Federal Office
for Information Security

Product Certification: Network Equipment Security Assurance Scheme (NESAS)

NESAS-Produkte (courtesy translation)

Version 1.3 dated 2024-10-01

Federal Office for Information Security (BSI)
Postfach 20 03 63
53133 Bonn
Tel.: +49 (0) 800 2741 000
Email: service-center@bsi.bund.de
Internet: https://www.bsi.bund.de

Change history

Version	*Date*	*Name/Org. unit*	*Description*
1.0	2022-07-01	Division SZ 33	First edition
1.1	2022-12-14	Division SZ 33	Revision: • Addition of conditions for the inclusion of the procedure regarding audits and conditions for the implementation of the evaluation. • Adjustments resulting from the use of the "NESAS-Zert" and other referenced documents • Editorial changes and clarification of procedural steps
1.2	2023-11-01	Division SZ 33	Revision: • Revision of chapter 3.2 • Specification of retention periods • Contact information for the BSI • Revisions of the process steps • Redactional changes
1.3	2024-10-01	Devision S 26	Revison: • Update section 4.1 Minor updates • Update section 4.3- Inclusion of different execution environments in the certificate • Revision of the necessary documents in the certification process (sections 3.3.2.2, 3.3.3.2, 3.3.4.2) • Additions to data exchange in section 3.3.3.2 • Removal of fig. 1: Document index (certification and licensing programme) in Chapter 1.1 and the relevant amendment in the Chapter. • Redactional changes

Table 1 Change history

Contents

1 Introduction

A product is certified at the instigation of the vendor, sponsor or distributor of IT products. This document is therefore primarily aimed at all applicants for a NESAS CCS-GI security certificate.

1.1 Aim and integration of the scheme

This scheme sets out the detailed requirements and information to supplement the document "Verfahrensbeschreibung zur Zertifizierung von Produkten, Prozessen und Dienstleistungen" (Procedure description for the certification of products, processes and services) [VB-Produkte.PD] if the applicant wishes to obtain a NESAS certification. The applicant can find information on how to implement the procedure here.

Based on these documents, an evaluation facility can provide information to the vendor in preparation for their application.

The tasks that an applicant must take into account to comply with the regulations and meet the stipulations and requirements for the procedure are specifically stated. Forms or other resources, etc. are indicated at the relevant points in the document.

The description of the various document categories is available in the higher-level file "Verfahrensbeschreibung zur Zertifizierung von Produkten, Prozessen und Dienstleistungen" (Procedure description for the certification of products, processes and services) [VB-Produkte.PD].

2 Certification scheme

The IT security certification scheme describes the following certification options:

- Certification of an IT product according to the “Network Equipment Security Assurance Scheme Cybersecurity Certification Scheme – German Implementation” (NESAS CCS-GI).

The currently valid documents required for the certification scheme are listed in the document “Verzeichnisse” (Indexes) [Verzeichnisse].

For ease of legibility, in the following document the abbreviation NESAS is used in place of NESAS CCS-GI. Other NESAS variants, where referenced, are explicitly indicated as such.

2.1 Certification of the IT security of IT products according to NESAS

2.1.1 General aspects of certification according to NESAS

The “Network Equipment Security Assurance Scheme” (NESAS) is a framework for assuring and improving security in mobile networks. NESAS is thus creating a basis for evaluating defined security properties of IT products that serve to provide a mobile network infrastructure, referred to below as network products. Thus, NESAS CCS-GI is a certification scheme for products, which have completely or partially been developed for the operation of mobile networks.

For verification, the corresponding network products must be developed by the vendor in accordance with pre-audited development and lifecycle processes. Compliance with the audited processes and product-specific security requirements is then verified in an evaluation at an evaluation facility.

The certification procedure used by the BSI is based on the GSMA-NESAS evaluation scheme, which was developed by the Groupe Speciale Mobile Association (GSMA).

Additional requirements may exist for specific procedural steps, audit or evaluation activities. These are published in the Application and Interpretations of the scheme (AIS) as separate documents by the certification body of the BSI. The AIS documents contain, among others, the procedural regulations for the audit or evaluation process. To delimit the AIS for certification pursuant to products in the common criteria (see [CC-Produkte] (CC products)), the AIS is organised in the number range “N#”, where # is the serial number of the AIS for certification according to NESAS.

The documents mentioned and further information is available on the BSI website in the topic area “Certification and recognition” under the heading “Product certification”. The documents will be used in the respective audit, evaluation and certification procedures based on their classification (e.g. as guidelines or mandatory).

In addition to the regulations, BSI certification must comply with the parameters of the “Act on the Federal Office for Information Security” [BSIG]. This results in a reservation of certification pursuant to BSIG (Act on the Federal Office for Information Security) Section 9, para 4 (2), for example, if overriding public interests, in particular concerns over the security policy of the Federal Republic of Germany, conflict with the granting of the certification. The assessment of a reservation of certification always takes place prior to the acceptance of an application for certification and finally before a certificate is issued.

3 Certification procedures

3.1 Bodies involved in a certification

Four bodies are involved in the entire certification process:

1. **The applicant:**
   An applicant may be a vendor, sponsor, distributor or an authority wishing to obtain certification for a network product.
2. **The audit team:**
   The audit team selected by the BSI to audit the development and lifecycle processes at the vendor's site. The auditors are bound to the BSI under a contract and are qualified to carry out NESAS audits. The regulations and processes implemented by the auditors ensure that confidentiality is maintained. A specific process-related confidentiality agreement (NDA) between the applicant and the auditor is not required due to the contract structure with the BSI.
3. **The evaluation facility:**
   The evaluation facility selected by the applicant and recognised for the respective scheme. The applicant commissions an evaluation facility that is qualified for the scheme to evaluate its product from the list of recognised evaluation facilities published by the BSI. The BSI has concluded contractual agreements or ancillary provisions under administrative law with the recognised evaluation facilities to carry out evaluations with a view to certification. The regulations and processes of the evaluation facility ensure that confidentiality is maintained at all times. The authorisations granted to evaluation facility employees relate to specific techniques, product groups and aspects of the evaluation.
4. **The BSI certification body:**
   The employees of the certification body support the audit process and the evaluation carried out by the evaluation facility. The certification body employees accept the audit report of the audit team and the evaluation report compiled by the evaluation facility and, if necessary, will request subsequent evaluations. The certification decision is taken on this basis and the applicant is informed accordingly.

