Certification Practice Statement

Certification Programme ”ICT Products’ Security”

of the Certification Body of Telekom Security (certification programme 041)

Foreword

Telekom Security operates a certification body accredited by DAkkS[1] in accordance with ISO/IEC 17065 and ETSI EN 319 403, DAkkS Registration No. D-ZE-21631-01 (former Certification Body of T-Systems, DAkkS Registration No. D-ZE-12025-01).

Furthermore, the Telekom Security certification body is a recognized "designated body" as per EU Regulation No. 910/2014 (eIDAS) and Commission Decision 2000/709/EC (see FESA) as well as per § 17 of Vertrauensdienstegesetzes (VDG, eIDAS-Durchführungsgesetz as of 18.07.2017) for the conformity certification of electronic signature creation devices**.**

This document describes the certification programme for issuing Telekom Security security certificates for ICT products, for example, as addressed in Title III 'Cybersecurity Certification Framework' of CSA. It is intended to provide parties interested in certification from Telekom Security with all the necessary information.

The document is regularly updated based on requirements and made available to download online at www.telekom-zert.com ("Service Area").

Distribution: public

For further information, the certification body can be contacted as follows:

✉ Certification Body of Telekom Security
c/o Deutsche Telekom Security GmbH, Bonner Talweg 100, 53113 Bonn
☎ +49-(0)228-181-0, FAX -49990
💻 www.telekom-zert.com

[1] Deutsche Akkreditierungsstelle (German Accreditation Body), www.dakks.de

Table of Contents

Revision list

Revision	Date	Activity
0.9	September 8, 2000	Initial creation (debis Systemahus)
1.0	February 28, 2001	Update
1.1	July 4, 2001	Update
1.2	August 1, 2001	Update based on new services
1.3	January 9, 2002	Renaming into Telekom Security
1.4	June 1, 2002	Services updated, minor corrections
1.5	January 2, 2003	Name changes, corresponding adjustments; addition of s4b
1.6	August 7, 2003	Additions in Sections 4.3 and 5.6
1.7	October 27, 2003	Changes: © and address specifications
1.8	July 22, 2004	Comparison with web
1.9	March 4, 2005	Assessment principles and procedure names updated
2.0	April 4, 2005	Addition of ETSI 101456
2.1	July 25, 2005	Update due to BNetzA
2.2	October 31, 2005	Minor corrections
2.3	February 23, 2006	Standards updated
2.4	January 18, 2007	Programme adjustments, various updates
2.5	June 6, 2007	Adjustments for procedure 08
2.6	July 19, 2007	General Terms and Conditions updated
3.0	March 18, 2008	Division into CPS and certification rules
3.1	June 1, 2010	Address change and editorial modifications; termination of programme 06
4.00-ICT-products	September 2, 2019	Modifications in the context of ISO 17065 accreditation by DAkkS; a dedicated CPS is issued for each program.
5.00-ICT-products	July 1, 2020	Renaming into Telekom Security
5.01-ICT-products	January 4, 2022	Technical changes
5.02-ICT-products	August 23, 2023	Editorial changes

1 Introduction

1.1 Certification Mission

Information and communications technology (ICT) has come to play an important and often vital role in all areas of modern society. Surveys and analyses have revealed a dependency on the continuous availability of technology and services. Modern enterprises see a threat to their existence if their IT is not available or does not work as expected.

In view of these dependencies, as well as the high number of manipulations and security holes, it is no wonder that the security of information and communications technology has become significantly more relevant in the commercial, governmental and private spheres.

IT security is now the subject of laws and regulations, a prerequisite for participating in tenders, and an important factor for many users when making purchasing decisions.

The security of information processing and business processes has thus become a cornerstone of business precautions. Here, the aim is to identify risks, reduce damage and eliminate vulnerabilities.

Security, in this sense, is determined by the classical security objectives of confidentiality, integrity, authenticity and availability of data. Objectives relating to non-repudiability, auditing acceptability, data protection and correctness may be associated with these security objectives.

In particular, the globalization of the economy, introduction of new communications services and the debate about personal rights have put more emphasis on new security objectives such as anonymity, copyright protection, integrity and protection against falsification for data and transactions (by means of electronic signatures, for example).

The risks associated with using information and communications technology will be even greater in future, unless effective security precautions are taken and appropriate assessment and acceptance procedures (verification and qualification) are implemented.

