



## Network Equipment Security Assurance Scheme Overview

Version 0.3

11 May 2016

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

---

### **Security Classification: Non-confidential**

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is confidential to the Association and 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 © 2016 GSM Association

### **Disclaimer**

The GSM Association ("Association") 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.

### **Antitrust Notice**

The information contain herein is in full compliance with the GSM Association's antitrust compliance policy.

## Table of Contents

<b>1</b>	<b>Introduction</b>	<b>3</b>
1.1	Overview	3
1.2	Scope	3
1.3	Definitions	4
1.4	Abbreviations	5
1.5	References	5
1.6	Conventions	6
<b>2</b>	<b>Introduction to Security Assurance in the Mobile Industry and NESAS</b>	<b>6</b>
<b>3</b>	<b>NESAS Overview</b>	<b>7</b>
3.1	Product Development and Lifecycle	8
3.2	NESAS High Level Overview	9
3.3	Accreditation of Vendor Processes	10
3.4	Accreditation of NESAS Security Test Laboratories	11
3.5	Network Equipment Evaluation	12
3.6	Dispute Resolution	13
3.7	Scope of NESAS	14
<b>4</b>	<b>NESAS Benefits</b>	<b>14</b>
<b>5</b>	<b>Involved Stakeholders, their Roles and Relationships</b>	<b>15</b>
<b>6</b>	<b>Status of NESAS Development and Outlook</b>	<b>17</b>
<b>Annex A</b>	<b>Document Management</b>	<b>19</b>
A.1	Document History	19
A.2	Other Information	19

# 1 Introduction

## 1.1 Overview

This document describes NESAS – the Network Equipment Security Assurance Scheme. NESAS will provide “out of the box” security assurance to operators and vendors, ensuring a common baseline security level for the industry. In addition, it is expected that NESAS will help vendors to avert fragmented regulatory and network operator customer requirements.

An introduction to NESAS is given in Section 2. 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 is one in a series that define NESAS. The present document is an overview document that describes NESAS and that provides references to the other relevant documents, which describe the different aspects and processes of NESAS in greater detail. The structure and relationship of documents to the various elements can be seen in Figure 1.

This document has been produced for readers who want to familiarise themselves with NESAS.

