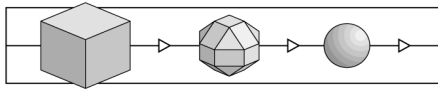




Certification Policy

Certification Body of T-Systems



Preface

Objective of this document is to inform interest parties on

- the rules of certification,
- the generic procedure of certification and
- the administrative framework to be observed.

This document will be updated as needed and provided for download on the web under www.t-systems-zert.com („Service Area“).

For a specific certification project, the version valid at the time of signing the certification contract will be applied.

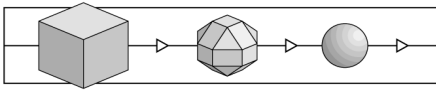
A description of the certification programme offered by T-Systems is contained in the “Certification Practice Statement” (CPS) accessible via Internet (address given above).

© T-Systems GEI GmbH, 2000-2008

Distribution: public

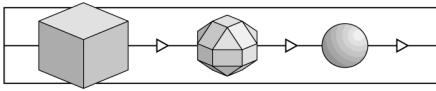
For further information and copies of this brochure contact the certification body:

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



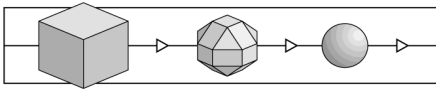
Contents

1	Generic Procedure.....	5
1.1	Preliminary Discussions.....	5
1.2	Application for Certification	5
1.3	Commencement of a Project	6
1.4	Assessment.....	6
1.5	Termination	6
1.6	Maintenance after Changes.....	7
2	Certification Rules.....	8
2.1	Responsibilities of the Certification Body	8
2.2	Responsibilities of the Sponsor.....	8
2.2.1	All Certification Programmes	8
2.2.2	Certification Programmes 01, 02, 04 and 09.....	9
2.2.3	Certification Programmes 03, 05, 06, 07 and 08.....	10
3	Miscellaneous.....	11
3.1	Confidentiality	11
3.2	Disclosure and Publication.....	11
3.3	Cost and Liability	11
3.4	Disputes	12



Revision List

Version	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 into CPS and Policy



1 Generic Procedure

In the subsequent sections the typical procedure for a certification project is described.

1.1 Preliminary Discussions

In this optional phase, the potential sponsor is provided with all information necessary to decide for a certification project.

Key issues are:

- object and scope to be certified
- confidentiality of information
- certification programme to be applied
- rights and duties of all participants
- security criteria
- documents existing / to be supplied
- outline of procedure
- milestone plan, timeframe and expenses

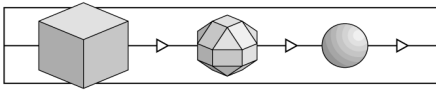
1.2 Application for Certification

In consideration of the preliminary discussions, the certification creates an offer for the planned certification project.

The offer identifies the object and scope of certification, the certification programme to be applied, the technical and administrative requirements to be met by the sponsor for a certification, provides for an initial schedule and further commercial terms.

The application for certification is endorsed by formal acceptance of this offer. A corresponding letter, to be signed by an authorised person acting on behalf of the sponsor, is required and should specify at least the name and legal form of the sponsor's organisation, and the address e. g. as contained in the official trade register.

This document "Certification Policy" is to be regarded an integral part of the offer and the contract.



1.3 Commencement of a Project

A project is started as soon as the sponsor has placed an application at the certification body.

The certification body assigns to the process a certification ID which may be used by the sponsor as a reference for official announcements. If the sponsor agrees, the project may also be announced by the certification body under www.t-systems-zert.com.

A joint kick-off meeting is held if the parties involved have agreed on. A milestone plan for the certification project will be set up jointly by the parties involved.

Place of work for the project are the facilities of the certification body - with the exception of audits and inspections at the sponsor's site, if such audits and inspections are part of the certification programme.

If required, all parties involved jointly decide on modifications to the object and scope of certification and the course of the assessment.

1.4 Assessment

Depending on the certification programme, assessments will be carried out by the chosen evaluation facility (monitored by the certification body), by auditors or by the certification body itself.

Assessment, audit and inspection reports are written to reflect the performed steps and the corresponding results. These reports are submitted to the sponsor. If the sponsor agrees to the contents of a report, this will be regarded as formal approval. If the sponsor disagrees, the certification body will take a formal decision on the objection according to their best judgement and inform the sponsor correspondingly.

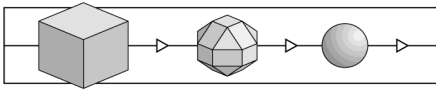
1.5 Termination

In case that the overall assessment was successful, a certificate or conformance declaration ("confirmation") will be issued. Depending on the certification programme, an additional certification report or an annex to the certificate may be issued. These documents are forwarded to the sponsor in electronic and printed form.

If the sponsors agrees, the issued certificate, confirmation, the certification report and / or an annex to the certificate may be published under www.t-systems-zert.com.