The task of certification is to set up and operate a system in which such assessment and acceptance procedures can be performed in an objective and independent way.

These verification and qualification processes are essential in reducing security risks because the verifying assessment and certification reports and qualifying marks of conformity (certificates, confirmations, quality and test seals) produce a degree of

transparency which is indispensable to ICT risk owners: operators, users, providers and developers.

1.2 Benefits of Certification

As in other fields of technology, the goal of a certification process in the area of IT security is issuing a mark of conformity, e.g., a certificate, which makes certain security properties of a product or system, a service or a business process clear to the parties concerned.

The mark of conformity is independent and objective confirmation that the security properties claimed by the provider actually exist and the intended security objectives are achieved.

The certification is based on normative documents such as legal regulations, standards or technical specifications that define the requirements for the certification objects (products/services/processes). Certification has a different meaning for the target groups involved (users, providers and ICT operators):

- Operators and users need reliable confirmation regarding the security properties of IT products and external services in order to be able to integrate them properly into their systems and business processes.
  In addition, system certifications and the certification of business processes may meet the requirements of companies and government authorities for evidence of holistic security.
- Service providers, especially in the areas of information processing, telecommunications and IT products, require confirmation of the security properties of their services and products in order to remain successful on the international market and meet legal and customer-specific requirements.

These processes shall be performed on the basis of relevant security criteria and standards if they are to provide substantial benefits for the specified target groups. In some cases, security assessment criteria and security standards have already influenced legal regulations relevant to the specified target groups, for example, in the context of electronic signatures, ID documents, health care, intelligent distribution networks (smart grid) and digital tachographs.

The use of internationally accepted criteria is an essential requirement for international acceptance of the marks of conformity issued.

1.3 Certification Body of Telekom Security

Against this background, the Telekom Security certification body offers a variety of services that allow objective security assessment and certification for the following:

- ICT products, systems and networks
- ICT services and corresponding business processes.

These services are based on standards and normative documents such as European and national regulations regarding

- certification of trust services: at EU level – in the context of eIDAS[2]: electronic signatures, seals, timestamps, services for delivering electronic registered letters, website authentication; at the national level – within the framework of the German Trust Services Act (VDG),
- certification of qualified electronic signature creation devices: European and national regulations (eIDAS and VDG),
- certification of ICT products, services and processes within the framework of the CSA[3],
- certification according to ETSI standards, the certification body's own assessment specifications, and industry-specific or customer-specific requirements.

The Telekom Security certification body was first accredited for its services in June 1998. The current accreditation certificate – issued by DAkkS – can be found at www.telekom-zert.com and www.dakks.de (D-ZE-21631-01). The annex to the accreditation certificate contains the certification body's accredited certification programs.

The certification body participates in assessment and certification schemes operated within the following frameworks:

- All frameworks requiring the application of Common Criteria;
  (procedure type 041);
  particular, the framework of EU Regulation (EU) No. 2019/881 (CSA). In conjunction with EU Regulation (EU) No. 2019/881, the Telekom Security

[2] Regulation (EU) No. 910/2014

[3] Regulation (EU) No. 2019/881

certification body is a conformity assessment body[4] for performing cybersecurity certifications in the sense of Art. 56 of CSA.

- EU Regulation (EU) No. 910/2014 (eIDAS) (procedure type 031):
  In conjunction with EU Regulation (EU) No. 910/2014, the Telekom Security certification body is a conformity assessment body[5] for trust service providers and the trust services that they offer.

- ETSI EN 319 4xx: Electronic Signatures and Infrastructures (ESI) (procedure type 032):

  - ETSI EN 319 401: General Policy Requirements for Trust Service Providers

  - ETSI EN 319 411-1: Policy and security requirements for Trust Service Providers issuing certificates;
    Part 1: General requirements
    Note: Conformity with these requirements is recognised by CA/Browser Forum (see CA/B Baseline and Extended Validation Requirements, Ballot 171 as of 01.07.2016)

  - ETSI EN 319 411-2: Policy and security requirements for Trust Service Providers issuing certificates;
    Part 2: Requirements for trust service providers issuing EU qualified certificates

  - ETSI EN 319 411-3: Policy and security requirements for Trust Service Providers issuing certificates;
    Part 3: Policy Requirements for Certification Authorities issuing public key certificates