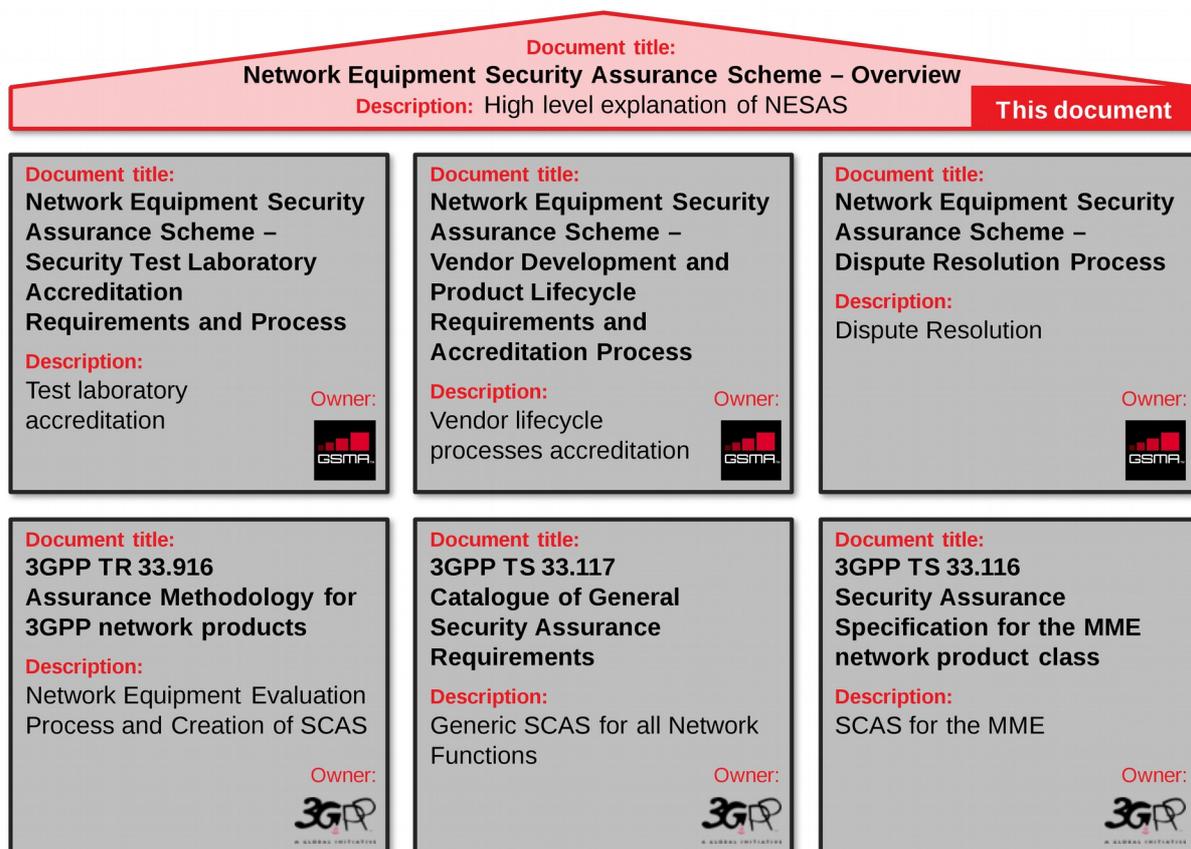


Figure 1 NESAS documents overview

### 1.3 Definitions

Term	Description
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
Evidence	The rationale created by the Equipment Vendor that allows the NESAS Security Test Laboratory to assess and measure compliance with the vendor's accredited internal processes when building the Network Product that are included in the Evaluation Report.
GSMA Audit Report	Document summarizing the results of the audit conducted at the Equipment Vendor by the GSMA Audit Team
GSMA Audit Team	Audit personnel used by GSMA to conduct Equipment Vendor audits
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.
ISO 17025 Accreditation Body	An ILAC member that is recognised as having competence to carry out ISO 17025 test laboratory audits
NESAS Accreditation Board	Responsible for developing requirements on vendor network product development, network product lifecycle management process, and NESAS accreditation of vendors and NESAS security test laboratories.
NESAS Dispute Resolution Process	The process used by the NESAS DRC to reach a ruling/decision.
NESAS Dispute Resolution Committee (DRC)	The impartial interpreter of NESAS processes and documentation that is required to adjudicate on disputes that may arise between two or more Parties.
NESAS Security Test Laboratory	A vendor owned or third party owned test laboratory that conducts network product evaluations
Network Product	Network equipment produced and sold to network operators by an Equipment Vendor
Network Product Development Lifecycle	The stages through which products journey throughout their development including planning, design, implementation, testing, release, production and delivery.
Network Product Lifecycle	The stages through which developed products journey to end of life including maintenance and update releases during their lifetime.
Network Product Evaluation	An assessment, carried out by a security test laboratory, of network products against the relevant 3GPP defined Security Assurance Specification

### 1.4 Abbreviations

Term	Description
3GPP	3 <sup>rd</sup> Generation Partnership Project
CC	Common Criteria

Term	Description
CIS	Center for Internet Security
DLC	Development Lifecycle
ETSI	European Telecommunications Standards Institute
GSM	Global System for Mobile Communications
GSMA	GSM Association
ICT	Information and Communication Technology
ILAC	International Laboratory Accreditation Cooperation
ISO	International Organisation for Standardisation
IT	Information Technology
LTE	Long Term Evolution
MNO	Mobile Network Operator
NESAS	Network Equipment Security Assurance Scheme
NESAS DRC	NESAS Dispute Resolution Committee
PLC	Product Lifecycle
SAS	Security Accreditation Scheme
SCAS	Security Assurance Specification
SIM	Subscriber Identity Module
TS	Technical Specification
TSG	Technical Specification Group
TTC	Telecommunication Technology Committee
UMTS	Universal Mobile Telecommunications System
WCDMA	Wideband Code Division Multiple Access
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
[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 Requirements and Accreditation Process
[6]	FS.16	Network Equipment Security Assurance Scheme – Dispute Resolution Process
[7]	GSMA NESAS WI 4a Doc	Network Equipment Security Assurance Scheme – Request for Information; to be published in April 2016
[8]	GSMA NESAS WI 4b Doc	Network Equipment Security Assurance Scheme – Request for Proposal; to be published in June 2016
[9]	GSMA NESAS WI 5 Doc	Network Equipment Security Assurance Scheme – Pilot Proposal
[10]	RFC 2119	“Key words for use in RFCs to Indicate Requirement Levels”, S. Bradner, March 1997. Available at <a href="http://www.ietf.org/rfc/rfc2119.txt">http://www.ietf.org/rfc/rfc2119.txt</a>

## 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 [10].



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

References

## 2 Introduction to Security Assurance in the Mobile Industry and NESAS

In introducing an effective security assurance scheme, constraints need to be considered, as the environment in which the scheme is introduced defines some boundaries. Technology is not the only aspect that counts and it is necessary to achieve a real balance between technical and organisational security improvement, visibility of security levels of network equipment, operational feasibility, and market acceptance and participation. The end goal is to involve a range of stakeholders that need to commit to the scheme so the likely effectiveness, cost, effort and complexity are important parameters that need to be taken into consideration. Solutions that are designed and agreed in the mobile industry must meet the needs of all involved stakeholders around the world to secure support for their delivery to market. The Network Equipment Security Assurance Scheme (NESAS) was designed to meet the various and different needs of mobile network operators, network equipment vendors, and regulators in a time of ever growing complexity of mobile networks.

