer und gedruckter Form übergeben.

Unter www.t-systems-zert.com kann in Abstimmung mit dem Auftraggeber das Zertifikat, die Sicherheitsbestätigung, der Zertifizierungsreport und / oder der Anhang zum Zertifikat veröffentlicht werden.

Verfahrensbedingt kann es erforderlich sein, diese Unterlagen an Aufsichtsstellen (Bundesamt für Sicherheit in der Informationstechnik, Bundesnetzagentur, Akkreditierer) weiterzuleiten oder diesen Stellen Einblick in die Unterlagen zu geben.



Hinsichtlich der Veröffentlichung der Zertifizierungsergebnisse durch solche Stellen ist die Zertifizierungsstelle der T-Systems an deren Fristen gebunden und kann keine Termine für die Veröffentlichung garantieren.

Ist das Zertifizierungsverfahren insgesamt nicht erfolgreich abgeschlossen worden, enthält der abschließende Bericht die maßgeblichen Gründe. Der Auftraggeber kann nach Behebung der Mängel eine erneute Prüfung veranlassen.

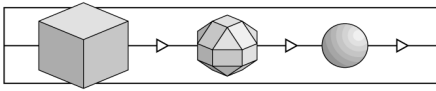
Alle Unterlagen aus dem Verfahren werden bei der Zertifizierungsstelle archiviert. Falls eine Hinterlegung des Prüfobjektes bei der Zertifizierungsstelle vereinbart ist (z. B. bei Produkten), wird eine entsprechende Verwahrung eingeleitet. Näheres wird zwischen den Beteiligten abgestimmt.

1.6 Aufrechterhaltung nach Änderungen

Hinsichtlich der Aufrechterhaltung des Zertifikats wird der Auftraggeber beim Abschluss eines Zertifizierungsprojektes beraten, kann sich aber später jederzeit mit der Zertifizierungsstelle abstimmen.

Nach Änderungen am Gegenstand der Zertifizierung, Änderungen an den Prüfgrundlagen oder bei neuen Sicherheitserkenntnissen ist über die Aufrechterhaltung, die Änderung, Erweiterung oder Rücknahme des Zertifikats zu entscheiden. Im Einzelnen:

- Wird der Gegenstand der Zertifizierung verändert oder erweitert, ist je nach Art der Änderung eine Erweiterung des Zertifikats auf die geänderte Fassung (ggf. unter Auflagen) oder die Beschränkung des Zertifikats auf die alte Fassung möglich.
- Bei Änderungen an den Prüfgrundlagen wird die Zertifizierungsstelle den Auftraggeber frühzeitig informieren und ihn insofern beraten, als die Auswirkungen der Änderung auf den Zertifizierungsgegenstand und seine Zertifizierung erläutert werden. Möglicherweise kann das Zertifikat auf der Basis der veränderten Prüfgrundlagen nicht ohne Weiteres aufrechterhalten werden und bedarf einer erneuten Prüfung.
- Führen neue Sicherheitserkenntnisse dazu, dass ein Zertifikat aus technischen Gründen nicht mehr zu rechtfertigen ist, besteht für den Auftraggeber die Gelegenheit, erkannte Schwachstellen in angemessener Frist zu beseitigen: Diese Vorgänge sind kriteriengerecht zu dokumentieren, die Zertifizierungsstelle ist entsprechend zu informieren. Die Zertifizierungsstelle entscheidet aufgrund dieser Mitteilung, ob die Zertifizierung (ggf. unter Auflagen) aufrechterhalten werden kann oder zurückgezogen werden muss.



2 Zertifizierungsregeln

2.1 Pflichten der Zertifizierungsstelle

Die Zertifizierungsstelle ist gemäß der einschlägigen Norm DIN EN 45011 bei DATech in TGA GmbH unter der DAR-Registriernummer DAT-ZE-015/98-01 akkreditiert.

Die Erfüllung der Normen DIN EN 45011 und die Aufrechterhaltung der entsprechenden Akkreditierung sind für die Zertifizierungsstelle unverzichtbar. Folgende Grundsätze und Verpflichtungen sind daraus für die Dienste der Zertifizierungsstelle ableitbar:

- Die Zertifizierungsprogramme der Zertifizierungsstelle sind allen Interessenten zugänglich.
- Neutralität und Objektivität sind gewahrt und eine Gleichbehandlung aller Auftraggeber ist sichergestellt.
- Soweit technische Prüfungen durch unabhängige Prüfstellen durchgeführt werden, ist eine Gleichbehandlung aller Prüfstellen garantiert.
- Interessen und Vorbehalte Dritter haben keinerlei Einfluss auf die Verfahren und Ergebnisse der Zertifizierungsstelle.

