ETSI TR 133 926 V17.9.0 (2024-04)

LTE;
5G;
Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes (3GPP TR 33.926 version 17.9.0 Release 17)

Reference
RTR/TSGS-0333926vh90

Keywords
5G,LTE

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

This Technical Report (TR) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found under https://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

Y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

The present document captures the network product class descriptions, threats and critical assets that have been identified in the course of the work on 3GPP security assurance specifications. The main body of the present document contains generic aspects that are believed to apply to more than one network product class, while Annexes cover the aspects specific to one network product class.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TR 33.916: "Security Assurance Methodology for 3GPP network products classes".

[3] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".

[4] 3GPP TR 33.821: "Rationale and track of security decisions in Long Term Evolution (LTE) RAN/3GPP System Architecture Evolution (SAE)".

[5] 3GPP TS 33.116: "Security Assurance Specification for MME network product class".

[6] 3GPP TS 33.511: "5G Security Assurance Specification (SCAS); NR Node B (gNB)"

[7] 3GPP TS 38.300 v15: "NR; NR and NR-RAN Overall Description; Stage 2".

[8] 3GPP TS 23.501 v15: "System Architecture for 5G System; Stage 2".

[9] 3GPP TS 38.323 v15: "NR; Packet Data Convergence Protocol (PDCP) specification".

[10] 3GPP TS 38.322 v15: "NR; Radio Link Control (RLC) protocol specification".

[11] 3GPP TS 33.250: "Security assurance specification for the PGW network product class".

[12] 3GPP TS 33.516: "5G Security Assurance Specification (SCAS) for the AUSF network product class".

[13] 3GPP TS 33.517: "5G Security Assurance Specification (SCAS) for the Security Edge Protection Proxy (SEPP) network product class".

[14] 3GPP TS 33.501 Release 15: "Security architecture and procedures for 5G system".

[15] 3GPP TS 33.518: "5G Security Assurance Specification (SCAS) for the Network Repository Function (NRF) network product class".

[16] 3GPP TS 33.519: "5G Security Assurance Specification (SCAS) for the Network Exposure Function (NEF) network product class".

[17] 3GPP TS 33.117: "Catalogue of general security assurance requirements".

[18] 3GPP TS 33.513: "5G Security Assurance Specification (SCAS); User Plane Function (UPF)".

[19] 3GPP TS 36.300: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN);Overall description;Stage 2."

[20] 3GPP TS 33.216: "Security Assurance Specification (SCAS) for the evolved Node B (eNB) network product class."

[21] 3GPP TS 33.514: "5G Security Assurance Specification (SCAS) for the Unified Data Management (UDM) network product class".

[22] 3GPP TS 33.512: "5G Security Assurance Specification (SCAS); Access and Mobility management Function (AMF)".

[23] 3GPP TS 33.521: "Security Assurance Specification (SCAS) for the Network Data Analytics Function (NWDAF) network product class".

[24] 3GPP TS 23.288: " Architecture enhancements for 5G System (5GS) to support network data analytics services".

[25] 3GPP TS 33.226: "Security assurance for IP Multimedia Subsystem (IMS)".

[26] 3GPP TS 33.501: "Security architecture and procedures for 5G system" (Release 16).

[27] 3GPP TS 33.522: "5G Security Assurance Specification (SCAS); Service Communication Proxy (SCP)".

[28] 3GPP TS 23.501: "System Architecture for 5G System; Stage 2" (Release 16).

[29] 3GPP TS 33.326: "Security Assurance Specification (SCAS) for the Network Slice-Specific Authentication and Authorization Function (NSSAAF) network product class".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

GNP Class (**Generic Network Product Class):** generic network product class is a class of network products that all implement a common set of 3GPP-defined functionalities for that particular network product

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

GNP	Generic Network Product
SCAS	Security Assurance Specification
SECAM	Security Assurance Methodology

4 Generic Network Product (GNP) class description

4.1 Overview

A 3GPP generic network product class defines a set of functions that are implemented on that product, which includes, but not limited to minimum set of common 3GPP functions for that product covered in 3GPP specifications, other functions not covered by 3GPP specifications, as well as interfaces to access that product. A generic network product also includes hardware, software, and OS components that the product is implemented on. The current document describes the threats and the critical assets in the course of developing 3GPP security assurance specifications for a particular network product class.

Applicability of the GNP security assurance specification to products: Assume a telecom equipment vendor wants to sell a product to an operator, and the latter is interested in following the Security Assurance Methodology as described in TR 33.916[2], then, before evaluation according to TR 33.916[2] in a testing laboratory can start, it first needs to be determined which security assurance specifications written by 3GPP apply to the given product.

Each 3GPP Network Product, is basically a device composed of hardware (e.g. chip, processors, RAM, network cards), software (e.g. operating system, drivers, applications, services, protocols), and interfaces (e.g. console interfaces and O&M interfaces) that allow the 3GPP network product to be managed and configured locally and/or remotely A GNP is a 3GPP network product.

GNP Security Assurance Specification (GNP SCAS): The GNP SCAS provides a description of the security requirements (which are including test cases) pertaining to that generic network product class.

Need for a GNP network product model: This minimum set of functions listed in clause 4.2 is exclusively meant as a membership criterion for the GNP Class. It is not meant to restrict the functionality of a GNP, or the scope of the present document in any way. On the contrary, it is clear that GNPs will contain many more functions than those from the minimum set listed in clause 4.2, and the GNP will contain requirements relating to functions not contained in this minimum set. Some of these functions, beyond the minimum set, can be found from various 3GPP specifications, but by far not all these functions. This implies that there is a need to describe the functions that cannot be found from 3GPP specifications in some other way before the GNP can be written so that the GNP can make reference to this description. This description is the GNP model, cf. clause 4.3.

EXAMPLE 1: 3GPP specifications do not describe a local management interface, but the GNP will have to take it into account, so a local management interface needs to be part of an GNP model.

EXAMPLE 2: The GNP sometimes says e.g.: "Authentication events on the local management interface shall be logged." This implies the presence of a logging function. The logging function is not part of the defining minimum set of functions from clause 4.2. If a product implements this minimum set, but no logging function, then this just means that the product is a GNP, but will fail the evaluation against the GNP SCAS.

The GNP model is further used in clauses 5 and 6 in various ways, e.g. the critical assets can point to parts of the GNP model, threats and requirements can refer to interfaces shown in the GNP model, etc.