



Network Equipment Security Assurance Scheme – Framework

Version 3.0

20 February 2025

Security Classification: Non-Confidential

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those permitted under the security classification without the prior written approval of the Association.

Copyright Notice

Copyright © 2025 GSM Association

Disclaimer

The GSMA makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Compliance Notice

The information contained herein is in full compliance with the GSMA Antitrust Compliance Policy.

This Permanent Reference Document is classified by GSMA as an Industry Specification, as such it has been developed and is maintained by GSMA in accordance with the provisions set out GSMA AA.35 - Procedures for Industry Specifications.



Contents

Licensing Statement	3
Foreword.....	3
Modal verbs terminology	3
Introduction	4
1 Scope	5
2 References	6
2.1 Normative references.....	6
2.2 Informative references	6
3 Definition of terms, symbols and abbreviations.....	6
3.1 Terms	6
3.2 Symbols	8
3.3 Abbreviations.....	9
4 Introduction to Security Assurance in the Mobile Industry	9
5 NESAS Methodology and Requirements Overview	10
5.1 General.....	10
5.2 Lifecycle Roles and NESAS Scope	11
5.3 Owner of and Responsibility for NESAS	11
5.4 NESAS High Level Overview	12
5.5 Authorisation of NESAS Auditing Organisations	13
5.6 Authorisation of NESAS Security Test Laboratories	14
5.7 Assessment of Vendor Development and Product Lifecycle Processes	15
5.8 Network Product Evaluation and Evidence Evaluation	17
5.9 Dispute Resolution.....	19
5.10 Extent of NESAS	19
5.11 Governance	19
6 Role and Tasks of the Scheme Owner.....	19
7 NESAS Benefits.....	21
8 Involved Stakeholders, their Roles and Relationships	22
9 Status of NESAS Development and Outlook.....	24
9.1 Versioning System of NESAS Specifications	24
9.2 Further Development and Extension of NESAS.....	24
9.3 Scheme Notes to be Maintained by Scheme Owner	25
9.4 Use of NESAS by Public Authorities	25
History	27

Licensing Statement

This GSMA document and its content is:

1. the exclusive property of the GSMA; and
 2. provided "as is", without any warranties by the GSMA of any kind.
-

Foreword

This Technical Specification was produced by the GSM Association.

The contents of the present document are subject to continuing work within the GSMA NESAS Group and can change following formal GSMA approval. When the NESAS Group modifies the contents of the present document, it will be re-released by the GSMA with an identifying change of release date and an increase in version number as follows:

Version x.y.

where:

- x the first digit is incremented for all major changes
 - y the second digit is incremented for all changes of corrections, technical enhancements, updates, etc.
-

Modal verbs terminology

In the present document, modal verbs have the following meanings:

shall indicates a mandatory requirement to do something

shall not indicates an interdiction (prohibition) to do something

"**shall**" and "**shall not**" are confined to the context of normative provisions.

"**must**" and "**must not**" are not used as substitutes for "**shall**" and "**shall not**".

should indicates a recommendation to do something

should not indicates a recommendation not to do something

may indicates permission to do something

need not indicates permission not to do something

"**may not**" is ambiguous and is not used in normative elements.

can indicates that something is possible

cannot indicates that something is impossible

The constructions "**can**" and "**cannot**" are not substitutes for "**may**" and "**need not**".

will indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

will not indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

All the document, including Annexes, is normative, unless otherwise explicitly stated.

Examples in the present document are used to provide additional information for understanding and are not intended to limit generality, applicability, and/or coverage of NESAS.

Introduction

The present document describes the Network Equipment Security Assurance Scheme (NESAS). The objective of NESAS is to provide an industry-wide security assurance framework to facilitate improvements in security levels across the whole industry.

NESAS defines security requirements and an assessment framework for secure product development and product lifecycle processes, as well as security test cases for the security evaluation of network equipment.

NESAS is of value to both operators and vendors, it is intended to be used alongside other mechanisms to ensure a network is secure, in particular an appropriate set of security policies covering the whole lifecycle of a network.

One of the motivations for developing NESAS is that the scheme will help vendors and operators avert fragmented regulatory security requirements. NESAS should be used globally as a common baseline, on top of which individual operators or national IT security agencies may want to put additional security requirements.

Scheme Owners implementing a specific NESAS implementation are encouraged to establish transparent and efficient procedures with a view to synergy and reusability across all NESAS implementations, and to accept existing Authorisations in other NESAS implementations to avoid fragmentation.

An introduction to the NESAS specifications, defining the NESAS methodology, requirements and guidelines, is given in the present document.

NESAS was originally created and developed by GSMA and responsibility for its maintenance and development of the NESAS specifications rests with the NESAS Group, which comprises representatives from mobile telecom network operators, infrastructure and equipment vendors, security auditors and test laboratories. The NESAS Group is an Industry Specification Issuing Group, and as such, it is bound to GSMA PRD AA.35 [3] governance.

The NESAS Group is responsible for maintaining the NESAS specifications and for facilitating periodic reviews involving all relevant stakeholders.

The Scheme Owner using NESAS specifications can add additional documentation and will be responsible for development and maintenance of its own documents.

1 Scope

The present document defines the role and tasks of the Scheme Owner and provides an overview on how to use the NESAS methodology and requirements, defined in the specification documents GSMA PRD FS.14 [4], GSMA PRD FS.15 [5], GSMA PRD FS.16 [6], GSMA PRD FS.47 [8], GSMA PRD FS.50 [9], GSMA PRD FS.62 [10] and GSMA PRD FS.63 [11]. GSMA PRD FS.46 [7] provides additional guidance on how to perform the Vendor Development and Product Lifecycle Processes assessment, defined in GSMA PRD FS.15 [5]. The structure and relationship of the specification documents within NESAS, including 3GPP reference documents, can be seen in Figure 1. Informative documents are marked as such. All the others are normative.

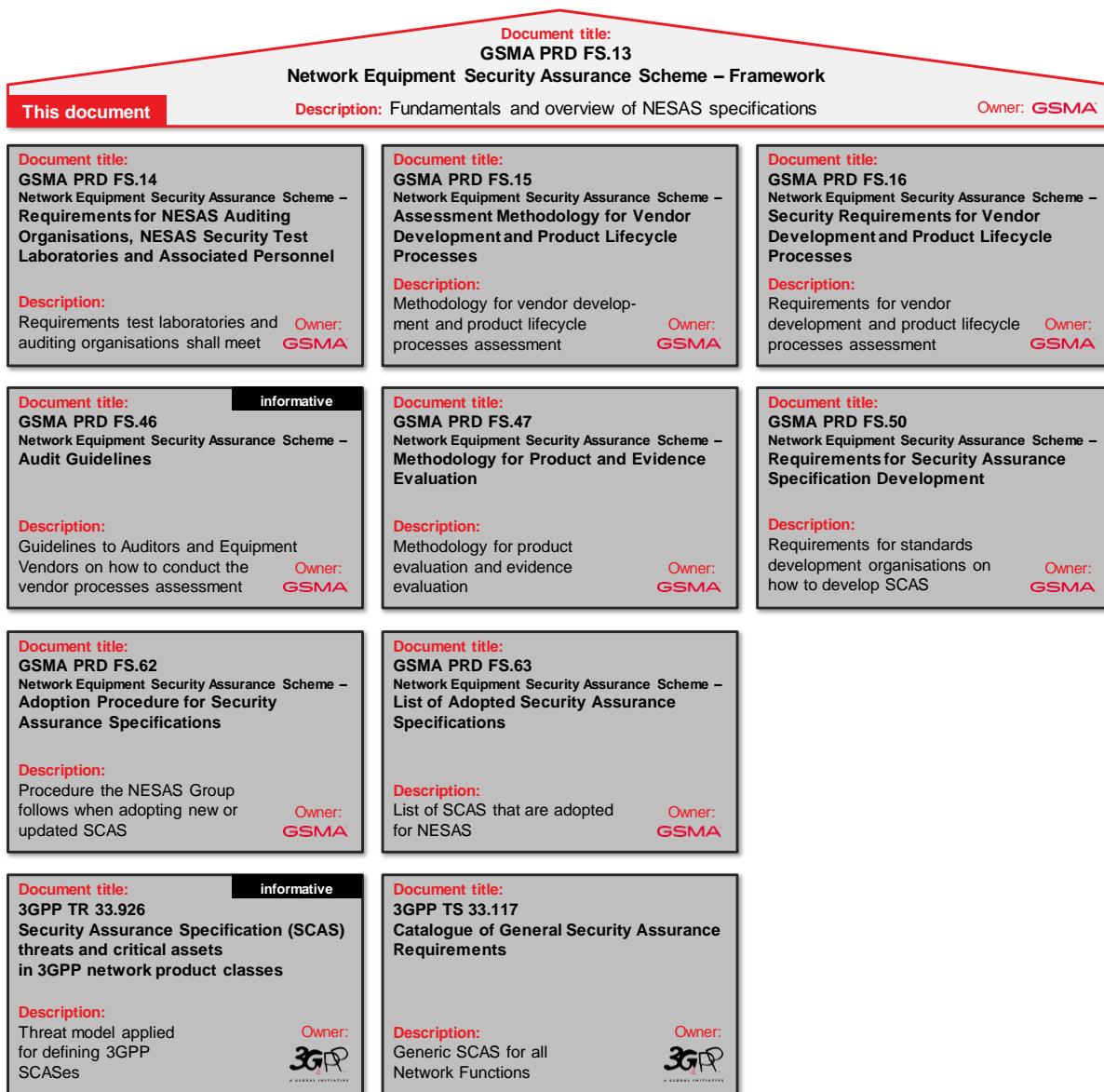


Figure 1: NESAS documents overview

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: Hyperlinks included in this clause were valid at the time of publication.

The following referenced documents are necessary for the application of the present document.

