



Network Equipment Security Assurance Scheme – Requirements for Security Assurance Specification Development

Version 2.0

20 February 2025

Security Classification: Non-Confidential

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

Copyright Notice

Copyright © 2025 GSM Association

Disclaimer

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

Compliance Notice

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

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

Contents

Licensing Statement	3
Foreword.....	3
Modal verbs terminology	3
Introduction	4
1 Scope	5
2 References	5
2.1 Normative references	5
2.2 Informative references	5
3 Definition of terms, symbols and abbreviations.....	6
3.1 Terms	6
3.2 Abbreviations.....	6
4 Security Assurance Specification Structure	7
5 Requirements for Writing Security Problem Definition	7
5.1 General.....	7
5.2 Threats Format.....	8
6 Requirements for Writing Security Requirements	8
6.1 General.....	8
6.2 Security Requirement Format	9
7 Requirements for Writing Test Cases	9
7.1 General.....	9
7.2 Verifiability and Repeatability.....	9
7.3 Product Under Evaluation.....	10
7.4 Test Case Format	10
Annex B (informative): SCAS Network Product Class Description and Security Problem Definition	
Example.....	12
B.1 Network Product Class Description for the gNB.....	12
B.2 Assets and Threats Specific to the gNB.....	12
B.2.1 Critical assets	12
B.2.2 Threats related to Control plane and User plane in the network	12
B.2.2.1 Control plane data confidentiality protection	12
Annex C (informative): SCAS Security Requirement and Test Case Example	14
History	15

Licensing Statement

This GSMA document and its content is:

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

Foreword

This Technical Specification was produced by the GSM Association.

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

Version x.y.

where:

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

Modal verbs terminology

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

shall indicates a mandatory requirement to do something

shall not indicates an interdiction (prohibition) to do something

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

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

should indicates a recommendation to do something

should not indicates a recommendation not to do something

may indicates permission to do something

need not indicates permission not to do something

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

can indicates that something is possible

cannot indicates that something is impossible

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

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

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

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

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

Introduction

The present document describes what structure and content Security Assurance Specifications (SCASes) that are to be adopted for use by NESAS shall meet.

It shall be ensured that 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. Organisations that develop SCASes shall adhere to the guidelines defined in the present document to ensure the quality of SCASes.

The NESAS Group will assess each SCAS that may be aimed for adoption under NESAS to ensure compliance with these guidelines, which may involve rejection of SCASes or requests to the developing organisation to make improvements to the candidate SCASes to ensure these guidelines are complied with. The adoption process is defined in GSMA PRD FS.62 [3]. The NESAS Group will engage in a process to facilitate continuous review and improvement of NESAS adopted SCASes.

The present document provides requirements on how to meet these objectives.

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 governance.

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

The Scheme Owner can add additional documentation using NESAS specifications and is responsible for developing and maintaining its own documents.

1 Scope

Authorised NESAS Security Test Laboratories perform security evaluations of Network Products against the security requirements and test cases defined in Security Assurance Specifications (SCASes), developed by 3GPP or other standards development organisations. Requirements for the development of SCASes are provided in the present document to ensure the necessary corresponding tests can be performed in a consistent and repeatable manner.

2 References

2.1 Normative references

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

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

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

- [1] 3GPP TS 33.117: Universal Mobile Telecommunications System (UMTS); LTE; Catalogue of general security assurance requirements
- [2] GSMA PRD AA.35: Procedures for Industry Specifications
- [3] GSMA PRD FS.62: Network Equipment Security Assurance Scheme – Adoption Procedure for Security Assurance Specifications
- [4] GSMA PRD FS.63: Network Equipment Security Assurance Scheme – List of Adopted Security Assurance Specifications

2.2 Informative references

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

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

- [i.1] 3GPP TS 33.501: 5G; Security architecture and procedures for 5G System
- [i.2] 3GPP TS 33.511 v18.0.0: Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class
- [i.3] 3GPP TR 33.926: Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes
- [i.4] NIST SP 800-30 Rev. 1 2012: NIST SP 800-30 Rev. 1, “Guide for Conducting Risk Assessments” September 2012., http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf
- [i.5] ISO/IEC 17025 2017: “General requirements for the competence of testing and calibration laboratories“

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

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

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 Class: A class of products that implements a common set of functionalities.

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.

Scheme Owner: Organisation or authority responsible for developing and maintaining 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).

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 NIST SP 800-30 Rev1 2012 [i.4].

3.2 Symbols

Symbols are not applicable in the present document.

