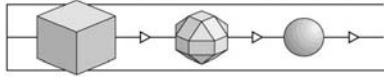




Certification Practice Statement

Services by T-Systems in the Area of
Certification



Preface

In this document the services offered by the certification and confirmation body of T-Systems are described. Objective is to inform interested parties on the certification programmes of T-Systems.

This document will be updated as needed and can be downloaded from the web under www.t-systems-zert.com („Service Area“).

© T-Systems GEI GmbH, 2000-2011

Distribution: public

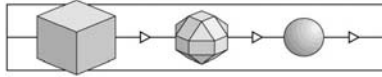
For further information and copies of this brochure contact the certification body:

Certification Body of T-Systems

T-Systems GEI GmbH, Vorgebirgsstr. 49, 53119 Bonn

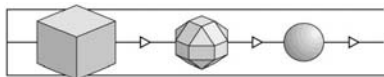
Phone: +49-(0)228-9841-0, Fax: -6000

www.t-systems-zert.com



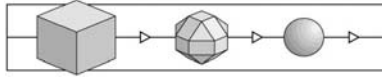
Contents

1	INTRODUCTION.....	5
1.1	MISSION OF CERTIFICATION.....	5
1.2	BENEFITS OF CERTIFICATION	6
1.3	CERTIFICATION BODY OF T-SYSTEMS	7
2	SERVICES SUPPLIED BY THE CERTIFICATION BODY OF T-SYSTEMS	10
2.1	CERTIFICATION PROGRAMMES	10
2.1.1	<i>01 Certification against CC/ITSEC</i>	<i>10</i>
2.1.2	<i>02 Security Confirmation for Technical Components acc. to the German Signature Act ..</i>	<i>11</i>
2.1.3	<i>Security Confirmation for Certification Service Providers according to the German Signature Act.....</i>	<i>11</i>
2.1.4	<i>03a PKI Certification according to ETSI 101456 resp. ETSI 102042</i>	<i>12</i>
2.1.5	<i>04 Deutsches IT-Sicherheitszertifikat [German IT Security Certificate]</i>	<i>13</i>
2.1.6	<i>05 Certification of Business Processes and Services</i>	<i>13</i>
2.1.7	<i>07 Certification of Organisation and IT</i>	<i>14</i>
2.1.8	<i>08 Security for Small and Medium-Sized Companies.....</i>	<i>14</i>
2.1.9	<i>09 Certification in the (German) Health Care Area.....</i>	<i>15</i>
2.2	SUPPLEMENTARY SERVICES.....	15



Revision List

Revision	Date	Activity
0.9	September 8, 2000	Initial Release
1.0	February 28, 2001	Updating
1.1	July 4, 2001	Updating
1.2	August 1, 2001	Updating due to new services
1.3	January 9, 2002	Renaming
1.4	June 6, 2002	Updating services, some minor corrections
1.5	January 2, 2003	Renaming, corresp. adaptations; Updating with s4b
1.6	August 7, 2003	Updates of section 4.3 and 5.6
1.7	October 27, 2003	© and addresses corrected
1.8	July 22, 2004	Sync with Web
1.9	March 4, 2005	Updating section on criteria and laws, names of services
2.0	April 4, 2005	Integrating ETSI 101456 services
2.1	July 25, 2005	Update due to BNetzA
2.2	October 31, 2005	Minor fixes
2.3	February 23, 2006	Update standards
2.4	January 18, 2007	Extension of Scheme, several updates
2.5	June 06, 2007	Update for programme / service 08
2.6	July 19, 2007	Update of General Business Terms
3.0	March 18, 2008	Separation in CPS and Certification Rules
3.1	June 01, 2010	Address change and editorial modifications; programme 06 is terminated.



1 Introduction

1.1 Mission of Certification

Information and Communication Technology (ICT) have come to play an important and often vital role in all sectors of modern societies. Surveys and analyses have revealed dependencies on the continuous availability of this technology: Large, modern enterprises see a threat to their existence if their IT remains unavailable for more than a day, or does not work properly for this period of time. The tolerance limit for small and medium-sized companies is about one week.

In the view of these dependencies, many cases of severe manipulations and security holes, it is quite clear that security of ICT has gained considerable relevance in the commercial, governmental and private sectors.

In the meantime, IT security has become an objective of national laws, is a prerequisite for participating in solicitation procedures and an important factor for clients and users.

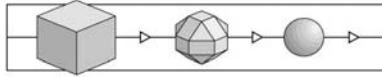
In this sense, the security of information processing and business processes has become an essential factor of enterprise management covering risk assessment, reduction of losses and removal of security weaknesses.