3.2 Object of Conformity Assessment

The object of conformity assessment in a NESAS certification procedure consists of two entities, for which separate requirements apply:

- The development and lifecycle processes belonging to a specific network product or a class of network products and
- The technical properties of specific or all functional units belonging to a network product.

The conformity assessment for the development and lifecycle processes is performed in an audit, while the conformity assessment for the technical properties of the network product is performed in an evaluation.

Throughout the product certification program NESAS the results from both entities and their respective requirements are generally combined.

3.2.1 Auditing of development and lifecycle processes

The focus of the audit is on the development and lifecycle processes of a network product or a class of network products with identical processes. Vendors who produce and commercialize products must define and implement measures to ensure such processes are conformant with the relevant security requirements.

The lifecycle process consists of product development, first commercial introduction, minor and major product updates, to fix vulnerabilities and adapt the functional scope, and end of life. The initial development process at the start of the lifecycle consists of the planning, design, implementation, testing, release, manufacturing and delivery phases (cf. „Network Equipment Security Assurance Scheme – Overview“ [FS.13]).

During the audit, an audit team analyses processes of a vendor and assesses whether the measures for the implementation of the security requirements defined by the vendor are appropriate and effective. Subsequently, on-site audits assess, whether the measures for the processes are also implemented in practice. Additionally, during the audit the evaluation criteria and evidences for the application and implementation of audited processes in the certified product, are defined.

The audit of the development and lifecycle processes forms the basis for a subsequent evaluation of the network product at an evaluation facility. Several network products may rely on the same audit as a basis for an evaluation within the time limit of the audit (see Section 5.4.2.1) if the network products were developed through the processes audited therein.

3.2.2 Evaluation of the Network product

The Evaluation deals with the technical testing of the network product and the review, whether the development and lifecycle processes have been applied for the respective product.

The evaluation is performed by an evaluation facility and consists of standardized security tests. Details of the evaluation and the applicable methodology are regulated in the document [AIS N2]. Additionally, the evaluation facility also reviews whether the evidences provided by the vendor fulfil the evaluation requirements included in the audit report and thus conformity regarding the development and lifecycle processes is ensured for the respective network product.

The applicant must select an evaluation facility recognised by the BSI for the NESAS CCS-GI scheme and shall conclude a contract with the evaluation facility to evaluate the network product. See notes on the evaluation contract in Section 5.3.2.

The security requirements and test cases arise from standardised network functionalities in the mobile communications sector and are based on the SeCurity Assurance Specifications (SCAS) defined by the 3rd Generation Partnership Project (3GPP) (SA3). The network product under evaluation must be assigned to a product class determined by the 3GPP for which SCAS tests are defined and specified. Furthermore, compliance with the requirements listed in the document [AIS N2] for the evaluation in accordance with the SCAS must be assured. If the network product cannot be assigned to a product class listed in [AIS N2], no evaluation according to NESAS can be carried out.

An essential condition is that the security properties that are attested in the certificate upon conclusion of the procedure relate to the preservation of confidentiality, availability, integrity and authenticity of the assets to be protected.

A network product may be a combination of hardware and software components or a mere software component with defined interfaces. The product certification according to NESAS addresses products that can be commercialised. Evaluations do not accompany the development process.

A prerequisite for the evaluation of a network product is a valid audit (see Section 5.4.2.1), which includes all the development and lifecycle processes implemented to develop the network product. The network product shall also be clearly assigned to the audited development and lifecycle processes.

3.3 Certification process

3.3.1 Overview of the certification process

The certification of network products is divided into four phases: the preparation, audit, evaluation and certification phases.

In principle, all four main phases must be carried out. Depending on the respective phase, the applicant/vendor must submit different evidence and information to the audit team, evaluation facility or certification body. The certificate is awarded following the successful completion of the certification process.

3.3.2 Preparation phase

3.3.2.1 General

During the preparation phase, all steps from the initial preparation of the application to the submission of the application and the official start of the certification procedure take place.

The applicant may request assistance from the evaluation facilities to prepare the application documents, in particular the annexes to the certification application.

Typical process in detail:

Tasks of the vendor	*Resources*	*Tasks of the evaluation facility*	*Tasks of the certification body*
• Exchange information with the parties involved and provide information on the technical properties	• NESAS-Produkte (courtesy translation) • AIS N2 • NESAS-Evaluatoren (courtesy translation)	• Inform vendors about the procedures • Obtain information on the product and vendor	• Describe the process and, parameters for certification
• Check the availability, basic suitability and completeness of the evidence required	• -	Review the order from the vendor: • Examine the requirements for accepting the order (e.g. impartiality, personnel, resources, technical feasibility of the required SCAS tests)	• -
• Conclude an evaluation contract with the evaluation facility • The evaluation contract regulates the commissioning of the evaluation facility to conduct the evaluation • Participate in the creation of the schedule	• DIN EN ISO/IEC 17025	• Conclude an evaluation contract with the applicant	• -
• Participate in the creation of the test plan	• AIS N2	Create a test plan:	• -

Tasks of the vendor	*Resources*	*Tasks of the evaluation facility*	*Tasks of the certification body*
		• Prepare/coordinate evaluation activities with the applicant	
• Create the application with the necessary annexes	• AIS N1 • AIS N2	• Provide supporting documentation where necessary	• -
• Submit an application for certification • Complete the application for certification in accordance with the instructions in the application, stamp it with your company stamp, sign it personally and send it to the certification body with the required annexes (application in paper form or electronically as a scan to the BSI, annexes preferably electronically) • Note: the applicant should also provide a PGP key	• Application form • Public PGP key of the BSI certification body (available on the website)	• Provide a draft evaluation plan in coordination with the applicant	• Confirm receipt of the application • Review the application and annexes in terms of form and content • Issue a statement on the basic certifiability from a technical perspective, subject to the legal framework
• Carry out scheduling and create a proposal for a schedule	• AIS N2	• Implement the schedule • Create an evaluation plan[1] and submit it to the certification body	• Coordinate a provisional schedule with the applicant and evaluation facility
• Wait for the start of the evaluation process	• -	• Make preparations for the evaluation activities • Modify the contract if necessary	• Send a letter regarding the start of the procedure

Table 2 Tasks in the preparation phase

3.3.2.2 Documents required for the preparation phase

The following evidence, information and items are required by the applicant/vendor during the certification process:

- Application for certification (German or English) with annexes.

The certification application contains explanations and instructions to help you complete it.

