Network Equipment Security Assurance Scheme – Methodology for Product and Evidence Evaluation

Version 3.0

20 February 2025

Security Classification: Non-Confidential

Copyright Notice

Disclaimer

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

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 modify 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 forms part of the documentation of the Network Equipment Security Assurance Scheme (NESAS). An overview of the scheme is available in GSMA PRD FS.13 – Network Equipment Security Assurance Scheme – Framework [2].

The present document describes the methodology for Evidence Evaluation and Network Product Evaluation.

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 [1] 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 evaluation methodology establishes how the product and Evidence Evaluation is done at the procedural and operational level. It is provided to assist the Equipment Vendor and the NESAS Security Test Laboratory in the performance of those activities.

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: While any 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] GSMA PRD AA.35: "Procedures for Industry Specifications".

[2] GSMA PRD FS.13: "Network Equipment Security Assurance Scheme – Framework".

[3] GSMA PRD FS.14: "Network Equipment Security Assurance Scheme – Requirements for NESAS Auditing Organisations, NESAS Security Test Laboratories, and Associated Personnel".

[4] GSMA PRD FS.50: "Network Equipment Security Assurance Scheme – Requirements for Security Assurance Specification Development".

[5] GSMA PRD FS.62: "Network Equipment Security Assurance Scheme – Adoption Procedure for Security Assurance Specifications".

[6] GSMA PRD FS.63: "Network Equipment Security Assurance Scheme – List of Adopted Security Assurance Specifications".

[7] ISO/IEC 17025 2017: "General requirements for the competence of testing and calibration laboratories".

[8] 3GPP TS 33.117: "Catalogue of General Security Assurance Requirements".

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: While any hyperlinks included in this clause were valid at the time of publication.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] NIST SP 800-30 Rev. 1 2012: "Guide for Conducting Risk Assessments", http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf

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

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.

Equipment Vendor: Organisation that develops, maintains and supplies 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.

Interim Audit Report: Document presenting the results of an Interim Audit performed at the Equipment Vendor by the Audit Team that is published as an addendum to an existing Audit Report.

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).

Software: Physically intangible set of instructions, defined in a formal language, written in digital format.

Testing Environment: Hardware, Software and infrastructure necessary to evaluate (operate) the Product under Evaluation.

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.

Vulnerability: A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.

NOTE: The term "Vulnerability" is as defined by NIST in SP 800-30 [i.1].

3.2 Symbols

Symbols are not applicable in the present document.

3.3 Abbreviations

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

3GPP	Third Generation Partnership Project
GSMA	GSM Association
IEC	International Electrotechnical Commission
ISAG	Industry Specification Approval Group
ISO	International Organisation for Standardization
NESAS	Network Equipment Security Assurance Scheme
NF	Network Function
PRD	Permanent Reference Document
PuE	Product under Evaluation
SCAS	Security Assurance Specification
SDO	Standards Development Organisation
TS	Technical Specification

4 Evidence and Network Product Evaluation Process

4.1 General

The security evaluation of network equipment in NESAS consists of Evidence Evaluation and Network Product Evaluation, as further explained in the present document. See also Figure 1.

The Equipment Vendor defines the scope of the Product under Evaluation (PuE) by declaring the Network Functions (NFs) provided.

The Evidence Evaluation demonstrates that the Equipment Vendor adheres to its previously assessed Vendor Development and Product Lifecycle Processes when developing and maintaining the PuE. Evidence Evaluation links Network Product Evaluation to the processes assessment.

The Network Product Evaluation covers all functionality and capabilities of the NFs included in the PuE, using applicable Security Assurance Specifications (SCASes). Guidance on defining the scope of evaluation can be found in clause 4.2. Authorised NESAS Security Test Laboratories are capable of performing Network Product Evaluations against the security requirements and test cases defined in SCASes, developed by 3GPP or other Standards Development Organisations (SDOs). Requirements on the development of SCASes are provided in GSMA PRD FS.50 [4]. The adoption procedure of SCASes is defined in GSMA PRD FS.62 [5].

Both Evidence Evaluation and Network Product Evaluation shall be performed by the same authorised NESAS Security Test Laboratory.

Equipment Vendors that wish to have their Network Products evaluated select and contract directly with one of the authorised NESAS Security Test Laboratories listed on the Scheme Owner's website. A NESAS Security Test Laboratory can be owned by any entity, but Network Product Evaluations can only be performed by test laboratories that are impartial (as defined in ISO/IEC 17025 2017 [7]) and independent of the Equipment Vendor that develops and maintains the PuE.