Die Zertifizierungsstelle ist gehalten, diese Grundsätze dauerhaft umzusetzen, und wird diesbezüglich durch den Akkreditierungsgeber und Aufsichtsstellen überwacht.

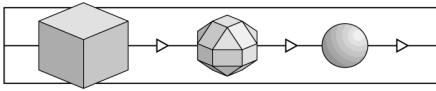
2.2 Pflichten des Auftraggebers

Der Auftraggeber verpflichtet sich mit Auftragserteilung zur dauerhaften Einhaltung der nachfolgenden Grundsätze (aus der DIN EN 45011 und den jeweiligen Prüfkriterien).

Bei wesentlicher Nichtbeachtung dieser Auflagen behält sich die Zertifizierungsstelle vor, Ankündigungen unter www.t-systems-zert.com zu löschen, Zertifikate oder Bestätigungen nicht zu erteilen, erteilte Zertifikate oder Bestätigungen zurückzuziehen.

2.2.1 Alle Zertifizierungsprogramme

1. Bei der Verteilung von Zertifikaten und Bestätigungen ist immer die aktuelle Version zu verwenden.
2. Eine Bezugnahme auf das zertifizierte Objekt in Presse-Erklärungen, Werbeschriften o.ä. muss in eindeutiger Form erfolgen und darf nicht irreführend sein; insbesondere darf die Zertifizierung nur benutzt werden, um auf die Konformität des zertifizierten Objektes zu dem angewendeten Standard hinzuweisen.



3. Wird ein Zertifikat entzogen, darf dieses nicht mehr verwendet werden.
4. Neue Erkenntnisse über Eigenschaften eines zertifizierten Objektes – z.B. aus Beanstandungen von Kunden - hat der Auftraggeber aufzuzeichnen und der Zertifizierungsstelle auf Verlangen zugänglich zu machen.
5. Führen neue Sicherheitserkenntnisse dazu, dass ein Zertifikat aus technischen Gründen nicht mehr zu rechtfertigen ist, besteht für den Auftraggeber die Gelegenheit, erkannte Schwachstellen in angemessener Zeit zu beseitigen, dies zu dokumentieren und die Zertifizierungsstelle entsprechend zu informieren.
6. Die Zertifizierungsstelle überwacht grundsätzlich die Verwendung ihrer Zertifikate, Bestätigungen und Prüfsiegel. Bei irreführender oder missbräuchlicher Verwendung behält sich die Zertifizierungsstelle korrigierende, bekanntmachende oder im Extremfall rechtliche Schritte vor.
7. Die Zertifizierung darf durch den Auftraggeber nicht so angewendet werden, dass die Zertifizierungsstelle in Verruf gebracht wird.

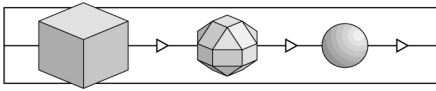
2.2.2 Zertifizierungsprogramme 01, 02, 04, 09

Zusätzlich zu den allgemeinen Regeln aus Abschnitt 2.2.1 sind die folgenden Regeln für Verfahren nach den Zertifizierungsprogrammen

- 01 Zertifizierung nach ITSEC/CC,
- 02 Sicherheitsbestätigung für technische Komponenten nach dem Signaturgesetz,
- 04 Deutsches IT-Sicherheitszertifikat,
- 09 Zertifizierungen im Gesundheitswesen.

zu beachten:

- a. Die Zertifizierungsstelle erhält das Recht zur Einsicht in alle prüfungsrelevanten Unterlagen des Auftraggebers sowie in die Prüfberichte der beauftragten Prüfstelle.
- b. Produkte und Systeme sowie ihre Dokumentation sind vom Auftraggeber so zu kennzeichnen, dass geänderte Versionen eindeutig an neuen Versionsnummern, Release-Ständen, etc. erkennbar sind.
- c. Spätestens 3 Monate nach Start des Zertifizierungsverfahrens ist eine Prüfstelle mit der technischen Evaluierung zu beauftragen.