[1] The evaluation plan contains information on the content of the evaluation, the SCAS tests to be used and requested by the applicant, the timetable, evaluators, a declaration of independence and impartiality and an attestation that the technical equipment used by the evaluation facility to carry out the SCAS tests is suitable for the purpose.

3.3.2.3 Application forms

The application forms request the information required to start and process the procedure. The form is available on the BSI website in the section "Certification and approval / Certification of products / Certification according to NESAS CCS-GI / Documents " (www.bsi.bund.de/dok/NESAS-Dokumente). The form contains explanations/notes to help you complete it.

This form relates solely to the NESAS certification of a network product.

If an application for product certification is not made by the vendor but by a sponsor or distributor of the product, the application must be accompanied by a written declaration from the vendor that the vendor ensures its participation in the procedure and the provision of the necessary product evidence.

If product parts or evidence that are relevant to the test are developed or provided by third parties, or if the applicant does not have the rights to all the test-relevant evidence or parts, the participation of the third parties involved must be ensured. The third party must therefore submit a declaration which confirms its participation in the procedure. The declaration letter must state: the name of the organisation that is declaring its participation, the obligations to cooperate and to provide information that have been specifically agreed, and a full description of the components of the evaluation object under certification to which the cooperation relates.

The application for certification must be signed by hand and bear a company stamp. It can then be scanned and sent via email to nesas@bsi.bund.de. For ease of handling, the application can also be accepted if it is signed, scanned and sent by email. No paper version is required in this case. The signature must be signed by hand, or the form must be electronically signed (eIDAS).

The annexes should be sent in electronic form. In addition to the application forms, a public PGP key for the above-mentioned NESAS mailbox is also available. As an alternative to electronic transmission, the application can also be sent in writing to the following address:

Federal Office for Information Security
Division S 26 - Certification body
Postfach 20 03 63
53133 Bonn

The auditors and the evaluation facility will make the documents available to the certification body separately in electronic form.

3.3.3 Audit phase

3.3.3.1 General

The audit phase examines the development and lifecycle processes. An audit will be carried out by a minimum of two auditors who form the audit team. One auditor acts as the team leader who is the main contact person for the vendor and the certification body.

If the network product was created based on development and lifecycle processes for which a valid audit already exists, evidence of this audit alone must be submitted in the audit phase.

The audit of the development and lifecycle processes and the resulting audit report form the basis for all further evaluation activities in the evaluation facility and the eventual certification. The audit must therefore be prepared with due diligence by the vendor, and the audit team must be supported throughout the audit process. The audit process is based on the GSMA documents referenced in the document [AIS N1], any supplementary documentation in [AIS N1] and ISO/IEC 27007. The audit process consists of an off-site review of the process documentation and a subsequent on-site audit at a site explicitly designated by the applicant where the appropriate development and lifecycle processes are implemented. When selecting the audit site, compliance must be assured with the conditions specified in [AIS N1] for the conduct of the on-site audit. A remote audit may be carried out in justified and exceptional cases as an alternative to repeat audits after consultation and approval by the certification body, provided that a sufficient level of auditing is ensured in the specific case. The certification body may determine the necessary specific requirements in each individual case.

The processing of the procedure will be postponed if the on-site audit cannot be carried out at the time the application is submitted due to the framework conditions specified in the document [AIS N1] and the above conditions for conducting a remote audit are not fulfilled. The applicant/vendor may withdraw the application and resubmit it in a correct form or at a later date.

3.3.3.2 Documents required for the audit process

The following evidence, information and items are required by the applicant/vendor during the certification process:

- A list of the product development sites. Where applicable, the example site to be audited must be specified.
- The documentation of processes and measures at the vendor's site which are designed to help ensure compliance with the security requirements in the document „NESAS Development and Lifecycle Security Requirements" [FS.16].

3.3.3.3 The vendor submits the documentation of the processes and measures directly to the audit team leader at the latest at the start of the audit phase. Documents are exchanged via the data exchange platform specified by the certification body (currently bscw.bund.de). Data that is provided on the data exchange platform shall be individually end-to-end encrypted for each recipient using OpenPGP. The certification body shall be included as a recipient for each data exchange by using the valid process key. Subsequent requests for documents to answer any questions are also sent to the auditors in this way. Assignment of an audit to an audit team

The selection and assignment of the auditors who will conduct the audit at the vendor's site is carried out by the certification body according to the procedure described in the document [AIS N1]. In justified cases, the vendor may lodge an objection against an assigned auditor within five working days of the notification of the auditor. The certification body will examine the objection, agree on how to proceed and then announce the decision to the vendor and auditor. If the objection is upheld, a new auditor will be appointed.

Typical audit procedure:

Tasks of the vendor	*Resources*	*Tasks of the audit team*	*Tasks of the certification body*
• -	• -	• -	• Selection of the audit team
• Objection against the auditor if applicable	• -	• Confirm the audit • Reject the audit if applicable	• Examine the objection and select a new auditor if applicable
• -	• -	• -	• Notify the vendor and auditors of the audit team

Table 3 Tasks upon the assignment of an audit

3.3.3.4 Audit process

The evaluation and certification concept is based on close cooperation between the parties involved, the applicant, the auditors assigned to the audit and the certifier in the certification body. Communication is generally in text form (e.g. documents, email, formal letter) or in the ongoing process by telephone or via web-based conference systems (e.g. telephone conferences regarding the status, clarification of minor technical issues that are not critical in terms of confidentiality) or in joint meetings. Emails that are exchanged between the vendor, audit team and the certification body must always be encrypted using OpenPGP. The public process keys required for this purpose must be exchanged in advance of the procedure.

A kick-off meeting is held at the start of the audit phase to enable the audit team and vendor to meet and to discuss the initial coordination of the subsequent procedure. The audit team is responsible for planning and conducting this meeting. The audit team also informs the certification body of the date of the kick-off meeting at least seven days in advance to enable the certification body to also attend the meeting if necessary.

All the parties must adhere to the schedule agreed at the start of the process. The audit team leader is responsible for ensuring the timely conduct of the audit (within three months from the date of the audit kick-off meeting). If it is apparent that the process will be delayed or is already delayed, the other parties must be notified to then agree on an updated process schedule. The updated schedule must be approved by the certification body.

The vendor's evidence and supporting documentation will be reviewed directly with the audit team, generally via the audit team leader. The applicant/vendor should be aware that the process documentation should be sufficiently prepared to ensure that the audit can be conducted within the respective schedule. The team leader will transmit the copies of the documents (in digital form) to the certification body.