For Evaluators, in addition to technical expertise, it is expected that:

- The Evaluators appointed to the Evaluation Team have relevant knowledge, working experience and/or education in order to fulfil the needs to be a NESAS Security Test Laboratory Evaluator;
- The Evaluation Team has a team leader who is highly experienced to supervise, oversee and monitor the activities of less experienced Evaluators and the additional specialists and technical experts, and
- The Evaluators are independent of the Equipment Vendor.

The specific requirements for NESAS Security Test Laboratory, Evaluation Team, and Evaluators, are defined in GSMA PRD FS.14 [3].

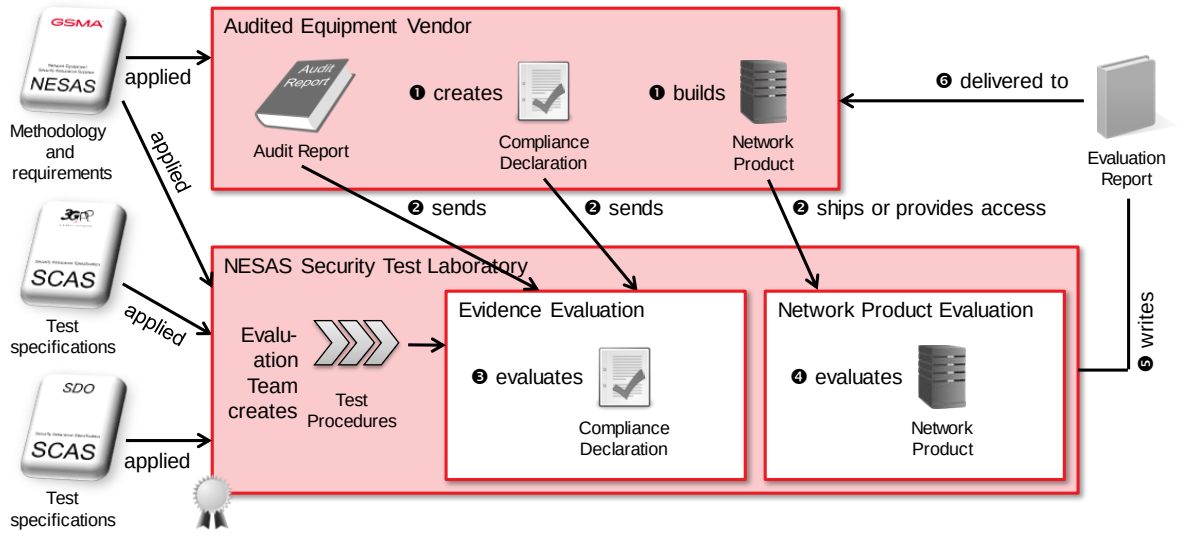

Figure 1: Evaluation of a Network Product

4.2 Evaluation Prerequisites

The Network Product is comprised of one or more NFs. Each NF provides a set of defined functionalities and interfaces, defined in a technical specification. The Equipment Vendor defines the scope of evaluation by declaring the NFs provided. If the Network Product is comprised of more NFs than those that are in scope of the evaluation, the Equipment Vendor shall describe these and declare them out of scope of evaluation. The Network Product may consist of additional functionality that is necessary to execute and manage the NF(s) in scope. This additional functionality is also in scope of evaluation without exception. The NESAS Security Test Laboratory shall document in the Evaluation Report the scope of evaluation and also list the NFs of the Network Product that are outside the scope of evaluation.

The NESAS Security Test Laboratory and the Equipment Vendor agree on the scope of evaluation. The applicable SCASes, against which the evaluation is to be performed, are identified and agreed by both parties. These are derived from the NFs that are in scope of evaluation. There are two types of SCASes that can apply to a Network Product. A generic SCAS applies to any Network Product and all its functionality, and a specific SCAS applies to specific NFs only. To identify the applicable SCASes, the following guidelines apply:

- For all PuE, the generic SCAS 3GPP TS 33.117 [8] applies in any case and shall not be excluded;
- For 3GPP-defined NF the corresponding 3GPP-defined specific SCASes shall apply;
- For functionality defined by any other SDO, the respective specific SCASes shall apply;
- If another SDO integrates 3GPP-defined functionality, the corresponding 3GPP SCASes shall apply in addition to the ones defined by the other SDO;
- If specific SCASes exist for the NFs that are part of the PuE, they shall be part of the scope of evaluation;
- If no specific SCAS exists for the PuE, only the generic SCAS can be used.

Specific SCASes apply to a specific NF only. In contrast, generic SCASes apply to the entire PuE.