- d. Die Zertifizierungsstelle hat das Recht, nach Ankündigung und zum Zwecke einer Prüfung die Entwicklungsumgebung des Auftraggebers zu betreten und zu inspizieren.
- e. Im Zertifizierungsangebot kann festgelegt sein, dass die Zertifizierungsstelle ein Exemplar des Zertifizierungsgegenstandes (Produkt oder System) archiviert.
- f. Der Auftraggeber hat die Pflicht, die Zertifizierungsstelle unverzüglich über Änderungen an dem zertifizierten Objekt zu informieren.
- g. Neue Versionen von früher zertifizierten Produkten / Systemen dürfen erst dann als „zertifiziert“ bezeichnet werden, wenn eine erfolgreiche Re-Zertifizierung durchgeführt worden ist.
- h. Die Zertifizierungsstelle ist zu informieren, wenn das zertifizierte Objekt nicht mehr lieferbar ist.

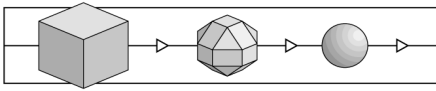
2.2.3 Zertifizierungsprogramme 03, 05, 06, 07, 08

Zusätzlich zu den allgemeinen Regeln aus Abschnitt 2.2.1 sind die folgenden Regeln für Verfahren nach den Zertifizierungsprogrammen

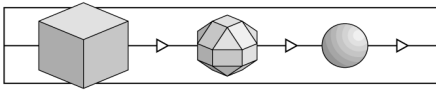
- 03 Sicherheitsbestätigung für Zertifizierungsdiensteanbieter nach dem Signaturgesetz,
- 05 Zertifizierung von Geschäftsprozessen und Services,
- 06 Bestätigung der Konformität zu EHI-Kriterien,
- 07 Zertifizierung von Organisation und Technik,
- 08 Sicherheit für den Mittelstand

zu beachten :

- A. Die Zertifizierungsstelle erhält das Recht zur Einsicht in alle Unterlagen des Auftraggebers, soweit dies für die Prüfung nach den zugrunde liegenden Kriterien erforderlich ist.
- B. Erforderliche Dokumente sind vom Auftraggeber so zu kennzeichnen, dass geänderte Versionen eindeutig an neuen Versionsnummern, Release-Ständen, etc. erkennbar sind.
- C. Die Zertifizierungsstelle hat das Recht, nach Ankündigung die Liegenschaften des Auftraggebers zu betreten und zu inspizieren, soweit dies für die Prüfung erforderlich ist.



- D. Änderungen am Gegenstand der Zertifizierung, seiner Dokumentation und seiner realen Implementierung müssen durch den Auftraggeber aufgezeichnet werden; die Zertifizierungsstelle ist entsprechend zu informieren.
- E. Ein geänderter Gegenstand darf erst dann als "zertifiziert" bezeichnet werden, wenn die Zertifizierungsstelle dies autorisiert.



3 Sonstiges

3.1 Vertraulichkeit

Die Wahrung der Vertraulichkeit von Informationen, die im Rahmen von Verfahren anfallen, ist ein zentraler Grundsatz der Zertifizierungsstelle. Hierfür ist ein System von drei Vertraulichkeitsstufen eingerichtet, deren Auswahl durch das Angebot und die Beauftragung vorgenommen wird:

Standard: Zugang zu bei der Zertifizierungsstelle gespeicherten verfahrensbezogenen Informationen haben alle Zertifizierer und Auditoren der Zertifizierungsstelle, die IT-Administration der T-Systems sowie die ggf. beteiligte Prüfstelle. Bei der elektronischen Übertragung von Daten wird individuell entschieden, ob Daten zu verschlüsseln sind.

Need-To-Know: Zugang zu bei der Zertifizierungsstelle gespeicherten bzw. zu übertragenen verfahrensbezogenen Informationen haben nur die am Verfahren beteiligten Zertifizierer, Auditoren und die ggf. beteiligte Prüfstelle. Bei der elektronischen Übermittlung werden Daten nach einem zwischen den Beteiligten abgestimmten Verfahren verschlüsselt.

