Certification Practice Statement

Certification Program ‘eIDAS qSCD’ (accredited area)
of the Certification Body of Telekom Security
(certification program 021)

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 program for issuing Telekom Security conformity certificates for qualified electronic signature and seal creation devices as defined in Article 30 and 39, respectively, of Regulation (EU) No. 910/2014 that fall within the accredited and recognized area as a designated body. 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
4.00-eIDAS-qSCD	July 11, 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 recognized area.
4.01-eIDAS-qSCD	August 11, 2016	sec. 1.3, ETSI EN 319 411-1: Reference to CA/Browser Forum
4.02-eIDAS-qSCD	January 2, 2017	Address change
4.03-eIDAS-qSCD	July 1, 2017	Phone number change
4.04-eIDAS-qSCD	August 1, 2017	Expiry of SigG, coming into force of VDG
4.05-eIDAS-qSCD	July 16, 2018	Editorial changes, chap. 2.3
4.06-eIDAS-qSCD	February 8, 2019	Editorial changes, chap. 2.3
4.07-eIDAS-qSCD	February 20, 2019	Editorial changes: ‘accredited area’ additionally to ‘recognised area’
4.08-eIDAS-qSCD	June 27, 2019	References to EN 319 431, EN 319 441, EN 319 521, EN 319 522 sowie auf EN 419 241, EN 419 221
5.00-eIDAS-qSCD	July 1, 2020	Renaming into Telekom Security

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 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 (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 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 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 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 within the following frameworks:

- EU Regulation (EU) No. 910/2014 (eIDAS)
  (procedure type 031):
  In conjunction with EU Regulation (EU) No. 910/2014, the Telekom Security

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

certification body is a conformity assessment body[3] 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
  - 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

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

- 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"[4]. This includes amongst others the above series of standards CEN EN 419 241 und CEN EN 419 221.

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

- 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].

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.

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

2 Certification program 021: certification for qualified electronic signature creation devices as per 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 electronic signature / seal creation devices (qSCD/qSEE[6]; a technical component) in accordance with Regulation (EU) No. 910/2014 (Article 30 and 39, respectively), with the aim of proving that qSCDs meet the requirements laid down in this Regulation (see Annex II to the Regulation). These assessments cover the technical specifications, user guidance and tests for the qSCD as well as an analysis of its weaknesses, which are necessary in order to make a statement regarding conformity with the relevant requirements. For this purpose, recognized assessment bodies (designated bodies) must evaluate these technical components in accordance with the Common Criteria or a security evaluation process (assessment criteria) other than this as per Article 30 (3) of Regulation (EU) No. 910/2014. The relevant conformity assessment report (certification report) is submitted to the applicant together with the confirmation of conformity (certificate). The applicant can present this certificate anywhere, if required.

The following specifications must be observed for this program:

- Regulation (EU) No. 910/2014
- Applicable implementing act of the EC
  Currently:
  - As per Article 30 (3): Standards for assessing the security of IT products (COMMISSION IMPLEMENTING DECISION (EU) 2016/650 of April 25, 2016),
  - As per Articles 27 (5) and 37 (5): Reference formats for advanced electronic signatures and seals (COMMISSION IMPLEMENTING DECISION (EU) 2015/1506 of September 8, 2015) as per Regulation (EU) No. 910/2014
- Current publications regarding approved cryptographic algorithms for creating signatures

[6] qualified signature creation device

- Specifications of the working group of recognized confirmation bodies (Arbeitsgruppe akkreditierter Bewertungsstellen, AGAB).

Note:

Within the scope of Regulation (EU) No. 910/2014, the certification body acts as a designated body in accordance with Article 30 and Commission Decision 2000/709/EC.

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 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 qualified electronic signature creation device in accordance with the annex „Certification and Conformity Assessment Policy".

The Telekom Security certification body offers SCD vendors and users evaluation and certification for the relevant technical components.

The evaluation and certification shall be performed on the basis of following implementing acts:

(i) "COMMISSION IMPLEMENTING DECISION (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014"

(ii) COMMISSION IMPLEMENTING DECISION (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognized by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014.

Certification is performed on the basis of Common Criteria or a security evaluation process (assessment criteria) other than this as per Article 30 (3) of Regulation (EU) No. 910/2014. 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) Recognition/licensing for implementing Common Criteria or "on the basis of a security evaluation process (assessment criteria) other than this as per Article 30 (3) of Regulation (EU) No. 910/2014" (usually in accordance with 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.
2) General requirements for evaluation facilities, see Section 4 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 international interpretations and Supporting Documents, issued by CCMC[7] (see https://www.commoncriteriaportal.org) as well as by SOGIS[8] (see http://www.sogis.eu). For the procedures "on the basis of a security evaluation process (assessment criteria) other than this as per Article 30 (3) of Regulation (EU) No. 910/2014",

[7] Common Criteria Management Committee

[8] Senior Officials Group Information Systems Security

the valid assessment methodology of the selected particular security evaluation process is applied.

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 level. The certifier responsible 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 component manufacturer. 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 and production sites (on-site) as well as tests and the analysis and evaluation 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 and production sites (on-site) can use reusable results of a site certification. The evaluation of a composite technical component can be performed as part of a composite evaluation.

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

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, containing a statement regarding the conformity of the properties of the electronic signature creation device with the relevant eIDAS requirements and hand this over to the certification body and the applicant as the basis for the certification.

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 eIDAS requirements 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 program 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 qSCD provider 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 *supervisory authority* that can be called in conjunction with the complaints procedure is:

> 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 calibration.
Operator of EF	Legal entity operating an evaluation facility

Term	Definition
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