Network Equipment Security Assurance Scheme - Overview

Version 2.0

05 February 2021

This is a Non-binding Permanent Reference Document of the GSMA

Security Classification: Non-confidential

Copyright Notice

Disclaimer

Antitrust Notice

Table of Contents

1 Introduction

1.1 Overview

This document describes the GSMA 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. These policies can also include the application of other published GSMA security recommendations and participation in the GSMA's operational security services such as CVD [8] and T-ISAC [9].

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.

An introduction to NESAS is given in Section 0. The sections thereafter explain NESAS in more detail but still at a high level and more detailed descriptions are contained in the various documents referenced in Section 1.5.

1.2 Scope

This document has been produced for readers who want to familiarise themselves with NESAS. It provides an overview of the NESAS scheme, GSMA documents.FS.14 [4], FS.15 [5] and FS16 [6] describe NESAS in greater detail. The structure and relationship of all the documents within NESAS, including 3GPP reference documents [10] describing methodology and Security Targets can be seen in Figure 1.

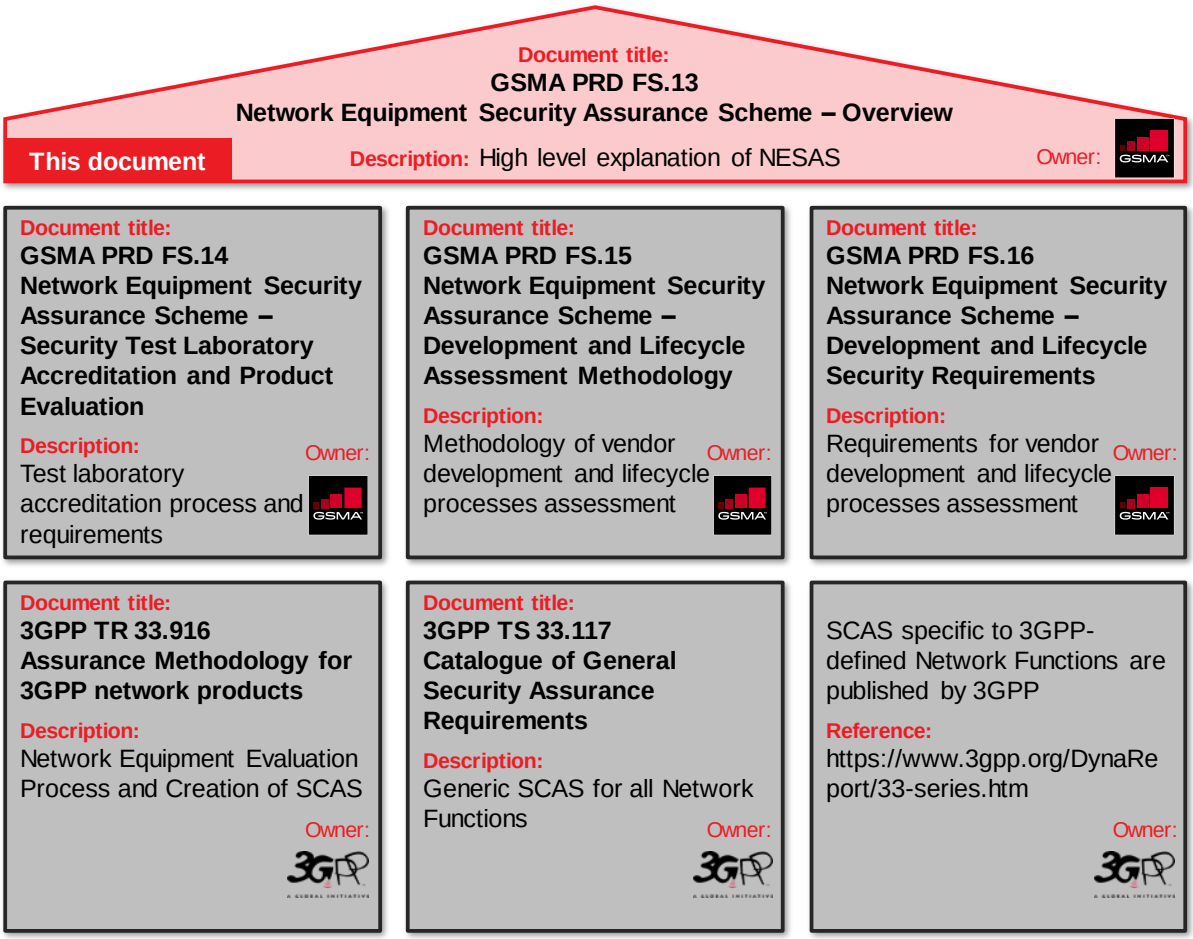

Figure 1 NESAS Documents Overview

1.3 Definitions

Term	Description
Audit	A review and assessment described in FS.15 that is undertaken and completed by an Audit Team against the requirements set out in FS.16.
Audit Report	Document presenting the results of the Audit conducted 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 undertake a Vendor Development and Product Lifecycle Processes Audit.
Auditing Organisation	Organisation selected by Equipment Vendor to conduct Audits of Vendor Development and Product Lifecycle Processes, employs or contracts Auditors.
Auditor	Individual that is qualified to perform Vendor Development and Product Lifecycle Processes Audits and makes up part of the Audit Team.
Compliance Declaration	A written statement by the Equipment Vendor that confirms it adheres to the previously assessed Development and Product Lifecycle Processes for

Term	Description
	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 Development and Product Lifecycle Processes to build the Network 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 Development and Product Lifecycle processes that are to be assessed.
Equipment Vendor	Organisation that develops, maintains and supplies to network operators network equipment that supports functions defined by 3GPP.
Equipment Vendor's 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.
Evaluation Report	Documented assessment produced by a NESAS Security Test Laboratory of the level of compliance of a Network Product with the relevant 3GPP defined Security Assurance Specification
GSMA Member	For the purpose of this document only, this is defined as a GSMA Parent Group Member, Full Member, Associate Member or Rapporteur Member.
Interim Audit	An Audit of an Equipment Vendor's 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.
ISO/IEC 17025 Accreditation Body	An ILAC member that is recognised as having competence to carry out ISO/IEC 17025 test laboratory audits
NESAS Oversight Board	The body overseeing NESAS, run by the GSMA. It is responsible for the governance of the Vendor Development and Product Lifecycle Process assessments and quality assurance of NESAS.
NESAS Dispute Resolution Process	The process used by the NESAS DRC to resolve disputes in accordance to Section 3.8
NESAS Dispute Resolution Committee (DRC)	A panel established to adjudicate on disputes pursuant to Section 3.8.
NESAS Security Test Laboratory	A test laboratory that is ISO/IEC 17025 accredited in the context of NESAS and that conducts network product evaluations. It can be owned by any entity.
Network Product	Network equipment produced and sold to network operators by an Equipment Vendor
Network Product Evaluation	An assessment, carried out by a security test laboratory, of network products against the relevant 3GPP defined Security Assurance Specification

Term	Description
Security Assurance Specification	Specification written by the 3GPP, containing security requirements and test cases for a dedicated 3GPP-defined Network Function or a group of Network Functions.

