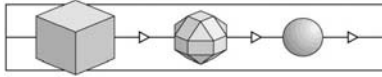




Certification Practice Statement

Dienstleistungen der T-Systems im Bereich
Zertifizierung



Vorwort

Im vorliegenden Dokument werden die Dienstleistungen der Zertifizierungs- und Bestätigungsstelle der T-Systems beschrieben. Ziel ist es, Interessenten über die existierenden Zertifizierungsprogramme der T-Systems zu informieren.

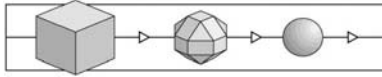
Das Dokument wird fortlaufend nach den Erfordernissen aktualisiert und auf dem Web unter www.t-systems-zert.com (Menü „Service-Bereich“) zum Download bereit gestellt.

© T-Systems GEI GmbH, 2000-2011

Verteiler: öffentlich

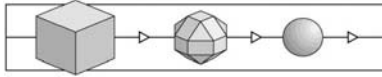
Für weitere Auskünfte ist die Zertifizierungsstelle wie folgt erreichbar:

Zertifizierungsstelle der T-Systems
T-Systems GEI GmbH, Vorgebirgsstr. 49, 53119 Bonn
Tel. +49-(0)228-9841-0, Fax -6000
www.t-systems-zert.com



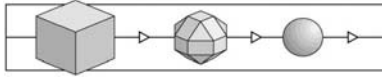
Inhaltsverzeichnis

1	EINFÜHRUNG.....	5
1.1	MISSION DER ZERTIFIZIERUNG	5
1.2	NUTZEN DER ZERTIFIZIERUNG	6
1.3	ZERTIFIZIERUNGSSTELLE DER T-SYSTEMS	7
2	DIENSTLEISTUNGEN DER ZERTIFIZIERUNGSSTELLE DER T-SYSTEMS	10
2.1	ZERTIFIZIERUNGSPROGRAMME.....	10
2.1.1	<i>01 Zertifizierung nach CC/ITSEC.....</i>	<i>10</i>
2.1.2	<i>02 Sicherheitsbestätigung für technische Komponenten nach dem Signaturgesetz</i>	<i>11</i>
2.1.3	<i>03 Sicherheitsbestätigung für Zertifizierungsdiensteanbieter nach dem Signaturgesetz... ..</i>	<i>11</i>
2.1.4	<i>03a PKI Zertifizierung nach ETSI 101456 bzw. ETSI 102042.....</i>	<i>12</i>
2.1.5	<i>04 Deutsches IT-Sicherheitszertifikat</i>	<i>13</i>
2.1.6	<i>05 Zertifizierung von Geschäftsprozessen und Services.....</i>	<i>13</i>
2.1.7	<i>07 Zertifizierung von Organisation und Technik</i>	<i>14</i>
2.1.8	<i>08 Sicherheit für den Mittelstand</i>	<i>14</i>
2.1.9	<i>09 Zertifizierungen im Gesundheitswesen</i>	<i>15</i>
2.2	ERGÄNZENDE SERVICES	15



Revisionsliste

Revision	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 101456
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 Zertifizierungsregeln
3.1	01.06.2010	Änderung der Anschrift und editorische Anpassungen; das Programm 06 wurde eingestellt.



1 Einführung

1.1 Mission der Zertifizierung

Informations- und Kommunikationstechnik (ICT) spielen in der modernen Gesellschaft eine so herausragende Rolle, dass kein Bereich ohne sie auskommt. Umfragen und Analysen haben gezeigt, dass eine Abhängigkeit von der stetigen Einsatzbereitschaft der Technik besteht: Moderne Großunternehmen sehen ihre Existenz bedroht, wenn ihre IT länger als einen Tag nicht zur Verfügung steht oder nicht wie erwartet funktioniert. Für Klein- und mittelständische Unternehmen beträgt die Toleranzfrist etwa eine Woche.

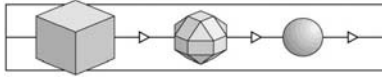
Angesichts solcher Abhängigkeiten, einer Vielzahl von Manipulationsfällen und Sicherheitslücken verwundert es nicht, dass die Sicherheit von Informations- und Telekommunikationstechnik im kommerziellen, behördlichen und privaten Umfeld an Relevanz gewonnen hat.