Security in this sense is outlined by classical security objectives comprising the confidentiality, integrity, authenticity and availability of data. Derived security objectives may be non-repudiability, auditing acceptability, privacy and accordance of accounting.

Particularly the globalisation of economies, introduction of new telecommunications services and increasing debate on personal rights have led to the emergence of new security objectives such as anonymity, the protection of copyrights, and assignability and integrity of data and transactions (by means of electronic signatures, for example).

Applying the information and telecommunication technology in all these fields will heighten the risks in future, unless qualified counter-measures as well as evaluation and acceptance procedures are implemented.

The mission of certification is to implement and operate a scheme where such evaluation and acceptance procedures can be performed in an objective and independent way.



These processes greatly promote security because evaluation and certification reports produce a degree of transparency which is indispensable to developers, suppliers, operators and users of ICT.

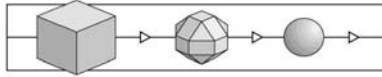
1.2 Benefits of Certification

As in other fields of technology, the goal of certification is to issue an IT security certificate by means of which specific security properties of a product or system, a service or a process become transparent to parties concerned.

The certificate is to be considered an independent confirmation that the claimed security properties actually exist and the promised security objectives are achieved.

Certification has a different importance to the parties involved (developer, provider, operator, user of ICT):

- Product developers need information on security holes in a very early stage of their development process, and expertise on the standard conformance of their development process. Evaluation and certification should thus run concurrent to product development.
- Suppliers of products need such confirmations of their product security in order to maintain their share of the international market and to meet legal and customer requirements.
- Security evaluations are also assuming increasing importance for the suppliers of services, particularly in the field of information and telecommunication services.
- System operators and users need reliable confirmations of the security of products and external services in order to integrate them properly into their systems and enterprise processes.
- System certification and certification of enterprise processes may contribute to the need of enterprises and government authorities for rating their overall security.



Certification must be performed on the basis of accepted security criteria and standards, if they are to prove useful for the target groups. These criteria and standards have already influenced laws and regulations relevant to the groups mentioned above, e.g. in the context of electronic signatures.

The use of internationally accepted criteria is an absolute prerequisite for international acceptance of the certificates issued.

1.3 Certification Body of T-Systems

On the background described above, the certification body of T-Systems offers a variety of services allowing an objective security assessment and certification of

- IT products, IT systems and networks, as well as
- IT services and IT-supported business processes.

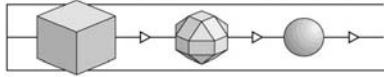
These services are based on standards / normative documents like Common Criteria, ITSEC, ISO/IEC 27001, ETSI standards, national and European regulations on electronic signatures, requirements from the (German) Health Care area, guidelines by the certification body as well as branch or customer specific requirements.

The certification body was accredited for their services applicable initially in June 1998. The recent accreditation certificate – issued by DATech in TGA GmbH – can be inspected under www.t-systems-zert.com.

The annex of this certificate indicates the accredited certification programme concerning the “*security of IT products, IT systems, IT services and IT supported business processes*”.

The certification body joins the following assessment and certification schemes:

- Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway (BNetzA):
 - The certification body of T-Systems was recognised by the German Federal Network Agency as confirmation body (“Bestätigungsstelle”) for compliance certification of products with respect to the German Signature Act.



- The certification body of T-Systems was recognised by the German Federal Network Agency for assessments and compliance certification (“Prüf- und Bestätigungsstelle”) of certification service providers (CSP) with respect to the German Signature Act.
- Notified Body as to EU Directive 1999/93/EG on electronic signatures: In the context of the EU Directive 1999/93/EG, the certification body of T-Systems is a Notified Body¹. Moreover, the certification body was accredited to perform assessments of CSPs according to ETSI TS 101456 and ETSI TS 102042.
- Gematik: The certification body of T-Systems was recognised by the Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH as a "Zertifizierungs-/ Bestätigungsstelle für IT-Sicherheitstechnik für Komponenten" [Certification Body for IT security components"] in the context of their approval scheme.

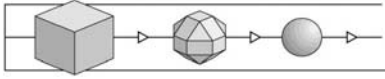
An important factor for clients undergoing certification processes is the confidentiality of their data. The certification body maintains an organisational and technical infrastructure being appropriate for handling of items up to level "secret".