- [1] 3GPP TR 33.926: Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes
- [2] 3GPP TS 33.117: Catalogue of general security assurance requirements
- [3] GSMA PRD AA.35: Procedures for Industry Specifications
- [4] GSMA PRD FS.14: Network Equipment Security Assurance Scheme – Requirements for NESAS Auditing Organisations, NESAS Security Test Laboratories, and Associated Personnel
- [5] GSMA PRD FS.15: Network Equipment Security Assurance Scheme – Assessment Methodology for Vendor Development and Product Lifecycle Processes
- [6] GSMA PRD FS.16: Network Equipment Security Assurance Scheme – Security Requirements for Vendor Development and Product Lifecycle Processes
- [7] GSMA PRD FS.46: Network Equipment Security Assurance Scheme – Audit Guidelines
- [8] GSMA PRD FS.47: Network Equipment Security Assurance Scheme – Methodology for Product and Evidence Evaluation
- [9] GSMA PRD FS.50: Network Equipment Security Assurance Scheme – Requirements for Security Assurance Specification Development
- [10] GSMA PRD FS.62: Network Equipment Security Assurance Scheme – Adoption Procedure for Security Assurance Specifications
- [11] GSMA PRD FS.63: Network Equipment Security Assurance Scheme – List of Adopted Security Assurance Specifications
- [12] NESAS website: <https://gsma.com/nesas>

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: Hyperlinks included in this clause were valid at the time of publication. Informative references are not applicable in the present document.

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

Audit: A review and assessment that is performed and completed by an Audit Team against the NESAS Development and Product Lifecycle Security Requirements following the NESAS assessment methodology.

Audit Guidelines: Document giving guidance to the Audit Team and Equipment Vendor on how to interpret the requirements.

Audit Report: Document presenting the results of the Audit performed at the Equipment Vendor by the Audit Team.

Audit Summary Report: A subset of the Audit Report created by the Audit Team that summarises the key results.

Audit Team: Collective group of Auditors, generally to consist of two or more people, that perform a Vendor Development and Product Lifecycle Processes Audit.

Auditor: Individual that performs Vendor Development and Product Lifecycle Processes Audits and makes up part of the Audit Team.

Authorisation: The procedures defined by the Scheme Owner of verifying and selecting auditing organisations and security test laboratories which meet the requirements set out for NESAS Auditing Organisations and NESAS Security Test Laboratories.

Compliance Declaration: A written statement by the Equipment Vendor that confirms it adheres to the previously assessed Vendor Development and Product Lifecycle Processes for the particular Network Product that is provided to a NESAS Security Test Laboratory for evaluation.

Compliance Evidence: Evidence to be provided by the Equipment Vendor to the NESAS Security Test Laboratory, demonstrating that the Equipment Vendor applied its previously internally assessed and independently audited Vendor Development and Product Lifecycle Processes to build the Product under Evaluation. All Compliance Evidence for one Network Product is collected in one Compliance Declaration.

Conformance Claim: A written statement by the Equipment Vendor that confirms it meets the NESAS security requirements for the Vendor Development and Product Lifecycle Processes that are to be assessed.

Equipment Vendor: Organisation that develops, maintains and supplies to network equipment that supports functions defined by 3GPP or another SDO.

Evaluation Report: Documentation of the results of Evidence Evaluation and Network Product Evaluation, produced by an authorised NESAS Security Test Laboratory.

Evaluation Team: Collective group of Evaluators, generally to consist of two or more people, established by a NESAS Security Test Laboratory that are assigned to evaluate an Equipment Vendor's Network Product.

Evaluator: Individual that performs NESAS Network Product Evaluations and Evidence Evaluations, and makes up part of the Evaluation Team.

Evidence Evaluation: Activity in NESAS of evaluating if the Product under Evaluation (PuE) was developed in accordance with the previously assessed Vendor Development and Product Lifecycle Processes of the Equipment Vendor.

Interim Audit: An Audit of an Equipment Vendor's Vendor Development and Product Lifecycle Processes focussed only on security requirements revised or introduced since the Equipment Vendor's last Audit that allows the Equipment Vendor to demonstrate compliance with the new requirements. The report from the Interim Audit is treated as an addendum to the Audit Report from the last Audit of the Equipment Vendor.

NESAS Auditing Organisation: Organisation that engages or contracts qualified Auditors and has authorisation to perform Vendor Development and Product Lifecycle Processes Audits.

NESAS Development and Product Lifecycle Security Requirements: The security requirements that Vendor Development and Product Lifecycle Processes comply with under NESAS and against which Audits are performed.

NESAS Group: The Industry Specification Issuing Group of the GSMA that is tasked with the overall implementation, governance, maintenance and further development of NESAS specifications.

NESAS Security Test Laboratory: A test laboratory that is authorised to perform Network Product Evaluations and Evidence Evaluations under NESAS.

Network Function: A defined processing function in a network, which has defined functional behaviour and defined interfaces.

Network Product: Network equipment developed, maintained and supplied by an Equipment Vendor, consisting of one or more Network Function(s).

Network Product Evaluation: Activity of evaluating the Product under Evaluation (PuE) in NESAS, according to requirements and test cases taken from NESAS-adopted Security Assurance Specifications (SCAS).

Product under Evaluation: The Network Product for which an evaluation is sought by the Equipment Vendor.

Release: Version of a Network Product being made available for deployment.

Scheme Owner: Organisation or authority responsible for developing, maintaining, or operating a specific security assurance or certification scheme that uses the NESAS specifications.

Security Assurance Specification: Specification containing security requirements and test cases for a defined Network Function or a group of Network Functions. It is created and maintained by a Standards Development Organisation (SDO).

Vendor Development and Product Lifecycle Processes: The stages through which Network Products journey throughout their development including planning, design, implementation, testing, release, production and delivery and the stages to end of life including maintenance and update releases during their lifetime.

Vendor Development Process: Stages through which Network Products journey throughout their development including planning, design, implementation, testing, release, production and delivery.

Vendor Product Lifecycle Processes: Stages through which developed Network Products journey to end of life including maintenance and update releases during their lifetime.

3.2 Symbols

For the purposes of the present document, the following symbols apply.

Key for the figures in the present document:

-  Actor
-  Authorised actor
-  External entity actor
-  Specification
-  Activity
-  Activity resulting in Authorisation
-  Detailed activity with individual steps
-  Step
-  Checkpoint – prerequisites must be fulfilled
-  In scope of NESAS
-  Outside of NESAS scope
-  Blue indicates specifics of a potential scheme

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

3GPP	3rd Generation Partnership Project
GSMA	GSM Association
ISAG	Industry Specification Approval Group
ISO	International Organisation for Standardization
MNO	Mobile Network Operator
NESAS	Network Equipment Security Assurance Scheme
PRD	Permanent Reference Document
PuE	Product under Evaluation
SCAS	Security Assurance Specification
SDO	Standards Development Organisation
TR	Technical Report
TS	Technical Specification
TSG	Technical Specification Group

4 Introduction to Security Assurance in the Mobile Industry

A security assurance scheme always needs to consider the environment in which the scheme will operate. For a scheme addressing mobile network security the following aspects need to be considered:

- Network technology and products;
- Organisational security;
- Visibility of network equipment security levels;
- Operational feasibility; and
- Market acceptance and participation.

All relevant stakeholders need to commit to the scheme. Consequently, the effectiveness, cost, effort and complexity are important parameters that contribute to the ultimate success of the scheme. Solutions designed and agreed by all involved stakeholders are more likely to secure support.

With the increasing complexity of mobile networks and heightened security awareness, NESAS was designed to meet the needs of disparate stakeholders including:

- Mobile Network Operators (MNO);
- Equipment Vendors;
- Official/Governmental information security agencies and regulators.

In many countries, Mobile Network Operators are tasked by regulation to deploy and run reliable and robust networks. As one element of achieving this MNOs rely on secure network equipment being provided by their vendors. Thus, for MNOs, it is important to be able to understand the level of security within any specific product provided by their chosen vendors. The following two approaches are considered suitable to achieve this:

- Firstly, assessment of the security related to the Vendor Development and Product Lifecycle Processes

This allows each vendor to define its own internal processes and describe how security is integrated into the design, development, implementation, and maintenance processes. An Audit Team examines these processes and determines if they are adequate and if they are applied in practice.

Whilst undergoing the Audit, only the Audit Team sees the vendor's internal processes. Thus, an Audit Report can increase trust in a vendor without the vendor having to reveal internal secrets.

- Secondly, security evaluation of network equipment by a competent test laboratory with standardised security tests against an agreed security target.

This is a security evaluation of the manufactured network equipment. If there is a pre-defined set of security tests for network equipment, and if all network equipment is tested against these requirements, the achieved level of security can be objectively measured. New network equipment, as well as upgraded equipment, can be evaluated. If these tests are performed by a recognised and authorised competent test laboratory, a high quality and consistency of testing can be assured. In addition, if evaluation reports are able to be made available on request to prospective customers, further efficiencies can be achieved as tests only need to be performed once.

Although network standardisation is moving away from rigid architectures, the concept of standardised Network Functions remains. Standards that clearly define the functionality and capabilities of Network Functions can be used as the basis for the creation of clear, dedicated security requirements and test cases for all defined Network Functions. Network equipment can then be tested against applicable test cases.

Both approaches – process assessment and evaluation by testing – help MNOs determine the achieved level of security of a network product.

5 NESAS Methodology and Requirements Overview

5.1 General

NESAS specifies methodology and requirements for a network equipment security assurance scheme. It defines a globally applicable security baseline that network equipment vendors can meet.

Briefly, the NESAS approach consists of the following steps:

1. Equipment Vendors define and apply secure design, development, implementation, and product maintenance processes;
2. Equipment Vendors assess and claim conformance of these processes with the NESAS defined security requirements;
3. Equipment Vendors demonstrate these processes to an independent Audit Team;
4. Level of security of network equipment is tested and documented;
5. Tests are performed by competent and authorised test laboratories against defined security requirements;
6. Documentation can be forwarded to purchasing operators.

5.2 Lifecycle Roles and NESAS Scope

Figure 2 depicts both Vendor and Operator lifecycles, together with assigned responsibilities and the scope of NESAS.