Die IT-Sicherheit ist mittlerweile Gegenstand von Gesetzen und Verordnungen, Voraussetzung für die Teilnahme an Ausschreibungen und ein wesentlicher Faktor bei Kaufentscheidungen vieler Kunden und Anwender.

Die Sicherheit der Informationsverarbeitung und der Geschäftsprozesse ist in diesem Sinne ein wesentlicher Eckpfeiler der Unternehmensvorsorge geworden. Hier gilt es Risiken zu erkennen, Schäden zu reduzieren und Schwachstellen auszumerzen.

Sicherheit in diesem Sinne ist durch die klassischen Sicherheitsziele der Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit von Daten bestimmt. Damit verbunden können auch Ziele der Verbindlichkeit, der Revisionssicherheit, des Datenschutzes und der Ordnungsmäßigkeit sein.

Nicht zuletzt im Zusammenhang mit der Globalisierung der Wirtschaft, der Einführung neuer Dienstleistungen im Bereich der Kommunikation und der Diskussion um Persönlichkeitsrechte treten neue Sicherheitsziele wie die Anonymität, der Schutz von Urheberrechten und die Zurechenbarkeit und Unfälschbarkeit von Daten und Transaktionen (z.B. durch elektronische Signaturen) stärker in den Vordergrund.



Die Risiken bei der Anwendung von Informations- und Kommunikationstechnik werden zukünftig noch ansteigen, wenn nicht durch qualifizierte Sicherheitsvorkehrungen und entsprechende Prüf- und Abnahmeprozesse gegengesteuert wird.

Die Aufgabe der Zertifizierung besteht in der Einrichtung und dem Betrieb eines Systems, in dem solche Prüfungen und Abnahmen in objektiver und unabhängiger Weise durchgeführt werden können.

Durch solche Prozesse wird die Sicherheit wesentlich gefördert, da mit den Prüf- und Zertifizierungsberichten eine Transparenz erzeugt wird, die für Entwickler, Anbieter, Betreiber und Nutzer von ICT unverzichtbar ist.

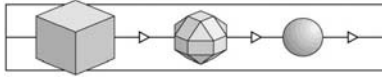
1.2 Nutzen der Zertifizierung

Wie in anderen Technikbereichen zielt ein Zertifizierungsprozess auf die Ausstellung eines Zertifikates, mit dem bestimmte Sicherheitseigenschaften eines Produktes oder Systems, einer Dienstleistung oder eines Geschäftsprozesses für die Betroffenen transparent gemacht werden.

Das Zertifikat ist eine unabhängige Bestätigung dafür, dass die behaupteten Sicherheitseigenschaften tatsächlich vorhanden sind und die beabsichtigten Sicherheitsziele erreicht werden.

Die Zertifizierung hat für die betroffenen Zielgruppen (Entwickler, Anbieter, Betreiber und Nutzer von ICT) unterschiedliche Bedeutung:

- Entwickler von Produkten benötigen im Entwicklungsprozess frühzeitig Informationen über Sicherheitslücken und Beratung über normenkonforme Entwicklungsverfahren. Prüf- und Zertifizierungsverfahren sollten deshalb parallel zur Produktentwicklung laufen.
- Anbieter von Produkten brauchen Bestätigungen über die Sicherheitsleistungen ihrer Produkte, um im internationalen Markt bestehen, gesetzlichen und kundenspezifischen Anforderungen genügen zu können.



- Immer wichtiger werden Sicherheitsbestätigungen auch für die Anbieter von Dienstleistungen, insbesondere in den Bereichen der Informationsverarbeitung und der Telekommunikation.
- Betreiber bzw. Nutzer brauchen zuverlässige Bestätigungen über die Sicherheit von Produkten und externen Dienstleistungen, um diese adäquat in ihre Systeme und Geschäftsprozesse integrieren zu können.
- System-Zertifizierungen und die Zertifizierung von Geschäftsprozessen können darüber hinaus den Bedarf von Unternehmen und Behörden nach ganzheitlicher Sicherheit decken.

