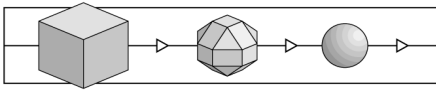


Abbreviations

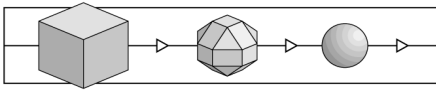
AIS	Anwendungshinweise und Interpretationen zum Schema [Guidance and Interpretations of Scheme Issues] (BSI procedure)
BGBl	Bundesgesetzblatt [German Federal Gazette]
BNetzA	Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen [(German:) Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway]
BSI	Bundesamt für Sicherheit in der Informationstechnik [(German) Federal Office for Information Security]
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
CSP	Certification Service Provider
DAR	Deutscher Akkreditierungsrat [German Accreditation Council]
DATech	DATech Deutsche Akkreditierungsstelle Technik in TGA GmbH [DATech German Accreditation Body Technology in TGA GmbH]
DIN	Deutsches Institut für Normung e.V. [German Standards Institution]
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
ETSI	European Telecommunications Standards Institute
ISO	International Organization for Standardization
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria
ITSEF	IT Security Evaluation Facility
ITSEM	Information Technology Security Evaluation Manual
JIL	Joint Interpretation Library
PP	Protection Profile
SF	Security Function
SigG	German Electronic Signature Act
SigV	German Electronic Signature Ordinance
SOF	Strength of (Security) Function



ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

References

- /AISx/ Anwendungshinweise und Interpretationen zum Schema [Guidance and Interpretations of Scheme Issues], BSI, endorsed versions
- /ALG/ Geeignete Kryptoalgorithmen [Approved Crypto-Algorithms], published in the Bundesanzeiger [German Federal Gazette] by the (German) Federal Network Agency, endorsed version
- /CC/ Common Criteria for Information Technology Security Evaluation, Version 3.1, www.commoncriteriaportal.com,
Part 1: Introduction and general model
Part 2: Security functional requirements
Part 3: Security assurance requirements
- /GEM/ Common Methodology for Information Technology Security Evaluation, Evaluation methodology, Version 3.1, www.commoncriteriaportal.com
- /ETSI1/ ETSI TS 101 456: Electronic Signatures and Infrastructures (ESI): Policy requirements for certification authorities issuing qualified certificates, Version 1.4.3, 2007-05
- /ETSI2/ ETSI TS 102 042: Electronic Signatures and Infrastructures (ESI): Policy requirements for certification authorities issuing public key certificates, Version 1.3.4, 2007-12
- /EU-DIR/ Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures
- /EU-REF/ Commission Decision of 14/7/2003 on the publication of reference numbers of generally recognised standards for electronic signature products
- /ISO27001/ ISO/IEC 27001:2005 Information technology. Security techniques. Information security management systems. Requirements
- /ITSEC/ Information Technology Security Evaluation Criteria (ITSEC), version 1.2 (1991), ISBN 92-826-3004-8
- /ITSEM/ Information Technology Security Evaluation Manual (ITSEM), version 1.0 (1993), ISBN 92-826-7087-2
- /JIL/ ITSEC Joint Interpretation Library, version 2.0, November 1998



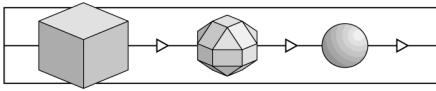
- /SiGAK/ Spezifizierung der Einsatzbedingungen für Signaturanwendungskomponenten: Arbeitsgrundlage für Entwickler / Hersteller und Prüf- / Bestätigungsstellen [Specification of the Operational Environment for Signature Application Components: Basics for Developers / Manufacturers and Assessment / Certification Bodies], Federal Network Agency, version 1.4, July 19, 2005
- /SigG/ Signaturgesetz vom 16. Mai 2001 (BGBl. I S. 876) [Signature Act as of May 16, 2001 (BGBl. I p. 876)], recently revised by Article 4 of the act as of February 26, 2007 (BGBl. Year 2007, Part I p. 179)
- /SigV/ Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) [Ordinance on Electronic Signatures (Signature Ordinance– SigV)], recently revised by Article 9 Sec 18 of the act as of November 23, 2007 (BGBl. I page 2631)

Glossary

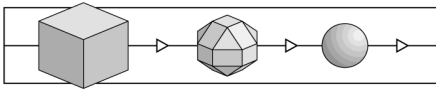
This glossary provides explanations of terms used within the certification scheme of T-Systems, but does not claim completeness or general validity. The term *security* here is always used in the context of information technology.