Due to national regulation, MNOs in many countries are, or will be, held accountable by law and/or regulation for running a reliable and robust mobile network. However, MNOs can only apply security controls during operation. They rely on secure network equipment being provided by their vendors from the outset. For MNOs, it is important to measure the achieved level of security of network equipment. The following approaches are particularly suitable to achieve this:

- Accreditation of the security related development and product lifecycle processes of a vendor;
- Security evaluation of network equipment by a competent test laboratory with defined and standardised security tests.

The first approach allows each vendor to define its own internal processes that describe how security is integrated into the design, development, implementation, and maintenance processes. An external auditor examines these processes and determines if they are actually applied in practice. If the auditor is satisfied, the vendor will be accredited. The accreditation demonstrates to the outside world that the vendor is capable of creating secure products. While undergoing the accreditation, the vendor does not have to reveal details about its internal processes to the public and only the auditor sees them. This way, a qualified and recognised auditor can increase trust in a vendor without the vendor having to reveal internal secrets to the public.

The second approach is security evaluation of the actual 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 and visualised. That way, new network equipment, as well as upgraded network 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. If, in addition, evaluation reports are made available to prospective customers, efficiencies can be achieved as tests only need to be performed once and do not need to be repeated by and for individual stakeholders.

The fact that network functions are standardised in the mobile industry is beneficial for security evaluation of network equipment by way of testing. The standards clearly define the functionality and capabilities of network functions. These network functions are implemented by equipment vendors and sold as network equipment. As the functional range of network equipment is clear, dedicated security requirements and test cases can be defined and standardised for all defined network functions. It is then easy to ensure that all network equipment is tested against these test cases, which will ensure that tests are comparable and as complete as the test cases are.

Both approaches – accreditation and evaluation by testing – significantly help the MNO to determine the achieved level of security of a network product. The MNO is well positioned to select its vendors according to its security requirements.

NESAS is a security assurance scheme that follows these approaches and is described below.

### **3 NESAS Overview**

The *Network Equipment Security Assurance Scheme* (NESAS) that is jointly defined by 3GPP and GSMA, and which is operated and maintained by the latter, is a voluntary network equipment security assurance scheme defined for the mobile industry. It provides a security baseline to evidence that network equipment satisfies a list of security requirements and has been developed according to standard guidelines.

In brief, NESAS defines the following approach:

- Vendors define and apply secure design, development, implementation, and product maintenance processes;
- Vendors demonstrate these processes to external auditors;
- Level of security of network equipment is tested and documented;
- Tests are conducted by competent test laboratories against 3GPP SA3 defined security requirements;
- Documentation can be forwarded to operators together with network equipment being purchased.

Therefore, NESAS follows the approaches outlined in Section 2, making the achieved level of security of network equipment measurable and visible. NESAS consists of both technical aspects, expressed by equipment tests, and organisational aspects, defined by processes.

#### **3.1 Product Development and Lifecycle**

The lifecycle of network equipment consists of a number of different stages. In its simplest form it starts with design, is followed by development and implementation, and then the equipment is operated until it reaches end-of-life. Design, development and implementation

are the responsibility of the equipment vendor, whereas the MNO is responsible for operation of the equipment. The figure below depicts this lifecycle and the assigned responsibilities.



**Figure 2 Responsibility and Accountability**

The MNO is responsible for operating a reliable mobile network and relies on the equipment vendor to provide an adequate level of security. Regulators expect MNOs to run robust, reliable and secure mobile networks and MNOs are increasingly being made accountable to satisfy that requirement. Network design, operating procedures and maintenance of deployed network equipment falls within the MNO's responsibilities but the vendor must ensure that the network equipment is secure and can be deployed securely from the outset. It is in the interests of all MNOs, and the customers that use those networks, to source secure network equipment from their vendors. Failure to do so makes it difficult to operate a secure mobile network.

Different national regulations and different security demands from MNOs introduce the potential for fragmentation and for extra overhead for vendors. Product design and development activities become more complex if varying and disparate security requirements must be met and network equipment products have to be customised for individual markets. The risk of conflicting requirements emerging poses even greater difficulty for equipment vendors seeking to produce products for a global market. This fragmentation has the potential to significantly raise the level of effort and cost for equipment vendors that ultimately impacts MNOs and their customers.