Diese Prozesse müssen auf der Basis einschlägiger Sicherheitskriterien bzw. -standards durchgeführt werden, wenn sie für die genannten Zielgruppen einen Nutzen bringen sollen. Sicherheitskriterien und Sicherheitsstandards haben teilweise schon Eingang in gesetzliche Vorgaben gefunden, die für die genannten Zielgruppen relevant sind, z.B. für den Kontext der elektronischen Signatur.

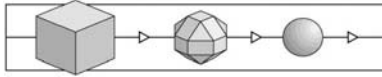
Die Anwendung international akzeptierter Kriterien bildet die unerlässliche Voraussetzung für eine internationale Anerkennung der ausgestellten Zertifikate.

1.3 Zertifizierungsstelle der T-Systems

Die Zertifizierungsstelle der T-Systems bietet vor dem beschriebenen Hintergrund eine Reihe von Services an, die eine objektive Prüfung und Zertifizierung der Sicherheit

- von IT-Produkten, IT-Systemen und -Netzwerken sowie
- von IT-Dienstleistungen und IT-gestützten Geschäftsprozessen

erlauben. Diese Services basieren auf Standards und normativen Dokumenten wie z.B. die Common Criteria, ITSEC, ISO/IEC 2700x, ETSI-Standards, nationale und europäische Vorgaben zur elektronischen Signatur, Anforderungen aus dem deutschen Gesundheitswesen, eigenen Prüfvorschriften der Zertifizierungsstelle sowie weiteren branchen- bzw. kundenspezifischen Vorgaben.



Die Zertifizierungsstelle der T-Systems ist für ihre Services erstmalig im Juni 1998 akkreditiert worden. Die aktuelle Akkreditierungsurkunde – ausgestellt durch die DATech in TGA GmbH – findet man unter www.t-systems-zert.com.

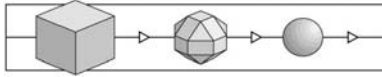
Sie enthält im Anhang die akkreditierten Zertifizierungsprogramme, die sich auf die „Sicherheit von IT-Produkten, IT-Systemen, IT-Dienstleistungen und IT-gestützten Geschäftsprozessen“ beziehen.

Die Zertifizierungsstelle wirkt in Prüf- und Zertifizierungsschemata mit, die von folgenden Institutionen betrieben werden:

- Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen:
 - Die Zertifizierungsstelle der T-Systems ist als Bestätigungsstelle für die Sicherheitsbestätigung von Produkten nach dem deutschen Signaturgesetz durch die Bundesnetzagentur anerkannt.
 - Die Zertifizierungsstelle der T-Systems ist für die Prüfung und Bestätigung von Zertifizierungsdiensteanbietern (ZDA) als Prüf- und Bestätigungsstelle nach dem deutschen Signaturgesetz durch die Bundesnetzagentur anerkannt.
- Notified Body gemäß EU Direktive 1999/93/EG Im Zusammenhang mit der EU Direktive 1999/93/EG ist die Zertifizierungsstelle der T-Systems ein Notified Body¹.
- Weiterhin ist die Zertifizierungsstelle der T-Systems für die Prüfungen nach ETSI TS 101456 und ETSI TS 102042 akkreditiert.
- Gematik: Die Zertifizierungsstelle der T-Systems als "Zertifizierungs- / Bestätigungsstelle für IT-Sicherheitstechnik für Komponenten" im Rahmen des Zulassungsverfahrens der Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH anerkannt.

Bei Prüfungen und Zertifizierungen spielt die Vertraulichkeit der Informationen des Auftraggebers stets eine große Rolle. Die Zertifizierungsstelle der T-Systems verfügt über eine

¹ gemäß Artikel 3 (4) dieser Richtlinie, s. www.europa.eu.int und www.fesa.rtr.at

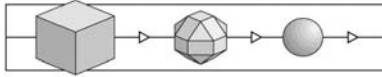


organisatorische und technische Infrastruktur, die für den Umgang mit staatlichen Ver-
schluss-sachen mindestens bis zum Grad „geheim“ geeignet ist.