  - ETSI EN 319 411-4: Policy and security requirements for Trust Service Providers issuing certificates;
    Part 4: Policy Requirements for Certification Authorities issuing attribute certificates

[4] as per Article 60 of this Regulation (Conformity Assessment Body, CAB)

[5] as per Article 20 of this Regulation (Conformity Assessment Body, CAB)

- ETSI EN 319 421: Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
- ETSI EN 319 431: TSP service components operating a remote QSCD / SCDev
- CEN EN 419 241 series: Trustworthy Systems Supporting Server Signing
- CEN EN 419 221 series: Cryptographic Module;
  amongst others - EN 419 221-5: Cryptographic Module for Trust Services
- ETSI EN 319 441: Policy and security requirements for TSPs providing signature validation services
- ETSI EN 319 521: Policy and security requirements for Electronic Registered Delivery Service Providers
- ETSI EN 319 522 Serie: Electronic Registered Delivery Service.

In conjunction with the above series of standards ETSI EN 319 4xx / 5xx, the Telekom Security certification body is a conformity assessment body for corresponding trust service providers and the trust services that they offer.

- Repealed by coming into force of Trust Services Act (VDG): *Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway) (procedure type 030):*
  - *The Telekom Security certification body is recognized by the Bundesnetzagentur as a confirmation body for security confirmation for products in accordance with the German Digital Signature Act.*
  - *The Telekom Security certification body is recognized by the Bundesnetzagentur as an assessment and confirmation body ("Prüf- und Bestätigungsstelle") for assessing and confirming certification service providers (CSPs) in accordance with the German Digital Signature Act.*
- Designated body as per EU Regulation (EU) No. 910/2014 and Commission Decision 2000/709/EC
  (procedure type 021):

In conjunction with EU Regulation (EU) No. 910/2014, the Telekom Security certification body is a "designated body"[6]. This includes amongst others the above series of standards CEN EN 419 241 und CEN EN 419 221.

- Repealed by coming into force of eIDAS: *Designated body as per EU Regulation 1999/93/EC and Commission Decision 2000/709/EC (procedure type 020):*

  In conjunction with EU Directive (EU) 1999/93/EC, the Telekom Security certification body is a "designated body"[7].

During assessments and certifications, the confidentiality of the information provided by the applicant (ordering party) always plays a key role. The Telekom Security certification body has an organizational and technical infrastructure that is also suitable for handling classified governmental information at least up to the level "secret".

The accreditor pays particular attention to ensuring that the procedures of the certification body are accessible to all external interested parties, that impartiality and objectivity are guaranteed and that all applicants are treated equally.

[6] as per Article 30 of this Regulation, see www.europa.eu.int and www.fesa.rtr.at

[7] as per Article 3 (4) of this Directive, see www.europa.eu.int and www.fesa.rtr.at

2 Certification Programme 041: Security Certification of ICT Products

2.1 Aim of the Programme

In this program, without a restriction for a specific geographic area respectively jurisdiction, assessments are conducted for the determination of the assurance level of ICT products in accordance with Common Criteria (CC) with the aim of proving that ICT product in question meets the requirements laid down in the product security policy defined in the product-related Security Target.

All different versions of CC can be applied in the scope of this certification program, for example, ISO/IEC 15408, CC issued by the Common Criteria Management Committee (see www.commoncriteriaportal.org), CC referred to by SOGIS (see www.sogis.eu) and other CC versions.

For the particular jurisdiction of the entire European Union, EU Regulation (EU) No. 2019/881 (CSA), Art. 49 rules the adoption of European cybersecurity certification schemes. Once a European cybersecurity certification scheme refers to a version of CC, this European certification scheme is also in the scope of the current certification program.
Issuing European cybersecurity certificates by CAB is regulated by Art. 56 of CSA, especially by paragraph 4 with respect to paragraphs 5 and 6 of this Article.

The assessments within the current certification programme cover all assurance classes defined by CC and optionally defined by the related Security Target as extended assurance components. Assurance classes usually include the definition of TOE security policy in the related Security Target, technical specifications and tests of the TOE, related user guidance for and life cycle of the TOE as well as a vulnerability assessment. The application of the related assurance components is necessary in order to make a (verification and qualification) statement regarding the TOE conformity with the relevant security requirements defined by the related Security Target. For this purpose, accredited conformity assessment bodies shall evaluate and certify the TOE in question in accordance with the applicable version of Common Criteria. The relevant conformity assessment report (certification report) is provided to the applicant together with the confirmation of conformity (certificate). The applicant can present this certificate anywhere, if required.

