Certification Practice Statement

Certification Programme ‘eIDAS TSP QATAR’ (licensed area) of the Certification Body of Telekom Security (Certification Programme 050)

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 Certification Body of Telekom Security 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.

Furthermore, the Certification Body of Telekom Security is a licensed Conformity Assessment Body in the State of Qatar as per Decision of the President of the Communications Regulation Authority of the State of Qatar No. (65) of 2025[2]. The legal framework for this activity is the “The Decision of the President of the Communications Regulation Authority of the State of Qatar No. (3) of 2025”.

This document describes the Certification Programme 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. 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 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, Friedrich-Ebert-Allee 71-77, 53113 Bonn
☎ +49-(0)228-181-0
💻 www.telekom-zert.com

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

[2] see https://www.cra.gov.qa/en/Services/Trust-Services/Law-and-Regulations

Table of Contents

Revision list

Revision	Date	Activity
5.00-eIDAS-TSP-QATAR	October 29, 2025	First issue of this Certification Programme for Qatar TSPs This document refers to the Certification Programmes 031 and 032 in their versions 5.xx. Hence, though it is the first issue of the present document, it shall bear the version 5.00 for the sake of versions synchronisation with the related programmes.

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 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 (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 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[3]: 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.

If the Certification Body of Telekom Security is accredited and/or licensed within the legal framework of another jurisdiction as the European Union, these services of the Certification Body of Telekom Security are additionally based on standards and normative documents being valid and applicable within the related legal frameworks.

For the State of Qatar, the related legal framework is the "The Decision of the President of the Communications Regulation Authority of the State of Qatar No. (3) of 2025".

The Certification Body of Telekom Security 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 Programmes.

The Certification Body of Telekom Security is accredited for the performance of the conformity assessment activities in the following substantive areas:

- EU Regulation (EU) No. 910/2014 (eIDAS)
  (Certification Programme 031):
  In conjunction with the Regulation (EU) No. 910/2014, the Certification Body of

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

Telekom Security is a conformity assessment body[4] for trust service providers and the trust services that they offer.

- ETSI EN 319 4xx (incl. TS 103 xxx, TS 119 xxx): Electronic Signatures and Infrastructures (ESI)
  (Certification Programme 032):

  In conjunction with the above series of standards, the Certification Body of Telekom Security is a conformity assessment body for corresponding trust service providers and the trust services that they offer.

- Designated body as per EU Regulation (EU) No. 910/2014 and Commission Decision 2000/709/EC
  (Certification Programme 021):

  In conjunction with the Regulation (EU) No. 910/2014, the Telekom Security certification body is a “designated body”[5]. This includes amongst other things the series of standards CEN EN 419 241 und CEN EN 419 221.

- The Decision of the President of the Communications Regulation Authority of the State of Qatar No. (3) of 2025
  (Certification Programme 050):
  In conjunction with the stated above Decision No. (3) of 2025 of the President of the CRA of Qatar, the Certification Body of Telekom Security is a conformity assessment body[6] for trust service providers and the trust services that they offer.

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

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

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

[6] in accordance with Article 18 of the Regulation for Certification Service Providers (no. CRATA/2025/01/14 issued by the CRA of Qatar), for the scope of services set out in the Decision attached with reference no. CRATA/2025/09/11-B

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 Programme 050: Certification for Trust Service Providers in accordance with the Decision of the President of the Communications Regulatory Authority No. (3) of 2025

2.1 Aim of the Programme

In this programme for the area of the State of Qatar, assessments are conducted for trust service providers (TSPs), in accordance with the Decision of the President of the Communications Regulatory Authority No. (3) of 2025 and the Regulation for Certification Providers CRATA/2025/01/14 (Article 17), 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 Communications Regulatory Authority of the State of Qatar in its role as Authority in accordance with the Regulation for Certification Providers CRATA/2025/01/14.

Within the framework of Article 24 .1a (c) 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 by using identification methods, which ensure the identification of the person with a high level of confidence.

Within the framework of Article 24 .1b (d) of Regulation (EU) No. 910/2014, the certification body establishes, where required, whether the qualified trust service provider verifies specific attributes of the natural or legal person for whom qualified electronic attestation of attributes are issued by using methods, which ensure the verification of the attributes with a high level of confidence.

The following specifications shall be regarded to for this programme:

- Regulation for Certification Providers CRATA/2025/01/14
- The rules laid down in the Decision of the President of the Communications Regulatory Authority No. (3) of 2025
-

- Current publications regarding approved cryptographic algorithms for the relevant technical components
- Specifications of the working group of recognized confirmation bodies (ACAB’c, AGAB), in which the Certification Body of Telekom Security participates, may be regraded, too, where applicable.

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 present Certification Programme:

This Certification Programme is a combination of the existing Certification Programmes 031 and 032. The content of this chapter is documented in both chapters 2.3 of the Certification Programmes 031 and 032.

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 Programme, the *supervisory authorities* that can be called in conjunction with the complaint’s procedure are:

a) for TSPs that provide all qualified trust services in the scope of this Certification Programme:
Communications Regulatory Authority of State of Qatar, Al-Nasr Tower B, Westbay, P.O. Box 23404, Doha, Qatar

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 (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 Programme 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 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
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 certification of products, processes and services are laid down by the Certification Programme.
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 Programme*.
Certification system (conformity assessment system)	Rules, procedure and management for the implementation of certifications
Object to be certified (object of	Product/service/process for which the applicant aims to

Term	Definition
certification, object of the conformity assessment)	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
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 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.
Consulting (in conjunction with the activities of certification bodies, the staff of certification bodies and organizations that are related	ISO/IEC 17065 (3.2): Participation in: a) Development, production, installation, maintenance or

Term	Definition
to or associated with certification bodies)	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: Deutsche Telekom Security GmbH
Head office: Friedrich-Ebert-Allee 71-77, 53113 Bonn
Address of CB: Bonner Talweg 100, 53113 Bonn
Phone: +49-(0)228-181-0
Web: www.telekom-zert.com
https://www.telekom.de/security