For criteria specific terms cf. the glossary in the relevant security criteria.

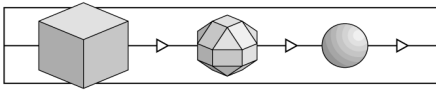
Accreditation	A process performed by an accreditation body to confirm that an evaluation facility [resp. a certification body] complies with the requirements of the relevant standard ISO 17025 [resp. EN 45011].
Audit	A procedure of collecting evidence that the scope of a certification has been implemented correctly.
Availability	Classical security objective: Data should always be available to authorised persons, i.e. this data should neither be made inaccessible by unauthorised persons nor be rendered unavailable due to technical defects.
Business Process	Cf. Process
Certificate	Summary representation of a certification result, issued by the certification body.
Certification	Independent confirmation of the correctness of an evaluation. This term is also used to describe the overall process consisting of evaluation, monitoring and subsequent issue of certificates and certification reports.
Certification Body	An organisation which performs certifications.



Certification Report	Report on the object, procedures and results of a certification; this report is issued by the certification body.
Certification Scheme	A summary of all principles, regulations and procedures applied by a certification body.
Certification Service Provider	An institution (named "certification service provider" in the German Electronic Signature Act) that confirms the relationship between signature keys and individuals by means of electronic certificates.
Certifier	Employee at a certification body authorised to monitor evaluations and to carry out the certification.
Common Criteria	Security Criteria based on the former US Orange Book / Federal Criteria, the European ITSEC and the Canadian CTCPEC; a world-wide accepted security standard (ISO/IEC 15408).
Confidentiality	Classical security objective: Data should only be accessible to authorised persons.
"Confirmation Body"	A body, recognised by the BNetzA, assessing the security of technical components and of certification service providers, issuing security confirmations according to the (German) SigG and SigV.
"Confirmation Procedure"	Procedure with the objective to issue a security confirmation.
Evaluation	Assessment of an (IT) product, system or service against published IT security criteria.
Evaluation (Assurance) Level	Level of assurance gained by evaluation; level of trust that a TOE meets its security target (according to ITSEC / CC).
Evaluation Facility	The organisational unit which performs evaluations (ITSEF).
Evaluation Technical Report	Final report written by an evaluation facility on the procedure and results of an evaluation.
Evaluator	Person in charge of an evaluation at an evaluation facility.
Integrity	Classical security objective: Only authorised persons should be capable of modifying data.
IT Product	Software and/or hardware which can be procured from a supplier (manufacturer, distributor).
IT Security Management	Implemented procedure to install and maintain IT security within an organisation.
IT Service	A service supported by IT systems.



IT System	An inherently functional combination of IT products. (ITSEC:) A real installation of IT products with a known operational environment.
License Agreement	Agreement between an Evaluation Facility and a Certification Body concerning the procedure and responsibilities of a joint assessment / evaluation and certification project.
Milestone Plan	A project schedule for the implementation of evaluation and certification processes.
Monitoring	Procedure implemented by the certification body in order to check whether an evaluation is performed correctly (compliance with criteria, use of standard processes and ratings etc.).
Problem Report	Report sent by an evaluation facility to the certification body and concerning special problems during evaluation, e. g. concerning the interpretation of IT security criteria.
Process	Sequence of networked activities (process elements) performed within a given environment – with the objective to provide a certain service.
Product Certification	Certification of IT products.
Re-Certification	Renewed certification of a previously certified object due to a new version following modification; re-certification might also be required after a change of tools, production / delivery processes and security criteria.
Security Certificate	Cf. „Certificate“.
"Security Confirmation"	SigG: A legally binding document stating the conformity of technical components or trust centers to SigG / SigV.
Security Criteria	Normative document that may contain technical requirements for products, systems and services, but at least describes the evaluation of such requirements.
Security Function	Technical function or measure to counteract certain threats.
Security Measure	Any organisational, personal, infrastructural or technical measure contributing to achieve security objectives.
Security Objective	For the context of information security typical objectives like confidentiality, integrity, availability, authenticity as well as derived objectives like compliance (e.g. in legal context).
Security Target	Document specifying a TOE and describing its configuration and environment, security objectives and threats, met security requirements and corresponding rationale; used as a basis for the evaluation of the TOE.



Service	Here: activities offered by a company, provided by its (business) processes and usable by a client.
System Certification	Certification of an installed IT system.
Target of Evaluation	An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.
Trust Centre	Cf. Certification Service Provider