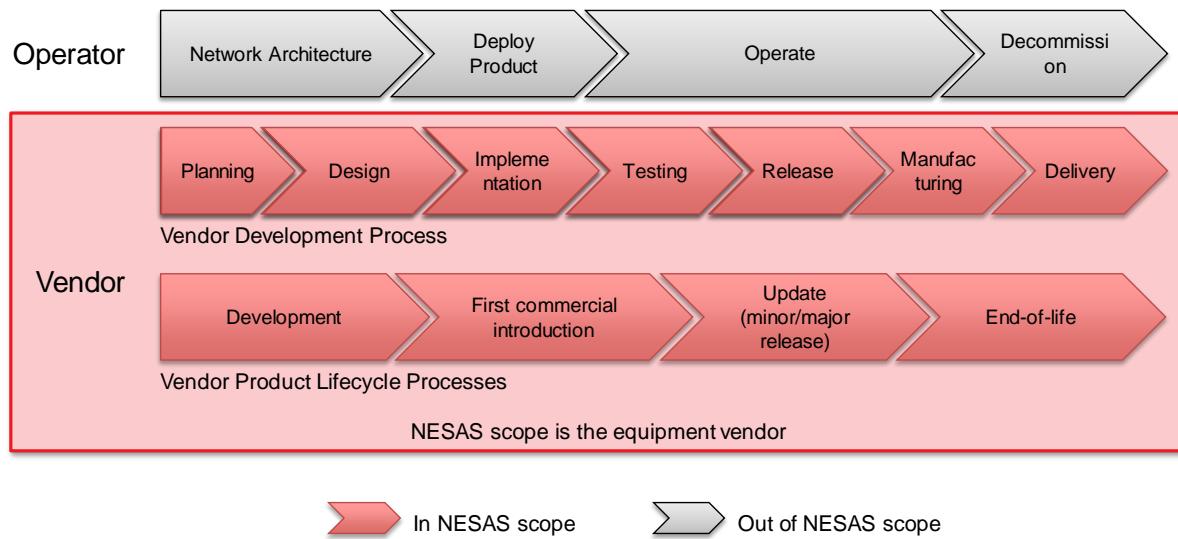


Figure 2: Responsibility, accountability and NESAS scope

Design, development and implementation of network equipment is performed by the Equipment Vendor. The MNO operates a reliable mobile network and relies on the Equipment Vendor to provide the required level of security resilience in their products. Network design, operating procedures and maintenance of deployed network equipment falls within the MNO's responsibilities.

The *Network Equipment Security Assurance Scheme* (NESAS) provides a solution to meet the needs of industry and other stakeholders. The focus of NESAS, which covers an essential element of supply chain security, is on equipment vendors and their role in the chain.

5.3 Owner of and Responsibility for NESAS

NESAS is a set of specifications, defined by the NESAS Group, 3GPP and other Standards Development Organisations (SDOs). The specifications are maintained by these organisations respectively.

The NESAS Group defines and maintains the NESAS specifications, which cover assessment of the Vendor Development and Product Lifecycle Processes, NESAS Security Test Laboratory Authorisation, and security evaluation of network equipment. 3GPP and other SDOs define security requirements and test cases for network equipment implementing one or more Network Functions – specified in *Security Assurance Specifications* (SCAS).

NESAS is defined by the NESAS specifications GSMA PRD FS.13 (the present document), GSMA PRD FS.14 [4], GSMA PRD FS.15 [5], GSMA PRD FS.16 [6], GSMA PRD FS.46 [7], GSMA PRD FS.47 [8], GSMA PRD FS.50 [9], GSMA PRD FS.62 [10] and GSMA PRD FS.63 [11]. The NESAS Group is the owner of these specifications and maintains them. The GSMA, being the home of the NESAS Group, maintains publicly accessible official information about NESAS on the NESAS website [12]. This includes providing NESAS specifications for download.

Figure 3 illustrates the roles of 3GPP and GSMA within NESAS. Next to 3GPP, also other SDOs can define and maintain Security Assurance Specifications (SCAS) for adoption by NESAS. Figure 3 only depicts 3GPP and no other SDO for simplicity. SCASes can be adopted if they adhere to the provisions set out in GSMA PRD FS.50 [9]. Adoption is performed by the NESAS Group as defined in GSMA PRD FS.62 [10]. Adopted SCASes are listed in GSMA PRD FS.63 [11].

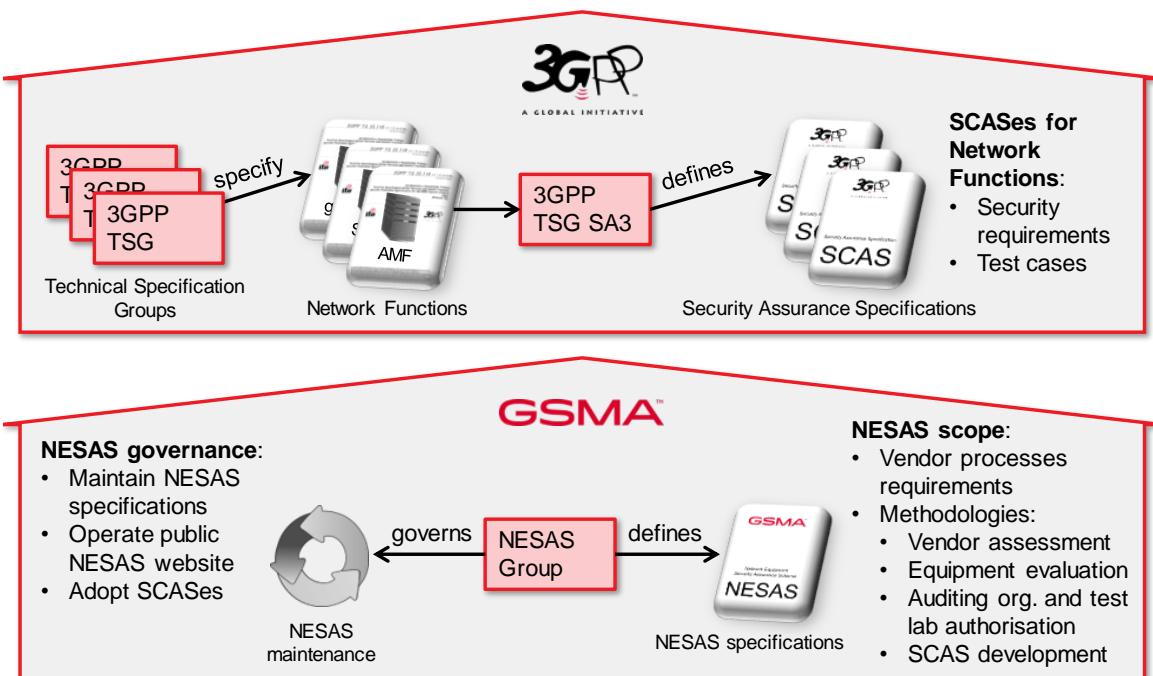


Figure 3: Roles of 3GPP and GSMA in NESAS

Network equipment that is produced and sold by an Equipment Vendor is called a Network Product in NESAS. It includes one or more Network Functions. A mobile base station from a particular vendor is an example of a Network Product.

NOTE 1: GSMA PRD FS.50 [9] provides requirements to SDOs on how to create and maintain SCASes that ought to be adopted by NESAS.

NOTE 2: GSMA PRD FS.62 [10] defines the SCAS adoption procedure.

NOTE 3: GSMA PRD FS.63 [11] contains all currently adopted SCASes.

5.4 NESAS High Level Overview

Figure 4 depicts the various NESAS actors and activities that are described briefly below. The following clauses provide detailed information on the different components of NESAS specifications.

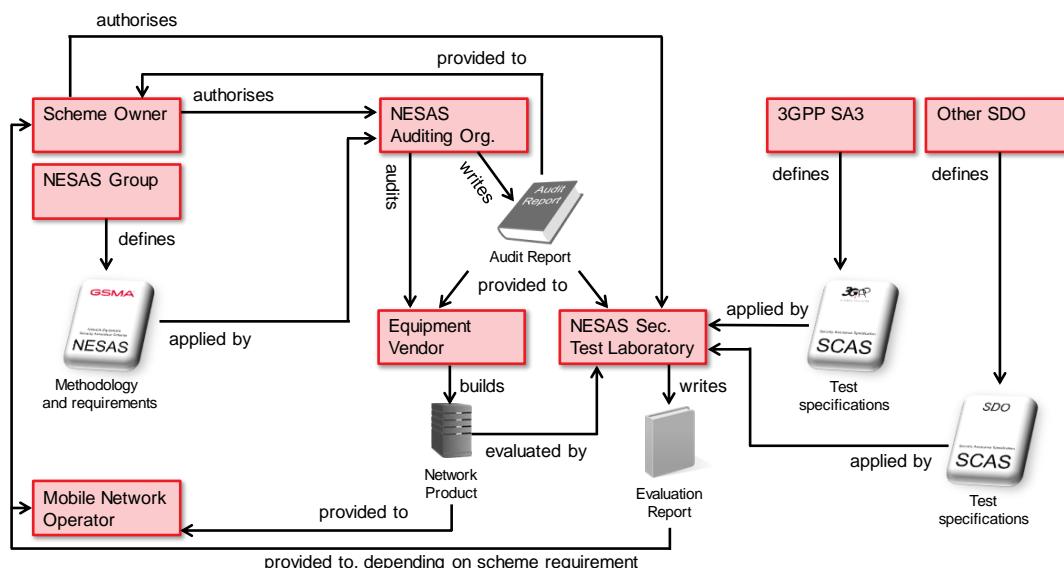
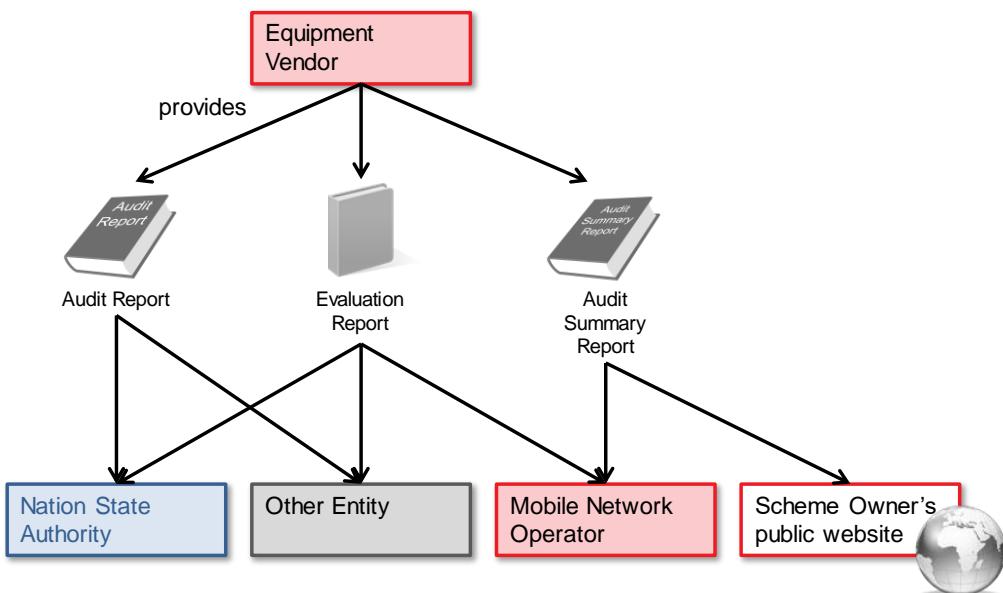


