NESAS - Product and Evidence Evaluation Methodology
Version 2.0
21 July 2023

Security Classification: Non-confidential

Copyright Notice

Disclaimer

Compliance Notice

The information contain herein is in full compliance with the GSM Association's 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 in GSMA AA.35 - Procedures for Industry Specifications.

Table of Contents

1. Introduction

This document describes the Network Equipment Security Assurance Scheme (NESAS) product and evidence evaluation methodology.

1.1. 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.

1.2. Document Maintenance

NESAS was originally created 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 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.

1.3. 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	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 Note: This definition does not mandate a certain employer for the Auditor, which is possibly employed by a dedicated Auditing Organisation (or could be a freelancer). The qualification is ensured by the certification of said individuals.
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 Certification Body, demonstrating that the Applicant applied its previously 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. Note: An Auditor defines in the Audit Report which Compliance Evidence is required for subsequent product evaluations
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 accredited NESAS Security Test Laboratory.
Evidence Evaluation	Activity in NESAS of evaluating that the Product under Evaluation (PuE) was developed in accordance with the previously assessed Vendor Development and Product Lifecycle Processes of the Equipment Vendor.
NESAS Security Test Laboratory	A test laboratory that is ISO/IEC 17025 accredited in the context of NESAS and that is authorised to conduct Network Product Evaluations, as defined in FS.14.
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 Development Process	Stages through which developed Network Products journey throughout their development including planning, design, implementation, testing, release, production and delivery

Term	Description
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).
Network Product Lifecycle Process	Stages through which developed Network Products journey to end of life including maintenance and update releases during their lifetime
Release	Version of a Network Product being made available for deployment. Note: The first Release of a Network Product is assumed to be a new Network Product
Product under Evaluation	The product for which an evaluation is sought by the Equipment Vendor
Scheme Owner	Organisation or authority responsible for developing and maintaining a specific security assurance or certification scheme that uses the NESAS specifications (refer to Annex B.2 for licensing of NESAS Documentation).
Security Assurance Specification	Specification containing security requirements and test cases for a 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 Note: Software is used by a machine to be interpreted or executed. It can exist in various formats, such as binary software, which is only machine-readable, and scripts and source code, which is human readable and/or machine readable. Software is used for many purposes. It can be the instruction set of hardware, in which case it is called “firmware”. It can be (part of) an operating system, an application, a library, or anything else that is executed or interpreted by a machine. In this definition, the term is to be understood in its broadest possible sense
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.

1.4. Abbreviations

Term	Description
3GPP	Third Generation Partnership Project
3GPP TS	3GPP Technical Specification
IEC	International Electrotechnical Commission
ISO	International Organisation for Standardization
NESAS	Network Equipment Security Assurance Scheme
NP	Network Product
PuE	Product under Evaluation
SCAS	Security Assurance Specification
SDO	Standards Development Organisation

1.5. References

Ref	Doc Number	Title
	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
	ISO/IEC 17025	General requirements for the competence of testing and calibration laboratories
	3GPP Security Assurance Specifications	List of 3GPP-defined Security Assurance Specifications, https://www.gsma.com/security/nesas-security-assurance-specifications/
	3GPP TS 33.117	Catalogue of General Security Assurance Requirements
	GSMA PRD FS.50	Network Equipment Security Assurance Scheme – Security Assurance Specification Development Guidelines
	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 RFC2119 [1].”