The following specifications shall be observed for this program:

- Common Criteria for Information Technology Security Evaluation (CC) in the specific version as stated in the Conformance Claim Statement of the related TOE Security Target
- Common Methodology for Information Technology Security Evaluation (CEM) pertaining to the CC version stated in the Conformance Claim Statement of the related TOE Security Target
- Additional interpretations for the CC and CEM (version stated in the Conformance Claim Statement of the related TOE Security Target), which are valid and applicable within the certification scheme intended by the applicant
- Regulation (EU) No. 2019/881 (only for the particular jurisdiction of the entire European Union)
- Applicable implementing and delegated act of the EC (only for the particular jurisdiction of the entire European Union)
  Currently: none
- Current publications regarding approved cryptographic algorithms, which are valid and applicable within the certification scheme intended by the applicant. In case, the certification scheme intended by the applicant does not refer to any such publications, the well-known state-of-art shall be applied
- Specifications of the working group of accredited confirmation bodies (CAB-WG, should be established); currently: none.

Note:

Within the scope of Regulation (EU) No. 2019/881, the certification body acts as a conformity assessment body (CAB) as per Art. 60 for performing cybersecurity certifications in the sense of Art. 56 of CSA.

2.2 Offer Request and Certification Agreement

This information can be found in the annex „Certification and Conformity Assessment Policy".

2.3 Certification with Evaluation and Monitoring

General information can be found in the annex „Certification and Conformity Assessment Policy".

The following applies specifically to the current certification program:

Following the evaluation, the evaluators draw up an evaluation report (Evaluation Technical Report - ETR), which forms the basis for the certification decision. The certification body assesses the evaluation based on the evaluation report that has been drawn up and monitors compliance with the procedural specifications on the basis of DIN EN ISO/IEC 17065. The certification decision is logged. The applicant is informed of the certification decision.

If the certification decision is positive, the certificate is issued. This certificate reflects the scope of application of the certification, has a validity period based on the object of certification itself (TOE) and its potential conditions of use (but a maximum period of seven years) and represents the mark of conformity. A valid certificate provides authorization for public use of the mark of conformity in connection with the certified TOE in accordance with the annex „Certification and Conformity Assessment Policy".

The Telekom Security certification body offers ICT products vendors and users/risk owners evaluation and certification for the relevant technical components.

The evaluation and certification shall be performed based on specifications stated in chap. 2.1 above.

The evaluation is performed by evaluators/auditors who are employees of the certification body or of a recognised evaluation facility (see entry "status 'recognised EF'" in Glossary).

Requirements for evaluation facilities:

1) Recognition/licensing for implementing Common Criteria (usually in accordance with ISO/IEC 17025). This recognition/licensing shall cover the technological domains to which the object of certification (TOE) belongs as well as the evaluation assurance level (rigor of evaluation) required by the related Security Target for the TOE in question.
   This recognition/licensing shall have been issued by the responsible national or supranational regulator.

2) General requirements for evaluation facilities, see Section 3 below.

Performing the evaluation:

The organizational and functional procedure for the evaluation process is set up in accordance with the applicable methodology for the selected security evaluation process. For Common Criteria, this is the Common Methodology for Information Technology Security Evaluation (CEM) and additional interpretations and Supporting Documents, which are valid and applicable within the certification scheme intended by the applicant. It could be, for example, additional interpretations and Supporting Documents issued by CCMC[8] (see https://www.commoncriteriaportal.org) as well as by SOGIS[9] (see http://www.sogis.eu).

The feasibility of an evaluation requires the applicant to disclose or make available all the construction details for all security-related components of the object of certification that are required for the intended evaluation assurance level. The responsible certifier and the evaluators coordinate the time schedule of the certification process with the applicant.

These contributions and provisions are verified by the evaluators in line with the applicable methodology. This verification and the result are documented in single evaluation reports. Evaluators inform the applicant regarding the reasons that they identify that result in documents needing to be revised by the applicant. In the event of any discrepancies, the certification body is consulted for clarification purposes.

Based on the applicable methodology, evaluators also perform all the necessary audits for the relevant development, test and production sites (on-site) as well as tests and the analysis and assessment of vulnerabilities for the object of certification. The results are documented in single evaluation reports.