1.4 Abbreviations

Term	Description
3GPP	3rd Generation Partnership Project
CC	Common Criteria
CIS	Center for Internet Security
DLC	Development Lifecycle
ETSI	European Telecommunications Standards Institute
FASG	Fraud and Security Group
GSMA	GSM Association
ICT	Information and Communication Technology
ILAC	International Laboratory Accreditation Cooperation
ISO	International Organisation for Standardisation
IT	Information Technology
MNO	Mobile Network Operator
NESAS	Network Equipment Security Assurance Scheme
NESAS DRC	NESAS Dispute Resolution Committee
NP	Network Product
PLC	Product Lifecycle
SAS	Security Accreditation Scheme
SCAS	Security Assurance Specification
SECAG	Security Assurance Group
TR	3GPP Technical Report
TS	Technical Specification
TSG	Technical Specification Group
TTC	Telecommunication Technology Committee
WG	Working Group

1.5 References

Ref	Doc Number	Title
[1]	3GPP TR 33.916	Security Assurance Methodology for 3GPP network products
[2]	3GPP TS 33.116	Security Assurance Specification for the MME network product class
[3]	3GPP TS 33.117	Catalogue of General Security Assurance Requirements

Ref	Doc Number	Title
[4]	FS.14	Network Equipment Security Assurance Scheme – Security Test Laboratory Accreditation Requirements and Process
[5]	FS.15	Network Equipment Security Assurance Scheme – Vendor Development and Product Lifecycle Assessment Methodology
[6]	FS.16	Network Equipment Security Assurance Scheme – Vendor Development and Product Lifecycle Security Requirements
[7]	RFC 2119	"Key words for use in RFCs to Indicate Requirement Levels", S. Bradner, March 1997. Available at http://www.ietf.org/rfc/rfc2119.txt
[8]	GSMA CVD	https://www.gsma.com/security/gsma-coordinated-vulnerability-disclosure-programme/
[9]	GSMA T-ISAC	https://www.gsma.com/security/t-isac/
[10]	3GPP 33 Series	https://www.3gpp.org/DynaReport/33-series.htm
[11]	NESAS Web Site	https://gsma.com/nesas

1.6 Conventions

The key words "must", "must not", "required", "shall", "shall not", "should", "should not", "recommended", "may", and "optional" in this document are to be interpreted as described in RFC 2119 [7].

References

This icon indicates that there are references to documents that tackle the topic of the section where it appears in greater detail.

Key for the figures in this document:

Actor

Accredited actor

External entity actor

Procedure or specification

Activity

Activity

Step

Checkpoint – prerequisites must be fulfilled

2 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,
- Equipment Vendors,
- Official/Governmental information security agencies and regulators.

In many countries, Mobile Network Operators (MNO) 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 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 Auditor examines these processes and determines if they are adequate and if they are applied in practice.

  Whilst undergoing the Audit, only the Auditor 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 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.

3 NESAS Overview

NESAS is a voluntary network equipment security assurance scheme operated and maintained by GSMA, with contributions from 3GPP, covering the methodology and security targets for equipment under test. 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 independent Auditors;
4. Level of security of network equipment is tested and documented;
5. Tests are conducted by competent test laboratories against 3GPP SA3 defined security requirements;
6. Documentation can be forwarded to purchasing operators.

3.1 Lifecycle Roles and NESAS Scope

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

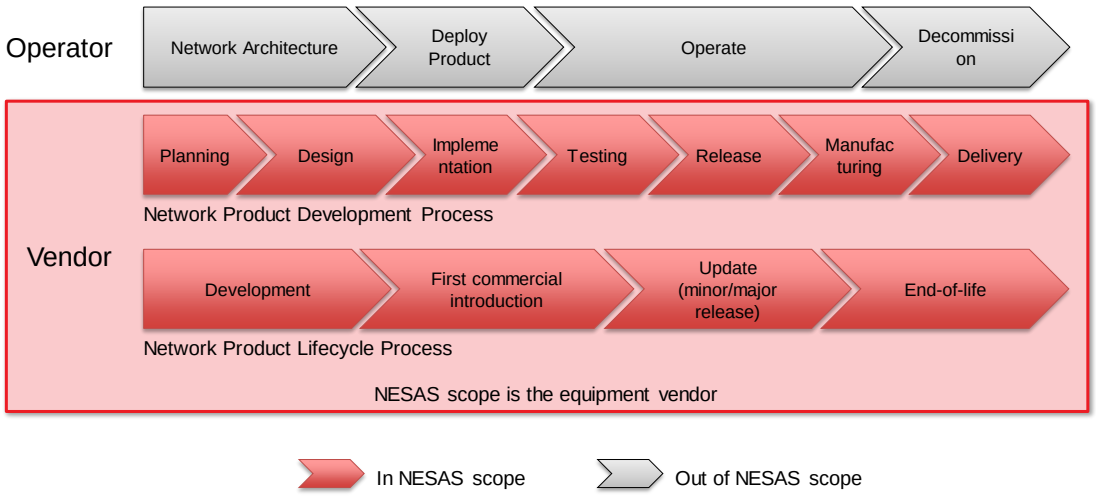

Figure 2 Responsibility, Accountability and NESAS Scope

Design, development and implementation of network equipment is undertaken 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.

3.2 Owner of and Responsibility for NESAS

The GSMA defines and maintains the NESAS specifications, which cover assessment of the Vendor Development and Product Lifecycle Processes, NESAS Security Test Laboratory accreditation, and security evaluation of network equipment. 3GPP defines security requirements and test cases for network equipment implementing one or more 3GPP network functions – specified in *Security Assurance Specifications* (SCAS). The GSMA also defines a NESAS Dispute Resolution Process. All these elements combine to form NESAS. Figure 3 illustrates the roles of 3GPP and GSMA within the scheme.