Figure 4: NESAS high level overview

The Scheme Owner authorises NESAS Auditing Organisations and defines the procedure to select one to audit the Equipment Vendor's Vendor Development and Product Lifecycle Processes. The selected NESAS Auditing Organisation appoints an Audit Team, which applies the NESAS methodology for the Audit, as defined by NESAS. Results of the Audit are documented in the Audit Report. If the Equipment Vendor is considered by the Audit Team to be NESAS compliant, having satisfied all of the NESAS security requirements, a copy of the Audit Summary Report may be published. It is the Scheme Owner's decision, if and how to publish the Audit Summary Report.

The Scheme Owner authorises NESAS Security Test Laboratories. The Equipment Vendor builds its Network Products and submits them for evaluation to an authorised NESAS Security Test Laboratory, selected by the Equipment Vendor. The selected NESAS Security Test Laboratory evaluates the Network Product against the relevant SCAses and verifies that the internally assessed and independently audited Vendor Development and Product Lifecycle Processes of the Equipment Vendor have been applied to the evaluated Network Product. The NESAS Security Test Laboratory then produces an Evaluation Report.

The Audit (Summary) Report and the Evaluation Report can then be provided to customers and additional interested parties, as illustrated in Figure 5. The Scheme Owner defines which entities are obligatory recipients.

**Figure 5: Potential recipients of NESAS results**

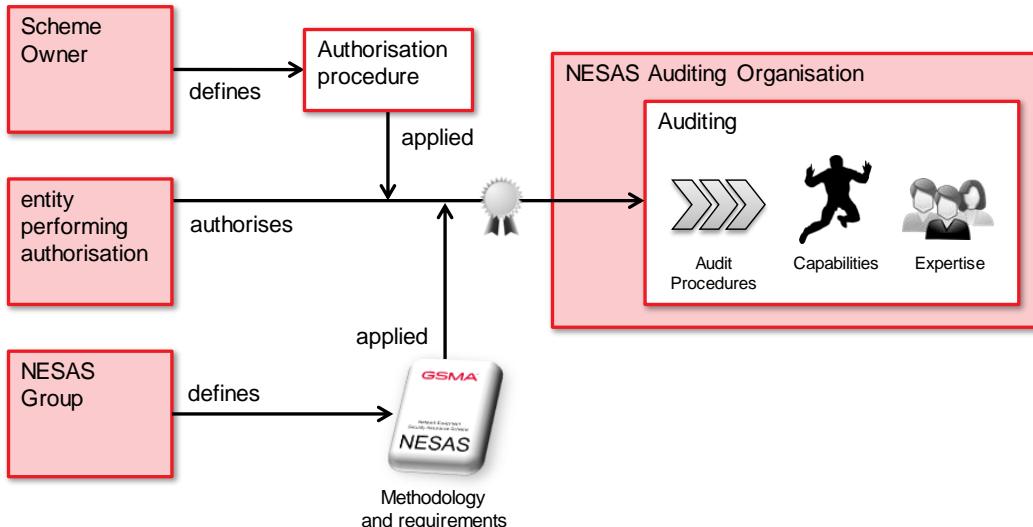
5.5 Authorisation of NESAS Auditing Organisations

The requirements for NESAS Auditing Organisations and the associated personnel are defined in GSMA PRD FS.14 [4]. NESAS Auditing Organisations and each Auditor engaged by this organisation shall meet these requirements at all times.

Authorisation is a prerequisite for auditing organisations to be eligible to perform Vendor Development and Product Lifecycle Processes assessments under NESAS. Authorisation is an instrument to demonstrate and verify adherence to the requirements defined in GSMA PRD FS.14 [4]. Auditing organisations can only be authorised if they demonstrate they meet these requirements and engage qualified Auditors.

The Scheme Owner has the responsibility to ensure that each NESAS Auditing Organisation and each Auditor engaged by this organisation meet the requirements of GSMA PRD FS.14 [4]. To achieve this, the Scheme Owner shall define an appropriate procedure for the Authorisation of NESAS Auditing Organisations, implement this procedure, ensure its effectiveness, and apply the procedure for verification. The Scheme Owner shall define the validity period of such Authorisation and can define measures to check compliance with the requirements during this term. Authorisation can be based on accreditation, assignment or other suitable means, chosen by the Scheme Owner.

Figure 6 illustrates the NESAS Auditing Organisation authorisation procedure.

**Figure 6: Authorisation of NESAS Auditing Organisations**

The Scheme Owner shall maintain a list of authorised NESAS Auditing Organisations in their respective scheme and define how to publish the list. For transparency, this list shall be publicly accessible, e.g. on a public website.

NOTE : GSMA PRD FS.14 [4] defines requirements for NESAS Auditing Organisations and Auditors engaged by this organisation to be eligible to perform Vendor Development and Product Lifecycle Processes assessments under NESAS.

5.6 Authorisation of NESAS Security Test Laboratories

The requirements for NESAS Security Test Laboratories and the associated personnel are defined in GSMA PRD FS.14 [4]. NESAS Security Test Laboratories and each Evaluator engaged by this laboratory shall meet these requirements at all times.

Authorisation is a prerequisite for security test laboratories to be eligible to perform Network Product Evaluations and Evidence Evaluations under NESAS. Authorisation is an instrument to demonstrate and verify adherence to the requirements defined in GSMA PRD FS.14 [4]. Security test laboratories can only be authorised if they demonstrate they meet these requirements and engage qualified Evaluators.

The Scheme Owner has the responsibility to ensure that each NESAS Security Test Laboratory and each Evaluator engaged by this laboratory meet the requirements of GSMA PRD FS.14 [4]. To achieve this, the Scheme Owner shall define an appropriate procedure for the Authorisation of NESAS Security Test Laboratories, implement this procedure, ensure its effectiveness, and apply the procedure for verification. The Scheme Owner shall define the validity period of such Authorisation and can define measures to check compliance with the requirements during this term. Authorisation can be based on accreditation, assignment or other suitable means, chosen by the Scheme Owner.

Figure 7 illustrates the NESAS Security Test Laboratory Authorisation procedure.

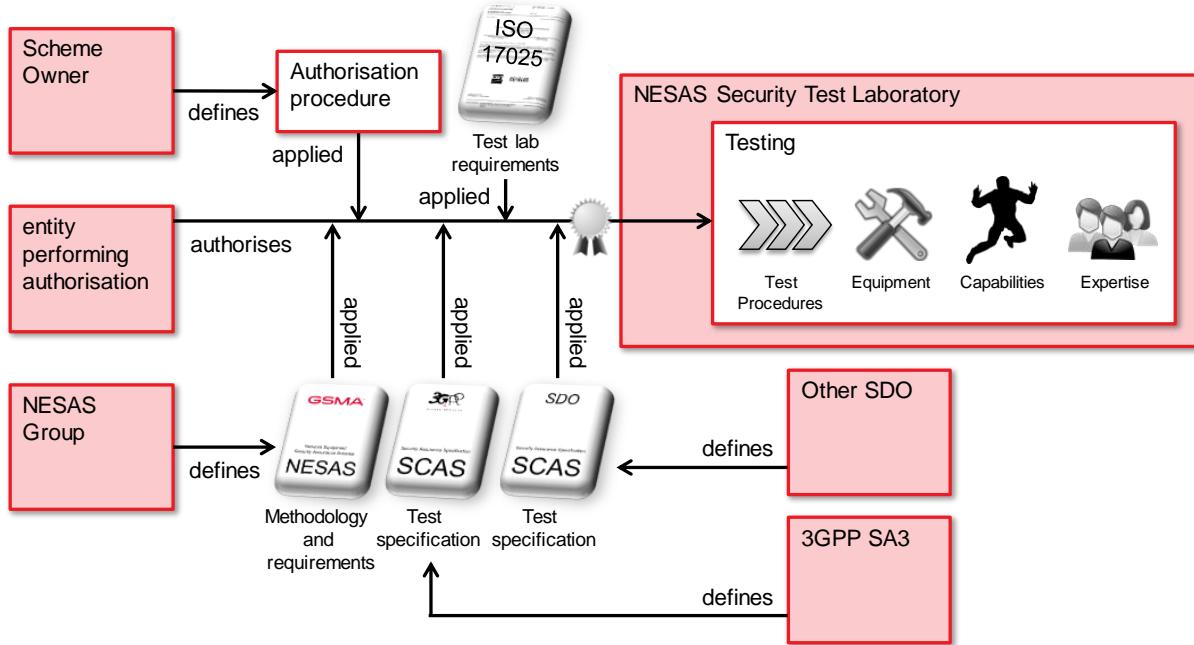


Figure 7: Authorisation of NESAS Security Test Laboratories

The Scheme Owner shall maintain a list of authorised NESAS Security Test Laboratories in their respective scheme and define how to publish the list. For transparency, this list shall be publicly accessible, e.g. on a public website.