Im Sinne der DIN EN 45011 untersteht die Zertifizierungsstelle einem Lenkungsgremium, in
dem Anwender, Hersteller, Prüfstellen und die T-Systems GEI GmbH als Betreiber der
Zertifizierungsstelle vertreten sind. Dem Lenkungsgremium gehören in der Mehrheit Si-
cherheitsexperten an, die nicht Mitarbeiter der T-Systems sind. Die Anschrift des
Lenkungsgremiums lautet:

Lenkungsgremium der Zertifizierungsstelle
T-Systems GEI GmbH
Vorgebirgsstr. 49
53119 Bonn

Das Lenkungsgremium und der Akkreditierungsgeber achten insbesondere darauf, dass die
Verfahren der Zertifizierungsstelle allen Interessenten zugänglich sind, Neutralität und
Objektivität gewahrt sind und eine Gleichbehandlung aller Auftraggeber sichergestellt ist.



2 Dienstleistungen der Zertifizierungsstelle der T-Systems

2.1 Zertifizierungsprogramme

Die Zertifizierungsstelle der T-Systems bietet die folgenden Zertifizierungsprogramme an:

2.1.1 01 Zertifizierung nach CC/ITSEC

Es können IT-Produkte und IT-Systeme nach den Common Criteria oder den ITSEC evaluiert und zertifiziert werden. Die Evaluierung wird von anerkannten Prüflaboratorien durchgeführt, die von der Zertifizierungsstelle der T-Systems lizenziert sind. Die Zertifizierungsstelle überwacht die Evaluierungen und stellt die Zertifikate und Zertifizierungsreporte aus.

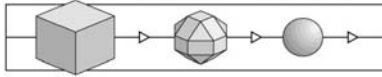
Maßgebend für dieses akkreditierte Programm sind folgende Dokumente:

- Common Criteria for Information Technology Security Evaluation^{2,3}
- Common Methodology for Information Technology Security Evaluation²
- Kriterien für die Bewertung der Sicherheit von Produkten und Systemen der Informationstechnik (ITSEC)^{4,3},
- Handbuch für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEM)⁴,
- „Guideline für Prüfstellen“, Zertifizierungsstelle der T-Systems, aktuelle Fassung.

² Die Dokumente sind unter www.commoncriteriaportal.org abrufbar.

³ in Verbindung mit den Europäischen (JIL, Joint Interpretation Library) und nationalen Kriterieninterpretationen des BSI (AIS)

⁴ Die Dokumente sind unter www.t-systems-zert.com (Service-Bereich) abrufbar.



2.1.2 02 Sicherheitsbestätigung für technische Komponenten nach dem Signaturgesetz

In diesem Programm werden Sicherheitsbestätigungen zur Vorlage bei der Bundesnetzagentur herausgegeben, und zwar für technische Komponenten, die gemäß deutschem Signaturgesetz einer Sicherheitsbestätigung bedürfen. Hierzu ist die Evaluierung solcher Komponenten nach den Common Criteria oder den ITSEC (s. Zertifizierungsprogramm 01) durch anerkannte und lizenzierte Prüflaboratorien erforderlich.

Neben den genannten Kriterien liegen folgende Vorgaben bei diesem akkreditierten Programm zugrunde:

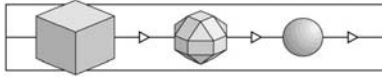
- Deutsches Signaturgesetz (SigG)
- Deutsche Signaturverordnung (SigV)
- aktuelle Veröffentlichungen hinsichtlich zugelassener kryptographischer Algorithmen für die relevanten technischen Komponenten
- Spezifikation von Einsatzbedingungen für Signaturanwendungskomponenten, Bundesnetzagentur
- Protokolle der Arbeitsgruppe anerkannter Bestätigungsstellen (AGAB)
- Guideline 02-SIG "Anforderungen an PKI-Produkte", Zertifizierungsstelle der T-Systems, aktuelle Fassung

2.1.3 03 Sicherheitsbestätigung für Zertifizierungsdiensteanbieter nach dem Signaturgesetz

In diesem Programm werden im Einklang mit dem deutschen Signaturgesetz Prüfungen des Sicherheitskonzeptes und seiner Umsetzung bei akkreditierenden Zertifizierungsdiensteanbietern (ZDA) durchgeführt und entsprechende Sicherheitsbestätigungen zur Vorlage bei der Bundesnetzagentur erteilt.