Collective and collaborative efforts are required by various stakeholders to effectively and efficiently address the risk of disparate security requirements emerging. All stakeholders, particularly in the mobile industry, need to work closely together to ensure good mobile network security. What the mobile industry needs most of all is:

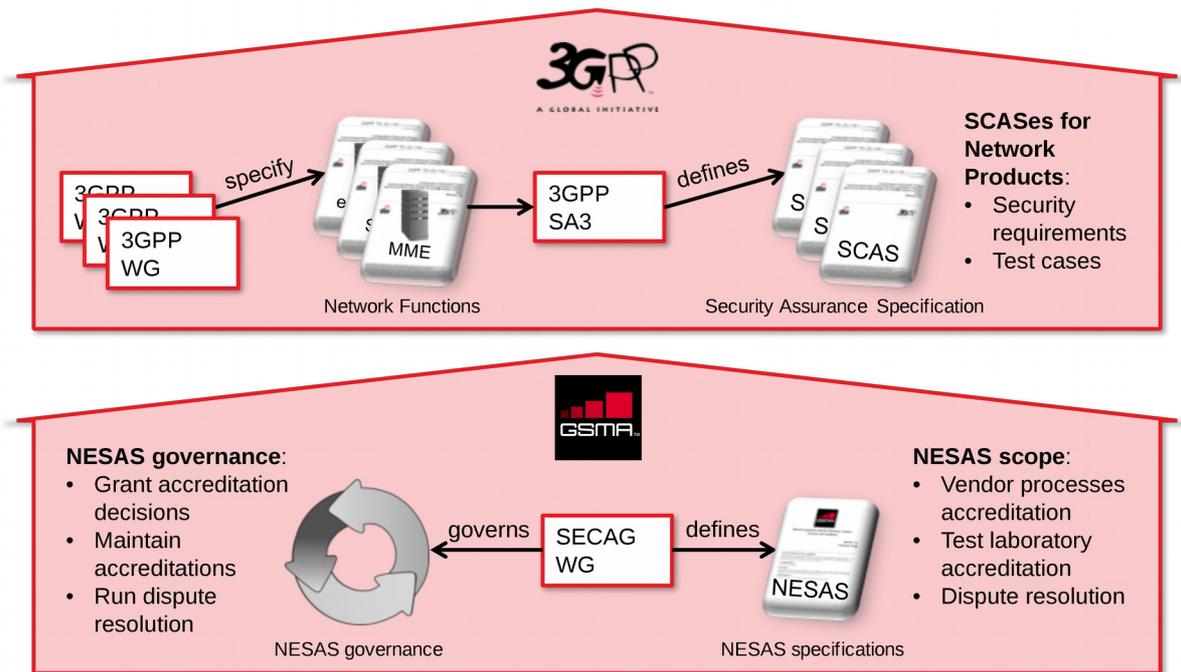
- Built-in security in network equipment;
- Consideration of security in all stages of design, development and operation;
- Objective measurement of security levels;
- Demonstration and visibility of compliance to security requirements.

The *Network Equipment Security Assurance Scheme* (NESAS) provides an industry solution to meet the needs of industry and other stakeholders.

### 3.2 NESAS High Level Overview

The GSMA defines and maintains the NESAS specifications which cover accreditation of the vendor development and product lifecycle processes, test laboratory accreditation, and security evaluation of network equipment. 3GPP defines security requirements and test cases for network products implementing one or more 3GPP network functions – specified in the so-called *Security Assurance Specification* (SCAS). The GSMA also defines a dispute

resolution process and governs the overall scheme. 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 *Network Product* in NESAS. A mobile base station from a particular vendor is an example of a Network Product.

Figure 4 illustrates the high level overview of NESAS.

The GSMA appoints an Audit Team that audits the Equipment Vendor. Results of the audit are documented in the Audit Report. The GSMA awards accreditation of the Equipment Vendor. The Equipment Vendor builds the Network Product which is given to a NESAS Security Test Laboratory for evaluation. The Test Laboratory is accredited by an ISO 17025 Accreditation Body that determines if the Test Laboratory is capable of performing meaningful Network Product tests as described in the SCASes. The Test Laboratory evaluates the Network Product against the relevant SCASes and verifies that the accredited development processes of the vendor are applied to the tested Network Product. The Audit Report provides the required information for verifying the processes. The Test Laboratory then produces an Evaluation Report containing the results. The Network Product can then be shipped to customers MNO, together with copies of the Evaluation Report.