NOTE : GSMA PRD FS.14 [4] defines requirements for NESAS Security Test Laboratories and Evaluators engaged by this laboratory to be eligible to perform Network Product Evaluations and Evidence Evaluations under NESAS

5.7 Assessment of Vendor Development and Product Lifecycle Processes

Figure 8 depicts, at a high level, the steps the assessment of Vendor Development and Product Lifecycle Processes consist of.

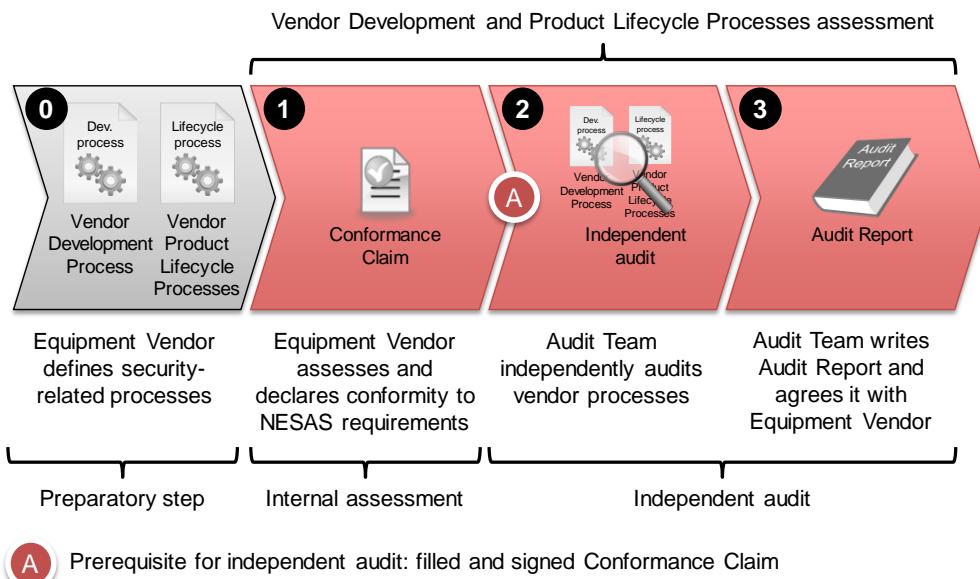


Figure 8: Sequence of activities of Vendor Development and Product Lifecycle Processes assessment

As a preparatory step (Step 0 in Figure 8), the Equipment Vendor defines its own processes for Development and Product Lifecycle. These processes should define how security resilience is integrated in the vendor processes.

Step 1 in Figure 8: The Equipment Vendor defined processes are first internally assessed by the participating Equipment Vendor, which shall claim conformance and describe how it believes it complies with the defined security requirements. The result is written down in the Conformance Claim, which is signed by the Equipment Vendor. Presenting the signed Conformance Claim is a prerequisite for entering the independent Audit (Checkpoint A in Figure 8).

Step 2 in Figure 8: Subsequently, the Vendor Development and Product Lifecycle Processes are audited by an Audit Team, which follows the auditing methodology, defined by NESAS in GSMA PRD FS.15 [5] and determines compliance of the Equipment Vendor to the NESAS requirements in GSMA PRD FS.16 [6]. For each individual Audit, an authorised NESAS Auditing Organisation is selected, which appoints and tasks the Audit Team. Both procedures for appointing Audit Teams and for selecting authorised NESAS Auditing Organisations are defined by the Scheme Owner.

Audits consist of off-site process documentation reviews and on-site Audits. The Scheme Owner can define certain circumstances under which Audits can be performed remotely. For example, a Scheme Owner may grant permission for remote Audits in cases where travel restrictions, time shifts, or other circumstances prevent the Audit Team from performing an on-site Audit or significantly impair its effectiveness. Each remote Audit requires prior consultation with, and approval from the Scheme Owner.

Step 3 in Figure 8: The Audit Team produces an Audit Report that contains the results of the Audit and recommendations. The Audit Team also indicates in the Audit Report the type of Compliance Evidence that is required for subsequent Evidence Evaluations. The Audit Report shall be agreed with the Equipment Vendor and be signed by both parties. It shall also be made available to the Scheme Owner, and the Audit Report may be provided to other relevant stakeholders at the discretion of the Equipment Vendor. An Audit Summary Report is also produced, that can be published for the purpose of highlighting NESAS participation by the Equipment Vendor. It is the Scheme Owner's decision, if and how to publish the Audit Summary Report.

The assessment of the Vendor Development and Product Lifecycle Processes is depicted in Figure 9.

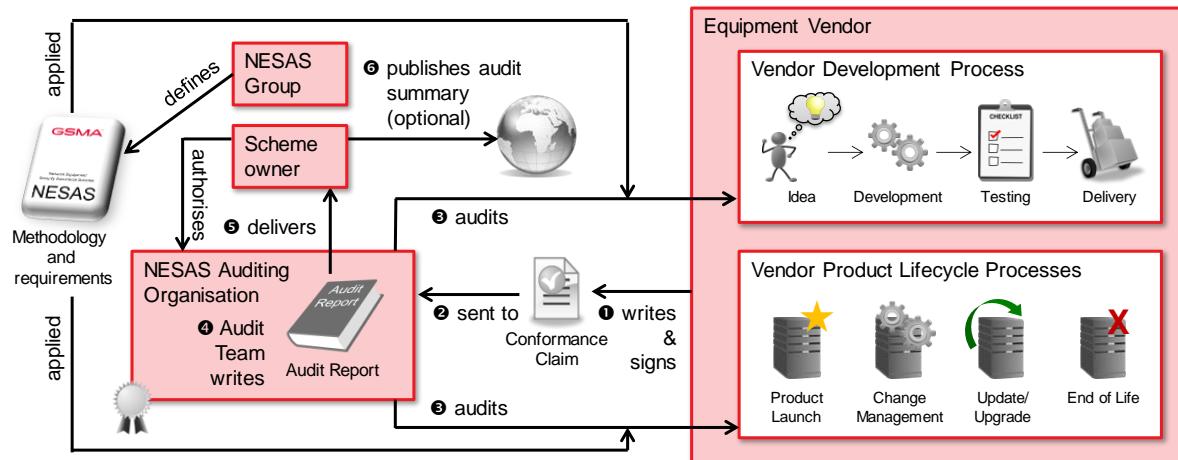


Figure 9: Assessment of vendor processes

The Equipment Vendor is only considered fully compliant, if the audited Equipment Vendor meets all the security requirements for Vendor Development and Product Lifecycle Processes, as outlined in GSMA PRD FS.16 [6], without exception. If the Equipment Vendor is found to be non-compliant with any one of the security requirements the overall Audit result considers the Equipment Vendor to be non-compliant.

The validity of an assessment is defined by the Scheme Owner and may expire earlier if the assessed vendor processes change. Audits are always to be performed against the current version of GSMA PRD FS.15 [5] and GSMA PRD FS.16 [6].

NESAS is a living scheme, so it is to be expected that security requirements will be added or changed and as a result, a new version of GSMA PRD FS.16 [6] is published. These significant changes could impact an Equipment Vendor that has already completed an Audit against the previous version of the security requirements insofar, as its Audit Report and related material will reference an out-of-date version of the security requirements. In order to allow the Equipment Vendor to maintain and demonstrate compliance to the current security requirements, it may be possible for it to

perform an Audit that is focussed only on the changes included in the security requirements update, rather than having to undergo a full Audit. Such a focussed Audit is called an Interim Audit and it allows the Equipment Vendor to keep its compliance to NESAS security requirements current, where the vendor's processes have not changed substantially, until the next full Audit of its Vendor Development and Product Lifecycle Processes falls due. Further details about Interim Audits can be found in GSMA PRD FS.15 [5]. The Scheme Owner may define additional procedures for Interim Audits or disallow them in its scheme.

NOTE 1: GSMA PRD FS.15 [5] defines the Vendor Development and Product Lifecycle Processes assessment methodology, which describes the process of performing the internal assessment and independent Audit.

NOTE 2: GSMA PRD FS.16 [6] defines the Vendor Development and Product Lifecycle Process security requirements that are to be met by the Equipment Vendor and to be assessed by the Audit Team.

NOTE 3: GSMA PRD FS.46 [7] provides additional guidance to Equipment Vendors and Audit Teams on how to perform the assessment of Vendor Development and Product Lifecycle Processes.

5.8 Network Product Evaluation and Evidence Evaluation

Once an Equipment Vendor's Vendor Development and Product Lifecycle Processes internal assessment and independent Audit result in full compliance to the NESAS security requirements defined in GSMA PRD FS.16 [6], Network Products can be evaluated by an authorised NESAS Security Test Laboratory. Full compliance to the NESAS security requirements is a prerequisite for Network Product Evaluation (Checkpoint B in Figure 10)

Figure 10 depicts at a high level the steps the evaluation consists of.