During the review of the documents, the vendor shall clarify and correct any supplementary documents, errors or inconsistencies that are identified in the vendor's information and evidence. The vendor must therefore provide resources and contact persons who have the relevant information and appropriate authority to make decisions. The vendor must ensure that all the necessary documents, information and evidence are available and shall also ensure that on-site meetings can be arranged.

The certifier may subject the vendor's documents to a random, internal inspection and may attend the meetings between the applicant/vendor and the auditor to gain a better understanding of the auditor’s evaluation statement and, if necessary, highlight any aspects that require clarification. The scope of the random inspection shall be at the discretion of the certification body. The certifier may also participate in on-site audits with the audit team and to gain an insight into the implementation of the processes described.

The framework conditions shall apply for the procedure in accordance with Chapter 5.3 “Verfahrensbeschreibung zur Zertifizierung von Produkten, Prozessen und Dienstleistungen” (Procedure description for the certification of products, processes and services) [VB-Produkte.PD], in particular for the rejection of an application or a negative decision. This could, for example, relate to a breach of impartiality or the applicant’s failure to fulfil their obligations, e.g. in the event of missing evidence or significant changes to the application or the object of certification.

An audit of the development and lifecycle processes at a vendor’s site may only be completed with a positive result if the measures and processes for compliance with the security measures in the document „NESAS Development and Lifecycle Security Requirements“ [FS.16] are considered by the auditor and the certification body to be complete, correct and technically sufficient.

The audit process will produce a negative result if it determines a non-compliance with the security requirements, even after any potential improvements have been implemented. The certification process would therefore be terminated with a negative notice and with no certificate being granted.

If, during an audit, it was ascertained that the vendor's measures and processes failed to comply with all the requirements defined in the document „NESAS Development and Lifecycle Security Requirements“ [FS.16], the vendor and the auditor may, in consultation with the certification body, opt to carry out a re-audit once the vendor has implemented the improvements required. This is only possible if the full audit and the additional audit do not exceed the maximum total duration of three months.

Once the vendor has been subjected to the audit, the audit report with all the attachments and the audit summary will be created in this phase for subsequent publication in the event of a successful certification.

Typical audit procedure:

Tasks of the vendor	***Resources***	***Tasks of the audit team***	***Tasks of the certification body***
• -	• -	• The lead auditor contacts the vendor	• -
• Participation in an audit kick-off meeting	• -	• Planning, invitation and implementation of the audit kick-off meeting	• For acknowledgement • Optional: participation in the kick-off meeting
• Coordination of the audit process with the audit team/lead auditor	• AIS N1	• Planning/coordination of the audit process with the vendor	• -
• -	• -	• Notification of the audit process to the certification body: • Scheduled duration of the audit • Scheduled date of the completion of the first document audit • Scheduled date of the completion of the document audit • Scheduled duration of the on-site audit • Proposed site of the audit • Scheduled date of submission of the audit report	• For acknowledgement
• Submission of the necessary documents to the audit team and the certification body	• AIS N1, data exchange platform provided by the certification body	• Receipt of the relevant documents provided	• Submission of a folder with the appropriate authorisations and receipt of the relevant documents
• -	• AIS N1	• Document audit round 1	• -
• Quality assurance and comments on the result of round 1 of the document audit	• -	• The results of the first document audit are sent to the vendor for quality assurance and comments	• -

Tasks of the vendor	*Resources*	*Tasks of the audit team*	*Tasks of the certification body*
• The comments on the results are sent to the auditor for a decision on the comments and their incorporation. The certification body receives the comments for acknowledgement.	• -	• Decision on acceptance of the comments and their potential incorporation	• Acknowledgement of the comments and necessary follow-up submissions by the vendor.
• Discussion on the results from round 1 of the document audit	• -	• Meeting to discuss the results from round 1 of the document audit	• -
• Fulfilment of the subsequent requirements arising from the discussion on the results	• Data exchange platform provided by the certification body	• -	• -
• -	• AIS N1	• Document audit round 2	• -
• Quality assurance and comments on the result of round 2 of the document audit	• -	• The results of the second document audit are sent to the vendor for quality assurance and comments	• -
• The comments on the results are sent to the auditor for a decision on the comments and their incorporation. The certification body receives the comments for acknowledgement.	• -	• Decision on acceptance of the comments and their potential incorporation and definition of priorities for the on-site audit	• Acknowledgement of the comments
• Coordination of the audit process with the audit team/lead auditor	• -	• Update on the date of the on-site audit • Notification of further instructions for subsequent steps	• -
• -	• -	• Notification to the certification body of the precise date for the on-site audit	• For acknowledgement
• Provision of the necessary resources and data for the audit (e.g. personnel, time, workspace for auditors)	• AIS N1	• On-site audit	• Optional: • Optional participation in the on-site audit
• -	• AIS N1	• Creation of the audit report and all the relevant annexes	• -
• Quality assurance and comments on the audit report	• -	• Submission of the audit report to the vendor for quality assurance and comments	• -

Tasks of the vendor	*Resources*	*Tasks of the audit team*	*Tasks of the certification body*
• -	• -	• Submission of the audit report with comments to the certification body for acknowledgement	• Acknowledgement of the comments
• -	• -	• Incorporation of the comments at the vendor's discretion, taking into account the referenced documents	• -
• -	• -	• Submission of the audit report to the certification body • Incorporation of the comments from the certification body where applicable	• Comments on the audit report • Acceptance of the audit report and notification to the audit team
• -	• AIS N1	• Finalisation of the audit report • Preparation of the audit summary	• -
• Acknowledgement and confirmation of receipt	• -	• The audit report, annexes and audit summary are sent to the vendor and the certification body	• Acknowledgement and confirmation of receipt
• -	• -	• Costs incurred by the auditor are sent to the certification body	• Review of the plausibility of costs

Table 4 Tasks in the audit process

3.3.4 Evaluation phase

3.3.4.1 General

In the evaluation phase, a review is carried out regarding compliance with the audited development processes during the development of the network product. This is based on the audit report and the appropriate evidence specified in the audit and required for the evaluation, which the vendor must provide to the evaluation facility. Standardised security tests (SeCurity Assurance Specifications (SCAS tests)) are also carried out on the actual network product. The SCAS tests to be selected for evaluation depend on the functionality provided by the network product and must be specified by the applicant in the application. An assignment is made using the document [AIS N2]. The test results from the SCAS tests are recorded and summarised by the evaluation facility in an evaluation test report (ETR).