3.2 Abbreviations

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

3GPP	Third Generation Partnership Project
TR	Technical Report
TS	Technical Specification
ISAG	Industry Specification Approval Group
NESAS	Network Equipment Security Assurance Scheme
NPCD	Network Product Class Description
PRD	Permanent Reference Document
PuE	Product under Evaluation
SCAS	Security Assurance Specification
SDO	Standards Development Organisation
SPD	Security Problem Definition

4 Security Assurance Specification Structure

For Security Assurance Specifications (SCASes), a Network Product Class Description (NPCD), a Security Problem Definition (SPD), security requirements and the relevant corresponding test cases shall be provided. Those elements can be documented in the SCASes or referenced. The Network Products are evaluated against the SCASes. SCASes apply to Network Functions and may be developed internally by GSMA or by an appropriate internationally recognised standards development organisation.

When developing a SCAS, it is essential that the developing organisation adheres to a structure that ensures the final specification meets certain quality requirements to ensure it has utility for the NESAS Security Test Laboratories and that it can be applied consistently. SCASes, for adoption by NESAS shall comply with the following minimum requirements:

- Are published in the English language,
- Are controlled documents with a clear version number/reference and a record of the formal approval by the publishing organisation,
- Describe the Network Functions to which the SCASes apply,
- Include a catalogue of security requirements and related test cases that describe the purpose of the tests, pre-conditions, execution steps, expected results and expected format of evidence to ensure verifiability and repeatability, in accordance with ISO/IEC 17025 2017 [i.5].

The process of writing SCAS documents for a given Network Product Class follows these steps:

- Provide a Network Product Class Description (NPCD): the Network Product Class is described in terms of software, hardware, interfaces and a set of functionalities so as to ensure that the security requirements can clearly describe what data and functions are intended to be protected and which functionalities shall be present, e.g. the physical and logical interfaces the product class supports to interact with external entities and the major functionalities of the Network Product Class. The description of the Network Product Class will be used as an input for the Security Problem Definition.
- Describe a Security Problem Definition (SPD): the security problem is described by identifying assets in the description of the Network Product Class that require protection and by describing how these assets can be exploited by an attacker. This part also contains the threat analysis employed to understand how an attacker performing the identified potential attacks could misuse the identified assets of the Network Product Class. This provides a concrete security problem that is to be solved, which allows the selection of security requirements that are necessary and sufficient to solve the identified security problem.
- Identify security requirements: The security requirements, which may include hardening requirements, are selected according to the Security Problem Definition and the requirements strictly related to the features implemented by the Network Product Class under analysis.
- Specify test cases: For each security requirement, the SCAS will define one or more test case(s) that verifies that the requirement is implemented by the product.

5 Requirements for Writing Security Problem Definition

5.1 General

For the Security Problem Definition (SPD) part of the SCAS writing phase, the steps to be accomplished for a given Network Product Class are:

- List the critical assets of the Network Product Class.
- Identify threats, i.e. attacker actions than can be performed on assets. The defined operating environment for the tested functionality assumes that the types of attackers, who are able to launch attacks, can be from the outside, as well as from the inside of this environment. This implies that the type of attackers to consider have

an attack potential 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. This assessment is accomplished during the SCAS writing phase and is related to the threat and risk analysis outcomes.

NOTE: For features that are (to some degree) proprietary and, hence, not (fully) standardized, a way of describing them in a general way needs to be found as, by their nature, no common understanding is generally available to the public. Without a general description of a feature, it could be difficult to perform a threat and risk analysis on it.

To ensure consistency across threats, the following set of guidelines should be applied when analysing proposed threats:

- Threat descriptions should avoid including security objectives or requirements or countermeasure implementation details.
- Check if there is an existing threat in another standard before attempting to create a new one. For example, a variant of an existing threat could be created.
- Attempt to map the threat to one of the existing threat categories before creating a new threat category.
- All threats should map to one or more threatened asset.

5.2 Threats Format

The structure for a threat description is provided here to indicate the information needed to produce a clear security problem definition. This can help to facilitate the identification of the security requirements. This following structure will be related to the threat modelling framework used for the analysis and consequently this proposal could be changed accordingly:

- **Threat Name:** each threat shall be assigned a unique name indicating the topics covered by the threat.
- **Threat Category:** a reference to the category to which the threat belongs based on the classification (threat methodology) that will be adopted.
- **Threat Description:** the adverse actions that can be performed by an attacker on an asset. These actions influence one or more properties of the asset from which that asset derives its value. Examples of attackers are perpetrators, users, computer processes, and accidents. The attacker can be further described by aspects, such as expertise, resources, opportunity, and motivation. Protection mechanisms or requirements are not selected.
- **Threatened Asset:** an indication of the Network Product assets that are object of the threat.

6 Requirements for Writing Security Requirements

6.1 General

A SCAS security requirement defines what has to be implemented in a specific Network Product Class to ensure the desired security baseline is achieved.

Each security requirement shall be defined in accordance with a structured approach with the participation of adequately qualified security experts, typically following a risk assessment or definition of the security problem to be addressed.