Sicherheitsbestätigte ZDA erfüllen auch die Anforderungen der EU-Direktive 1999/93/EG.

Bei diesem akkreditierten Verfahren sind folgende Vorgaben zu beachten:



- Deutsches Signaturgesetz (SigG)
- Deutsche Signaturverordnung (SigV)
- aktuelle Veröffentlichungen hinsichtlich zugelassener kryptographischer Algorithmen für die relevanten technischen Komponenten
- Spezifikation von Einsatzbedingungen für Signaturanwendungskomponenten, Bundesnetzagentur
- Protokolle der Arbeitsgruppe anerkannter Bestätigungsstellen (AGAB)
- Guideline 03-SIG "Anforderungen an PKI-Betreiber", Zertifizierungsstelle der T-Systems, aktuelle Fassung.

2.1.4 03a PKI Zertifizierung nach ETSI 101456 bzw. ETSI 102042

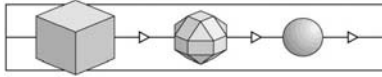
Im internationalen Bereich hat die Norm ETSI TS 101456 eine wichtige Bedeutung für Zertifizierungsdiensteanbieter von qualifizierten Zertifikaten erlangt. Eine Reihe von Schemata (z.B. in den Niederlanden und in der Schweiz) legen diese Norm zugrunde.

Mit dem Zertifizierungsprogramm 03a bietet die Zertifizierungsstelle der T-Systems die Prüfung, Auditierung und Zertifizierung von ZDA nach ETSI TS 101456 an.

Die Norm ETSI 102042 adressiert Zertifizierungsdiensteanbieter, deren Zertifikate nicht zwangsläufig qualifiziert im Sinne der EU-Direktive sind.

Bei diesem akkreditierten Zertifizierungsprogramm 03a sind folgende Dokumente maßgebend:

- EU-Direktive 1999/93/EG
- Entscheidung der Kommission vom 14. Juli 2003 über die Veröffentlichung von Referenznummern
- ETSI TS 101456: Policy requirements for certification authorities issuing qualified certificates, aktuelle Fassung



- ETSI TS 102042: Policy requirements for certification authorities issuing public key certificates, aktuelle Fassung
- Guideline 03-SIG "Anforderungen an PKI-Betreiber", Zertifizierungsstelle der T-Systems, aktuelle Fassung.

Dieses Zertifizierungsprogramm ist auch für andere Länder im Bereich der **EU** und darüber hinaus einsetzbar. Bezüglich der entsprechenden Vorschriften für die **Niederlande**, **Österreich** und die **Schweiz**⁵.

2.1.5 04 Deutsches IT-Sicherheitszertifikat

Es können IT-Produkte und IT-Systeme nach den ITSEC oder den Common Criteria evaluiert und zertifiziert werden. Die Evaluierung wird von anerkannten Prüflaboratorien durchgeführt, die von der Zertifizierungsstelle der T-Systems und vom BSI lizenziert sind. Die Zertifizierungsstelle der T-Systems überwacht die Evaluierungen und stellt die Zertifikate und Zertifizierungsberichte aus.

Dieses akkreditierte Programm wird z. Zt. eingestellt, da es vom BSI nicht weiter unterstützt wird. Entsprechende Evaluierungen können nunmehr unter dem Zertifizierungsprogramm 01 (s.o.) durchgeführt werden.

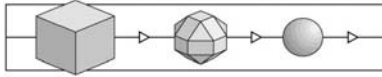
2.1.6 05 Zertifizierung von Geschäftsprozessen und Services

Unter Anwendung der methodischen Grundlage der **Common Criteria** werden Geschäftsprozesse und Services von Unternehmen in Bezug auf ihre Sicherheit geprüft und zertifiziert.

In der Prüfung enthalten sind eine Dokumentenprüfung sowie eine Umsetzungsprüfung in Form von (periodischen) Audits.