The NESAS Group maintains a list of adopted SCASes in GSMA PRD FS.63 [6]. The Scheme Owner uses all or a subset of the SCASes from the list.

NOTE: An evaluation based only on the generic SCAS might not cover threats associated with the specific use cases for the evaluated NF.

NOTE: Authorised NESAS Security Test Laboratories perform security evaluations of Network Products against the security requirements and test cases. These security requirements and environmental assumptions described in the SCAS test cases define the capacity to resist a given attack potential. The SCASes are designed to resist threats of an attacker possessing an attack potential of a level that is in the middle level on the scale of attack potential range. That is, at least higher than the basic level but lower than the high level which corresponds to an attack potential of an attacker at least possessing significant skills and resources.

For a NESAS Network Product Evaluation to be performed, the Equipment Vendor shall provide the NESAS Security Test Laboratory with a number of key enablers, including the following:

- Access to the Network Product to be evaluated and all relevant documentation pertaining to its functionality, set-up, configuration, etc;
- Confirmation of the specific Release of the Network Product to be evaluated and the relevant adopted SCAS versions, contained in GSMA PRD FS.63 [6], under which the evaluation is to be performed as these details are to be recorded in the Evaluation Report;
- Audit Report, and any related Interim Audit Reports, from the independently audited Vendor Development and Product Lifecycle Processes that are used for developing and maintaining the PuE;
- Compliance Declaration containing Compliance Evidence from the Equipment Vendor confirming its adherence to the specific Vendor Development and Product Lifecycle Processes that have been NESAS assessed and under which the PuE was developed.

The NESAS Security Test Laboratory and the Equipment Vendor agree on the 3GPP defined functions supported by the PuE. The relevant SCAS versions against which the evaluation is to be performed are identified and agreed by both parties and this defines the scope of the evaluation.

4.3 Evaluation Preparation

In preparation for a Network Product Evaluation the Equipment Vendor, shall provide to the NESAS Security Test Laboratory the following:

- Diagrammatic identification of the PuE and simulated systems, interfaces and protocols necessary to interact;
- Hardware used with configuration parameters, clearly identifying which parts are running in the different hardware elements, if applicable;
- Description of Software layers between the hardware and the NF, if applicable;
- Tools and the versions of them necessary to trigger functionalities or capture specific test evidence and results, if applicable;
- Simulated systems and versions of them that are necessary to perform the evaluation tests, if applicable.

The Equipment Vendor and the NESAS Security Test Laboratory shall agree on a test plan, aligned with the relevant adopted SCAS documents from GSMA PRD FS.63 [6], that describes the following:

- Scenarios and configurations to be used, as described in the previous clause;
- Specific product test case to validate the Release of the PuE;
- Step by step procedure to fulfil the pre-conditions defined in the applicable SCASes;
- Step by step test execution for the PuE necessary to perform the tests defined in the applicable SCASes;
- Step by step expected results for the PuE in accordance with the applicable SCASes;
- Execution evidence and current execution results.

All test cases of all applicable SCASes are applicable. If a test case cannot be applied for a particular PuE, the NESAS Security Test Laboratory shall justify, in writing, after dialogue with the Equipment Vendor that the test case is not applicable.

4.4 Evaluation Performance

Network Product Evaluations may be performed at the premises of the NESAS Security Test Laboratory but may also be performed at other locations where the Network Product and/or the Testing Environment necessary to perform the tests. This could include third party facilities, including at the Equipment Vendor premises.

NESAS recognises that the PuE could be distributed across different locations and that tests can be executed remotely. Testing can involve the use of simulated network devices and other elements that are not under evaluation but are necessary to trigger operations on the PuE.

Consequently, tests may be executed remotely, particularly where it makes little sense to physically ship the Network Product to the NESAS Security Test Laboratory or the Testing Environment is too complex to be re-created in the NESAS Security Test Laboratory, or both. Remote testing can be carried out in the following ways:

1. Remote testing at the Equipment Vendor facilities;
2. Remote testing at the NESAS Security Test Laboratory facilities;
3. Remote testing at third party facilities.

Security and quality requirements to be fulfilled by third parties are the same as those for the NESAS Security Test Laboratory.

In all cases, Evaluators shall execute the tests, but close support from Equipment Vendor or third-party technical staff may be necessary. The test execution and procedures shall comply with ISO/IEC 17025 2017 [7] requirements at all times.

The test location shall be agreed by the Equipment Vendor and NESAS Security Test Laboratory and formally stated in written form in the contract or in a different document during the evaluation process. The test location approach (scenarios, requirements and location) shall comply with the test purpose and needs to be assessed and validated by the NESAS Security Test Laboratory.