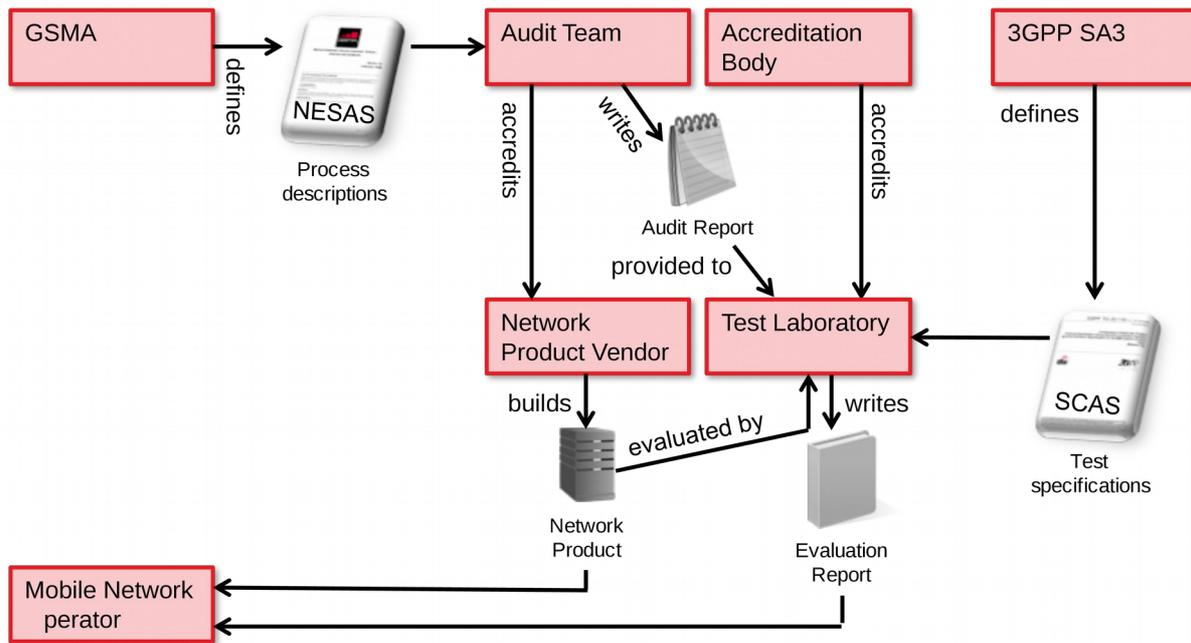


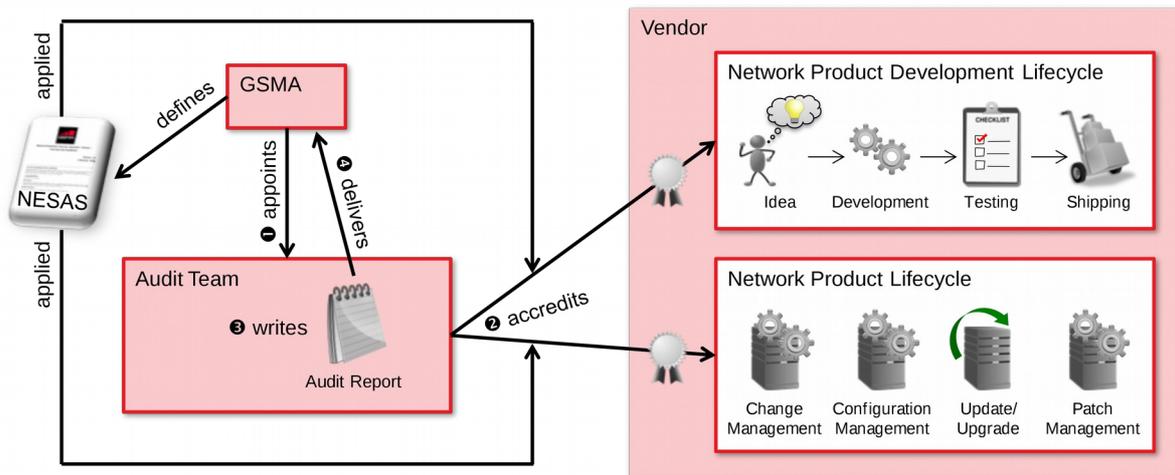
Figure 4 NESAS High Level Overview

### 3.3 Accreditation of Vendor Processes

The Equipment Vendor defines its own processes for the Network Product development lifecycle and the Network Product lifecycle. These processes also define how security is integrated in all stages of both processes. The processes are audited by the GSMA appointed Audit Team which can issue a recommendation to the NESAS Accreditation Board. NESAS describes how accreditation is to be performed and which requirements are to be fulfilled by the vendor defined processes. Accreditation consists of both off site process documentation review and on-site audit. See Figure 5.

The vendor defined processes need to ensure that, for the Network Products to achieve desired security levels, requirements are defined and design and implementation of the Network Product must follow these requirements in a comprehensible way. This is what the Audit Team seeks to verify in the course of a successful audit.

The Audit Team produces an Audit Report that contains the results of the audit. Based on the Audit Report, and its recommendations, the GSMA may award accreditation.