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

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

2. Evidence and Network Product Evaluation Process

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

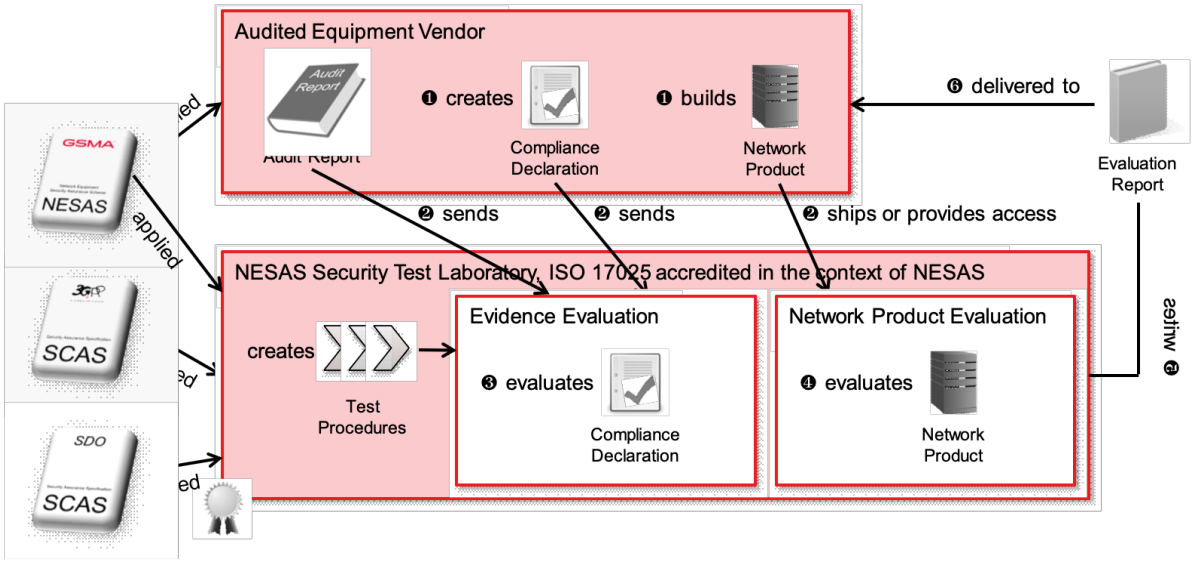
The Equipment Vendor defines the scope of the Product under Evaluation by declaring the Network Functions provided.

The Evidence Evaluation demonstrates that the Equipment Vendor adheres to its previously assessed Equipment Vendor's Network Product development and lifecycle processes when developing and maintaining the Product under Evaluation. Evidence Evaluation links Network Product Evaluation to the processes assessment.

The Network Product Evaluation covers all functionality and capabilities of the Network Functions included in the Product under Evaluation, using applicable Security Assurance Specifications (SCASes). Guidance on defining the scope of evaluation can be found in Section 2.1. Accredited NESAS Security Test Laboratories are capable of performing Network Product Evaluations against the security requirements and test cases defined in Security Assurance Specifications (SCASes), developed by 3GPP or other Standards Development Organisations (SDOs). Guidance on the requirements for the development of SCASes is provided in FS.50 [5] and guidance on the adoption of SCASes is provided in Annex A.

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

Equipment vendors that wish to have their Network Products evaluated can select and contract directly with one of the recognised NESAS Security Test Laboratories listed on the Scheme Owner's Web Site. 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 [2]) and independent of the Equipment Vendor that develops and maintains the Product under Evaluation.



1. Evaluation of a Network Product

2.1. Evaluation Prerequisites

The Network Product is comprised of one or more Network Functions (NF). 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 Network Functions 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 dedicated Network Functions only. To identify the applicable SCASes, the following guidelines apply:

- For all Network Products under Evaluation, the generic SCAS 3GPP TS 33.117 [4] applies in any case and shall not be excluded.
- For 3GPP-defined Network Functions (NF) the corresponding 3GPP-defined specific SCASes shall apply.
- For functionality defined by any other Standards Development Organisation (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 Network Functions that are part of the Product under Evaluation, they shall be part of the scope of evaluation.
- If no specific SCAS exists for the Product under Evaluation, only the generic SCAS can be used.

Specific SCASes apply to a specific Network Function only. In contrast, generic SCASes apply to the entire Product under Evaluation.

GSMA maintains a list of SCASes [3], which are adopted for use in NESAS Product Evaluations.

