NESAS Security Assurance Specification Development Requirements

Version 1.0

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 3
1.1 Scope 3
1.2 Document Maintenance 3
1.3 Definitions 3
1.4 Abbreviations 4
1.5 References 4
1.6 Conventions 4
2 Security Assurance Specification Structure 5
3 Requirements for Writing Security Problem Definition 6
3.1 General 6
3.2 Threats Format 6
4 Requirements for Writing Security Requirements 7
4.1 General 7
4.2 Security Requirement Format 8
5 Requirements for Writing Test Cases 8
5.1 General 8
5.2 Verifiability and Repeatability 8
5.3 Product Under Evaluation 9
5.4 Test Case Format 9
Annex A SCAS Template 9
Annex B SCAS Network Product Class Description and Security Problem Definition Example (Informative) 11
Annex C SCAS Security Requirement and Test Case Example (Informative) 12
Annex D Document Management 13
D.1 Document History 13
D.2 Licensing of NESAS Documentation 13
D.3 Other Information 13

1 Introduction

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

GSMA recognises the need 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 requires organisations that develop SCASes to adhere to the requirements defined in this document to ensure the quality of SCASes.

GSMA will assess each SCAS that may be aimed for adoption under NESAS to ensure compliance with these requirements, which may involve rejection of SCASes or requests to the developing organisation to make improvements of the adopted SCAS to ensure these requirements are complied with. The adoption process is described in Annex A in FS.47 [5]. GSMA will engage in a process to facilitate continuous review and improvement of NESAS adopted SCASes.

This document defines requirements to meet these objectives.

1.1 Scope

Accredited 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 this document to ensure the necessary corresponding tests can be performed in a consistent and repeatable manner.

1.2 Document Maintenance

NESAS was originally created and developed by GSMA and responsibility for its maintenance and development of the NESAS specifications rests with the GSMA's 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, who adopts NESAS and may add additional documentation, is responsible for development and maintenance of its own documents.

1.3 Definitions

Term	Description
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.

Term	Description
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.
Product under Evaluation	The Network Product for which an evaluation is sought by the Equipment Vendor.
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).
Testing Environment	Hardware, software and infrastructure necessary to evaluate (operate) the Product under Evaluation.

1.4 Abbreviations

Term	Description
3GPP	Third Generation Partnership Project
3GPP TR	3GPP Technical Report
3GPP TS	3GPP Technical Specification
NESAS	Network Equipment Security Assurance Scheme
NPCD	Network Product Class Description
SCAS	Security Assurance Specification
SDO	Standards Development Organisation
SPD	Security Problem Definition

1.5 References

Ref	Doc Number	Title
[1]	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
[2]	ISO/IEC 17025	General requirements for the competence of testing and calibration laboratories
[3]	3GPP TR 33.926	Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes
[4]	3GPP TS 33.511	Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class
[5]	GSMA PRD FS.47	NESAS - Product and Evidence Evaluation Methodology

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 Security Assurance Specification Structure

For Security Assurance Specifications (SCASes), Network Product Class Description (NPCD), 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:

- Is published in the English language ,
- Is a controlled document with a clear version number/reference and a record of the formal approval by the publishing organisation,
- Describes the Network Functions to which the SCAS applies,
- Includes 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 [2].

The process of writing SCAS documents for a given network product class follows these steps:

- Provide 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 are required, e.g. the physical and logical interfaces the product class supports to interact with external entities and the major functionalities of the NPC. The description of network product class will be used as an input for Security Problem Definition.
- Describe 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 step 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, SCAS will define one or more test case(s) that verifies that the requirement is implemented by the product.

3 Requirements for Writing Security Problem Definition

3.1 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 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 requirements 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.

3.2 Threats Format

The structure for a threat description is provided here to indicate the information needed for having 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 hackers, users, computer processes, and accidents. The attacker may 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.

4 Requirements for Writing Security Requirements

4.1 General

A SCAS security requirement defines what has to be implemented in a specific 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 defines that network product class.

4.2 Security Requirement Format

Descriptions of security requirements must 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 reference can be <Specification> <clause>. If requirement reference is not described, the requirement description can be derived from the industry practise.
- **Requirement Description**: A detailed description of the security requirement.

Optionally, a **Threat Reference** may be provided that points to a document source that describes the identified threat as defined according to Section 3 to which the security requirement applies and to which it is defined to mitigate.

5 Requirements for Writing Test Cases

5.1 General

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

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

In the interests of simplifying document maintenance, duplication of test case descriptions should 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.

5.2 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 should 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 target of evaluation and be able to verify whether the target passes or fails the tests.

For a test to be verifiable, it needs to 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 target of 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.

5.3 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.

5.4 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 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 sections can be added as necessary. In addition, the "network product class description" and "asset and threat" section, as well as the "security requirements and test cases" section, can be separated into different specifications. The following shall be included:

Scope

The scope of SCAS.

References

The references used in SCAS.

Definitions and Abbreviations

The definitions and abbreviations used in 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 Section 1.6. 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 the testing.

Network Product Class Description

Network product class description. An example is described in 0.

Assets and Threats

Assets and threats related to the network product class description. An example is described in 0.

Security Requirements and Test Cases

Security requirements and test cases related to the network product class description. An example is described in Annex C.

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

This text is copied from 3GPP TR 33.926 v18.0.0 [3]:

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.

2. Assets and Threats Specific to the gNB

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.

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

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 SCAS Security Requirement and Test Case Example (Informative)

This text is copied from 3GPP TR 33.511 v18.0.0 [4]:

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.

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.

Annex D Document Management

D.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	July 2023	First version developed to provide guidance on SCAS development	GSMA ISAG	James Moran, GSMA

D.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.

D.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.