ETSI TR 133 926 V15.2.0 (2019-10)

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/150c94a-674c-4c66-870f-2f57cf6bfcc9/etsi-tr-133-926-v15.2.0-2019-10

LTE;
Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes
(3GPP TR 33.926 version 15.2.0 Release 15)

Reference

RTR/TSGS-0333926vf20

Keywords

LTE,SECURITY

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 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.
The content of the PDF version shall not be modified without the written authorization of ETSI.
The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2019.
All rights reserved.

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.

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is 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 IPR Policy, no investigation, 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.

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 http://webapp.etsi.org/key/queryform.asp.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/b150c94a-674c-4c6e-87f6-2f57cf6bfce9/etsi-tr-133-926-v15.2.0-2019-10

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/b150c94a-674c-4ce6-870f-2f57cf6bfcc9/etsi-tr-133-926-v15.2.0-2019-10

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/0156e94a-674c-4c66-870f-2f57cf6bfcc9/etsi-tr-133-926-v15.2.0-2019-10

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/b150e94a-674c-4c66-870f-2f57cf6bfcc9/etsi-tr-133-926-v15.2.0-2019-10

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/b150c94a-674c-4c66-870f-2f57cf6bfcc9/etsi-tr-133-926-v15.2.0-2019-10

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 33.250: "Security assurance specification for the PGW network product class".

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/150e4da-674c-4c...870f-2f57cf05fcc9/etsi-tr-133-926-v15.2.0-2019-10

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.

4.2 Minimum set of functions defining the GNP class

According to TR 33.916 [2], a network product class is a class of products that all implement a common set of 3GPP-defined functionalities. This common set is defined to be the list of functions contained in pertinent 3GPP specifications, such as clause 4.3 of 3GPP TS 23.401 [3], Release 8 [3].

NOTE: The reason why the definition of the common set of functions refers to a particular Release 8 version of TS 23.401 [3], contrary to what is customary in 3GPP when referencing other 3GPP specifications, is that a Security Assurance Specification is to avoid having a moving target when defining a network product class. Nevertheless, the set of functions in clause 4.3.1 of 3GPP TS 23.401, Release 8 [3] is expected to be stable, as only FASMO corrections are allowed to Release 8. Furthermore, this set is believed to be minimal, i.e. implemented by all network products, which may not be true for the corresponding set of functions from later releases of TS 23.401 [3]. For the description of these functions compliance with TS 23.401 Release 8 [3] later version is allowed as, obviously, a generic network product should still remain a member of the GNP class when it implements a FASMO correction to Release 8.

4.3 Generic network product model

4.3.1 Generic network product model overview

Figure 4.3-1 depicts the components of a generic network product model at a high level. These components are further described in the following subclauses.

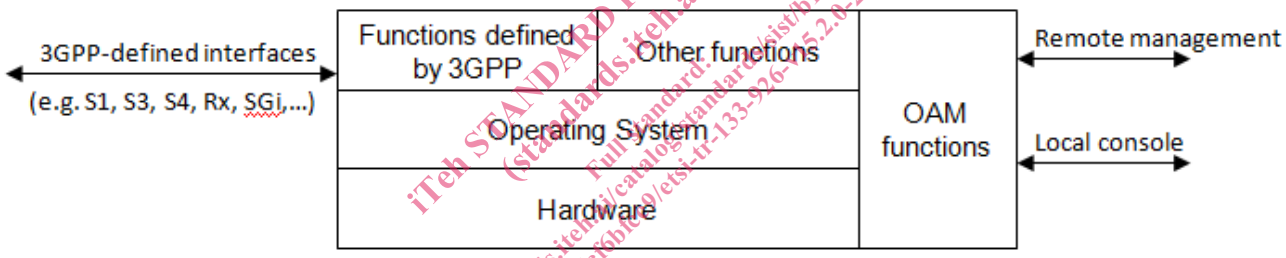

Figure 4.3-1: GNP model

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/b150c94a-174c-4e66-870f-657c6b1e/etsi-tr-133-926-v15.2.0-2019-10

4.3.2 Functions defined by 3GPP

A GNP will, in many cases, implement 3GPP-defined functions from various releases of pertinent 3GPP specifications. Vendors are, to a large extent, free to select the features implemented in their GNPs. E.g. a GNP could lack support for relay nodes, as introduced in Release 10, but implement all other features defined up to and including Release 10.

4.3.3 Other functions

A GNP will also contain functionality not or not fully covered in 3GPP specifications.

Examples include, but are not limited to, local or remote management functions.

4.3.4 Operating System (OS)

The present document assumes that the GNP is implemented on dedicated hardware that requires an operating system to run.

4.3.5 Hardware

The present document assumes that the GNP is implemented on dedicated hardware. Aspects of virtualization and cloud are not taken into account in the present version.

NOTE: Aspects of virtualization and cloud are FFS in future releases of the GNP SCAS. They deserve separate study for finding out how to define the boundaries between the GNP class and the hosting environment (e.g. shared HW and Virtual Machine) and which security assumptions to make on this environment.

4.3.6 Interfaces

There are two types of logical interfaces defined for the GNP:

- remote logical interfaces; and
- local logical interfaces.

A **remote logical interface** is an interface which can be used to communicate with the GNP from another network node.

The entire protocol stack implementing the communication is considered to be part of the remote logical interface.

Remote Logical Interfaces also include the remote access interfaces to the GNP for its maintenance through e.g. an Element Management System (EMS).

A **local logical interface** is an interface that can be used only via physical connection to the GNP. That is, the connection requires physical access to the GNP.
The entire protocol stack is considered to be part of the local logical interface. The entire protocol stack and the physical parts of the interface can be used by local connections.

Local Logical Interfaces also include the local hardware interfaces and the Local Maintenance Terminal interface (LMT) of the GNP used for its maintenance through a console.

This means that for both, **local and remote logical interfaces**, the GNP model does not only cover the application layer protocol, for which a GNP function terminates the interface (e.g. S5), but also the protocols (e.g. SCTP, IP, Ethernet, USB) in the protocol stack below the application layer protocol.

There are some major differences between local and remote interfaces from security perspective. For example attaching to a local interface may cause execution of complex internal procedures in the GNP like loading USB device drivers, enumeration of attached devices, mounting file systems etc.

A GNP hosts the following interfaces:

Remote logical interfaces:

- Service interfaces that are defined in pertinent 3GPP specifications
- Service interfaces that are not defined by 3GPP
- Remote OAM interface
- EMS (Element Management System) interface

Local logical interfaces:

- OAM local console
- LMT (Local Maintenance Terminal) interface
- GNP local hardware interfaces

NOTE: There is some overlap between the present clause 4.3.6 and clauses 4.3.1 and 4.3.2 in as far as a GNP function (e.g. S5) is part of the termination point for a logical interface.

4.4 Scope of the present document

4.4.1 Introduction

The present subclause refers to the GNP model in clause 4.3.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
https://standards.iteh.ai/catalog/standards/sist/b150c94a-674c-4f66-870f-2f57cf6bfcc9/etsi-tr-133-926-v15.2.0-2019-10