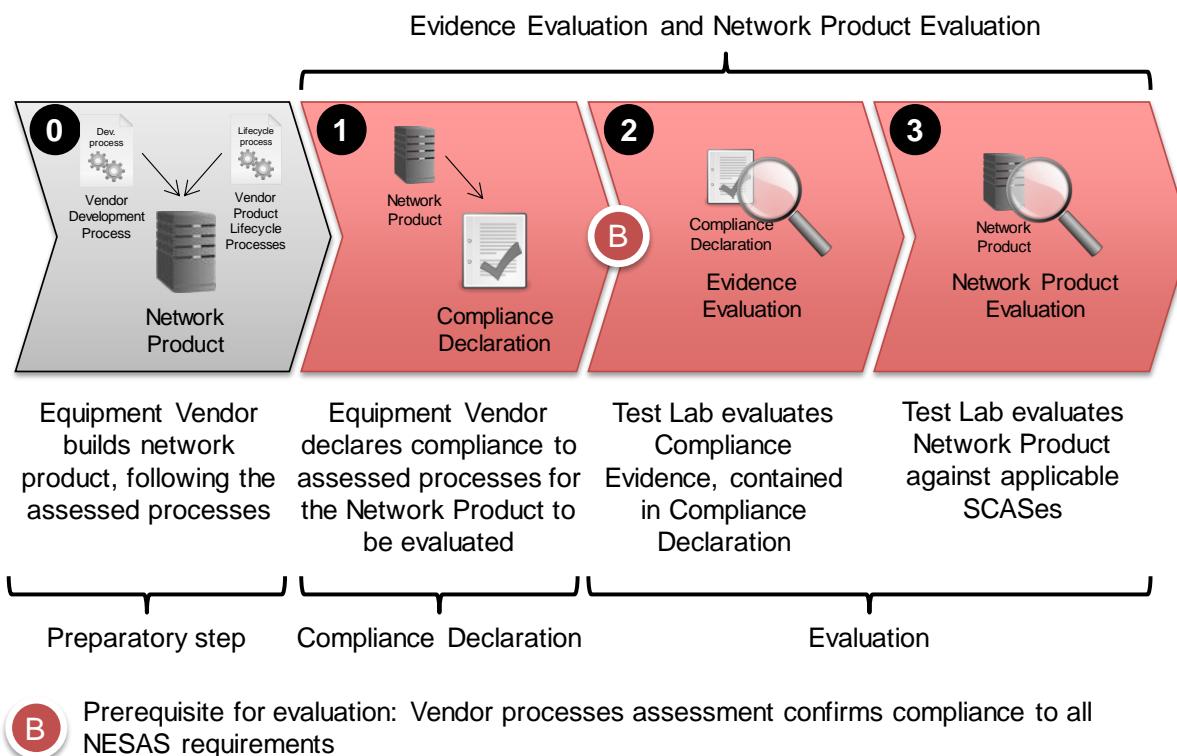


Figure 10: Sequence of activities of Evidence Evaluation and Network Product Evaluation

As a preparatory step (Step 0 in Figure 10), the Equipment Vendor builds the Network Product in full accordance to the previously assessed Vendor Development and Product Lifecycle Processes.

Step 1 in Figure 10: The Equipment Vendor produces the Compliance Declaration, which contains all the Compliance Evidence for the Product under Evaluation, broken down for each of the security requirements as defined in GSMA PRD FS.16 [6].

For evaluation, the Equipment Vendor selects an authorised NESAS Security Test Laboratory and contracts directly with it. The Scheme Owner may define additional constraints for selecting the NESAS Security Test Laboratory that

will perform the evaluation. Once the NESAS Security Test Laboratory is selected, the Equipment Vendor provides the Network Product and Compliance Declaration to the NESAS Security Test Laboratory. The Evaluation Team, consisting of competent Evaluators, is appointed by the NESAS Security Test Laboratory.

Step 2 in Figure 10: The Evaluation Team follows the evaluation methodology defined by NESAS in GSMA PRD FS.47 [8], and evaluates the provided Compliance Evidence and comprehends if the Equipment Vendor is following its own internally assessed and independently audited Vendor Development and Product Lifecycle Processes when building the Product under Evaluation. The Audit Report that was produced during the Equipment Vendor Development and Product Lifecycle Processes Audit, gives guidance to the NESAS Security Test Laboratory on how to evaluate the Compliance Evidence. In some cases, it may not be possible to provide Compliance Evidence for a particular security requirement. In these cases, the Equipment Vendor shall provide a rationale instead, giving reasons. The results of Evidence Evaluation are recorded in an Evaluation Report.

Step 3 in Figure 10: Test specifications from the adopted SCASes, as listed in GSMA PRD FS.63 [11], are used to create and perform detailed tests for the Network Product. The Evaluation Team follows the evaluation methodology defined by NESAS in GSMA PRD FS.47 [8]. SCASes to be selected for evaluation depend on the functionality provided by the Product under Evaluation. Preparation of the test environment and configuration of the Product under Evaluation are defined in the SCASes. Test results are added to the Evaluation Report. Test results shall be documented in a level of detail that allows reproduction of the tests.

It is the Evidence evaluation that links the tested Network Product to the internally assessed and independently audited vendor processes and this is why only an Evaluation Report that contains both results – from Network Product Evaluation and from Evidence Evaluation – is meaningful to a MNO.

Network Product Evaluation and Evidence Evaluation are illustrated in Figure 11 in more detail.

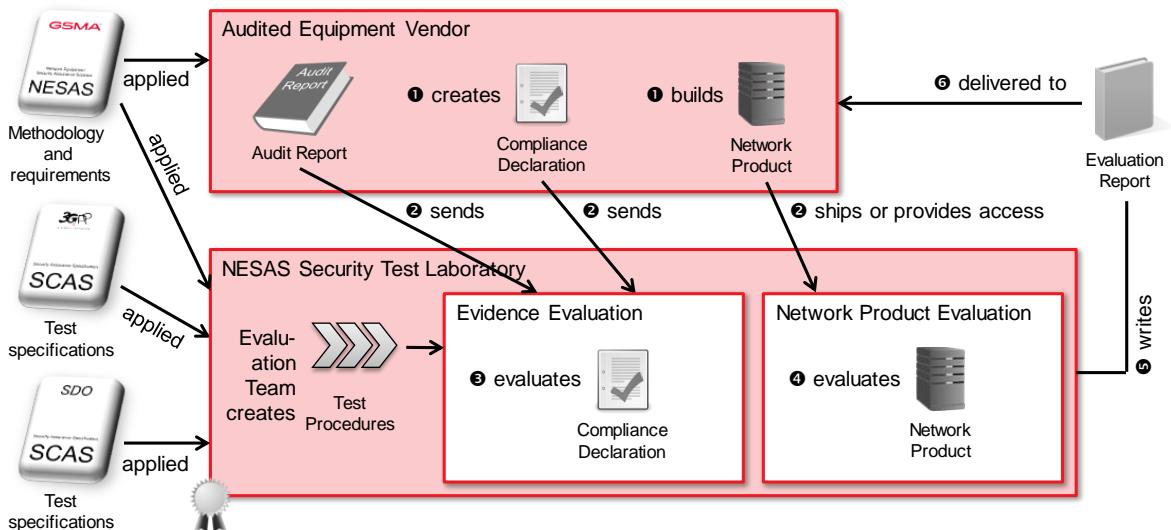


Figure 11: Network Product Evaluation and Evidence Evaluation

The completed Evaluation Report is handed over to the Equipment Vendor. The Equipment Vendor can then provide it to any interested entity. For example, a MNO can request the Evaluation Report together with the Network Product when sourcing equipment. The Scheme Owner defines, which additional entities, if any, shall receive the Evaluation Report.

Post evaluation, the Scheme Owner may use the completed Evaluation Report as input to additional procedures, for example, publication of the fact that the product was evaluated. These procedures will be defined by the Scheme Owner.

Each Network Product Evaluation is bound to a dedicated Release of the Network Product and to a dedicated version of GSMA PRD FS.47 [8]. Validity period and expiry criteria are defined by the Scheme Owner. A new Release of the Network Product will trigger the need for an up-to-date evaluation. Changes to GSMA PRD FS.47 [8] may trigger the need for a new Network Product Evaluation. Further details can be found in GSMA PRD FS.47 [8].

NOTE 1: GSMA PRD FS.46 [7] describes the Compliance Evidence the Equipment Vendor is expected to provide to the NESAS Security Test Laboratory for Evaluation.

NOTE 2: GSMA PRD FS.47 [8] defines how Network Product evaluation and Evidence Evaluation are performed.

NOTE 3: GSMA PRD FS.50 [9] provides requirements to SDOs on how to create and maintain SCASes that ought to be adopted by NESAS.

NOTE 4: GSMA PRD FS.62 [10] defines the SCAS adoption procedure.

NOTE 5: GSMA PRD FS.63 [11] contains all currently adopted SCASes.

NOTE 6: SCASes of the 3GPP (e.g. the generic SCAS for any network equipment 3GPP TS 33.117 [2]) and other SDOs contain test specifications the NESAS Security Test Laboratory shall use to perform Network Product Evaluations.

NOTE 7: 3GPP TR 33.926 [1] describes the threat model that was chosen to define security requirements and test cases in 3GPP SCASes.

5.9 Dispute Resolution

The Scheme Owner should define a dispute resolution process, which can be followed in case an entity has a dispute with another stakeholder related to the scheme. The Scheme Owner should also define acceptable disputes.

5.10 Extent of NESAS

As illustrated above, the focus of NESAS is exclusively on network equipment. NESAS addresses the industry's needs and challenges by taking the following multifaceted approach:

- 1) Assessment of Vendor Development and Product Lifecycle Processes;
- 2) Network Product Evaluation and Evidence Evaluation by competent NESAS Security Test Laboratories using defined and standardised security tests.

To achieve the necessary balanced approach that is accepted by all stakeholders, certain aspects have been excluded from the initial scope and these are as follows:

- 1) NESAS specifications do not address certification of Equipment Vendors or network equipment. The Scheme Owner can add a certification component for its own scheme.
- 2) It is generally acknowledged that the absence of undocumented functionality (e.g. backdoors, malware, etc.) in network equipment cannot be guaranteed and this is also the case for NESAS.
- 3) The scheme does not replace existing operator or national requirements.
- 4) The scheme is not intended to include security of interoperability and interworking between network equipment.
- 5) The scheme does not address the need for end-to-end security.

5.11 Governance

NESAS specifications are governed by the provisions set out in GSMA PRD FS.13 (the present document), GSMA PRD FS.14 [4], GSMA PRD FS.15 [5], GSMA PRD FS.16 [6], GSMA PRD FS.47 [8], GSMA PRD FS.50 [9], GSMA PRD FS.62 [10] and GSMA PRD FS.63 [11]. In case of any conflict between GSMA PRD FS.13 (the present document) and any other NESAS specification, the other NESAS specification shall prevail.

6 Role and Tasks of the Scheme Owner

NESAS specifications are the core of any NESAS-based scheme. If a Scheme Owner decides to use NESAS in their scheme, the methodology, requirements, and guidelines of the NESAS specifications should be followed, while additional procedures may be defined by the Scheme Owner. The Scheme Owner shall create and maintain a scheme definition and shall govern and operate its scheme. This clause describes the role of the Scheme Owner by collecting all

the aspects the Scheme Owner shall define, govern, and operate. These are collected from descriptions elsewhere in the present document.