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

NOTE: Accredited 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 dedicated release of the Network Product to be evaluated and to the SCAS versions, contained in the SCAS List [3], 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 development and product lifecycle management processes that are used for developing and maintaining the Product under Evaluation
- Compliance Declaration containing Compliance Evidence from the Equipment Vendor confirming its adherence to the specific development and product lifecycle management processes that have been NESAS assessed and under which the Network Product under evaluation was developed

The NESAS Security Test Laboratory and the Equipment Vendor agree on the 3GPP defined functions supported by the Network Product under evaluation. 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.

2.2. 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 Network Product under evaluation and simulated systems, interfaces and protocols required 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 Network Function, 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 SCAS documents from the SCAS list [3], that describes the following;

- Scenarios and configurations to be used, as described in the previous section;
- Specific product test case to validate the version of the Network Product under evaluation;
- Step by step procedure to fulfil the pre-conditions defined in the applicable SCASes;
- Step by step test execution for the Network Product under Evaluation necessary to conduct the tests defined in the applicable SCASes;

- Step by step expected results for the Network Product under evaluation 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 Product under Evaluation, the NESAS Security Test Laboratory shall justify, in writing, after dialogue with the Equipment Vendor that the test case is not applicable.

2.3. Evaluation Performance

Network Product evaluations may be conducted at the premises of the NESAS Security Test Laboratory but may also be conducted at other locations where the Network Product and/or the test environment necessary to perform the tests exists. This could include third party facilities, including at the Equipment Vendor premises.

NESAS recognises that Network Products under evaluation 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 stimulate operations on the Network Product that is under evaluation.

Consequently, tests may be required to be executed remotely, particularly where it makes little sense to physically ship the Network Product to the NESAS Security Test Laboratory or the test environment required 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 required for the NESAS Security Test Laboratory.

In all cases, NESAS Security Test Laboratory personnel shall execute the tests, but close support from Equipment Vendor or third-party technical staff may be required. The test execution and procedures must comply with ISO/IEC 17025 [2] requirements at all times.

The test location must 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) must comply with the test purpose and needs to be assessed and validated by the NESAS Security Test Laboratory.

The test 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.

2.4. Evaluation Observance

The NESAS Security Test Laboratory requires assurance that the Network Product under evaluation is the version declared by the Equipment Vendor and recorded in the evaluation report. This may 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 must agree on how to provide the necessary assurance.

The preferred approach is on-site witnessing by NESAS Security Test Laboratory 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 NESAS Security Test Laboratory 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, test environment and verification of the Network Product under Evaluation.

2.5. Evidence Evaluation

An essential component of the Network Product evaluation is to verify that the Network Product under evaluation was developed in accordance, and full compliance, with the independently audited development and product lifecycle management process. 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.

2.6. 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 Web Site.

The following NESAS Evaluation Report contents are suggested, as a minimum;

1. Company names and contact details of test lab and vendor
2. Full description of the product under evaluation, e.g. software, hardware, interfaces, data, services and scope
3. Product name, version and description of product configuration
4. Version of GSMA document FS.47, evaluation methodology, 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 test environment
8. Timeline of the evaluation activities
9. List of SCAS documents, and versions, used for the evaluation and mapping of SCAS standards to network functions within the evaluated product
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 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 undertaken and tools used
18. Details of the vulnerability analysis for all identified vulnerabilities
19. 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
20. NESAS Audit Report version and list of evidence examined to assess compliance of product development process to the product under evaluation

GSMA recognises that for candidate NESAS Security Test Laboratories to obtain recognition of their competence to undertake product evaluations in the scope of their ISO/IEC 17025 accreditation the national accreditation body may require the test laboratory to perform a trial evaluation. GSMA will recognise and accept Evaluation Reports that are produced by test laboratories seeking NESAS recognition in the course of trial evaluations if all of the following criteria are met;

- Personnel, utilities and processes used during the trial evaluation were deemed adequate for the performance of NESAS Network Product Evaluations and Evidence Evaluations by the national accreditation body;
- The national accreditation body formally recognised the competency of the test laboratory to undertake NESAS Product Evaluations and Evidence Evaluations based on the trial evaluation;
- The personnel, utilities and processes used during the trial evaluation have not been altered or improved in any way, at the insistence of the national accreditation body, that would materially alter the evaluation outcome;
- Written notification is provided by the test laboratory to GSMA confirming the adequacy of the personnel, utilities and processes used during the evaluation trial and that these were not subsequently materially altered to achieve national accreditation body recognition.

