Certification Practice Statement

Certification Program ‘eIDAS TSP’ (accredited area)
of the Certification Body of Telekom Security
(certification program 031)

Foreword

Telekom Security operates a certification body accredited by DAkkS[1] in accordance with ISO/IEC 17065 and ETSI EN 319 403, 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) for the conformity certification of electronic signature creation devices**.**

This document describes the certification program for issuing Telekom Security certificates for qualified trust service providers and the trust services they provide as provided for in Article 20 of Regulation (EU) No. Nr. 910/2014 that fall within this accredited area. 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 https://www.t-systems-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
💻 https://www.t-systems-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 Systemhaus)
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	Program 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 program 06
4.0-eIDAS	June 2, 2016	Modifications in the context of ISO 17065 accreditation by DAkkS; a dedicated CPS is issued for each program. The scope of the document covers only the eIDAS program in the accredited area.
4.01-eIDAS	June 22, 2016	Editorial adjustments
4.02-eIDAS-TSP	July 11, 2016	Editorial adjustments
4.03-eIDAS-TSP	August 11, 2016	sec. 1.3 and 2.3, ETSI EN 319 411-1: Reference to CA/Browser Forum; annual monitoring audits, if ETSI is applied.
4.04-eIDAS-TSP	January 2, 2017	Address change
4.05-eIDAS-TSP	July 1, 2017	Phone number change
4.06-eIDAS-TSP	August 1, 2017	Expiry of SigG, coming into force of VDG
4.07-eIDAS-TSP	July 17, 2018	Glossary supplemented; sec. 2.3 (program-specific requirements on evaluation facilities)
4.08-eIDAS-TSP	March 29, 2019	a) optional: ETSI TS 119 431-1: remote signature service components, chap. 1.1, chap. 2.3 b) optional: ETSI TS 119 441-1: signature validation service, chap. 1.1, chap. 2.3 c) optional: ETSI EN 319 522 series: eRDS, chap. 1.1, chap. 2.3 d) optional: PSD2: optional conformity assessment with respect to certificates profiles for electronic seals and website authentication acc. to Article 34 of DELEGATED REGULATION (EU) 2018-389; chap. 2.3.
4.09-eIDAS-TSP	June 27, 2019	a) optional: ETSI EN 319 521: eRDS (additionally to ETSI EN 319 522), chap. 1.1, chap. 2.3
5.00-eIDAS-TSP	July 1, 2020	Renaming into Telekom Security
5.01-eIDAS-TSP	August 12, 2020	sec. 2.6: BSI as supervisory authority for TSPs that issue qualified certificates for website authentication (id = A3)

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 clients and 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 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 to issue 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 (ICT operators, users, providers and developers):

- 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.
- Developers of IT products require information on security gaps at a very early stage in their development process, and advice with regard to standard-compliant development processes. Assessment and certification processes should therefore run in parallel to product development.

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 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:

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

These services are based on standards and normative documents such as European and national regulations regarding trust services (at EU level – in the context of the eIDAS[2]: electronic signatures, seals, timestamps, services for delivering electronic registered letters, website authentication; national – within the framework of the German Trust Services Act (VDG)) – and European and national regulations regarding the certification of qualified electronic signature creation devices (eIDAS and VDG), 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 https://www.t-systems-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 by the following institutions:

- 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[3] for trust service providers and the trust services that they offer.

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

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

- 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
  - ETSI EN 319 421: Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
  - ETSI TS 119 431: 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 TS 119 441: Policy requirements for TSP 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"[4]. 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"[5].

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

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

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.

2 Certification program 031: Certification for trust service providers in accordance with Regulation (EU) No. 910/2014

2.1 Aim of the program

In this program for the area of the entire European Union, assessments are conducted for trust service providers (TSPs), in accordance with Regulation (EU) No. 910/2014 (Articles 20 and 21), with the purpose of proving that the TSPs themselves and the qualified trust services they provide meet the requirements laid down in this Regulation. These assessments cover both the TSP’s security concept and its practical implementation. The corresponding conformity assessment report including the confirmation of conformity (certificate) is submitted to the trust service provider to be presented to the Bundesnetzagentur in its role as supervisory authority in accordance with the eIDAS.

Within the framework of Article 24 (1) d) of Regulation (EU) No. 910/2014, the certification body establishes, where required, whether the qualified trust service provider verifies the identity and specific attributes of the natural or legal person for whom the qualified certificate is issued using identification methods that provide equivalent security with regard to reliability when the person is present.

The following specifications shall be observed for this program:

- Regulation (EU) No. 910/2014
- Applicable implementing act of the EC
- Current publications regarding approved cryptographic algorithms for the relevant technical components
- Specifications of the working group of recognized confirmation bodies (Arbeitsgruppe anerkannter Bestätigungsstellen, AGAB).