Specification:

- Define the procedure of authorising auditing organisations and security test laboratories, based on accreditation, assignment or other suitable means;
- Define validity period of Authorisations of NESAS Auditing Organisations and NESAS Security Test Laboratories;
- Define how to publish the list of authorised NESAS Auditing Organisations and NESAS Security Test Laboratories (e.g. on a public website);
- Define the procedure of selecting the NESAS Auditing Organisation for a particular Vendor Development and Product Lifecycle Processes Audit (e.g. by allowing the Equipment Vendor to select from the previously authorised NESAS Auditing Organisations);
- Define the procedure to appoint Audit Teams and how to task an Audit Team with a particular Vendor Development and Product Lifecycle Processes Audit;
- Define obligatory recipients of Audit Reports and Audit Summary Reports;
- Define how Audit Summary Reports are published (e.g. on a public website), if the Equipment Vendors are considered by the Audit Team to be NESAS compliant;
- Define validity period of vendor processes assessments;
- Interim Audits:
 - Define if they are allowed in the scheme;
 - If allowed, declare if they follow GSMA PRD FS.15 [5] or if additional procedures apply;
 - If additional procedures apply, define them;
- Define circumstances that permit remote Audits and a procedure for approving remote audits, if desired and provided by the specific scheme;
- Define in which cases Network Products shall be evaluated;
- Define if the scheme relies on all the adopted SCAses listed in GSMA PRD FS.63 [11] or if it only uses a subset. If it only uses a subset, define criteria for creating the subset and where the resulting list is published;
- Define additional constraints for Equipment Vendors to select a NESAS Security Test Laboratory for evaluation, if desired;
- Define which additional entities shall receive the Evaluation Report, if any;
- Define expiry criteria and validity period of Evaluation Reports;
- Define post evaluation procedures, if any, that use the completed Evaluation Report as input, for example, publication of the fact that the product was evaluated;
- Define procedures to assess the impact that material changes to NESAS specifications have on the scheme and involved stakeholders;
- Define the content that is to be put in the scheme notes and the events that trigger an update of the scheme notes;
- Provide reference to Scheme Owner's website;
- Define a dispute resolution process and define which sorts of disputes will be ruled upon.

Governance and operation:

- Authorise auditing organisations to perform Vendor Development and Product Lifecycle Processes assessments;
- Authorise security test laboratories to perform Network Product Evaluations and Evidence Evaluations;
- If defined by the scheme itself, apply SCAS usage criteria, whenever new/changed SCASes are adopted by the NESAS Group in GSMA PRD FS.63 [11], and publish the resulting list;
- Apply remote audit approval process upon Equipment Vendor request;
- Maintain and publish scheme notes;
- Maintain Scheme Owner's website, containing:
 - List of authorised NESAS Auditing Organisations;
 - List of authorised NESAS Security Test Laboratories, if different from the list published on NESAS website [12];
 - List of adopted SCASes, if only a subset of those listed in GSMA PRD FS.63 [11] is used;
- Manage the dispute resolution process and initiate it whenever cases are filed.

As outlined in clause 0, NESAS is designed to be enhanced iteratively. The NESAS Group is always receptive to enhancement and improvement proposals. When the Scheme Owner (or any other stakeholder) has such proposals, or questions on the interpretation of the NESAS specifications, they are invited to contact the NESAS Group at nesas@gsm.org.

7 NESAS Benefits

NESAS brings a number of benefits for various stakeholders in the mobile industry and regulatory and user communities.

The level of security assurance, and as such the level of security resilience, achieved by network equipment, is measurable, visible, comparable and understood. MNOs benefit as this introduces transparency that helps MNOs determine if the network equipment of individual vendors meets the security requirements of the MNO. For vendors, this provides a platform to highlight the vendor's ability to achieve/maintain good security standards.

Most vendors demonstrate a commitment to secure Vendor Development and Product Lifecycle Processes. This is beneficial for MNOs, since it increases trust in the vendor and confidence for MNOs when engaged in vendor selection decision making. In return, it encourages and rewards vendors to reinforce security in their products and it engenders a security-by-design culture across the entire vendor community.

Evaluation of network equipment, performed by competent authorised NESAS Security Test Laboratories, allows MNOs determine the level of security of that equipment before it is deployed. Furthermore, it reduces the security testing burden on vendors, MNOs and interested regulators and national authorities.

While all stakeholders are free to set their individual security requirements, NESAS is designed to ensure a baseline security level and a common set of security requirements for all. Both vendors and MNOs will benefit from the reduced set of requirements, as requests for quotation processes and contract negotiations require less security requirements to be listed, considered, and agreed. This should be significantly beneficial for Equipment Vendors as the overhead of dealing and responding to different, but similar, security requirements coming from various stakeholders is reduced.

With NESAS, a single Audit for the vendor replaces the need to host and fund audits from individual operators and regulators, aimed at reducing overheads for the vendor.

One of the goals set by industry for NESAS is to demonstrate to regulators its value. If it can be shown that NESAS security requirements are commensurate with national security requirements in individual countries, national authorities are likely to endorse and support NESAS as a requirement for mobile network equipment deployments. This is beneficial for equipment vendors, since the overhead of satisfying different security requirements from individual

regulators and countries is reduced. Therefore, NESAS is designed to interface well with regulatory frameworks, as further detailed in clause 0.

NESAS builds upon established international standards for the Authorisation of auditing organisations and security test laboratories, and thus delivers security gains and improvements whilst keeping work and costs for all stakeholders at manageable levels.

8 Involved Stakeholders, their Roles and Relationships

The stakeholders that are involved in NESAS, and their roles and relationships, are described in this clause.

The **Scheme Owner** uses the NESAS specifications to create a security assurance or certification scheme, which it maintains and operates. The Scheme Owner needs to define some details of the scheme, which are not defined in the NESAS specifications, in order to make the scheme applicable. Clause 0 lists all the aspects that are to be defined and maintained.

Mobile Network Operators (MNO), operate mobile networks. They are interested in operating a robust and reliable network which requires them to obtain robust and secure network equipment. MNOs are interested in obtaining NESAS evaluated network equipment from NESAS assessed vendors.

The network equipment used in mobile networks, such as the radio base stations, Internet gateways, etc. are developed and provided by **Equipment Vendors**. Equipment Vendors have predefined secure Vendor Development and Product Lifecycle Processes by which they create and produce their network equipment.

NESAS Security Test Laboratories are contracted to perform network equipment security evaluations as defined by NESAS.

The appointed independent **Evaluation Team** performs network equipment security evaluations as defined by NESAS.

The **NESAS Group** and **Industry Specification Approval Group (ISAG)** of the GSMA are the approval bodies within the GSMA for all NESAS documentation.

3GPP SA3 defines the Security Assurance Specifications (SCAS) for the 3GPP defined Network Functions. SA3 also defines the methodology by which SA3 defines SCASes.

A **Standards Development Organisation (SDO)** defines its Network Functions and the corresponding Security Assurance Specifications (SCAS). GSMA PRD FS.50 [9] gives requirements on how to define and maintain SCASes and their expected content and structure.

NESAS Auditing Organisations are contracted to audit Vendor Development and Product Lifecycle Processes as defined by NESAS.

The appointed independent **Audit Team** performs Audits of network equipment Vendors' Vendor Development and Product Lifecycle Processes, as defined by NESAS.

Relationships between the stakeholders listed above are illustrated in Table 1 and Figure 13 below. The table is to be read beginning with an item in the first column, then a cell in the same row, and then the corresponding item in the first row. Example: Equipment Vendor sells Network Product to MNO. See Figure 12.

	MNO
Equipment Vendor	Sells Network Product to

How to read the following table:

Order of reading:

Item in left column → cell → item in top row.

Example: Equipment Vendor → sells Network Product to → MNO

Figure 12: Explanation of how to read Table 1

	Mobile Network Operator (MNO)	Equipment Vendor	NESAS Security Test Laboratory	Evaluation Team	NESAS Auditing Organisation	Audit Team	NESAS Group	3GPP SA3 or another SDO	Scheme Owner
Mobile Network Operator (MNO)	Obtains evaluated Network Product from						Can be member of	Can be member of	
Equipment Vendor	Sells Network Product to	selects	Collaborates during evaluations with	Selects	Is audited by and collaborates during audit with	Can be member of	Can be member of	Applies the specifications of the scheme from the	
NESAS Security Test Laboratory		Evaluates Network Product of		Forms and tasks			Can be member of		Is authorised by
Evaluation Team		Performs Network Product evaluation for	Works on behalf of						
NESAS Auditing Organisation		Audits			Forms and tasks	Can be member of		Is authorised by	
Audit Team		Performs Audit of processes of		Works on behalf of					
NESAS Group	Has members from	Has members from	Has members from		Has members from		Collaboratively develops NESAS with	Is open to receive feedback on NESAS specification from	
3GPP SA3 or another SDO	Has members from	Has members from				Collaboratively develops NESAS with		Has members from	
Scheme Owner			Authorises		Authorises		Collaborates with	Can be member of	