Für dieses akkreditierte Programm verwendet die Zertifizierungsstelle folgende Dokumente als Grundlage:

⁵ s. Links unter www.t-systems-zert.com (Menü „Service-Bereich“)



- Guideline 05-DPZ "Zertifizierung von Prozessen und Dienstleistungen", Zertifizierungsstelle der T-Systems, aktuelle Fassung
- Common Criteria for Information Technology Security Evaluation^{2,3}
- Common Methodology for Information Technology Security Evaluation².

2.1.7 07 Zertifizierung von Organisation und Technik

Unter Anwendung einer von T-Systems entwickelten Methode können IT-Systeme und Netzwerke einschließlich der Management-Prozesse in Bezug auf ihre Sicherheit geprüft und zertifiziert werden.

In diesem Programm enthalten sind eine Dokumentenprüfung auf verschiedenen Ebenen, technische Tests sowie eine Umsetzungsprüfung in Form von periodischen Audits.

Für dieses akkreditierte Programm verwendet die Zertifizierungsstelle folgende Dokumente:

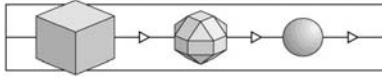
- Guideline 07-DOT "Zertifizierung von Organisation und Technik", Zertifizierungsstelle der T-Systems, aktuelle Fassung.

2.1.8 08 Sicherheit für den Mittelstand

In diesem Zertifizierungsprogramm wird das Verfahren 07 in einem speziellen Zuschnitt verwendet: Dabei sind drei Sicherheitsstufen festgelegt; die höchste Stufe „Professionelle Sicherheit“ enthält eine Zertifizierung.

Bei diesem akkreditierten Programm verwendet die Zertifizierungsstelle folgende Dokumente:

- Guideline 08-S4B "S4B – Professionelle Sicherheit: Kriterien für die Zertifizierung", Zertifizierungsstelle der T-Systems, aktuelle Fassung
- Guideline 07-DOT "Zertifizierung von Organisation und Technik", Zertifizierungsstelle der T-Systems, aktuelle Fassung
- ISO/IEC 2700x und ISO/IEC 17799



- Beschreibungen der Sicherheitsstufen "Basissicherheit", "Standardsicherheit", "Professionelle Sicherheit".

2.1.9 09 Zertifizierungen im Gesundheitswesen

Das Zertifizierungsprogramm 09 beinhaltet Zertifizierungen von technischen Komponenten nach den Regeln der Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik).

Die entsprechenden Vorgabedokumente finden sich auf den Web-Seiten der gematik⁶.

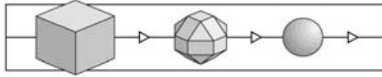
Die Verfahren werden auf der Grundlage der Zertifizierungsprogramme 01 und 02 durchgeführt.

2.2 Ergänzende Services

Die folgenden Dienstleistungen sind für jeden Verfahrenstyp verfügbar:

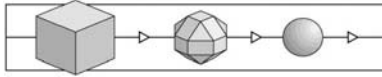
- Vorbereitung von Prüf- und Zertifizierungsverfahren in Form von Workshops.
- Ausbildung und Training von Entwicklern im Hinblick auf kriterienkonforme Entwicklung und Optimierung der Verfahren (auch Inhouse).
- Ausbildung von IT-Sicherheitsbeauftragten (mehrstufig mit Abschlusszertifikat; auch Inhouse).
- Übersetzung von Zertifikaten, Bestätigungen und Zertifizierungsreports in andere Sprachen.
- Vervielfältigungs- und Druckarbeiten bei der Herausgabe von Zertifikaten, Bestätigungen und Zertifizierungsreports.
- Präsentationen über das Zertifizierungsschema und die erzielten Ergebnisse auf Kunden-Veranstaltungen und Kongressen.

⁶ www.gematik.de



- Ankündigung von Verfahren bzw. Bekanntgabe von Ergebnissen (Presse-Erklärungen, Fachzeitschriften).
- Vergabe von Prüfsiegeln, die auf Handbücher, Datenträger oder Hardware aufgebracht werden können.

Ende von Certification Practice Statement



Certification Practice Statement

Hrsg.: T-Systems GEI GmbH
Adresse: Vorgebirgsstr. 49, 53119 Bonn
Telefon: +49-(0)228-9841-0
Fax: +49-(0)228-9841-6000
Web: www.t-systems-zert.com
www.t-systems.de/ict-security