Note:

Within the framework of Regulation (EU) No. 910/2014, the certification body acts as “conformity assessment body (CAB)” in accordance with Article 3, Point 18 and Articles 20, 21 and 24.

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 (conformity assessment report in accordance with Article 20 (1) of the eIDAS), 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 customer 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 maximum validity period of 24 months (Article 20 (1) of the eIDAS) and represents the mark of conformity. A valid certificate provides authorization for public use of the mark of conformity in connection with the certified qualified trust service in accordance with the annex „Certification and Conformity Assessment Policy".

Single trust services:

The Telekom Security certification body provides assessment and certification for the following qualified trust services for qualified trust service providers[6] in accordance with EU Regulation No. 910/2014 dated July 23, 2014 (eIDAS):

[6] Abbreviated below to TSP

ID	Description of the trust service	"Qualified trust service type" ETSI TS 119 612 V2.1.1 (2016-04) Section 5.5.1.1; please also refer to Chapter 2 of IMPLEMENTING DECISION (EU) 2015/1505
A1	Creating qualified certificates for electronic signatures	(a) …/CA/QC (b) …/Certstatus/OCSP/QC (c) …/Certstatus/CRL/QC
A2	Creating qualified certificates for electronic seals	(a) …/CA/QC (b) …/Certstatus/OCSP/QC (c) …/Certstatus/CRL/QC
A3	Creating qualified certificates for website authentication	(a) …/CA/QC (b) …/Certstatus/OCSP/QC (c) …/Certstatus/CRL/QC
A4	Creating qualified electronic timestamps	(d) …/TSA/QTST
A5	Creating qualified electronic signatures	(i) …/RemoteQSCDManagement/Q[7]
A6	Creating qualified electronic seals	(i) …/RemoteQSCDManagement/Q[7]
B1	Checking and validating qualified electronic signatures, seals, timestamps and corresponding qualified certificates	(h) …/QESValidation/Q
B2	Checking and validating qualified certificates for website authentication	(h) …/QESValidation/Q
C1	Storing qualified electronic signatures, seals or corresponding qualified certificates	(g) …/PSES/Q
D1	Delivering electronic registered letters	(e) …/EDS/Q

[7] Not covered by IMPLEMENTING DECISION (EU) 2015/1505

ID	Description of the trust service	"Qualified trust service type" ETSI TS 119 612 V2.1.1 (2016-04) Section 5.5.1.1; please also refer to Chapter 2 of IMPLEMENTING DECISION (EU) 2015/1505
		(f) …/EDS/REM/Q

The assessment and certification can be performed on the basis of relevant ETSI standards:

ETSI EN 319 401 defines general requirements for TSPs that offer one or more of the qualified trust services specified above (A - D).

ETSI EN 319 411-2 defines additional requirements for TSPs that issue qualified certificates. These requirements are relevant for the qualified trust services A1 - A3. ETSI EN 319 411-2 refers to the requirements of ETSI EN 319 411-1[8] and distinguishes between the following certification policies:

- QCP-n: Certification policy for EU qualified certificates for natural persons
- QCP-n-qscd: Certification policy for EU qualified certificates for natural persons that requires the use of qualified electronic signature creation devices (QSCD)
- QCP-l: Certification policy for EU qualified certificates for legal persons
- QCP-l-qscd: Certification policy for EU qualified certificates for legal persons that requires the use of qualified electronic signature creation devices (QSCD)
- QCP-w: Certification policy for EU qualified certificates for website authentication.

ETSI EN 319 421 defines requirements for TSPs that issue qualified electronic timestamps. These requirements are relevant for the qualified trust service A4.

ETSI TS 119 431-1 defines requirements for TSPs concerning TSP service components implementing a remote QSCD / SCDev. These requirements are relevant for the qualified trust service A5 and A6[7].

[8] *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 TS 119 441 defines requirements for TSPs providing signature validation services. These requirements are relevant for the qualified trust services B1 and B2.

ETSI EN 319 521 and ETSI EN 319 522 Series: Electronic Registered Delivery Service. These requirements are relevant for the qualified trust service D1.

PSD2:

Additionally, the assessment and certification can be performed with respect to the conformity of the qualified certificates profiles for electronic Seal and website authentication according to the requirements of Article 34 of DELEGATED REGULATION (EU) 2018-389 in the context of Payment Services DIRECTIVE (EU) 2015-2366 (PSD2). Such additional assessment can also be done - additionally to Article 34 - with respect to ETSI TS 119 495 "Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366".

The certification is performed on the basis of ETSI EN 319 403. The evaluation is performed by evaluators/auditors who are employees of the certification body or are approved by the certification body.