In the sense of EN 45011, the certification body operates under a Management Board consisting of user and vendor representatives, representatives from licensed evaluation facilities and T-Systems GEI GmbH as operator of the certification body. The majority of members of the management board are security experts not belonging to T-Systems. The management board can be contacted under:

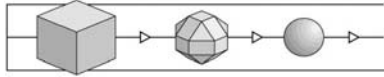
Management Board of the Certification Body
T-Systems GEI GmbH
Vorgebirgsstr. 49
53119 Bonn, Germany

The management board as well as the accreditor, in particular, assess regularly that the certification body's services are accessible to all applicants, impartiality and objectivity are

¹ according to article 3 (4) of this directive, cf. www.europa.eu.int and www.fesa.rtr.at



maintained and the procedures performed by the certification body are equally applied independent of the specific sponsor.



2 Services supplied by the Certification Body of T-Systems

2.1 Certification Programmes

The certification body of T-Systems offers the following certification programmes.

2.1.1 01 Certification against CC/ITSEC

IT products and IT systems can be evaluated and certified against the Common Criteria or the ITSEC. The evaluation is performed by accredited evaluation facilities licensed by the certification body of T-Systems. The certification body monitors the evaluations and issues the certificates and a certification report.

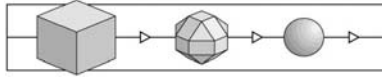
The following documents are relevant for this accredited service:

- Common Criteria for Information Technology Security Evaluation^{2,3}
- Common Methodology for Information Technology Security Evaluation²
- Information Technology Security Evaluation Criteria (ITSEC)^{4,3},
- Information Technology Security Evaluation Manual (ITSEM)⁴,
- „Guideline für Prüfstellen“ [Guidelines for Labs], certification body of T-Systems, recent version.

² The documents can be found on www.commoncriteriaportal.org

³ in conjunction with the European (JIL, Joint Interpretation Library) and national interpretations of criteria by BSI (AIS)

⁴ The documents can be found on www.t-systems-zert.com (service area).



2.1.2 02 Security Confirmation for Technical Components acc. to the German Signature Act

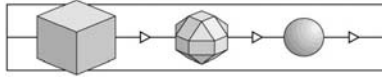
With this service, so-called “security confirmations” to be submitted to German Federal Network Agency are issued for technical components requiring an assessment according to the German Electronic Signature Act. For such components, an evaluation against the Common Criteria or the ITSEC (cf. service 01) has to be performed by an accredited and licensed evaluation facility.

In addition to the criteria mentioned, the following normative documents have to be observed:

- German Signature Act (SigG)
- German Signature Ordinance (SigV)
- Official Announcement by the (German) Federal Network Agency concerning approved algorithms
- Spezifikation von Einsatzbedingungen für Signaturanwendungskomponenten [Specification of the operational environment for signature application components, in German only], (German) Federal Network Agency
- Minutes of the „Arbeitsgruppe anerkannter Bestätigungsstellen (AGAB)“ [working group of recognised confirmation bodies]
- Guideline 02-SIG "Anforderungen an PKI-Produkte" [Requirements to PKI Products], certification body of T-Systems, recent version.

2.1.3 Security Confirmation for Certification Service Providers according to the German Signature Act

In accordance with the German Electronic Signature Act, assessments are performed concerning the security concept and its implementation governing the operation of a Certification Service Provider (CSP) to be accredited. Corresponding “security confirmations” are issued to be submitted to the German Federal Network Agency. CSPs who have suc-



cessfully passed this assessment meet the requirements of the EU Directive 1999/93/EG as well.

The following normative documents form the basis of this accredited service:

- German Signature Act (SigG)
- German Signature Ordinance (SigV)
- Official Announcement by the (German) Federal Network Agency concerning approved algorithms
- Spezifikation von Einsatzbedingungen für Signaturanwendungskomponenten [Specification of the operational environment for signature application components, in German only], (German) Federal Network Agency
- Minutes of the „Arbeitsgruppe anerkannter Bestätigungsstellen (AGAB)“ [working group of recognised assessment bodies]
- Guideline 03-SIG "Anforderungen an PKI-Betreiber" [Requirements to PKI Operators], certification body of T-Systems, recent version.

2.1.4 03a PKI Certification according to ETSI 101456 resp. ETSI 102042

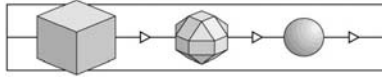
In the international context, the standard ETSI TS 101456 has gained an essential meaning for Certification Service Providers (CSP) offering qualified certificates. Several schemes (e.g. in the Netherlands and in Switzerland) rely on this standard.

By the service 03a, the certification body of T-Systems provides for assessments, audits and certification of CSPs according to ETSI TS 101456.

The standard ETSI TS 102042 addresses CSPs offering general purpose certificates not necessarily qualified in the sense of the EU Directive.