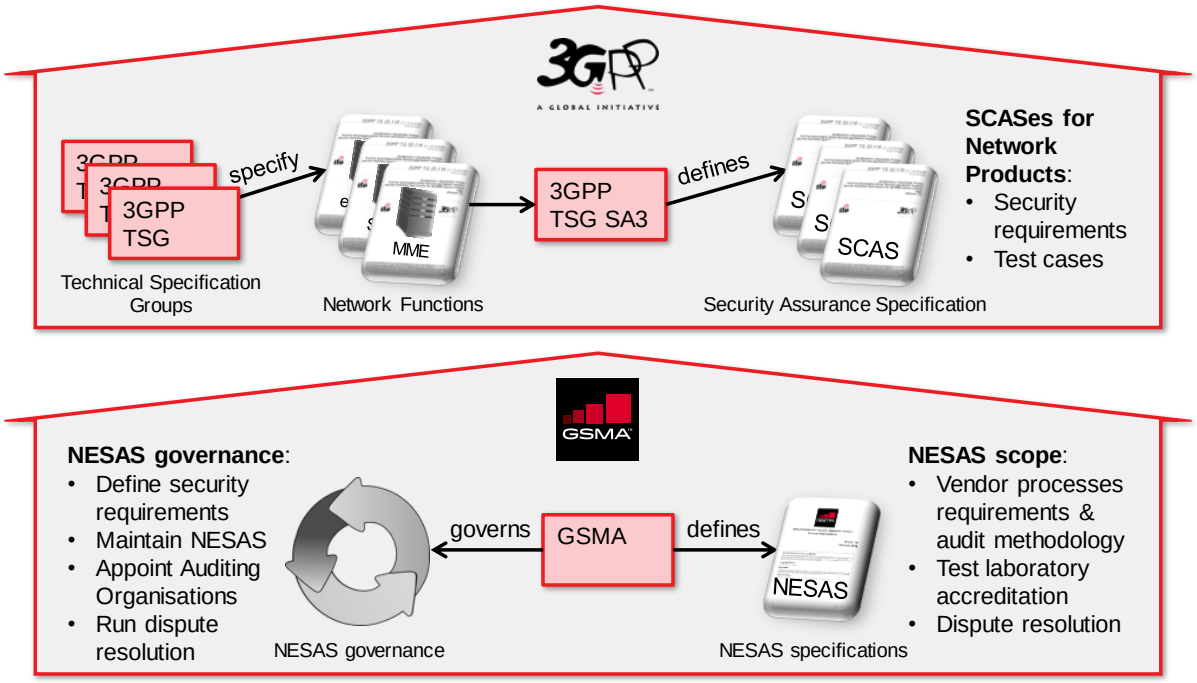

Figure 3 Roles of 3GPP and GSMA in NESAS

Network equipment that is produced and sold by an Equipment Vendor is called a *Network Product* in NESAS. A mobile base station from a particular vendor is an example of a Network Product.

3.3 NESAS High Level Overview

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

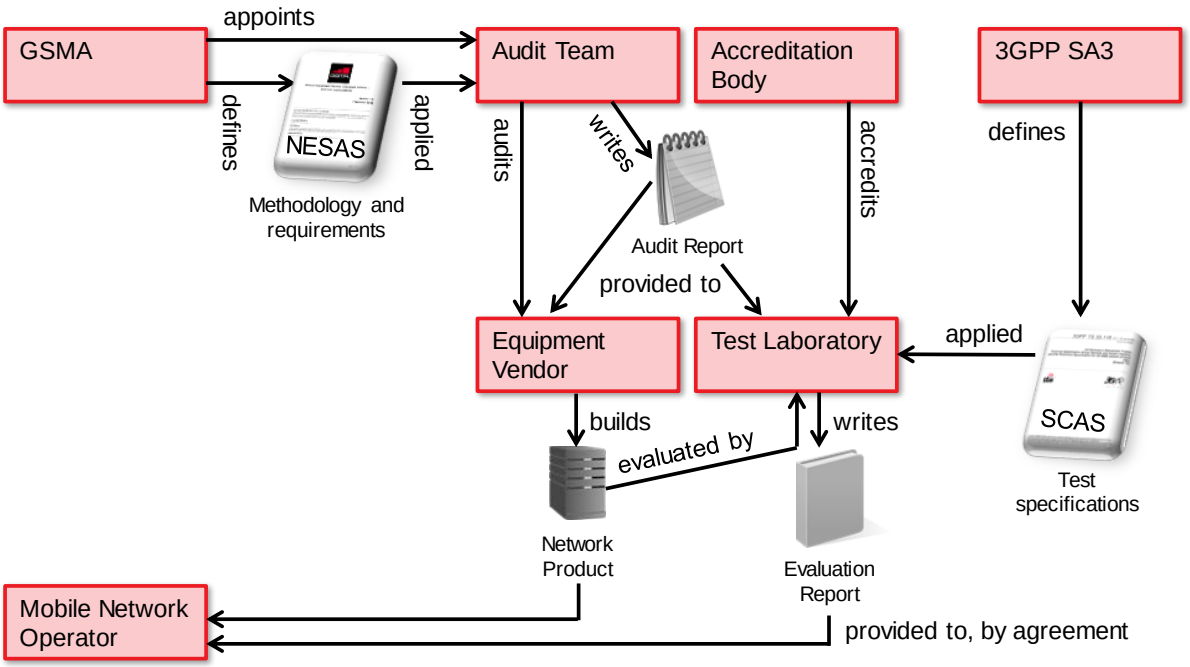

Figure 4 NESAS High Level Overview

The GSMA appoints a panel of Audit Organisations, from which participating Equipment Vendors can select one to Audit their Vendor Development and Produce Lifecycle Processes The selected Auditing Organisation appoints an Audit Team, which applies the NESAS methodology for the Audit, as defined by GSMA. 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 on the GSMA's NESAS Web Site [11].

The Equipment Vendor builds its Network Products which are given to a NESAS Security Test Laboratory for evaluation. All NESAS Security Test Laboratories are accredited by an ISO/IEC 17025 Accreditation Body that determines if the NESAS Security Test Laboratory is capable of performing meaningful Network Product tests. The chosen NESAS Security Test Laboratory evaluates the Network Product against the relevant SCASes and verifies that the internally assessed and independently audited Development and Product Lifecycle Processes of the Equipment Vendor have been applied to the tested Network Product. The NESAS Security Test Laboratory then produces an Evaluation Report.

The Audit (Summary) Report and the Network Product Evaluation Report can then be provided to customers and additional interested parties, as illustrated in Figure 5.

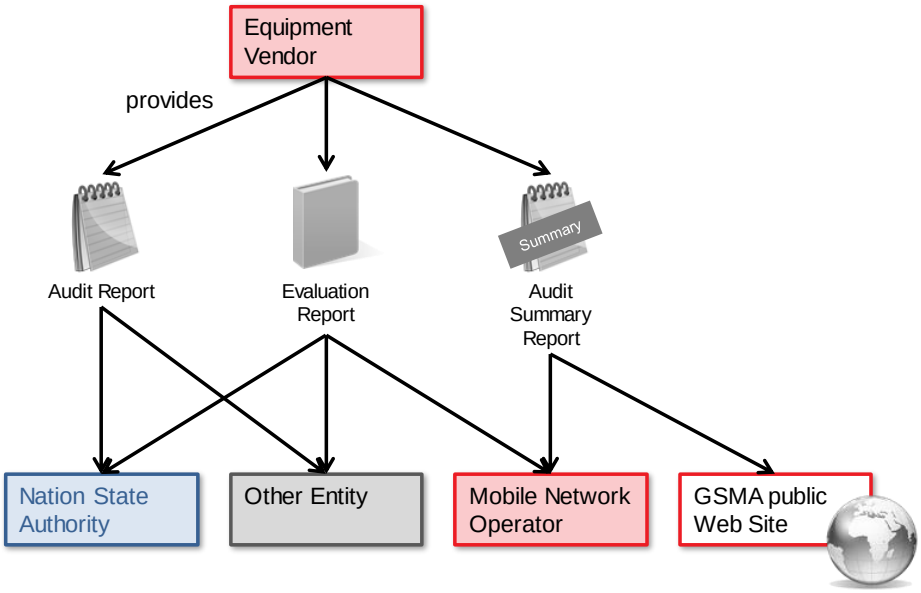

Figure 5 Potential recipients of NESAS results

3.4 Appointment of Auditing Organisations

The GSMA, with the input of the NESAS Oversight Board, has created specific criteria to select and appoint Auditing Organisations. Such appointments are made periodically as part of an open tender process.

All appointed Auditing Organisations are assigned to the panel of Auditing Organisations, from which a participating Equipment Vendor can choose an Auditing Organisation to conduct their Vendor Development and Product Lifecycle Processes assessment.

The panel of Auditing Organisations consists of two (2) Auditing Organisations. Currently appointed Auditing Organisations are listed on the NESAS Web Site [11].