**Figure 5 Accreditation of vendor processes**



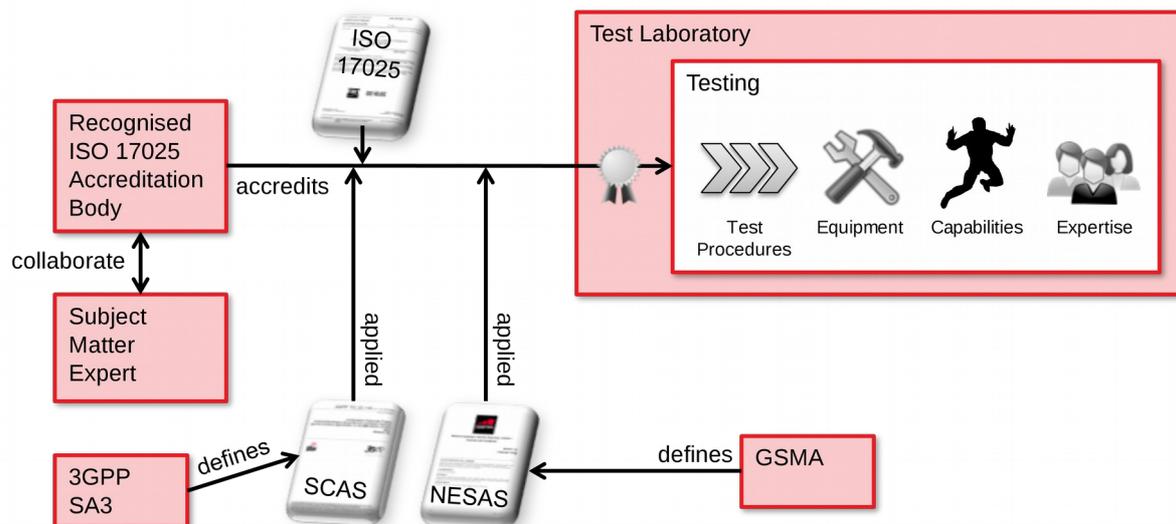
References

- FS.15 [5] defines vendor processes accreditation requirements and the process of performing the accreditation.
- NESAS Request for Information and Request for Proposal documentation [7], [8] define the criteria and processes of selecting an auditor for vendor process accreditation.

### 3.4 Accreditation of NESAS Security Test Laboratories

Nesas Security Test Laboratories can either be owned by the vendor or be owned by external third parties. In either case, they need to be accredited in accordance with ISO 17025 [16], which covers general requirements on testing procedures, documentation, maintenance and review of procedures, competence, independence, and impartiality. As ISO 17025 is a generic accreditation regime, test laboratories are always accredited in the context of additional standards from the field in which the laboratories will perform their tests. For NESAS, this means that NESAS Security Test Laboratories need to demonstrate during ISO 17025 accreditation that they are capable of performing tests described in NESAS SCASes and that they meet the additional requirements applicable to NESAS.

An officially recognised ISO 17025 Accreditation Body performs an audit upon request by the Test Laboratory. As illustrated in Figure 6, the Test Laboratory is audited against ISO 17025 in the context of NESAS and SCASes. A subject matter expert performs the audit in collaboration with the Accreditation Body, as it is this subject matter expert who brings the required expertise in the field of network equipment security to the audit. Once the audit is conducted successfully, and the requirements have been satisfied, the Test Laboratory becomes an accredited NESAS Security Test Laboratory.



**Figure 6 Accreditation of Test Laboratories**



References

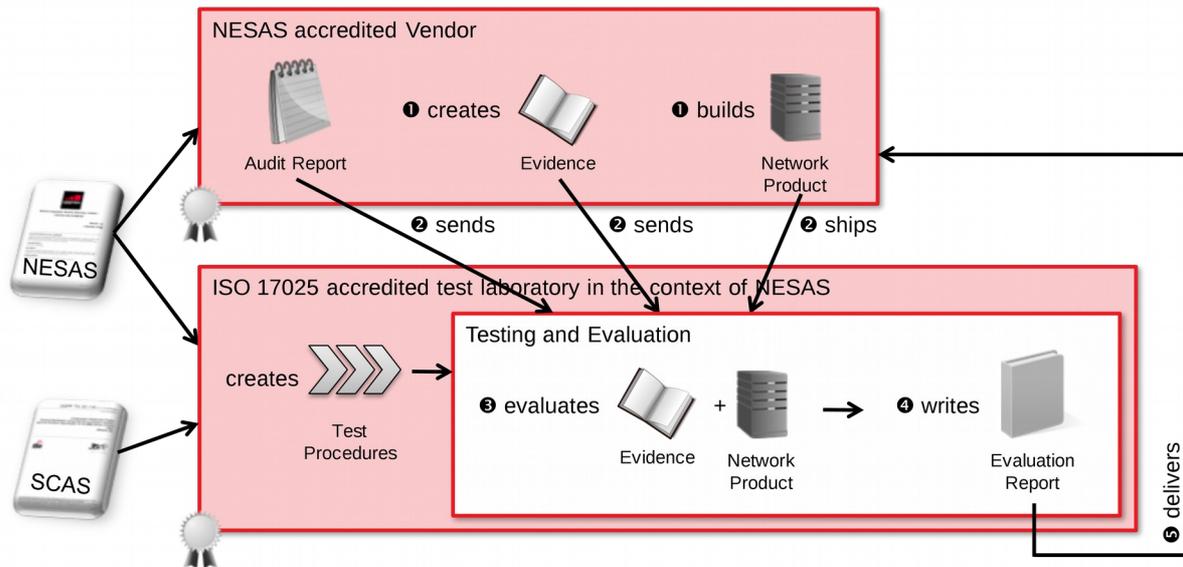
- FS.14 [4] defines test laboratory accreditation requirements and the process of performing the accreditation.
- SCASes of the 3GPP (e.g. the generic SCAS for any network equipment TS 33.117 [3] and the particular SCAS for the MME TS 33.116 [2]) contain test specifications the NESAS Security Test Laboratory must be capable to perform.
- 3GPP TR 33.916 [1] describes the methodology to create and maintain SCASes.