Relevant for this accredited service 03a are the following documents:

- EU Directive 1999/93/EG



- Commission Decision of 14/7/2003 on the publication of reference numbers of generally recognised standards
- ETSI TS 101 456: Policy requirements for certification authorities issuing qualified certificates, recent version
- ETSI TS 102 042: Policy requirements for certification authorities issuing public key certificates, recent version
- Guideline 03-SIG "Anforderungen an PKI-Betreiber" [Requirements to PKI Operators], certification body of T-Systems, recent version

This certification service is applicable to further countries in the EU and beyond. For the relevant applicable legal framework in **Austria**, the **Netherlands** and **Switzerland**⁵.

2.1.5 04 Deutsches IT-Sicherheitszertifikat [German IT Security Certificate]

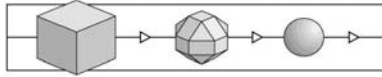
IT products and IT systems can be evaluated and certified against the ITSEC or the Common Criteria. The evaluation is performed by accredited evaluation facilities licensed by the certification body of T-Systems and the BSI. The certification body of T-Systems monitors the evaluations and issues certificates and certification reports. The certificate is a *Deutsches IT-Sicherheitszertifikat [German IT Security Certificate]* as defined by the BSI (with German federal emblem "eagle").

This accredited service is about to cease, since it is no longer supported by the BSI. Corresponding evaluations can now be performed under **service 01** (see above).

2.1.6 05 Certification of Business Processes and Services

By using the **Common Criteria** as a baseline method, enterprise business processes and services are assessed and certified as to their security. The assessments cover documentation checks and (periodical) audits on location to verify a correct implementation.

⁵ follow links on www.t-systems-zert.com under "Service Area"



For this accredited service, the certification body uses the following normative documents:

- Guideline 05-DPZ "Zertifizierung von Prozessen und Dienstleistungen", [Certification of Processes and Services], certification body of T-Systems, recent version
- Common Criteria for Information Technology Security Evaluation^{2,3}
- Common Methodology for Information Technology Security Evaluation².

2.1.7 07 Certification of Organisation and IT

Using a method developed by T-Systems, IT systems and networks including their management procedures can be assessed and certified with respect to their security.

This service includes a documentation check on different levels, technical tests and an implementation check performed as a (periodical) audit.

For this accredited services, the certification body uses the following documents:

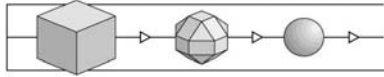
- Guideline 07-DOT "Zertifizierung von Organisation und Technik" [Certification of Organisation and IT], certification body of T-Systems, recent version.

2.1.8 08 Security for Small and Medium–Sized Companies

For the programme "Security for Small and Medium-Sized Companies", the service 07 is applied in a tailored form: Three security levels are defined, the highest level „Professionelle Sicherheit“ [Professional Security] includes a certification.

For this accredited service, the certification body uses the following documents:

- Guideline 08-S4B "S4B – Professionelle Sicherheit: Kriterien für die Zertifizierung" [S4B – Professional Security: Criteria for Certification], certification body of T-Systems, recent version
- Guideline 07-DOT "Zertifizierung von Organisation und Technik" [Certification of Organisation and IT] , certification body of T-Systems, recent version
- ISO/IEC 2700x and ISO/IEC 17799



- Description of the security levels "Basissicherheit" [Basic Security], "Standardsicherheit" [Standard Security], "Professionelle Sicherheit" [Professional Security].

2.1.9 09 Certification in the (German) Health Care Area

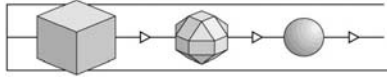
The service 09 offers certification according to the rules given by Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik). Their normative documents can be obtained from the corresponding web-site⁶. This service 06 internally re-uses the services 01 and 02 (see above).

2.2 Supplementary Services

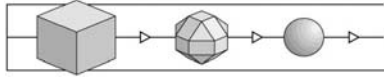
The following supplementary services are available for the entire certification programme:

- Preparation of evaluation and certification projects in workshop style.
- Briefing and training of developers with respect to criteria compliant and optimised development procedures (inhouse as well).
- Training of IT Security Officers (multi-level, with certificate; inhouse as well).
- Translation of certificates, confirmations and certification reports into other languages.
- Printing and mailing of certificates, confirmations and certification reports in specified quantities.
- Presentations on the Certification Scheme and results achieved at customer events and congresses.
- Announcements (press releases, articles) of procedures started or finished and achieved results.
- Issuance of seals to be attached to manuals, data media or hardware.

⁶ www.gematik.de



End of: Certification Practice Statement



Certification Practice Statement

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