3.5 Accreditation of NESAS Security Test Laboratories

NESAS Security Test Laboratories need to be accredited in accordance with ISO/IEC 17025 [16], which covers general requirements on testing procedures, documentation, maintenance and review of procedures, competence, independence, and impartiality. They can be owned by any entity.

As ISO/IEC 17025 is a generic accreditation, test laboratories are always accredited in the context of additional standards against which the laboratories will perform their tests. For NESAS, this means that laboratories need to demonstrate that, as well as holding ISO/IEC 17025 accreditation, they are capable of performing tests described in NESAS SCASes and that they meet the additional requirements applicable to NESAS.

An officially recognised ISO/IEC 17025 Accreditation Body is required to Audit and accredit test laboratories. On successful completion of the Audit, the test laboratory becomes an accredited NESAS Security Test Laboratory. This process is illustrated in Figure 6.

The validity of NESAS Security Test Laboratory accreditation is defined by ISO/IEC 17025.

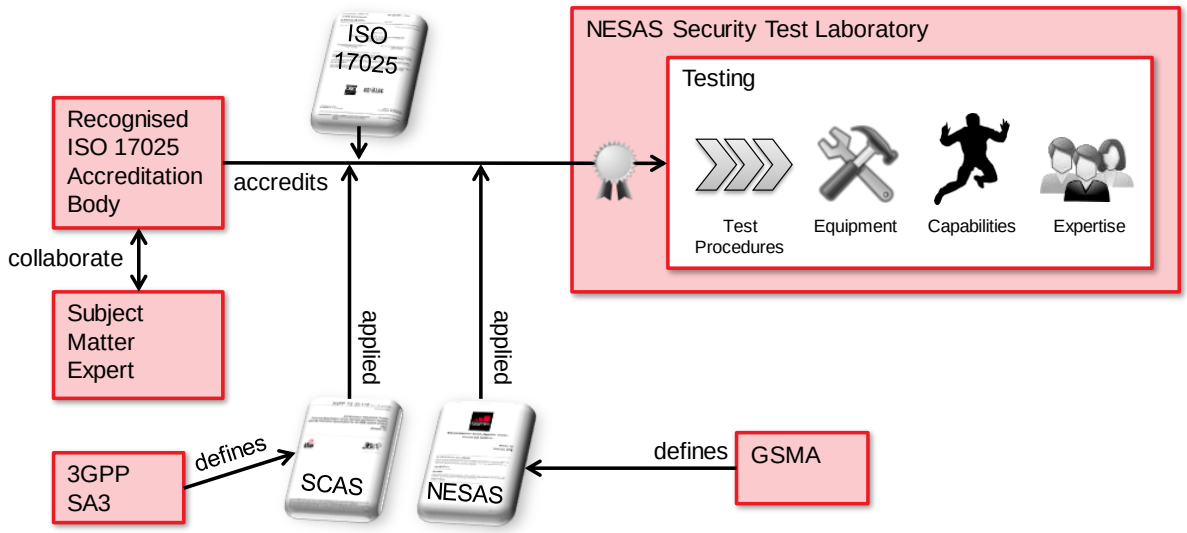

Figure 6 Accreditation of Test Laboratories

References

- FS.14 [4] defines test laboratory accreditation requirements and the process of performing the Audit and accreditation.
- SCASes of the 3GPP (e.g. the generic SCAS for any network equipment TS 33.117 [3]) contain test specifications the NESAS Security Test Laboratory must be capable of performing. All current SCASes can be found at the NESAS Web Site.
- 3GPP TR 33.916 [1] describes the methodology to create and maintain SCASes.

3.6 Assessment of Vendor Development and Product Lifecycle Processes

Figure 7 depicts, at a high level, the steps the assessment of Vendor Development and Product Lifecycle Processes consist of.

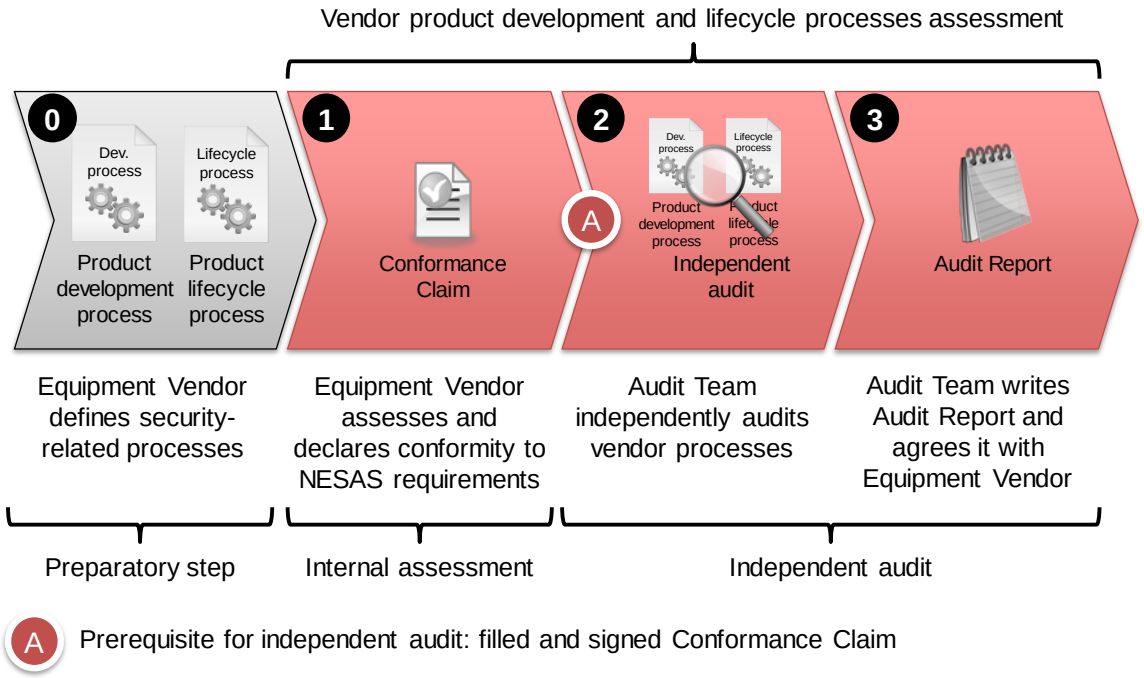

Figure 7 Sequence of activities of vendor processes assessment

As a preparatory step (Step 0 in Figure 7), 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 7: The Equipment Vendor defined processes are first internally assessed by the participating Equipment Vendor, which must 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 7).

Step 2 in Figure 7: Subsequently, the Development and Product Lifecycle processes are audited by one of the GSMA appointed Auditing Organisations. The Equipment Vendor contracts directly with the chosen Auditing Organisation. The Audit Team follows the auditing methodology, defined by NESAS, and determines compliance of the Equipment Vendor to the NESAS requirements.

Audits consist of off-site process documentation reviews and on-site Audits. In exceptional circumstances where travel restrictions prevent the Auditors from attending product development sites at which Audits should be conducted, remote Audits may be performed with prior consultation with, and approval of GSMA.

Step 3 in Figure 7: The Audit Team produces an Audit Report that contains the results of the Audit and recommendations. The Audit Report must be agreed with the Equipment Vendor and be signed by both parties. It must also be made available to GSMA, 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 on the NESAS Web Site [11] for the purposes of highlighting NESAS participation by the Equipment vendor.