### 3.5 Network Equipment Evaluation

After both the Equipment Vendor and the NESAS Security Test Laboratory are accredited, Network Products can be evaluated. This is done as depicted in Figure 7.

After the Network Product is built by the Equipment Vendor, it is provided to the NESAS Security Test Laboratory. The NESAS Security Test Laboratory takes the test specifications from the corresponding SCASes, derives detailed test cases from them, and tests the Network Product. Results of the tests are recorded in an Evaluation Report.

In addition, the Equipment Vendor creates the so-called *Evidence* that contains a rationale that allows the NESAS Security Test Laboratory to assess and comprehend if the vendor is following its own accredited internal processes when building the Network Product. The Audit Report that was produced during Equipment Vendor process accreditation (see Section 3.3) gives guidance to the NESAS Security Test Laboratory on how to evaluate the Evidence. Additionally, the results of Evidence evaluation are added to the Evaluation Report. It is the Evidence evaluation that links the tested Network Product to the accredited 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.



**Figure 7 Evaluation of a Network Product**

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.

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. The Evaluation Report contains the information that makes Network Product security and security of the corresponding development lifecycle measurable and visible to the MNO.



References

- FS.15 [5] defines the 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] and the particular SCAS for the MME TS 33.116 [2]) contain test specifications the Test Laboratory must perform for Network Product evaluation.
- 3GPP TR 33.916 [1] describes the methodology to create and maintain SCASes.

**3.6 Dispute Resolution**

The Network Equipment Security Assurance Scheme Dispute Resolution Committee (NESAS DRC) is the authority responsible for handling any significant interpretation disputes that may arise between two or more NESAS participants, (for example network operators, equipment vendors, test laboratories, and auditors) with respect to NESAS processes and documentation and for publishing an objective ruling/decision on the matters raised.

The NESAS DRC is a standing committee consisting of a subset of the NESAS Accreditation Board membership that are expert in all matters pertaining to NESAS. It acts as an impartial interpreter of NESAS processes and documentation that could be the subject of disagreement between two or more Parties and the NESAS DRC must only be contacted if there is a dispute between two or more Parties with respect to interpretation of the NESAS processes or documentation.

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.

The NESAS DRC must proceed according to the Dispute Resolution Process described in FS.16 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 seek to resolve disputes as soon as practical and without undue delay (normally within 10 days of the notification). A majority decision must then be made by the NESAS DRC members.

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, and for future disputes as specified in the ruling/decision.



- FS.16 [6] defines the the NESAS dispute resolution process. Stakeholders who raise a dispute need to follow this process.

References

### 3.7 Scope 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:

- Accreditation of vendors' product development processes;
- Accreditation of vendors' product lifecycle processes;
- 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 in the mobile industry, certain aspects have been excluded from the initial scope and these are as follows:

- There is no certification of network equipment by an officially recognised authority.
- There is no proof of absence of certain functionality (e.g. backdoor) in the network equipment.
- The scheme does not replace existing operator or national requirements.
- The scheme does not include security of interfaces between network equipment.
- The scheme does not address the need for end-to-end security.

## 4 NESAS Benefits

NESAS brings a multitude 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, achieved by network equipment, is measurable, visible, comparable and understood. MNOs benefit significantly 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 product development and maintenance 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 MNOs are free to set their individual security requirements, NESAS ensures a baseline security level and a common set of security requirements for all customers and markets. Both vendors and MNOs 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 is 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. This results in cost savings and reduced overhead on the vendor side, which may ultimately be reflected in Network Product prices.