The evaluation phase can only be initiated with a valid audit (see 5.4.2.1) and the respective audit report. The documents required for the evaluation are listed in Chapter 3.3.4.2.

3.3.4.2 Documents required for the evaluation phase

The following evidence, information and items are required by the applicant/vendor during the certification process:

- An existing audit report with all the associated annexes if a product evaluation based on a previous audit is required.
- Evidence of conformity from the vendor is required in the audit report to prove that the product under evaluation was developed in accordance with the audited development and life cycle processes. This enables the vendor to confirm to the evaluation facility that the audited development and lifecycle processes were observed during the development of the network product.
- Network product, manuals and product specifications and the required peripherals/test equipment and the associated description must be made available to the evaluation facility to enable the facility/ evaluators to carry out a test in the evaluation facility’s own test environment.
- Where applicable: instructions on how to bring the network product into an operational state.
- All other evidence and information mentioned in [AIS N2], chapter 2.4.1.

The audit report and the evidences of conformity required in the audit report shall be made available to the certification body by the vendor (if not available through a previous audit). The certification body will then send the documents to the evaluation facility.

3.3.4.3 Evaluation process

The evaluation and certification concept is based on close cooperation between the parties involved, the applicant, the evaluators assigned to the evaluation, the leader of the evaluation project in the evaluation facility and the certifier in the certification body. Communication is generally in text form (e.g. documents, email, formal letter) or in the ongoing process by telephone or via web-based conference systems (e.g. telephone conferences regarding the status, clarification of minor technical issues that are not critical in terms of confidentiality) or in joint meetings.

All participants must adhere to the schedule agreed at the start of the process. The evaluation facility is responsible for ensuring that the evaluation is carried out on schedule. If it is apparent that delays will occur, the other parties must be notified to then agree on an updated schedule.

A kick-off meeting is held at the start of the evaluation which, if possible, should take place in person at the evaluation facility. Alternatively, a video conference may be held in accordance with the provisions of the certification body. The network product, the SCAS documents used and the intended scope by the evaluation facility will be presented during the meeting. This enables questions and comments from the certification body or applicant/vendor.

If individual tests/test cases cannot be carried out at an evaluation facility at a reasonable cost, individual tests may be conducted at the vendor’s site. The corresponding activities must be coordinated with the certification body at least four weeks before they are carried out by the evaluation facility. Here, explanations must be provided on how the independence of the evaluation will be guaranteed. Tests at the vendor’s site must be carried out by an evaluator from the evaluation facility. Remote evaluation activities are not permitted.

Any requirements for supplementary documents, errors or inconsistencies in the vendor's evidence identified during the evaluation must be clarified and rectified by the applicant. The applicant must provide the resources and processes for this purpose. This generally requires the various evaluation steps to be repeated. Any delays arising from this must be reported to the BSI in a timely manner.

If improvements and subsequent tests are carried out, the ETR must clearly state which tests failed with which version of the network product and what tests were repeated using which version(s).

It is crucial for the certification process that the evaluation report contains the following information:

- The review of evidence of the information provided by the vendor specified in the audit report, and
- The results of the SCAS tests.

The certification body can only achieve a meaningful certification result by combining the results stated (evidence review and results of the SCAS tests).

The certifier may subject the vendor's documents to a random, internal inspection and may attend the meetings between the applicant/vendor and the evaluation facility to gain a better understanding of the evaluator's test statement and, if necessary, highlight any aspects that require clarification. The scope of the random inspection shall be at the discretion of the certification body. The certifier may also participate in evaluations or parts thereof to gain an insight into the implementation of the evaluation activities to ensure a uniform approach, methodology and comparable assessments and to highlight any potential non-compliance with the certification requirements at an early stage. The evaluation facility also has the opportunity to clarify any issues regarding the evaluation with the certification body.

Updates to the test requirements (e.g. new SCAS tests) that are published during the ongoing process need not be implemented. Updated test requirements may be implemented at the explicit request of the applicant and with the consent of all parties involved. The test requirements actually used must be stated in the evaluation report.

A certification procedure may be cancelled by the certification body after hearing the parties, or terminated with a negative result in the event of missing or insufficient evidence from the applicant or the evaluation facility, or of a breach of impartiality.

The framework conditions shall apply for the procedure in accordance with Chapter 5.3 "Verfahrensbeschreibung zur Zertifizierung von Produkten, Prozessen und Dienstleistungen" (Procedure description for the certification of products, processes and services) [VB-Produkte.PD], in particular for the rejection of an application or a negative decision. This could be due, for example to a breach of impartiality, the applicant's failure to fulfil their obligations, e.g. in the case of missing product certificates or significant changes to the application or the object of certification.

Typical evaluation procedure:

Tasks of the vendor	*Resources*	*Tasks of the evaluation facility*	*Tasks of the certification body*
Provision/handover of: • Network product including peripherals • Operating instructions • Required peripherals/test equipment, where applicable, if possible to the evaluation facility	• AIS N2	Receipt • Network product including peripherals • Operating instructions • Required peripherals/test equipment, where applicable • Other components	• -

Tasks of the vendor	*Resources*	*Tasks of the evaluation facility*	*Tasks of the certification body*
Provision/handover of: • Audit report • Evidence of the security requirements • Justification for the missing security requirements, where applicable, to the certification body	• AIS N2	• Receipt of the documents by the vendor	• Receipt of the documents from the vendor for informational purposes
• Optional: participation in the creation of the test plan	• AIS N2	Create/adjust the test plan • Prepare/coordinate evaluation activities with the applicant	• -
• Participation in the kick-off meeting to clarify questions about the evaluation	• -	• Participation in the kick-off meeting to clarify questions about the evaluation	• Participation in the kick-off meeting to clarify questions about the evaluation
• -	• -	• Wait for approval from the certification body	• Approval of the evaluation
• Free provision of capacities and resources for evaluation activities by the evaluation facility • Enable free access to the sites relevant for the test and vendor environments for evaluators and certifiers	• AIS N2	• Carry out the evaluation • Test activities for the required evidence of conformity in the annexes of the audit report • Carry out test activities on the aspects required in the SCAS tests • Create test documentation • Make the full test results and evaluation report available to the certification body • Process the comments and supplementary requirements • Clarify open questions with the applicant/vendor, where applicable	• Supervise the evaluation (test supervision) • Optional: participation in the evaluations • Assess and comment on the evaluation report