The Evaluation Report does not expire but only 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.

A. Security Assurance Specification Adoption

The structure of Security Assurance Specifications (SCASes) is defined in FS.50 [5]. SCASes may be developed internally by GSMA or by an appropriate internationally recognised Standards Development Organisation, e.g. 3GPP.

When a new SCAS is being created, it is essential that the developing organisation adheres to a structure that ensures the final specification meets certain quality requirements, can be applied consistently, and has utility for the NESAS Security Test Laboratories. For adoption by NESAS, the SCAS shall follow FS.50 [5].

The developing organisation shall be an appropriate internationally recognised Standards Development Organisation that develops specifications in a manner that ensures they are developed on the basis of:

- open decision-making accessible to all interested parties in the market or markets affected by those technical specifications;
- a collaborative and consensus based decision-making process;
- transparent discussions and decision-making processes for which records exist;
- participation of all relevant categories of interested parties with a view to achieving balance;
- intellectual property rights policies that grant access to and use of the specifications on an open, fair, non-discriminatory and royalty-free basis.

Publication of a new/revised SCAS will be notified to GSMA and the document, having undergone appropriate quality control by the developing organisation, will be input to the NESAS Group for review and consideration. The new/revised SCAS shall be accompanied by any other specification documents that are essential to review and evaluate the SCAS.

The NESAS Group will then verify that the submitted SCAS complies with the requirements defined in FS.50 [5].

In the event the SCAS is formally accepted and adopted by GSMA it will be referenced on the NESAS Web Site [6]. If a SCAS is rejected, the NESAS Group will document and communicate the reasons and remedial suggestions to the developing organisation.

NOTE: SCASes that were adopted before the SCAS adoption procedure in this Annex was published, will remain adopted. The SDO that owns these specifications is encouraged to update these SCASes to meet the requirements in FS.50 [5].

GSMA is desirous to ensure SCASes can be practically applied by NESAS Security Test Laboratories, the defined requirements are testable, compliance can be consistently and unambiguously assessed to a high quality and conformity can be ensured. GSMA will engage with NESAS Security Test Laboratories to gather feedback on the utility of the SCASes, particularly after first use. GSMA will gather feedback that could result in enhancement proposals to be submitted to the developing organisation by the NESAS Security Test Laboratory or by GSMA members contributing directly to the developing organisation, if considered necessary. This engagement process facilitates continuous review and improvement of NESAS adopted SCASes.

B. Document Management

B.1. Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	Feb 2022	First version developed to describe evaluation process	GSMA ISAG	James Moran, GSMA
2.0	Jul 2023	A formal SCAS adoption process has been added to the scheme to allow SDOs submit SCASes to allow the scope of NESAS to be extended. Additional changes include; • Attacker potential vulnerability analysis added. • Clarification added that product evaluations shall be performed by independent test labs. • Clarification added which SCASes are to be selected for evaluation and which test cases are applicable. • Added clarification that evaluation in NESAS consists of product and evidence evaluation. • Guidelines on how to define the scope of Evaluation added. • Definitions, abbreviations and references have been updated and editorial corrections have been made where	GSMA ISAG	James Moran, GSMA

B.2. Licensing of NESAS Documentation

This GSMA document and its content is:

i. the exclusive property of the GSMA; and

ii. provided “as is“, without any warranties by the GSMA of any kind.

Any official government (or government appointed) body wishing to use this GSMA document or any of its content:

i. for the creation of; or

iii. as referenced in;

its own documentation regarding the same or a similar subject matter, is hereby granted a licence to the copyright in this document.

This grant is subject to and upheld, as long as the above body:

a) informs the GSMA about the use of the GSMA document prior to commencing work on;

b) provides the GSMA with the finalised, i.e. most up-to-date version of; and

c) properly references the GSMA document and any extracts thereof in;

its own documentation.

B.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 welcome.