The assessment of the Vendor Development and Product Lifecycle processes is depicted in Figure 8.

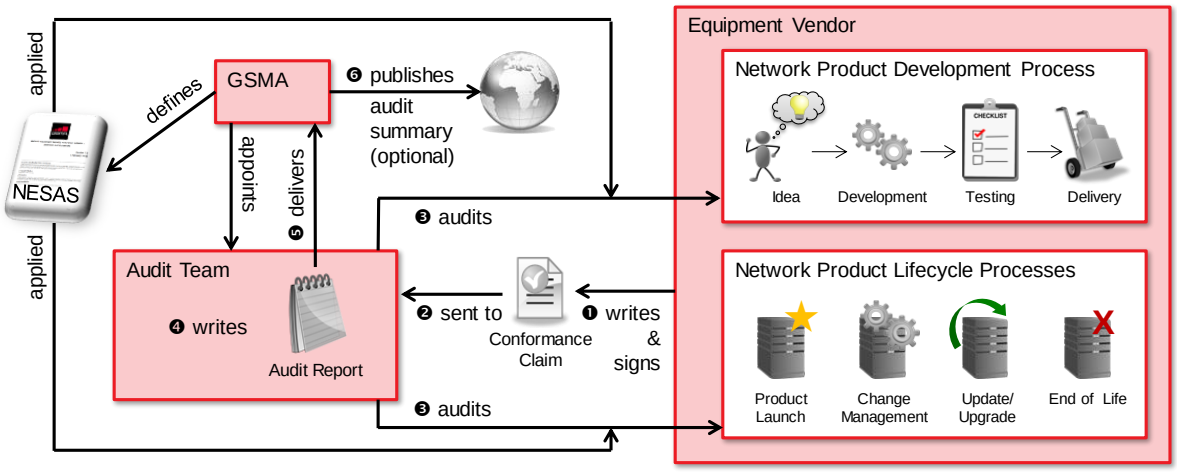

Figure 8 Assessment of vendor processes

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 lasts at most two years and may expire earlier if the assessed vendor processes change. Audits are always to be conducted against the current NESAS Release.

NESAS is a living scheme, so it is to be expected that security requirements will be added or changed. 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 undertake 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 process have not changed substantially, until the next full Audit of its Development and Product Lifecycle processes falls due. Further details about Interim Audits can be found in FS.15 [5].

References

- FS.15 [5] defines the Vendor Development and Product Lifecycle Process assessment methodology, which describes the process of performing the internal assessment and independent Audit.
- 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.

3.7 Network Product and Evidence Evaluation

Once an Equipment Vendor's Development and Product Lifecycle Processes internal assessment and Audit result in full compliance to the the NESAS security requirements defined in GSMA PRD FS.16 [6], Network Products can be evaluated by an accredited NESAS Security Test Laboratory. Full compliance to the NESAS security requirements is a prerequisite for Network Product Evaluation (Checkpoint B in Figure 9)

Figure 9 depicts at a high level the steps Network Product and Compliance Evidence evaluation consists of.

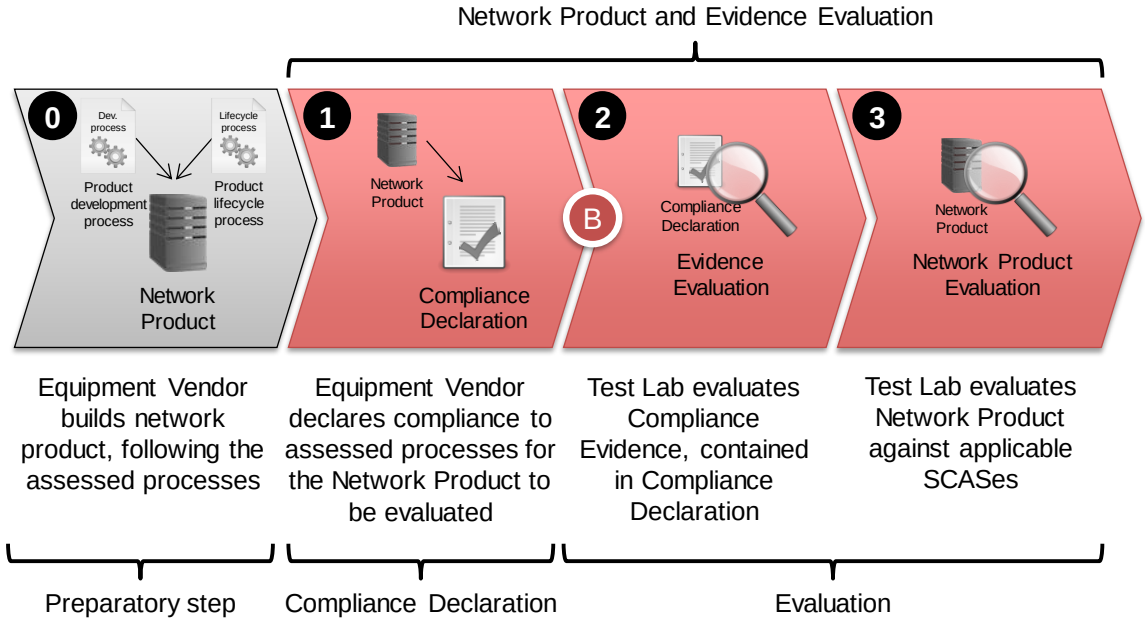

Figure 9 Sequence of activities of Network Product and Evidence evaluation

As a preparatory step (Step 0 in Figure 9), the Equipment Vendor builds the Network Product in full accordance to the previously assessed Development and Product Lifecycle processes.

For evaluation, the Equipment Vendor chooses an accredited NESAS Security Test Laboratory and contracts directly with it. The Compliance Declaration contains all the Compliance Evidence for theNetwork Product under evaluation, broken down for each of the security requirements as defined in FS.16 [6].

Once this is done, the Equipment Vendor provides the Network Product and Compliance Declaration to the NESAS Security Test Laboratory.

Step 2 in Figure 9: The NESAS Security Test Laboratory 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 Network Product under evalaution. The Audit Report that was produced during the Equipment Vendor Development and Product Lifecycle Process 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 must provide a rationale instead, giving reasons. The results of Evidence evaluation are recorded in an Evaluation Report.

Step 3 in Figure 9: Test specifications from the corresponding SCASes are used to create and run detailed tests for the Network Product. SCASes to be selected for evaluation depend on the functionality provided by the Network Product under Evaluation. Preparation of the test environment and configuration of the Network Product under evaluation are defined in the SCASes. Test results are added to the Evaluation Report. Test results must 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 and Evidence Evaluation are illustrated in Figure 10 in more detail.