Each security requirement shall be testable. That is, the security requirement is to be specific enough so that test(s) can be written that effectively decide whether the requirement is fulfilled or not.

All security requirements need to be taken into account throughout the entire product development and lifecycle management by the Equipment Vendors to optimise the likelihood of the Network Product to pass a product security evaluation.

The security requirements will include security functional requirements as well as hardening requirements and Vulnerability testing requirements. The security functional requirements are intended to ensure the existence of security

functionalities in Network Products. Hardening requirements are intended to ensure the absence of unneeded or insecure functionality, or impose a restriction on a function forcing the Network Product to behave in a more secure way. Vulnerability testing requirements specify the areas to be subjected to Vulnerability testing.

It is essential that terminology used to describe security requirements is clear and consistent to avoid the risk of the requirements being misinterpreted. For example, if a requirement mentions "management traffic", a clear definition on what the "management traffic" is should be documented, and this will greatly assist NESAS Security Test Laboratories.

Each security requirement shall have at least one test case. Security requirements that are specific to a particular Network Product Class, shall always be derived from a threat analysis that is performed based on the technical specifications that define that Network Product Class.

6.2 Security Requirement Format

Descriptions of security requirements shall be clear, concise, and unambiguous. The following data points shall be used, as a minimum, when writing each security requirement:

- **Requirement Name:** Each requirement shall be assigned a unique name, indicating the topic covered by the requirement.
- **Requirement Reference:** A reference of the security requirement. An example of a reference can be <Specification> <clause>. If a requirement reference is not described, the requirement description can be derived from the industry practise.
- **Requirement Description:** A detailed description of the security requirement.
- **Threat Reference** may be provided that points to a document source that describes the identified threat as defined according to clause 0 to which the security requirement applies and to which it is defined to mitigate.

7 Requirements for Writing Test Cases

7.1 General

Test cases defined in SCASes shall be sufficiently specific to allow NESAS Security Test Laboratories to accurately, efficiently, and consistently assess if the security requirements have been fulfilled. The following guidelines shall be followed by organisations developing SCASes:

- Each test case shall be uniquely named and the purpose of the test shall be clearly defined to describe the aim of the test and what it is trying to demonstrate.
- Each test case shall apply to at least one specific security requirement.
- The test case shall correspond to the security requirement and shall not extend the requirement.

In the interests of simplifying document maintenance, duplication of test case descriptions shall be avoided. If a test case applies to multiple security requirements, it is sufficient to provide a reference to the original test case description where it subsequently applies in the SCAS.

7.2 Verifiability and Repeatability

The level of detail of a test case shall correspond to the detail of its associated security requirement. Tests shall be verifiable and, once performed, there shall be no ambiguity as to whether the test passed or failed. Tests shall be repeatable and a third party shall be able to repeat the tests defined in SCASes against the Product under Evaluation (PuE) and be able to verify whether the PuE passes or fails the tests.

For a test to be verifiable, it shall clearly specify the pre-conditions and the execution steps to be taken by the tester, to a level of detail sufficient to enable a third party to execute similar tests and achieve similar outcomes. The expected results shall also be defined and shall be sufficiently detailed to unambiguously determine whether the test passed or failed.

It is not necessary to document how the tests are written but the four essential elements that shall be present, clear, and unambiguous are as follows:

- The initial state of the Product under Evaluation and the pre-conditions for the tester,
- The steps taken to perform the test,
- The expected results of a successful test,
- The expected format of evidence.

7.3 Product Under Evaluation

With the exception of 3GPP TS 33.117, SCASes and the security requirements they contain, apply to a particular Network Function or group of Network Functions. Consequently, it is essential that the Network Function is clearly defined in the SCAS and that the tests that verify whether a security requirement has been met are mapped to a specific Network Function. The expected results of the tests should prove that the Network Product acts as expected.

7.4 Test Case Format

The following data points shall be used, as a minimum, when writing a test case:

- **Test Name:** Each test case shall be assigned a unique name, indicating the covered topic.
- **Purpose:** The goal of the test (i.e. what it is intended to check) shall be described.
- **Procedure and Execution steps:** The pre-conditions and the operational steps to perform the test shall be described.
- **Expected Results:** The expected results shall be described (i.e. the behaviour expected for the test).
- **Expected Format of Evidence:** The expected format of the evidence shall be described. If this is not applicable for a specific test, not applicable (NA) shall be noted.

Annex A (informative): SCAS Template

The main purpose of the template is to display the primary factors contained within the SCAS documents. However, it is not limiting in terms of content or format, and new clauses can be added as necessary. In addition, the "Network Product Class Description" and "asset and threat" clause, as well as the "security requirements and test cases" clause, can be separated into different specifications. The following shall be included:

Scope

The scope of the SCAS.