Tasks of the vendor	*Resources*	*Tasks of the evaluation facility*	*Tasks of the certification body*
• Wait for acceptance of the ETR by the certification body: if the result of the evaluation is positive, the technical requirements for the award of the certificate are provided	• -	• Create final ETR with all the test results	• Review and, if necessary, comment on the ETR • Carry out technical acceptance of the evaluation with respect to the certification decision • Inform the applicant and evaluation facility regarding acceptance

Table 5 Tasks in the evaluation phase

3.3.5 Certification phase

Tasks of the vendor	*Resources*	*Tasks of the evaluation facility*	*Tasks of the certification body*
• Participate in the preparation of the certification report, if applicable, and response to the hearing: • If necessary, comment on the draft certification report • Response to a formal hearing, if applicable	• -	• Comment on the certification report, if applicable	• Make the certification decision and complete the procedures • In the event of a positive certification decision: • Create certificate, certification report, certification notice • Formal hearing of the applicant on ancillary provisions (in particular regarding conditions and requirements) in the notice (deadline 14 days) • Issuance of the certificate • In the event of a negative certification notice: • Negative notice after a formal hearing • Postal delivery of the notice, certificate and certification report to the applicant (objection deadline 1 month or declaration of waiver of objection) • If required: • Provide certification button

Tasks of the vendor	*Resources*	*Tasks of the evaluation facility*	*Tasks of the certification body*
• Send an acknowledgement of receipt and, if applicable, a waiver of objection: • Send confirmation of receipt to the BSI • Issue a waiver of objection and send it to the BSI, or send a written objection to the certification decision to the certification body within an objection period of 1 month • (With a waiver of objection, the publication period will be shorter)	• -	• -	• Processing of the objection, if applicable • The notice will be final upon expiry of the waiver deadline • Publication of the result of the certification and the certification report including the audit summary
• Reimbursement of costs: reimburse the BSI for the costs of the procedure (fees and expenses) (see Chapter 5.5)	• BMIBGebV (Special Fee Ordinance of the Federal Ministry of the Interior, Building and Community)	• -	• Send a notification of costs to the applicant
• Archiving: archive all evidence relevant to the evaluation and the product under evaluation for the period of validity of the certificate plus three years	• -	• Archive all the evidence relevant to the evaluation	• Archive all the evidence relevant to the certification
• Compliance with the ancillary provisions in the notice and the regulations of the code of symbols	• Code of symbols	• -	• If applicable: process subsequent deliveries arising from ancillary provisions

Table 6 Tasks in the certification phase

3.3.6 Final documents

The certification report created by the certification body after a positive conclusion of the evaluation contains, in addition to a security-related description of the product, selected information on the result of the audit and the evaluation as well as instructions and requirements for the use of the certified network product.

The relevant document also states that the audit and the evaluation were conducted based on the recognised procedures and criteria, and that the security requirements defined in the SCAS tests have been satisfied in terms of functionality and the scope of evaluation. The report contains information and requirements for the user that must be observed when using the network product.

The certification notice represents the official approval of the certification body in the legal sense and contains in particular, as ancillary provisions, the conditions and requirements that must be observed by the applicant.

The certificate and the certification report may be created in German or English. This is generally the same language as the language selected for the application.

4 Maintenance of the certification

4.1 Minor updates

A certificate is issued for a product version that has been uniquely identified and evaluated. Minor updates to a product are the exception and may be subject to certification. A minor update to a product must be clearly identified in the product version. All the versions of the product relating to the certificate are always listed on the BSI website.

If the applicant publishes changes to the certified network product during the certification period which are only minor updates, these can also be covered by the existing security certificate (i.e. the product including the minor update is still certified). Minor updates do not change the validity period of the certificate.

The following definition applies to the NESAS certification scheme: minor updates are adjustments to security functions or the nature of the product that serve to maintain or restore the certified security performance (as the sum of the security statements of the product evaluation) or which are irrelevant for the security performance.

These adjustments are either of a functional nature (to achieve the intended, functional process of the network product; elimination of functional errors) or security corrections (to avoid an unintended, generally improper use of the product; elimination of security vulnerabilities). An adjustment that preserves the function or security correction that requires a new functionality (e.g. a new filter layer, an additional firewall, additional virtualisation) does not represent only a minor update, as it is no longer possible to make an unambiguous security statement for the security certificate.

A minor update must be requested from the certification body. The audit of the development and life cycle processes must be valid at the time of submission to the certification body.

The following evidence and information is required from the applicant/vendor:

- Certification application/application form with attachments,
- Impact Analysis Report (IAR),
- Evidence of conformity of the manufacturer required in the audit report as evidence of compliance with the audited development and life cycle processes during the development of the minor update and an
- Assessment of the change with a clear vote of the expert body (evaluation facility that has evaluated the network product).

The applicant/vendor must obtain a written assessment based on the IAR from the expert body (evaluation facility that evaluated the network product) with a clear vote for the certification body that the changes described in the IAR fall under the definition of minor updates and that the audited processes were used. The applicant/vendor must provide additional information and evidence if required or requested by the expert body.

The minor update is covered temporarily by the certification from the time at which the applicant has sent the listed documents and information to the certification body.

The certification body reserves the right to object to the vote of the expert body within 30 calendar days of receipt of the application.

If the certification body concludes on the basis of the IAR and the vote of the expert body that the update is a minor update, the certification report will be supplemented by an annex with the product version specified in the IAR. A minor update does not change the formal validity period of the certificate.

If the certification body concludes on the basis of the IAR and the vote of the expert body that the update is not a minor update, it gives the applicant the opportunity to resolve the concerns of the certification body within 5 working days. If this is not successful, the security certificate is limited to the product in its last certified state together with any valid minor updates. This period may be extended once for objective reasons.

The applicant/vendor will be informed of the certification body's final decision by means of a notification. The certification notice represents the official vote of the certification body in the legal sense and contains, in particular, conditions and requirements to be complied with by the applicant as ancillary provisions. The applicant must state the scope of validity of the certificate, including any restrictions, in all the information on the security certificate. This will also be noted on the list of certified products.

If the applicant in the certification program NESAS provides minor updates for assessment within the founding security certificate, additional procedural costs for assessment may incur. The BSI will determine the amount of the costs in a separate notification of costs.

4.2 Inclusion of different execution environments in the certificate

The following definition of terms applies to the NESAS certification scheme: “Execution environments” are computer systems and their configuration and parameterisation that serve to execute the network product and provide the environmental conditions required to operate the network product.