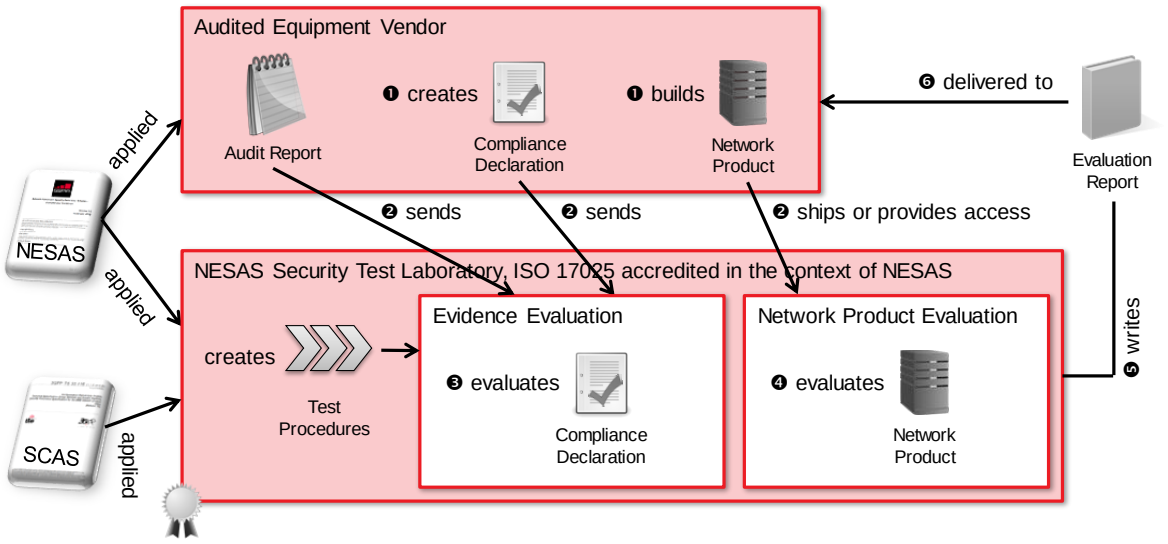

Figure 10 Evaluation of a Network Product and Compliance Evidence

The completed Evaluation Report is handed over to the Equipment Vendor. The Equipment Vendor can then provide the Evaluation Report to any interested MNO together with the Network Product when supplying equipment. A copy of the Evaluation Report is provided to GSMA, if the evaluated product is to be listed on the NESAS Web Site [11].

Each Network Product Evaluation is bound to a dedicated release of the Network Product and to a dedicated NESAS Release. The Evaluation Report does not expire. A new release of the Network Product or of NESAS will trigger the need for an up-to-date evaluation.

It is at the discretion of the MNO to determine from the Evaluation Report if the level of security that is reached by the Network Product is sufficient for deployment in the mobile network.

References

- FS.14 [4] defines how Network Product evaluation and Evidence Evaluation are performed.
- FS.16 [6] defines the Compliance Evidence the vendor is obliged to provide to the NESAS Security Test Laboratory for Evaluation.
- SCASes of the 3GPP (e.g. the generic SCAS for any network equipment TS 33.117 [3]) contain test specifications the Test Laboratory must perform for Network Product evaluation. All current SCASes can be found at the NESAS Web Site.
- 3GPP TR 33.916 [1] describes the methodology to create and maintain SCASes.

3.8 Dispute Resolution

3.8.1 NESAS Dispute Resolution Process (NESAS DRP)

The Network Equipment Security Assurance Scheme Dispute Resolution Committee (NESAS DRC) acts to handle disputes that may arise with regards to the implementation and/or interpretation of NESAS documentation that could be subject to disagreements between two or more parties. The NESAS DRC shall be appointed on a per dispute basis to ensure each dispute is handled in a non-partisan manner.

Disputing parties shall use all resources reasonably available to resolve disputes before involving the NESAS DRC.

Subject to the above, the GSMA must only be contacted if there is a dispute between two or more parties with respect to the interpretation and implementation of NESAS procedures or documentation.

The NESAS Dispute Resolution Process (DRP) can be invoked by the requesting parties sending a written request (e-mail) to the appropriate GSMA designated contact who, upon review, will forward the written request to all other parties involved in the dispute, giving all the respondent parties the opportunity to comment on the wording of the invocation.

Upon the opportunity for parties to comment, if the dispute cannot be resolved within a period of no more than twenty (20) calendar days:

(i) The requesting party may invoke the NESAS DRP; and

(ii) All parties concerned are asked to supply all arguments and points of view in relation to the matter to the GSMA. The GSMA in turn will supply the same to the respective NESAS DRP upon its formation.

At the time of invoking the NESAS DRP, the GSMA should determine if a similar dispute has been previously resolved by the NESAS DRC. If such a dispute has previously been ruled on and published, the affected parties may decide to follow the decision made.

For each dispute, the NESAS DRC shall consist of three individuals who have not been directly involved in the matter and who are not employees of entities that may be affiliated either with the appellant or a respondent company group.

The appellant(s) shall appoint one impartial member of the NESAS DRC. The named respondent(s), shall also appoint one impartial member. When more than one respondent is named, the respondents will collectively agree on the appointment of a single member. The appellant and the respondent(s) must each identify their appointed panel member within five (5) business days of the GSMA's determination that a hearing is necessary. The two members so selected by the parties shall then appoint the third member; this appointment of the third member shall occur within ten (10) business days of the determination that an adjudication is necessary.

Disputing parties shall use all resources reasonably available to resolve disputes before involving the NESAS DRC. All parties involved should identify the disputed issue(s) in advance in order to have a common understanding of the issue(s). All parties involved in the dispute should agree on the wording of the NESAS DRC invocation, including the time at which the issue causing the dispute occurred.

For the purpose of the NESAS Dispute Resolution Process (DRP), the GSMA will, to the extent available and accessible, provide to the appellant and respondent the relevant NESAS documentation in effect at the time of the dispute. Later versions of these documents may also be considered upon request, if relevant to the dispute.

The NESAS DRC must proceed according to the Dispute Resolution Process (DRP) and may provide additional guidelines and/or define further proceedings as it may deem necessary for the achievement of a resolution. The NESAS DRC will use reasonable commercial efforts to seek to resolve disputes as soon as practical and without undue delay (normally within ten (10) days of the notification). A majority decision must then be made by the NESAS DRC members.

The GSMA is responsible for the distribution of the NESAS DRC ruling/decision in writing.

The NESAS DRC ruling/decision is binding between the Parties involved in the NESAS Dispute Resolution Process at the time of the dispute as agreed during the invocation of the NESAS Dispute Resolution Process.

Rulings/decisions of the NESAS DRC could vary in terms of their nature and severity and could result in sanctions such as the revocation of product evaluations held by vendors or test lab accreditations. Sanctions to be imposed, if any, are entirely a matter for the NESAS DRC to decide on.

Any ruling/decision of the NESAS DRC may be anonymised, shared with the NESAS Oversight Board and used as an example for improving the current NESAS scheme as long as it is not attributable to a particular involved party.

Note: In the event that a need to change NESAS documentation has been identified as a result of the decision, the NESAS DRC must refer the case to the NESAS Oversight Board, which will develop the appropriate change request and propose it to the relevant document approval authority.

The NESAS DRP shall be administered and documented by the GSMA, as the GSMA deems appropriate.

3.8.2 Possible Dispute Scenarios

The GSMA neither assesses, reviews nor interprets the received Audit Report, the Evaluation Report, and the Audit Summary Report in any way. The GSMA keeps the Audit Report and the Evaluation Report confidential in case a dispute is filed by an involved stakeholder which could lead to the invocation of the NESAS Dispute Resolution Process. Should any involved party see the need to challenge any decision of an Audit Team, or a NESAS Security Test Laboratory, it may refer the matter to the NESAS Dispute Resolution Process. Similarly, should any party see the need to challenge the Audit Guidelines, it may refer the matter to the NESAS Oversight Board. The following table illustrates a number of possible dispute scenarios that could arise within the Security Test Laboratory accreditation element of NESAS that involve a variety of parties. The table merely captures example scenarios and is not intended to be exhaustive.