It may be necessary to dispatch these documents to other supervising agencies (Federal Office for Information Security (BSI), Federal Network Agency, Accreditor) or to provide an insight.

As far as these institutions publish the certification results, the certification body of T-Systems is bound to their schedule and cannot guarantee for a specific publication date.



In case that the overall assessment was not successful, the final report explains the relevant reasons. After having removed the stated deficiencies, the sponsor may apply for a re-assessment.

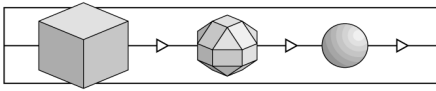
All documents relevant for the project are archived at the certification body. If archiving of the certified object (e.g. products) at the certification body has been agreed on, appropriate measures will be taken. Details are discussed with the sponsor.

1.6 Maintenance after Changes

As to maintaining of the certified status, the sponsor will be informed at the end of the initial certification, but may access the certification body at any time for advice.

A decision has to be taken as to the effect on the certificate caused by modifications to the certified object, changes to the underlying criteria or new security findings: This may result in maintaining, changing, extending or withdrawing the certificate. In details:

- If the scope of certification is modified or extended, depending on the nature of the changes it may occur that the certificate can be extended to the modified scope (possibly with additional stipulations) or remains restricted to the old version.
- The certification body will inform the sponsor as soon as possible about changes to the underlying criteria and provide advice on the effect of these changes to the scope and its certification. Possibly, the certificate may not be maintained for the new criteria without an additional assessment.
- If new security findings lead to a conclusion that an issued certificate can no longer be maintained, the sponsor may provide a solution to the corresponding problem in a reasonable time frame; this has to be documented according to the criteria; the certification body has to be informed correspondingly. Based on this information, the certification body decides whether the certificate may be maintained (possibly with further stipulations) or has to be withdrawn.



2 Certification Rules

2.1 Responsibilities of the Certification Body

The certification body was accredited against the standard EN 45011 by DATech in TGA GmbH under DAR registration number DAT-ZE-015/98-01.

Meeting the requirements of EN 45011 and maintaining the corresponding accreditation is an indispensable policy for the certification body. From this policy, the following fundamentals and responsibilities can be derived:

- The certification body's services are accessible to all interested parties.
- Impartiality and objectivity are key principles; the procedures performed by the certification body are equally applied independent of the specific sponsor.
- Equal treatment of all evaluation facilities, as far as involved in technical assessments, is guaranteed.
- Special interests and reservations of other parties as regards IT security have no bearing whatsoever on the processes employed by the certification body and the results obtained.

The certification body is responsible for strictly and continuously adhering to these policy rules and is audited periodically by the accreditor and supervising agencies.

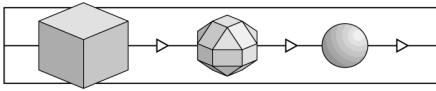
2.2 Responsibilities of the Sponsor

With applying for a certificate at the certification body, the sponsor agrees to continuously meet the following obligations (arising from EN 45011 and the applied criteria).

If these obligations are not met in their essence, the certification body will take appropriate measures: removing any announcement under www.t-systems-zert.com, not issuing certificates or confirmations, withdrawal of issued certificates or confirmations.

2.2.1 All Certification Programmes

- a. For the distribution of certificates by the sponsor, only the most recent version is to be used.
- b. References to the certified object or status in press releases, advertising brochure etc. must be made in a precise form and may not be considered misleading; in particular, the certification may only be used to prove the compliance of the certified object to the criteria applied.



- c. If a certificate was withdrawn, it must not be used further for any purpose.
- d. The sponsor has to record new findings (e.g. by customer complaints) on the properties of the certified object and pass these records to the certification body on request.
- e. If new security findings lead to a conclusion that an issued certificate can no longer be maintained, the sponsor may provide a solution to the corresponding problem in a reasonable time frame; this has to be documented according to the criteria, the certification body has to be informed correspondingly.
- f. The certification body monitors - as a fundamental approach - the use of issued certificates, confirmations and logos. If a certificate, confirmation or logo is misused or used erroneously, the certification body reserves the right to take corrective, public or, in extreme cases, legal action.
- g. The sponsor must not use the certification in a manner as to bring the certification body into disrepute.

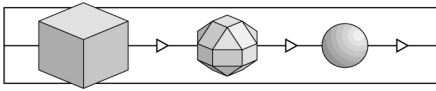
2.2.2 Certification Programmes 01, 02, 04 and 09

For the certification programmes

- 01 Certification against ITSEC/CC,
- 02 Security Confirmation for Technical Components according to the German Signature Act,
- 04 Deutsches IT-Sicherheitszertifikat [German IT Security Certificate],
- 09 Zertifizierungen im Gesundheitswesen [Certification for the (German) Health Care Area].

the following rules are to be adhered to in addition to section 2.2.1:

- a. The certification body has the right to inspect any sponsor document relevant for the assessment as well as any evaluation report of the participating evaluation facility.
- b. Products and systems as well as their documentation must have a unique identification, changes must be reflected by new version numbers, release dates etc.
- c. Within a period of three months after commencement of the certification project, the sponsor has to contract an evaluation facility with the technical evaluation.
- d. The certification body, after written notice, has the right to access and inspect the sponsor's development site for assessment.