If the applicant adds further execution environments to their list of potential execution environments for the network product during the validity period of the certificate, such environments may also be covered by the existing security certificate (i.e. the network product is operated in these execution environments in accordance with the terms of the certificate).

An application must be made to the certification body for the inclusion of a different execution environment. The audit of the development and life cycle processes shall be valid at the time of application.

The following evidence and information is required from the applicant/vendor:

- Certification application/application form with attachments,
- Impact Analysis Report (IAR) and an
- Assessment of the change with a clear vote of the expert body (evaluation facility that has evaluated the network product).

The applicant/vendor must obtain a written assessment from the expert body (evaluation facility that evaluated the network product) on the basis of the IAR with a clear vote for the certification body that the security statements of the certificate for the product are also valid in the supplemented execution environment. The applicant/vendor must provide additional information and evidence if required or requested by the expert body.

If the certification body concludes on the basis of the IAR and the vote of the expert body that the security statements of the certificate for the product are also valid in the supplemented execution environment, the certification report with the execution environment specified in the IAR is supplemented by an annex. The change to the execution environment does not change the formal validity period of the certificate.

If the certification body concludes on the basis of the IAR and the vote of the expert body that the security statements of the certificate are not valid for the product in the supplemented execution environment, it gives the applicant the opportunity to resolve the concerns of the certification body within 5 working days.

The applicant/vendor will be informed of the certification body's final decision by means of a notification. The certification notice represents the official vote of the certification body in the legal sense and contains, in particular, conditions and requirements to be complied with by the applicant as ancillary provisions. The applicant must state the scope of validity of the certificate, including any restrictions, in all the information on the security certificate. This will also be noted on the list of certified products.The applicant may incur extra procedural costs for the additional evaluation if the applicant issues execution environments for evaluation under the underlying security certificate in the NESAS certification scheme. The BSI will determine the amount of the costs in a separate notification of costs.

4.3 Recertification

For a changed product version that does not fall under the regulation of a minor update to be declared as recertified, a renewal of the certificate taking into account the changes is required.

The basic process of recertification corresponds to an initial certification procedure. The audit of development and lifecycle processes must be carried out again if it is no longer valid.

Following a positive conclusion, the technical results will be documented by the certification body in an updated certification report and a new certificate will be issued.

The formal validity of a certificate and the security assessment of the product are renewed as part of a recertification. Following the recertification, the applicant may retain the certificate number that was originally assigned and add the additional alphanumeric elements to the number assigned.

5 Special framework conditions

5.1 Basis for the certification

The security certification service for IT products by the BSI according to NESAS is provided as an application procedure. Certification may be granted if the respective test regulations have been fulfilled and overriding public interests, in particular security policy concerns of the Federal Republic of Germany, do not conflict with the issuance of the certificate (BSIG Section 9, para 4 (2)). The inspection pursuant to BSIG Section 9, para 4 (2) will take place when the application is accepted, but subject to a final decision at the time of signing a certification notice and the certificate.

Certification procedures for IT products for the BSI must be carried out using test specifications that have been recognised as suitable by the BSI. Test specifications for NESAS arise from the document „NESAS Development and Lifecycle Security Requirements“ [FS.16] and the SCAS tests provided by 3GPP. If no SCAS test recognised as suitable by the BSI is available for a product type (see [AIS N2]), the BSI will decide on the basic certifiability in individual cases prior to starting the procedure.

The potential SCAS tests are selected by the BSI on the basis of risk management for the operational environment and the application of a product that requires a security statement, or they arise from requirements pursuant to national IT security projects or national or EU laws or regulations.

The procedure may be prioritised within the certification body if a specific public interest has been identified, or for products that are used in national IT infrastructures.

5.2 Confidentiality and document exchange

The applicant's company policy and practice regarding the confidential handling or disclosure of the documentation for the evaluated product to third parties who are not subject to monitoring by the certification body will influence the assessment of the exploitability of potential vulnerabilities within the framework of the evaluation, for example, if information about the product issued by the vendor is considered available to an attacker and may therefore make the product more vulnerable.

In certain cases, the source code of products or other highly sensitive information which is classified based on a documented security policy of the vendor and must not leave the development environment, may also be assessed and analysed by the auditor, evaluator and certifier at the applicant's site instead of at the evaluation facility, e.g. in the development environment. To do this, the applicant must make a credible case to the certification body that disclosure of documents conflicts with the applicant's essential interests. This procedure generally incurs a greater expenditure of time and increased costs for all parties, which must be borne by the applicant.

The exchange of documents between the applicant, evaluation facility and the certification body generally takes place electronically via encrypted email. OpenPGP is used for this pursuant to the recommendations in TR-02102-1. The key exchange for communication via OpenPGP must take place before the kick-off meetings for the evaluation and audit. To submit the application, applicants are required to use the public key available on the website for the email address nesas@bsi.bund.de, under the heading “Certification and approval / Certification of products / Certification according to NESAS CCS GI” (www.bsi.bund.de/nesas).

Electronic documents for a certification procedure must be sent to the email address: nesas@bsi.bund.de. The delivery to personal BSI email addresses of certifiers generally also includes a copy for information purposes.

The regulations in the higher-level document “Verfahrensbeschreibung zur Zertifizierung von Produkten, Prozessen und Dienstleistungen” (Procedure description for the certification of products, processes and services) [VB-Produkte.PD] apply to documents that are sent to the BSI in paper form or delivered directly to the door of the BSI by courier, and for any DVDs/CDs provided.

If the documents required to audit the development and lifecycle processes are sent electronically, such documents must be provided in encrypted zip archives on the server designated by the certification body. The password of the zip archive should be sent separately via email to nesas@bsi.bund.de.

5.3 Framework conditions for the procedure

5.3.1 Evaluation plan

The evaluation plan contains information on the organisational and content-related implementation of the evaluation, the applicable criteria and interpretations, the schedule and a declaration of independence and impartiality. The evaluation facility must also confirm to the certification body that the technical equipment is sufficient to carry out the SCAS tests required for the respective network product.

The certification body may compile an evaluation plan and may also reject such plan if it is incomplete, if no agreement can be reached on the schedule or if the professional competence of the evaluation facility or the evaluators is not sufficiently proven.

The participants shall notify the other participants of any deviations from the agreed schedule and shall revise the schedule. Regular telephone conferences to discuss the status of the proceedings are recommended.