	Operator	Vendor	Audit Team	Test Lab	NESAS OB
Operator		NP or development and lifecycle process security inconsistency	Vendor assessment undertaken by Audit Team and challenged by operator		Operator believes SCAS is inadequate or challenges Audit Team competency
Vendor	NP or development and lifecycle process security inconsistency		Audit Team assessment disputed by vendor	Test lab refuses product evaluation or evaluation results are disputed by vendor	SCAS documentation ambiguous or not fit for purpose
Audit Team	Vendor assessment undertaken by Audit Team and challenged by operator	Audit Team assessment disputed by vendor			Audit Team has concerns about NESAS document quality
Test Lab		Test lab refuses product evaluation or evaluation results are disputed by vendor			SCAS documentation ambiguous or not fit for purpose
NESAS Oversight Board (OB)	Operator believes SCAS is inadequate or challenges Audit Team competency	SCAS documentation ambiguous or not fit for purpose	Audit Team has concerns about NESAS document quality	SCAS documentation ambiguous or not fit for purpose	

Table 1 Example Dispute Scenarios

3.8.3 Matters outside the Scope of NESAS DRC

The NESAS DRP only deals with disputes in respect to the interpretation and implementation of NESAS or its documentation. Any dispute with regards to the facts, findings or recommendations of an evaluation report should be resolved between the respective NESAS Security Test Laboratory and Equipment Vendor.

3.8.4 Liability of the NESAS DRC Members

Any ruling by the NESAS DRC is undertaken “as is” with no liability (e.g. for the correctness nor for any damages caused by or resulting from any decision/ruling made by the NESAS DRC) to the GSMA, any NESAS DRC members, GSMA staff members or NESAS Oversight Board or GSMA members.

As a condition to invoking the NESAS DRP, the appellant agree to hold the GSMA and the aforementioned individuals involved in rendering a ruling/decision harmless from any and all liabilities or damages arising from or related to the appellants invocation of the NESAS Dispute Resolution Process and associated matters.

References

FS.14 [4] and FS.15 [5] follow the NESAS dispute resolution process defined here. Stakeholders who raise a dispute need to follow this process.

3.9 Extent of NESAS

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

1. Assessment of vendors' Development and Product Lifecycle processes;
2. Network equipment product evaluation by competent NESAS security Test Laboratories using 3GPP 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. There is no certification of Equipment Vendors or network equipment by an officially recognised authority.
2. It is generally acknowledged that the absence of undocumented functionality (e.g. backdoors, malware, etc.) cannot be proved 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.

3.10 Governance

NESAS is governed by the provisions set out in FS.13 (this document), FS.14 [4], FS.15 [5] and FS.16 [6]. Save in the case of Section 3.8 in FS.13, in case of any conflict between FS.14 [4], FS.15 [5] and FS.16 [6] or any other provisions in other NESAS documentation, FS.14 [4], FS.15 [5] and FS.16 [6] shall prevail.

4 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 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, conducted by competent accredited 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 wll 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 Section 6.

NESAS reuses mature accreditation models which deliver security gains and improvements whilst keeping work and costs for all stakeholders at manageable levels.

5 Involved Stakeholders, their Roles and Relationships

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

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 (NE) 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 **Network Equipment Vendors**. Network equipment vendors have predefined secure 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 **GSMA** has multiple roles in NESAS:

1. The **Fraud & Security Group** (**FASG**) Working Group (WG) of the GSMA is the approval body within the GSMA for all NESAS documentation.
2. The **NESAS Oversight Board** shall have overall responsibility for Audit quality control.
3. The **NESAS Dispute Resolution Committee** is established whenever a dispute is to be resolved according to the NESAS defined processes.
4. **GSMA staff** manage and operate NESAS on a daily basis providing support to the **NESAS Oversight Board**.

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

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

A national **ISO/IEC 17025 Accreditation Body** accredits test laboratories upon request against ISO/IEC 17025 in the context of NESAS.

The ISO/IEC 17025 Accreditation Body is supported by a **Subject Matter Expert** who is experienced in all the NESAS related technical details, such as mobile networks, network and equipment security, and testing of network equipment and network services.

Relationships between the stakeholders listed above are illustrated in Table 2 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: NESAS Oversight Board appoints Auditor Team. See Figure 11.

	Audit Team
NESAS Oversight Board (AB)	Appoints and assigns disputes to

How to read the following table:

Order of reading:
Item in left column → cell → item in top row.

Example: NESAS Oversight Board → appoints → Audit Team

Figure 11 Explanation of how to read the table below

	MNO	Vendor	Test Lab	GSMA FASG	NESAS OB	NESAS DRC	GSMA	3GPP SA3	Auditing Organisation/Audit Team	IAB	SME
Mobile Network Operator (MNO)		Obtains evaluated Network Product		Can be member of	Can be member of	Can raise disputes to		Can be member of			
Equipment Vendor	Sells Network Product to		Assigns for Network Product evaluation	Can be member of	Can be member of	Can raise disputes to		Can be member of	Selects, contracts with and Is audited by		
NESAS Security Test Laboratory (Lab)		Performs Network Product evaluation for				Can raise disputes to				Is accredited by	Is audited by
GSMA Fraud & Security Group (FASG)	Has members from	Has members from			Establishes			Collabo-ratively develops NESAS with			
NESASOversight Board (OB)	Has members from	Records participation of					Is supported by		Appoints and assigns disputes to		
NESAS Dispute Resolution Committee (DRC)	Handles disputes with	Handles disputes with	Handles disputes with		Forwards decisions to		Forwards decisions to		Handles disputes with		
GSMA		Contracts with and maintains status of	Maintains status of		Supports	Supports			Coordinates	Is available for inquiries from	Is available for inquiries from
3GPP SA3	Has members from	Has members from		Collabo-ratively develops NESAS with							
Auditing Organisation/Audit Team		Audits and adjudicates on disputes				Can raise disputes to	Reports to				
ISO/IEC 17025 Accreditation Body (IAB)			Accredits								Collaborates with
Subject Matter Expert			Audits							Collaborates with	