The Testing Environment needs to be set up in a way, and that set-up needs to be documented in sufficient detail, that it can be re-built at a later time to reproduce the tests, if ever considered necessary.

4.5 Evaluation Observance

The NESAS Security Test Laboratory requires assurance that the Release of the PuE is the one declared by the Equipment Vendor and recorded in the Evaluation Report. This can be easily achieved in the case of on-site testing but in the case of remote testing the NESAS Security Test Laboratory and the Equipment Vendor shall agree on how to provide the necessary assurance.

The preferred approach is on-site witnessing by Evaluators. In the event that on-site witnessing is not feasible, remote witnessing would be acceptable. In this case, the witnessing will be led by the Evaluators, who can require the

Equipment Vendor to provide pictures, live video streaming or facilitate live interviews with relevant Equipment Vendor staff.

A representative test will be chosen to be executed in order to verify and validate correctness of the remote test execution, Testing Environment and verification of the PuE.

4.6 Evidence Evaluation

An essential component of the Network Product Evaluation is to verify that the PuE was developed in accordance, and full compliance, with the independently audited Vendor Development and Product Lifecycle Processes. This requires the NESAS Security Test Laboratory to review the Compliance Declaration and the Compliance Evidence provided by the Equipment Vendor.

The Audit Report, and any relevant Interim Audit Report, provides guidance to the NESAS Security Test Laboratory on how the Compliance Evidence is to be evaluated. Compliance Evidence for a specific security requirement may not be available and in such a case, the Equipment Vendor provides a justifiable explanation and rationale as to why the Compliance Evidence does not exist for that particular security requirement.

4.7 Evaluation Report

At the conclusion of the evaluation, a completed Evaluation Report is provided to the Equipment Vendor, which contains the results of the security tests performed on the Network Product, including the results of the Vulnerability analysis and the results of the Evidence Evaluation. A copy of the Evaluation Report is provided to the Scheme Owner, if the evaluated Network Product is to be listed on the Scheme Owner's website.

The Evaluation Report shall contain the following contents as a minimum:

1. Company names and contact details of the NESAS Security Test Laboratory and Equipment Vendor;
2. Full description of the PuE, e.g. Software, hardware, interfaces, data, services and scope;
3. Product name, Release and description of product configuration;
4. Version of the present document, evaluation methodology that was followed;
5. Details of the location(s) at which the evaluation was performed;
6. Description how testing was performed, on-site or remotely;
7. Description of the Testing Environment;
8. Timeline of the evaluation activities;
9. List of SCASes from GSMA PRD FS.63 [6], and versions, used for the evaluation and mapping of SCAS standards to NFs within the PuE;
10. Details of product or system component elements or NFs that may not have been tested;
11. Details of product and operational documentation provided by the Equipment Vendor;
12. List of all executed test cases, test names and test results;
13. Description of test cases executed and documentation used by Evaluator to do so;
14. List of test cases from used SCASes that are fully or in part not applicable for the PuE, together with the justification why these test cases are not applicable;
15. List of any test cases, which could not be fully or in part completed, along with justification as to why the tests could not be completed;
16. All evidence each SCAS test case requires to support the test result;
17. Details of basic Vulnerability testing performed and tools used;
18. Details of the Vulnerability analysis for all identified Vulnerabilities;
19. Date when Vulnerability testing was performed;
20. Documentation of all tools used for testing, with their unique name, version and configuration, and in each test case a reference to the tools used;
21. NESAS Audit Report version and list of evidence examined to assess compliance of Vendor Development and Product Lifecycle Processes to the PuE.

The Evaluation Report applies to a specific Network Product Release and SCAS version. An update of either may trigger the need for an up-to-date evaluation.

The Equipment Vendor can provide the Evaluation Report to interested stakeholders.

It is at the discretion of Evaluation Report recipients to determine from the report contents if the level of security of the evaluated Network Product is sufficient for its needs.

History

Version	Date	Brief Description of Change
1.0	Feb 2022	New document created to describe the methodology for NESAS evidence evaluation and network product evaluation.
2.0	Jul 2023	Attacker potential vulnerability analysis added, clarifications added on need for independent test labs, which SCASes are to be selected for evaluation and which test cases are applicable, evaluation in NESAS consists of product and evidence evaluation. Guidelines added on how to define the scope of evaluation.
3.0	Feb 2025	Evaluator requirements added, new requirement added on vulnerability testing, SCAS adoption process moved to FS.62, list of adopted SCASes moved to FS.63, content on trial evaluations moved to FS.51, alignment of terms and definitions and details of GSMA NESAS scheme moved to FS.51.