5.3.2 Evaluation contract

As the evaluation facility must comply with the requirements of the certification scheme through the recognition agreement with the BSI, the evaluation contract must contain no regulations that could obstruct the proper evaluation and test monitoring, in particular no regulations that could obstruct the transfer of information regarding findings from the evaluation to the certification body. The contract must take into account that new or additional issues (e.g. additional tests, corrections and additions to the evaluation report as deemed necessary by the certification body, workshops, etc.) may arise in the ongoing process that would affect the evaluation effort.

5.3.3 Validity of standards and interpretations

The relevant versions of the test criteria and Application and Interpretations (AIS) are defined upon the official acceptance of an application for certification. A transition to newer versions, recognised by the certification body and listed in the document "Verzeichnisse" (Indexes) [Verzeichnisse], is permitted upon the explicit request of the applicant and with the consent of all parties involved during the ongoing process.

The use of the schema documents is mandatory for NESAS in the version published by the BSI. If a new version of the criteria is available, once it has been approved by the BSI a transitional period will be granted for new procedures based on the extent of the changes.

Documents in the GSMA, SCAS tests or other NESAS-related documents for which the certification body is not responsible apply in the version existing on the date of the application. Changes to the versions during the ongoing process are possible at the explicit request of the applicant and with the consent of all parties involved during the ongoing process.

5.3.4 Reuse of test results

Test results from the evaluation of a network product cannot be reused for another certification procedure for a network product from the same applicant.

5.3.5 Certification number

The certification number is the process identifier at the BSI, and is used in all the correspondence to identify documents and the certification report.

Product certificate: **BSI-DSZ-NESAS-nnnn-yyyy**

(DSZ = German IT security certificate, NESAS = specification of the set of criteria, nnnn = sequential application number, yyyy = year of issue of the certificate (will only be added when the certificate is issued)).

Recertification: **BSI-DSZ-NESAS-nnnn-Vx-yyyy**

Addition of a version number to the respective certification number: (nnnn = previous sequential application number, Vx = version identifier for the recertification, yyyy = year of recertification).

5.4 Framework conditions for maintaining a NESAS certificate

5.4.1 Validity and, parameters

A product certificate relates to the specific version of the product and minor updates to the product whereby all the conditions regarding the generation, configuration and use of the product described in the certification report are observed.

A certificate confirms the reliability and security of the product in accordance with the underlying audit and evaluation specifications at the date of issue.

Requirements for the user arise from the certification report. Conditions and other ancillary provisions for the certificate holder arise from the certification notice. Users of a certified product must take account of the results, parameters and requirements expressed with the certificate in their risk management process.

5.4.2 Time limit

Pursuant to the legal basis, the certification body must set a time limit for the formal validity of a certificate for the respective certification scheme. However, the content and technical certificate statement on reliability and security refers to the date of issue, as it is difficult to predict resistance to attack in the future and may vary greatly in individual cases. Minor updates do not extend the validity period of the certificate. Minor updates do not change the validity period of the certificate.

5.4.2.1 Validity of a NESAS audit

A NESAS audit is valid for two years from the date of the finalised audit report for the version of the security requirements specified in the document „NESAS Development and Lifecycle Security Requirements“ [FS.16]. An audit shall not be older than two years at the start of an evaluation. If:

- The vendor made significant changes to the processes examined during the audit, or
- A security breach is detected at the vendor that has an impact on audited processes, a new audit shall be carried out for evaluations based on such changes.

5.4.2.2 Validity of a NESAS certificate

The content and technical certificate statement on the reliability and security relates to the date on which the certificate was issued. Due to advances in technology, the formal validity of an IT security certificate is generally limited to two years. Deviating cases may be stipulated for certain product classes under specific legal framework conditions.

5.5 Costs

The BSI will invoice the applicant for fees and expenses based on the Special Fee Ordinance of the Federal Ministry of the Interior, Building and Community - BMI [BMIBGebV]. The invoice will be based on expenditure. The preliminary discussions with the BSI prior to submitting an application are free of charge.

The expenses also include the costs incurred in the audit. The remuneration of the auditors is based on expenditure and travel expenses are paid in accordance with the Bundesreisekostengesetz (Federal Travel Expenses Act).

Payment of the evaluation costs incurred by the evaluation facility will be contractually agreed between the applicant and the evaluation facility. The cost of the evaluation will be based on the complexity of the product and the product type and cannot be quantified as a flat rate. On request, the evaluation facilities may provide cost estimates or prepare corresponding offers.

A notification of costs will be issued by the BSI for billing. Applicants may request the information required for billing by the BSI from the following email address: forderungsmanagement-z21@bsi.bund.de

Specific regulations apply if an application is submitted by an authority which will be discussed on a case-by-case basis.

5.6 Contact with the certification body

The first point of contact for ongoing certification procedures is the assigned certifier. The contact details are available in the respective letter sent when the procedure is launched (ID assignment).

Higher-level questions about the certification or the test criteria may be addressed to:

- Email: nesas@bsi.bund.de
- Telephone: +49 (0) 800 274 1000, or to the
- Organisational unit: referat-s26@bsi.bund.de.

If the certifier is unavailable, applicants can contact the main telephone number of the BSI (+49 (0) 800 274 1000) and then request the certification Division S 26 or the office of the Directorate-General S .

Documents for certification must be sent to the main email address: nesas@bsi.bund.de. A PGP key is available on the BSI website in the “Certification and approval / Certification of products / Certification according to NESAS CCS-GI”.

6 Publication of the certification

6.1 Publication by the BSI

Information on certified network products is issued by the BSI in the following publication, which is regularly updated:

- BSI Forum (organ of the BSI in the magazine KES): this publication summarises the content of a certificate that was recently issued since the last edition of the magazine.
- The “Certification and recognition” section on the BSI website: certificates are listed here in the form of summary lists, and the certification report and any supplements are available for download.

The applicant will not be mentioned in these publications if the applicant revokes in writing their consent to the publication of the certification result issued in the application to the BSI, or if consent was not granted in the application.

7 References and glossary [Verzeichnisse] (Indexes)

The document “Verzeichnisse” [Verzeichnisse] (Indexes) is a reference work for interested persons and those involved in certification and licensing procedures and provides an overview of all the necessary requirements, sources and resources with a glossary and list of abbreviations.

The lists with respect to requirements, sources and resources shall be understood as a master list and include information about current source references for all the requirements and documents.