Table 2 Relationships between Stakeholders

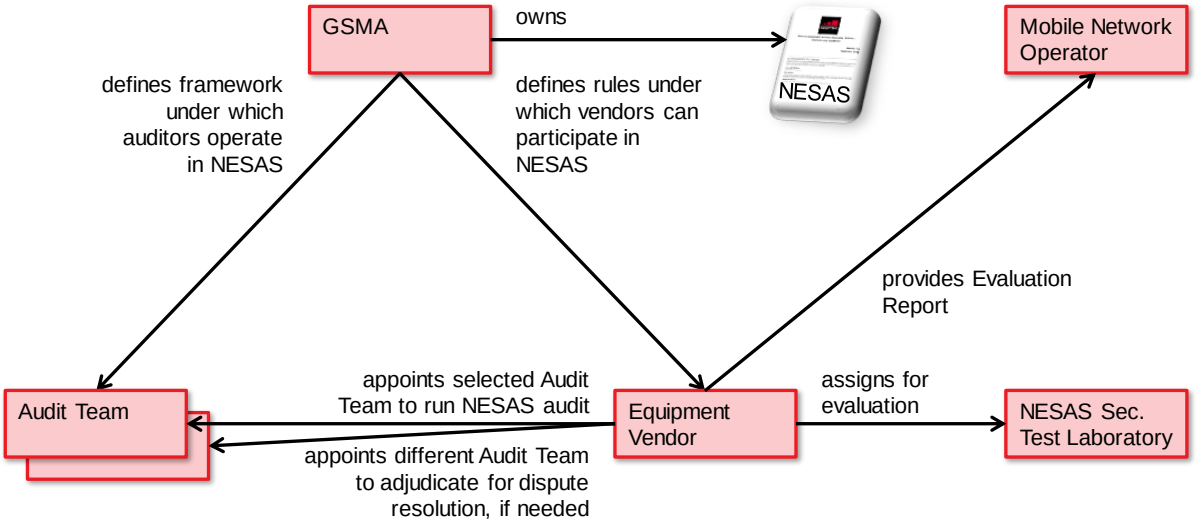

Figure 12 Relationships between NESAS Participants

6 Status of NESAS Development and Outlook

NESAS has been released in its second official release. It is called “NESAS Release 2”. All NESAS documents (FS.13 (this document), FS.14 [4], FS.15 [5] and FS.16 [6]) in a particular version comprise a NESAS Release. The official NESAS Web Site [11] provides a mapping of NESAS Releases to NESAS documentation, recognising that Release numbering and document version numbering are distinct and independent of each other. For that reason, each NESAS document will clearly state which Release(s) it applies to and this information is presented in a table in a document annex.

NESAS is designed to be improved iteratively. All the lessons learnt from the application of NESAS will be considered and reflected in future releases. Updated releases will take feedback from the various stakeholders into account and will also strengthen NESAS’s ability to support Equipment Vendors to deliver continual security improvements. This facilitates and encourages stakeholders to get involved in order to help develop 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.

Future NESAS Releases are either minor or major. They are distinguished as follows.

Minor NESAS Releases are those that meet at least one of the following criteria:

- Editorial changes
- Error corrections, additions or modifications that provide clarity on matters previously unclear.
- Changes to informative content that do not result in material changes to the intent of the existing NESAS scheme and its documentation.
- Is not classified as a major change.

NOTE: Assessments that have been conducted against the major release against which they were undertaken remain valid after a minor release has been published.

Major NESAS Releases are those that meet at least one of the following criteria:

- The scope has changed due to the addition, removal or material modification of requirements, procedures or any other content that covers aspects not covered in previous NESAS releases.
- Modification of content that materially changes the intent of the existing scheme and its documentation.

NOTE: After a major release has been published, assessments that have been conducted against the previous major release remain valid but only against that Release. To achieve currency and relevancy to newer NESAS Releases, assessments will need to be undertaken against the prevailing Release.

Minor releases are indicated by an increment of the release number behind the dot, whereas major releases increment the release number before the dot i.e. if NESAS Release 1.0 is the current release, a minor release will be numbered 1.1 and a major release will be numbered 2.0.

The current status of NESAS development and the latest versions of the NESAS documents can be obtained from the official NESAS Web Site [11].

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 the scheme by producing and approving new corresponding SCASes. Additionally, Equipment Vendor Development and Product Lifecycle process assessment and NESAS Security Test Laboratory accreditation can be extended by adding/modifying requirements as considered necessary.

NESAS is designed to be recognised and adopted by regulatory authorities and the scheme 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 appointment,
- Test Laboratory accreditation,
- Vendor processes and Nework Product-related security requirements, and
- the vendor processes assessment and product 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 13.

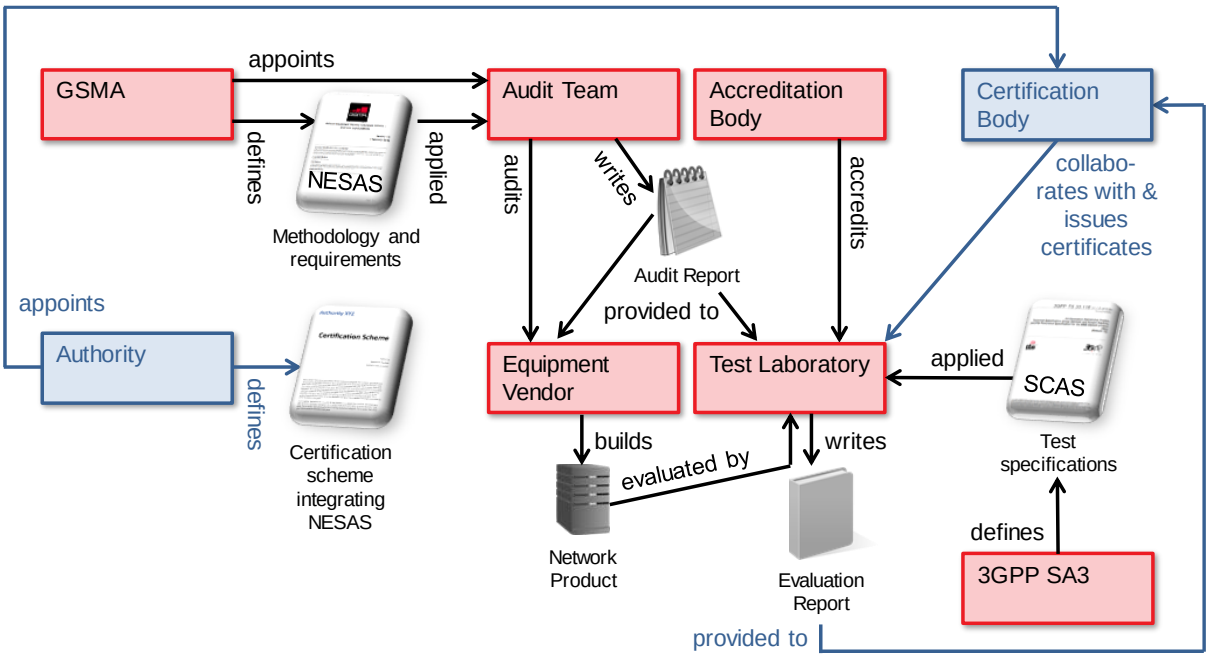

Figure 13 Example adoption of NESAS by a regulatory initiative with certification added

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 the scheme and its objective of delivering real security improvement will succeed. Stakeholders interested in NESAS and adopting it are invited to contact nesas@gsma.com.

Annex A Document Management

A.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	Sep 2019	Release 1 approved by SECAG	GSMA TG	James Moran / GSMA
1.1	Aug 2020	Minor clarifications added	GSMA FASG	James Moran / GSMA
2.0	Feb 2021	Changes made to reflect changes to other scheme documents FS.14, FS.15 and FS.16	GSMA FASG	James Moran / GSMA

A.2 Document and NESAS Release Mapping History

Document Version	Applicable NESAS Release
1.0	NESAS 1.0
1.1	NESAS 1.1
2.0	NESAS 2.0

A.3 Other Information

Type	Description
Document Owner	GSMA SECAG
Editor / Company	James Moran / GSMA

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at nesas@gsma.com.

Your comments or suggestions & questions are always welcome.