One of the goals set by industry is to demonstrate to regulators the value of NESAS. If it can be shown that NESAS security requirements are commensurate with national security requirements in individual countries the national authorities in those countries are likely to endorse and support NESAS as a legal requirement for the regulation of mobile network security deployments without having additional requirements. This is significantly beneficial for Equipment Vendors, since the overhead of dealing with, and having to satisfy, different security requirements from individual regulators worldwide is reduced. In fact, the needs of regulators are one of the key drivers for the mobile industry to develop a tailored security assurance scheme.

NESAS reuses effective and 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)**, as the term suggests, 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 accredited 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.

**Test laboratories** are contracted to perform network equipment security evaluations as defined by NESAS.

The **GSMA** has multiple roles in NESAS:

- The **Fraud & Security Group (FASG)** Working Group (WG) of the GSMA defines and maintains NESAS and all its processes.
- The **NESAS Accreditation Board** that consists only of GSMA MNO members, make decisions on awarding vendor process accreditation.
- The **NESAS Dispute Resolution Committee** is established whenever a dispute is to be resolved according to the NESAS defined processes. It consists of GSMA MNO members only.
- **Operational GSMA staff** maintains accreditation status of vendors and test laboratories and keeps the official NESAS Web site up to date.

**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 **Audit Team** performs audits of network equipment vendors' development and product lifecycle processes, as defined by NESAS.

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

The ISO 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 1 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 Accreditation Board appoints Audit Team. See Figure 8.

	<b>Audit Team</b>
<b>NESAS Accreditation Board (AB)</b>	appoints

How to read the following table:

Order of reading:

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

Example: NESAS Accreditation Board □ appoints □ Audit Team

**Figure 8 Explanation of how to read the table below**

	MNO	Vendor	Test Lab	GSMA FASG	NESAS AB	NESAS DRC	GSMA Staff	3GPP SA3	Audit Team	IAB	SME
Mobile Network Operator (MNO)		Obtains evaluated Network Product		Can be member of	Can be member of	Can be member of		Can be member of			

Equipment Vendor	Sells Network Product to		Assigns for Network Product evaluation	Can be member of				Can be member of	Is audited by		
Test Laboratory (Lab)		Performs Network Product evaluation for								Is accredited by	Is audited by
GSMA Fraud & Security Group (FASG)	Has members from	Has members from			Establishes	Establishes		Collaboratively develops NESAS with			
NESAS Accreditation Board (AB)	Has member from	Accredits				Assigns disputes to	Is supported by		Appoints		
NESAS Dispute Resolution Committee (DRC)	Has member from Handles disputes with	Handles disputes with	Handles disputes with								
Operational GSMA Staff		Maintains accreditation status of	Maintains accreditation status of		Supports	Supports			Coordinates	Is available for inquiries from	Is available for inquiries from
3GPP SA3	Has members from	Has member from		Collaboratively develops NESAS with							
Audit Team		Audits					Reports to				
ISO 17025 Accreditation Body (IAB)			Accredits								Collaborates with
Subject Matter Expert			Audits							Collaborates with	

**Table 1 Relationships between stakeholders**

## 6 Status of NESAS Development and Outlook

At the time of writing, in March 2016, the concepts, processes and documents pertaining to NESAS have almost reached pilot testing stage. In 2016, a pilot will be conducted to learn and assess how the scheme works in practice and to resolve any issues that exist prior to full launch in 2017.

NESAS is designed to be improved iteratively. All the lessons learnt from the pilot will be considered and reflected in the initial official release of NESAS. Thereafter, updated releases will be issued regularly that will take the feedback from the various stakeholders into account. This facilitates and encourages stakeholders to get involved in order to help develop the scheme in a way that it satisfies their needs and that accredited vendors and more secure network equipment benefit the mobile ecosystem.

The current status of NESAS development and the latest versions of the NESAS documents can be obtained from the official NESAS portal on GSMA's Web site when it is live.

If it is determined necessary in the future, the scope of NESAS can be extended and additional security requirements can be added to existing SCASes. New network equipment

types can be added to the scheme by producing and approving new corresponding SCASes. Additionally, vendor process accreditation and test laboratory accreditation can be extended by adding/modifying requirements as considered necessary. In essence, NESAS is a living breathing scheme that will evolve over time and the 2016 pilot testing marks an important first step for the industry.

## Annex A Document Management

### A.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
0.1	Mar 2016	First draft NESAS overview document	SECAG	Sven Ichmund, Deutsche Telekom
0.2	Mar 2016	Second draft presented following SECAG#13	SECAG	Sven Lachmund, Deutsche Telekom
0.3	May 2016	Final version for NESAS Pilot Release	SECAG	Sven Lachmund, Deutsche Telekom

### A.2 Other Information

Type	Description
Document Owner	SECAG
Editor / Company	Sven Lachmund, Deutsche Telekom

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 [prd@gsma.com](mailto:prd@gsma.com).

Your comments or suggestions & questions are always welcome.