Hoch: Es werden die Verfahren aus dem staatlichen Verschlusssachenbereich angewendet. Alle Mitarbeiter von der Zertifizierungsstelle unterliegen der Geheimschutzbetreuung durch das „Bundesministerium für Wirtschaft“ und sind zum Umgang mit staatlichen Verschlusssachen mindestens bis zum Grad „geheim“ ermächtigt.

3.2 Auskünfte und Veröffentlichungen

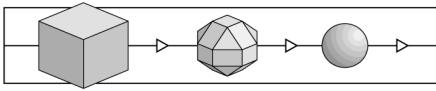
Auskünfte über den Stand laufender Prüfungen werden von der Zertifizierungsstelle nicht an Dritte weitergegeben - es sei denn, der Auftraggeber stimmt explizit zu.

Eine Veröffentlichung von Prüfergebnissen durch die Zertifizierungsstelle erfolgt nur mit Zustimmung des Auftraggebers. Verfahrensbedingt muss die Zertifizierungsstelle aber Dritten (z.B. aufsichtsführenden Behörden, Akkreditierer) eine Einsicht in Prüfergebnisse gewähren.

Alle von der Zertifizierungsstelle veröffentlichten Dokumente enthalten Copyright-Vermerke, die Auskunft über die Möglichkeit der Vervielfältigung durch Dritte geben: Die T-Systems GEI GmbH behält das Copyright für ihre Zertifikate, Bestätigungen und Berichte, jedoch ist der Auftraggeber berechtigt, diese Unterlagen zu vervielfältigen und zu verteilen – vorausgesetzt, dass Inhalt und Format ungeändert bleiben.

3.3 Verfahrenskosten und Haftung

Für die Durchführung eines Verfahrens werden Kosten nach Aufwand erhoben. Näheres wird im Angebot festgelegt.



Zertifizierungskosten werden stets im vereinbarten Umfang erhoben - unabhängig davon, ob ein Zertifikat erteilt worden ist oder wegen technischer Mängel nicht erteilt werden konnte, das Verfahren durch den Auftraggeber abgebrochen oder wegen Nicht-Bereitstellung der notwendigen Informationen durch die Zertifizierungsstelle eingestellt worden ist.

Werden vom Auftraggeber Änderungen an von ihm bereits abgenommenen Berichten, Zertifikaten und Bestätigungen gewünscht, wird der Mehraufwand dem Auftraggeber zusätzlich in Rechnung gestellt. Dies gilt auch für die Durchführung von Wiederholungsprüfungen, wenn solche aus Gründen, die beim Auftraggeber liegen, erforderlich werden. Auftraggeber und Zertifizierungsstelle stimmen sich hierüber vorher ab.

Die jedem Angebot beigefügten Allgemeinen Geschäftsbedingungen (AGB) beschreiben die Art und den Umfang der Haftung durch die T-Systems.

3.4 Beschwerdeverfahren

Gegen Entscheidungen der Zertifizierungsstelle kann vom den beteiligten (Auftraggeber, Prüfstelle) Beschwerde eingelegt werden. Das Beschwerdeverfahren sieht vor,

- zunächst eine Einigung über den strittigen Sachverhalt mit dem für das betreffende Verfahren zuständigen Zertifizierer zu erzielen,
- wenn dies nicht möglich ist, eine Einigung mit dem Leiter von der Zertifizierungsstelle herbeizuführen,
- wenn dies nicht möglich ist, sich an das Lenkungsgremium zu wenden; letzteres entscheidet über die Beschwerde unter Anhörung der Betroffenen und gibt seine Entscheidung gemäß seiner Geschäftsordnung den Betroffenen bekannt.

Die Anschrift des Lenkungsgremiums lautet:

Lenkungsgremium der Zertifizierungsstelle
c/o T-Systems GEI GmbH
Rabinstr.8
53111 Bonn

Dieses Schlichtungsverfahren präjudiziert weder den Rechtsweg, noch schließt es ihn aus.

Im Lenkungsgremium sind Anwender, Hersteller, Prüfstellen und die T-Systems GEI GmbH als Betreiber der Zertifizierungsstelle vertreten. Dem Lenkungsgremium gehören in der Mehrheit Experten an, die nicht Mitarbeiter der T-Systems sind.

Ende von: Zertifizierungsregeln

Zertifizierungsregeln

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