Requirements for evaluation facilities:

1) Either accreditation as a conformity assessment body as defined in Article 3 (18) of Regulation (EU) No. 910/2014 by the national accreditation body responsible in accordance with Regulation (EU) No. 765/2008

2) Or recognition/licensing for implementing any other process/service/product assessment criteria covering process/service/product security audit (usually in accordance with ISO/IEC 17021 or/and ISO/IEC 17025).
   This recognition/licensing shall cover the technological domains to which the object of certification belongs as well as the evaluation assurance level (rigor of evaluation) required by Regulation (EU) No. 910/2014 (incl. the relevant implementing act).
   This recognition/licensing shall have been issued by the responsible national or supranational regulator.

3) General requirements for evaluation facilities, see Section 4 below.

Performing the audit:

The auditors examine the TSP with regard to conformity with the eIDAS requirements relevant for the qualified trust service, taking account of the requirements in the ETSI standards specified above. The audit establishes whether the organizational and technical measures of the TSP meet the requirements.

The audit of the trust service is divided into two phases:

- The documentation assessment
- The subsequent on-site audit.

The certifier responsible and the auditors coordinate the time schedule of the certification process with the customer.

In the first phase of auditing the TSP, the auditors analyze the documentation required in the standards and check it for conformity. If this assessment reveals that the trust service does not meet the requirements, no on-site audit is carried out. The applicant has the opportunity to adapt the TSP’s documentation in line with the requirements and have it checked by the auditors again.

After assessing the TSP documentation, if the auditors reach the conclusion that the documentation meets the requirements of the applicable standards, they proceed to the second phase of the evaluation, the on-site audit. The aim of this audit is to determine that the trust service is implemented as described in the documentation and is implemented in accordance with the requirements. The on-site audit is performed on the premises of the TSP on a date agreed with the applicant beforehand.

The on-site audit consists of checking the organizational, structural and technical implementation of the measures described in the documentation for meeting the requirements.

During this process, the auditors collect random samples of evidence by carrying out surveys, checking documents, observing activities and conditions, and performing technical tests. Where available, assessments by other independent bodies relating to individual parts of the service to be assessed may also be used. For example, it is not necessary for the auditors to perform their own evaluations of technical components. They can use the audit reports and certificates of other independent bodies for their assessment.

The extent of reuse is agreed between the certifier responsible and the auditors. It must be ensured here that the reused results are suitable for use in accordance with the eIDAS for

the certification of the qualified trust service provider and the qualified trust services that it provides.

Once the on-site audit has been performed, the auditors use the documentation assessment and audit as a basis to draw up a conformity assessment report in accordance with Article 20 (1) of the eIDAS, making a statement regarding the compliance of the trust service with the relevant eIDAS requirements and, where appropriate, ETSI standards. This report forms the basis for the decision regarding certification. The decision regarding certification is made by the management of the certification body. Depending on the results of the audit, the certificate is issued with a maximum validity period of two years (Article 20 (1) of the eIDAS). After two years at the latest, a full audit is necessary in order to extend the certificate validity.

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 program involves the following:

- Limiting the validity of the mark of conformity to a maximum of 24 months with the possibility of a full assessment to determine whether the underlying conformity statement (certification decision) can be maintained – see Regulation (EU) No. 910/2014, Article 20 (1).
- Performing regular monitoring audits – as a rule at least annually, cf. ETSI EN 319 403, sec. 7.9 „Surveillance“, if the assessment and certification is perfrmed on the base of the related ETSI standards.
- 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 – see Regulation (EU) No. 910/2014, Article 20 (2).

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 TSP 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 audit is necessary or whether the changes can be checked as part of the next monitoring audit or recertification audit.

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 *supervisory authorities* that can be called in conjunction with the complaints procedure are:

a) for TSPs that issue qualified certificates for website authentication (Id “A3” in chap. 2.3 above):
   Bundesamt für Sicherheit in der Informationstechnik, Referat SZ 25, Postfach 20 03 63, 53133 Bonn
b) for TSPs that provide all other qualified trust services in the scope of this Certification Program:
   Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (German Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway), Referat Qualifizierte elektronische Signatur (Qualified Electronic Signature), Canisiusstraße 21, 55122 Mainz

3 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 (including in-house)
- Training IT security officers with regard to possible verification and certification of development, test and production infrastructures (including in-house)

  If consulting sessions 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 findings or the clarification of assessment and certification requirements.
- 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).

4 General requirements for evaluation facilities

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

1) The evaluation facility shall have a legally binding contractual basis (license contract/license agreement) with the Telekom Security certification body (ISO/IEC 17065, 6.2.2).

2) 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 program can be applied.

3) 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 program and is applicable to the specific certification procedure, and clearly document the evaluation results for each aspect of evaluation.

5 Glossary

Term	Definition
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.
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
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.
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)	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 Program offered by the CB
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 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

Term	Definition
	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.
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.

End of Certification Practice Statement

Certification Practice Statement

Issuer: Deutsche Telekom Security 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