- e. As part of the certification contract, the certification body may require to archive one copy of the certified object (product or system).
- f. The sponsor is responsible to inform the certification body as soon as possible when changes to the certified object have been applied.
- g. Modified versions of certified product / system may not be named "certified" unless a successful re-certification has been performed.
- h. The sponsor has to inform the certification body as soon as the certified product / system is no longer available.

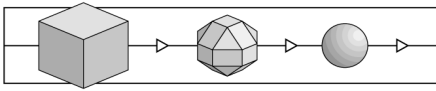
2.2.3 Certification Programmes 03, 05, 06, 07 and 08

For the certification programmes

- 03 Security Confirmation for Certification Service Providers according to the German Signature Act,
- 05 Certification of Business Processes and Services,
- 06 Conformance Assessment against EHI Criteria,
- 07 Certification of Organisation and IT,
- 08 Security for Small and Medium-Sized Companies

the following rules are to be adhered to in addition to section 2.2.1:

- A. The certification body has the right to access and inspect any document of the sponsor relevant for the assessment according to the applied criteria.
- B. Required documents must be clearly identifiable, changes must be reflected by new version numbers, release dates etc.
- C. The certification body has the right to access and inspect the sponsor's site to the extent needed for the assessment.
- D. Changes to the scope of certification, its documentation and implementation must be recorded by the sponsor, the certification body has to be informed correspondingly.
- E. A modified scope must not be named "certified" unless authorized by the certification body.



3 Miscellaneous

3.1 Confidentiality

A key principle followed by the certification body is to maintain the strict confidentiality of information gathered during certification projects. A system of three confidentiality levels has been implemented which can be chosen from at the time of applying for the certificate.

- Standard: Access to data stored with the certification body is restricted to certifiers of the certification body, IT administrators of T-Systems and (if applicable) the evaluation facility involved. Concerning electronic transmission of data, a decision on encryption is made case by case.
- Need-To-Know: Access to data stored with the certification body or electronically transmitted is granted only certifiers, auditors and (if applicable) evaluators directly involved in the project. For electronic transmission data has to be encrypted using an algorithm accepted by the parties involved.
- High: The procedures for handling governmental classified information are applied. All employees of the certification body are at least cleared up to level "secret" by the responsible „Bundesministerium für Wirtschaft“.

3.2 Disclosure and Publication

Information on the status of evaluations in progress are not disclosed to third parties without the explicit approval of the sponsor.

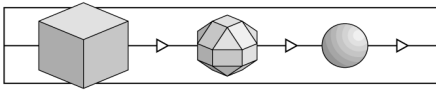
Technical results achieved in an evaluation will be published only with explicit approval of the sponsor. As an exception and due to recognition and accreditation agreements, supervising government authorities and accreditors must be given access by the certification body to technical results whenever required.

All documents published by the certification body contain copyright statements explaining the possibility of reproduction. For its certificates, confirmations and reports, T-Systems GEI GmbH keeps the copyright, but grants permission the sponsor for copying and distributing these documents, provided that contents and layout are maintained.

3.3 Cost and Liability

The costs for a certification project are charged on a time and material basis. Details are specified in the certification offer for each sponsor.

Certification fees are always charged as agreed with the sponsor - independent of whether a certificate was successfully issued, could be not issued due to technical defi-



ciencies, the sponsor cancelled the certification project or the certification body suspended the certification project due to insufficient information on the object to be certified.

If the sponsor requires modifications to already approved reports, certificates and confirmations, the additional effort will be charged. This holds also for performing repetitive assessments if necessary due to reasons caused by the sponsor. Sponsor and certification body will jointly agree on any additional effort in advance.

T-Systems assumes liability in accordance with its General Business Terms attached to each individual offer.

3.4 Disputes

Participants (sponsor, evaluation facility) in a certification project may appeal against decisions taken by the certification body. The procedure for the consideration of such appeals consists of three levels:

- trying to solve problems with the certifier assigned to the process under consideration,
- if not successful: trying to achieve a solution with the head of the certification body,
- if not successful: to appeal to the Management Board; after hearing the parties involved, the Management Board takes a decision and informs the parties according to its rules of procedure.

The address of the Management Board is:

Management Board of the Certification Body
c/o T-Systems GEI GmbH
Rabinstr.8
D-53111 Bonn, Germany

This escalation procedure does neither preclude nor anticipate any legal proceedings.

The Management Board consists of user and vendor representatives, representatives from licenced 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.

End of: Certification Policy

Certification Policy

Editor: T-Systems GEI GmbH
Address: Rabinstr.8, D-53111 Bonn, Germany
Phone: +49-(0)228-9841-0
Fax: +49-(0)228-9841-60
Web: www.t-systems.com/ict-security
www.t-systems-zert.com