References

The references used in the SCAS.

Definitions and Abbreviations

The definitions and abbreviations used in the SCAS.

Conventions

Language conventions of the SDO shall be included here and be used consistently in the SCAS. NESAS specifications use the conventions set out in clause modal verbs terminology. Where an SDO's definitions differ from these, the SDO should provide a mapping between NESAS and the SDO's conventions so that SCASes from multiple SDOs can be used together without risk of conflicting conventions.

Guidance for Testing

Applicable guidance for testing, e.g. pre-requisites, tool requirements, and documentation requirements for testing.

Network Product Class Description

The Network Product Class description. An example is described in [i.2].

Assets and Threats

Assets and threats related to the Network Product Class Description. An example is described in [i.3].

Security Requirements and Test Cases

Security requirements and test cases related to the Network Product Class Description. An example is described in [i.2].

Annex B (informative): SCAS Network Product Class Description and Security Problem Definition Example

This text is copied from 3GPP TR 33.926 v18.0.0 [i.3], Annex D:

B.1 Network Product Class Description for the gNB

As part of the gNB network product, it is expected that the gNB to contain gNB application, a set of running processes (typically more than one) executing the software package for the gNB functions and OAM functions that are specific to the gNB network product model. Functionalities specific to the gNB network product introduce additional threats and/or critical assets as described below.

B.2 Assets and Threats Specific to the gNB

B.2.1 Critical assets

In addition to the critical assets of a GNP, the critical assets specific to the gNB to be protected are:

- gNB Application;
- Mobility Management data: e.g. subscriber's identities (e.g. SUCI, GUTI), subscriber keys (i.e. KUPenc, KUPint, KRRCenc, KRRCint, NH), authentication parameters, APN name, data related to mobility management like UE measurements, UE's IP address, etc., QoS and so on, etc.
- user plane data
- The interfaces of gNB whose data needs to be protected and which are within SCAS scope:
 - N2 interface
 - Xn interface
 - N3 interface
 - Uu interface
 - Console interface, for local access: local interface on gNB
 - OAM interface, for remote access: interface between gNB and OAM system
- gNB Software: binary code or executable code

NOTE 2: gNB files may be any file owned by a user (root user as well as non-root uses), including User account data and credentials, Log data, configuration data, OS files, gNB application, Mobility Management data or gNB Software.

B.2.2 Threats related to Control plane and User plane in the network

B.2.2.1 Control plane data confidentiality protection

- *Threat name:* gNB control plane data confidentiality protection.
- *Threat Category:* Information Disclosure.
- *Threat Description:* If the gNB does not provide confidentiality protection for control plane packets on the N2/Xn/Uu reference points, then the control plane packets sent over the N2/Xn/Uu reference points can be intercepted by attackers without detection. This means the UE identifiers, security capabilities, the security

algorithms and key materials exchanged can be accessed by the attackers leading to huge security breach. This threat scenario assumes that the N2 and Xn reference points are not within the security environment.

- *Threatened Asset:* Mobility Management data.

Annex C (informative): SCAS Security Requirement and Test Case Example

This text is copied from 3GPP TS 33.511 v18.0.0 [i.2], clause 4.2.2.1.1 :

Requirement Name:

Ciphering of RRC-signalling

Requirement Reference:

3GPP TS 33.501, clause 5.3.2

Requirement Description:

"The gNB shall support ciphering of RRC-signalling over the NG RAN air interface" as specified in 3GPP TS 33.501, clause 5.3.2 [i.1].

Threat references:

3GPP TR 33.926, clause D.2.2.1 – Control plane data confidentiality protection.

Test Name:

TC-CP-DATA-CIP-RRC-SIGN_gNB

Purpose:

To verify that the RRC-signalling data sent between UE and gNB over the NG RAN air interface are confidentiality protected.

Procedure and Execution steps:

Pre-Conditions:

- The gNB network product shall be connected in emulated/real network environments. The UE may be simulated.
- The tester shall have access to the NG RAN air interface or can capture the message at the UE.

Execution Steps

- 1) The UE sends a Registration Request to the AMF.
- 2) The AMF sends a KgNB and the UE security capability to the gNB.
- 3) The gNB selects an algorithm and sends AS SMC to the UE.
- 4) The gNB receive AS SMP from the UE.

Expected Results:

Control plane packets sent to the UE after the gNB sends AS SMC is ciphered.

Expected Format of Evidence:

Evidence suitable for the interface, e.g. Screenshot containing the operational results.

History

Version	Date	Brief Description of Change
1.0	Jul 2023	First version developed to provide guidance on SCAS development.
2.0	Feb 2025	Removal of SCAS adoption procedure, alignment of definitions and references, fixed normative language