Where available, assessments by other independent bodies relating to individual parts of the object of certification may also be used. For example, the verification of the relevant development, test and production sites (on-site) can use reusable results of a site certification. The evaluation of a composite TOE can be performed as part of a composite evaluation.

[8] Common Criteria Management Committee

[9] Senior Officials Group Information Systems Security

The extent of reuse is agreed between the responsible certifier and the evaluators. It is important to ensure that the reused results can be used for the certification of the TOE in accordance with the certification scheme chosen by the applicant.

Upon completion of the evaluation, the evaluators draw up a final evaluation report (Evaluation Technical Report – ETR) for the evaluation of the object of certification and hand this over to the applicant and the certification body as the basis for the certification. The ETR contains a statement regarding the conformity of the security properties of the TOE in question with the Security Requirements Statement made in the related Security Target.

This report forms the basis for the decision regarding certification. The decision regarding certification is made by the management of the certification body. The certificate is issued with a period of validity based on the results of the evaluation, and this validity period depends on the object of certification and its possible operational environment. The maximum period of validity is seven years. Once this period has expired, it is necessary to re-evaluate the conformity of the properties of the object of certification with the relevant requirements laid down in the TOE Security Target in order to extend the validity of the certificate.

Monitoring the use of the mark of conformity:

General information can be found in the annex „Certification and Conformity Assessment Policy".

Monitoring of the use of the mark of conformity for a specific certification programme involves the following:

- Limiting the validity of the mark of conformity to a maximum of seven years with the possibility of a full assessment to determine whether the underlying conformity statement (certification decision) can be maintained.
- Performing an event-based assessment to determine whether the underlying conformity statement (certification decision) can be maintained. Such an event may, for example, be a security-related problem that has become known in the specific object of certification or the relevant technology.

If changes are made to the object of certification within the certificate's validity period, the corresponding rules from the annex „Certification and Conformity Assessment Policy" apply; in particular, the section "Maintenance of the mark of conformity following changes".

The applicant must inform the certification body immediately of any changes that affect the certification and provide a description of the changes. Based on the description, the certification body decides whether another evaluation is necessary or whether the changes can be checked as part of the next monitoring procedure or recertification procedure.

2.4 Publishing the Certificate and Using the Mark of Conformity

General information can be found in the annex „Certification and Conformity Assessment Policy", in the sections "Disclosure and publication" and "Monitoring the use of the mark of conformity".

2.5 Certification Expenses

General information can be found in the annex „Certification and Conformity Assessment Policy", in the section "Procedure costs and liability".

2.6 Complaints and Objections

General information can be found in the annex „Certification and Conformity Assessment Policy", in the section "Procedure for complaints and objections".

For the specific certification program, the *national cybersecurity certification authority* that can be called in conjunction with the complaints procedure is:

> Bundesamt für Sicherheit in der Informationstechnik, Abteilung SZ Standardisierung und Zertifizierung, Postanschrift: Postfach 20 03 63, 53133 Bonn.

3 General Requirements for Evaluation Facilities

The following requirements for evaluation facilities apply irrespective of the specific certification programme chosen:

1) The evaluation facility shall have a legally binding contractual basis (Recognition Agreement – document No. 041) with the Telekom Security certification body (ISO/IEC 17065, 6.2.2).

2) The evaluation facility shall possess the status 'recognised EF' granted by the CB.

3) For each individual certification procedure, the evaluation facility shall be able to present a legally enforceable agreement with the applicant that allows the evaluation facility to perform all examinations necessary in the context of the requested certification procedure at least to the degree of assessment envisaged in the certification application. Among other things, this agreement must cover drawing up a plan for the evaluation activities (evaluation plan) by the evaluation facility, so that the necessary rules of the relevant certification programme can be applied.

4) The evaluation facility must document the results of all evaluation activities. This documentation is drawn up in the form of evaluation, audit, inspection or observation reports. These reports must address every single aspect of evaluation that is required in the certification programme and is applicable to the specific certification procedure, and clearly document the evaluation results for each aspect of evaluation.