Table 1: Relationships between Stakeholders

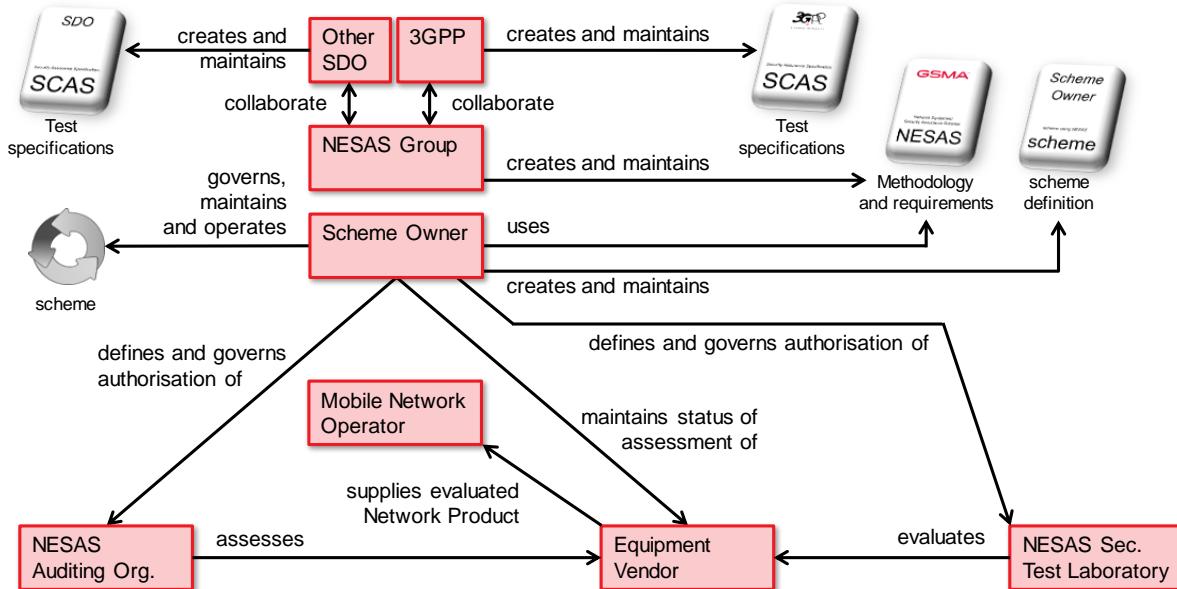


Figure 13: Illustration of relationships between NESAS Participants

9 Status of NESAS Development and Outlook

9.1 Versioning System of NESAS Specifications

NESAS publications use a versioning system by which every NESAS document has its own version number, which will only change when there are changes made to each individual document. The current NESAS is always comprised of the latest version of each of these documents. The current and previous versions of all NESAS documents can be found on the NESAS website [12].

9.2 Further Development and Extension of NESAS

NESAS is designed to be improved iteratively. All the lessons learnt from the application of NESAS will be considered and reflected in future versions. Updated NESAS documentation will reflect feedback from the various stakeholders and will strengthen NESAS's ability to support Equipment Vendors to deliver continual security improvements. This facilitates and encourages stakeholders to get involved in order to develop and evolve the scheme in a way that it satisfies their needs. Equipment Vendors that have had their processes assessed will be able to offer more secure network equipment which will benefit the mobile ecosystem.

If it is determined necessary in the future, the scope of NESAS can be extended and additional security requirements can be added to existing specifications. New network equipment types can be added to NESAS by producing and approving new corresponding SCAses against which those network equipment types can be evaluated. Additionally, Vendor Development and Product Lifecycle Processes assessment and Authorisation of NESAS Auditing Organisations and NESAS Security Test Laboratories can be extended by adding/modifying requirements as considered necessary.

NESAS specification updates are accompanied by a statement from the NESAS Group per individual NESAS document that indicates if requirements, methodologies and/or procedures are modified, added, and/or removed, and whether these changes are material or non-material.

Material and non-material changes are distinguished as follows.

Material NESAS changes are those that meet at least one of the following criteria:

- The scope has changed due to the addition, removal or modification of requirements, methodologies, procedures or any other content that covers aspects not covered previously in NESAS or that were covered differently.
- Modification of content that changes the intent of the existing specifications and documentation.

All other changes are non-material.

The current status of NESAS development and the latest versions of the NESAS documents can be obtained from the official NESAS website [12].

NOTE: The version number of a NESAS specification documents does not indicate if changes are non-material or material.

For its scheme implementation, the Scheme Owner shall define procedures to apply when NESAS specifications are updated. These procedures shall cover an assessment of the impact of material changes to determine:

- The consequences for previously performed and currently being performed Authorisations of NESAS Auditing Organisations and NESAS Security Test Laboratories, and the continuation of their validity;
- The consequences for previously performed and currently being performed Audits, and the continuation of their validity;
- If Interim Audits are possible and allowed for requirements that were added or changed in GSMA PRD FS.16;
- If Network Product Evaluations and Evidence Evaluations are to be performed and within which timeframe, if the particular scheme requires currency against the latest NESAS specifications;
- The consequences for the processes and procedures defined by the Scheme Owner based on the scheme specifications.

The Scheme Owner shall give clear advice to involved stakeholders on what they are expected to do, based on the assessment of material changes in the NESAS documentation update. The Scheme Owner shall provide this information in the scheme notes, as required in clause 0.

Non-material NESAS changes have no impact on involved stakeholders. The Scheme Owner is not expected to assess non-material changes.

9.3 Scheme Notes to be Maintained by Scheme Owner

The Scheme Owner shall maintain scheme notes for its scheme implementation that collect relevant news and updates on the scheme, which impact involved stakeholders. In particular, the assessment of the impact of at least material NESAS updates, per individual NESAS specification, and the consequences for the various stakeholders shall be stated explicitly.

9.4 Use of NESAS by Public Authorities

NESAS is designed to be recognised and used by regulatory authorities and NESAS provides the methodology, security requirements and security test cases necessary to support a robust security framework. In its current construction, NESAS does not include vendor or product certification, but does include the enablers for a certification scheme to be developed, if considered necessary, by nation states. In designing a certification scheme, the existing NESAS-defined

- Auditing organisation Authorisation,
- Security test laboratory Authorisation,
- Vendor processes and Network Product-related security requirements, and
- The vendor processes assessment and network equipment evaluation methodologies

can all be used. Thus, the only enabler that would need to be developed to support certification, is the establishment of a Certification Body and its related functions. An example of how NESAS could be augmented by the addition of certification elements and responsibilities, is illustrated in Figure 14.

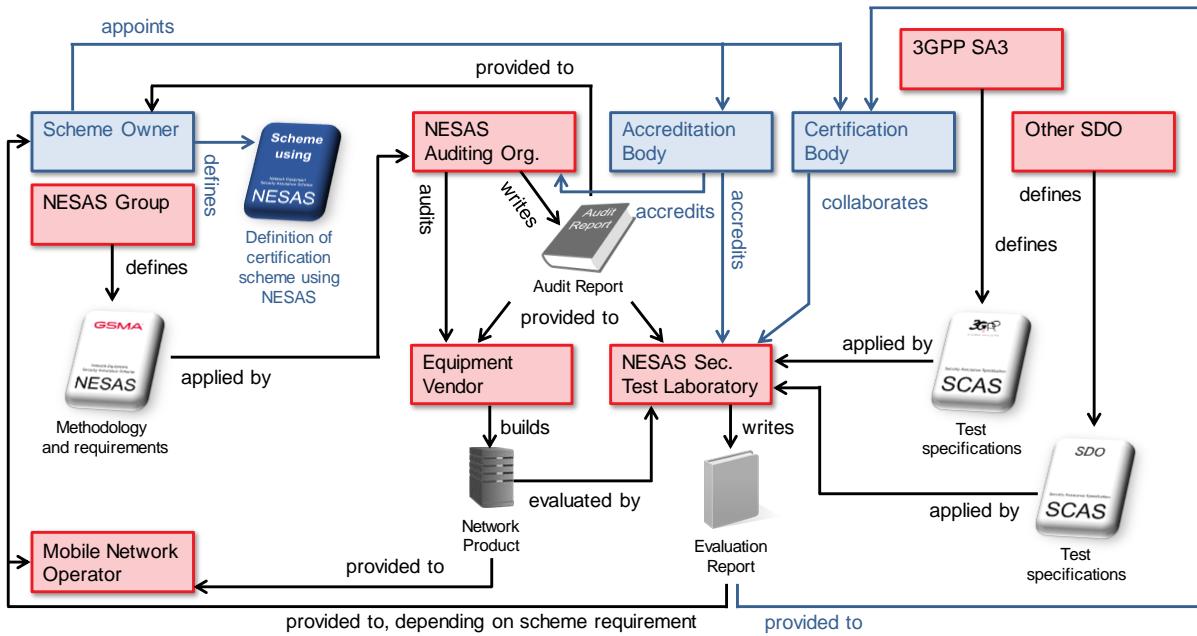


Figure 14: Example adoption of NESAS by a regulatory initiative with certification added

Scheme Owners are encouraged to ensure their scheme uses NESAS in a way that existing NESAS Auditing Organisations and NESAS Security Test Laboratories can obtain Authorisation for all existing NESAS-based schemes. This will ensure that Equipment Vendors can run assessments and evaluations once and the results can be used and recognised by all NESAS-based schemes. This will avoid fragmentation and therefore avoid hindering innovation. For the mobile ecosystem this is a critical aspect, as fragmentation would increase the effort for Equipment Vendors significantly with no discernible security benefit. A global approach has the potential to focus on effective security enhancements.

Although NESAS originated as an industry initiative, it has been developed with the needs of national authorities in mind. NESAS provides a global security baseline and assurance framework that, if supported, will avoid the risk of fragmentation and will ensure NESAS and its objective of delivering real security improvements will succeed. Stakeholders interested in NESAS and using it are invited to contact nesas@gsm.org.

History

Version	Date	Brief Description of Change
1.0	Sep 2019	Release 1 approved by NESAS Group
1.1	Aug 202	Minor clarifications added.
2.0	Feb 2021	Changes made to reflect changes to other scheme documents FS.14, FS.15 and FS.16.
2.1	Jan 2022	Changes made to reflect changes to other scheme documents FS.14 and FS.47. Migrating from NESAS Release to version numbering system for NESAS documentation. Addition of provisions pertaining to the licensing of NESAS documentation.
2.2	Oct 2022	Changes made to facilitate the introduction of fees and contract changes to place NESAS on a sustainable financial footing.
2.3	Jul 2023	Adding other SDOs to 3GPP as potential authors and maintainers of SCASes. Reference to new NESAS document FS.50 on SCAS development guidelines added. Minor editorial corrections and consistencies made.
3.0	Feb 2025	Removal of content related to the GSMA NESAS. This document defines the framework of the NESAS specifications, including NESAS methodology, requirements and guidelines. It also defines the role and tasks of the Scheme Owner. A separate document now covers the GSMA NESAS. Alignment of definitions and references and consistent use of terms across NESAS specifications. Generalisation of Authorisation of NESAS Auditing Organisations and NESAS Security Test Laboratories. Update of relationships between involved stakeholders. Minor/major NESAS updates replaced by non-material/material updates and text changed to reflect separation of specifications from scheme. Requirement on Scheme Owner to produce and maintain scheme notes added.