4 Supplementary Services

The following services are available for each type of procedure as well as outside of one of the certification programs listed above:

- Preparing assessment and certification procedures in the form of workshops
- Training developers with regard to criteria-compliant development and optimization of certification procedures
- Training IT security officers with regard to possible verification and certification of development, test and production infrastructures

If workshops or training courses are offered for certification body applicants, these are limited exclusively to the exchange of information between the certification body and its customers, such as explanations regarding assessment statements or the clarification of valid assessment and certification requirements.

Consultation in the sense of ISO/IEC 17065, ch. 3.2 does not take place as a matter of principle.

- Translating the body's own marks of conformity and reports into other languages
- Performing reproduction and printing tasks with regard to issuing the body's own marks of conformity and reports
- Holding presentations on the certification schema and the achieved results at customer events and conventions

- Announcing procedures and publishing results (press releases, specialist journals, publications on the certification body's website).

5 Glossary

Term	Definition
CSA	REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)
eIDAS	REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
CC	Common Criteria for Information Technology Security Evaluation (independent of their issuer)
Security Target (ST)	CC v.3.1, rev. 5, part 1 (issued by CCMC): implementation-dependent statement of security needs for a specific identified TOE (see 'Object to be certified' below)
ICT product ICT service ICT process	REGULATION (EU) 2019/881 (CSA), Art. 2: 'ICT product' means an element or a group of elements of a network or information system 'ICT service' means a service consisting fully or mainly in the transmission, storing, retrieving or processing of information by means of network and information systems 'ICT process' means a set of activities performed to design, develop, deliver or maintain an ICT product or ICT service
Certification program/procedure type	following ISO/IEC 17065: *Certification system* (conformity assessment system) that relates to a certain class or certain type of *objects to be certified*, to which the same defined requirements, specific rules and procedures are applied. The rules, procedures and management of the

Term	Definition
	certification of products, processes and services are laid down by the certification program.
Certification/conformity assessment procedure	A specific qualification procedure (conformity assessment procedure) that is applied to the *object to be certified* by the certification body by order of the applicant. A certification/conformity confirmation procedure must be carried out as part of a *certification program*.
Certification system (conformity assessment system)	Rules, procedure and management for the implementation of certifications
Object to be certified (object of certification, object of the conformity assessment, TOE – target of evaluation)	Product/service/process for which the applicant aims to obtain a mark of conformity.
Applicant (ordering party)	Legal entity who applied at the CB for the issuing a certificate in accordance with a Certification Programme offered by the CB
Mark of conformity (certificate)	ISO/IEC 17030: "Protected mark issued by a body performing third-party conformity assessment, indicating that an object of conformity assessment (product, process, person, system or body) is in conformity with specified requirements". Conformity assessments can be confirmed by the certification body in the form of certificates, confirmations and quality or test seals.
Holder of a mark of conformity	Applicant, whose requested certification procedure is completed with the issuance of a mark of conformity.
Owner of a mark of conformity	ISO/IEC 17030: "person or organization that has legal rights to a third-party mark of conformity" In the current context: The Certification Body of Telekom Security
Issuer of a mark of conformity	ISO/IEC 17030: "body that grants the right to use a third-party mark of conformity" In the current context: The Certification Body of

Term	Definition
	Telekom Security
Evaluation facility (EF)	Derived from ISO/IEC 17025 (laboratory): body that performs evaluation of IT services and/or IT products by one or more of the following activities: - testing; - audit; - calibration; - sampling, associated with subsequent testing or calibration.
Operator of EF	Legal entity operating an evaluation facility
Recognition Agreement	A legally binding contract with an EF who applied for or already acts as EF with the status 'recognised EF' granted by the CB (document #041).
status 'recognised EF'	A status granted by the CB to an EF, who successfully passed the EF recognition procedure laid down in the related document #040.
Consulting (in conjunction with the activities of certification bodies, the staff of certification bodies and organizations that are related to or associated with certification bodies)	ISO/IEC 17065 (3.2): Participation in: a) Development, production, installation, maintenance or distribution of a certified product or a product to be certified; or b) Development, implementation, operation or maintenance of a certified process or a process to be certified; or c) Development, implementation, provision or maintenance of a certified service or a service to be certified.

End of Certification Practice Statement

Certification Practice Statement

Issuer: Telekom Security International GmbH
Address: Bonner Talweg 100, 53113 Bonn
Phone: +49-(0)228-181-0
Fax: +49-(0)228-181-49990
Web: https://www.t-systems-zert.com/
https://www.telekom.de/security