

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)**

[ETSI TR 133 926 V17.9.0 \(2024-04\)](https://standards.iteh.ai/catalog/standards/etsi/cd631f6f-8388-4214-b179-7d43ee024073/etsi-tr-133-926-v17-9-0-2024-04)

<https://standards.iteh.ai/catalog/standards/etsi/cd631f6f-8388-4214-b179-7d43ee024073/etsi-tr-133-926-v17-9-0-2024-04>



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

Important notice

The present document can be downloaded from:

<https://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/CommitteeSupportStaff.aspx>

If you find a security vulnerability in the present document, please report it through our

Coordinated Vulnerability Disclosure Program:

<https://www.etsi.org/standards/coordinated-vulnerability-disclosure>

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.

No recommendation as to products and services or vendors is made or should be implied.

No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.

In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

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 2024.
All rights reserved.

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. (2024-04)

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

Intellectual Property Rights	2
Legal Notice	2
Modal verbs terminology.....	2
Foreword.....	10
1 Scope	11
2 References	11
3 Definitions and abbreviations.....	12
3.1 Definitions	12
3.2 Abbreviations	12
4 Generic Network Product (GNP) class description.....	13
4.1 Overview	13
4.2 Minimum set of functions defining the GNP class.....	14
4.3 Generic network product model	14
4.3.1 Generic network product model overview.....	14
4.3.2 Functions defined by 3GPP	14
4.3.3 Other functions	14
4.3.4 Operating System (OS).....	14
4.3.5 Hardware	14
4.3.6 Interfaces.....	15
4.4 Scope of the present document.....	15
4.4.1 Introduction.....	15
4.4.2 Scope regarding GNP functions defined by 3GPP	16
4.4.3 Scope regarding other functions	16
4.4.4 Scope regarding Operating System (OS)	16
4.4.5 Scope regarding hardware	16
4.4.6 Scope regarding interfaces.....	16
5 Generic assets and threats.....	16
5.1 Introduction	16
5.2 Generic critical assets	16
5.3 Generic threats.....	17
5.3.0 Generic threats format	17
5.3.1 Introduction.....	17
5.3.2 Threats relating to 3GPP-defined interfaces	18
5.3.3 Spoofing identity	18
5.3.3.1 Default Accounts.....	18
5.3.3.2 Weak Password Policies	18
5.3.3.3 Password peek.....	19
5.3.3.4 Direct Root Access.....	19
5.3.3.5 IP Spoofing	19
5.3.3.6 Malware	19
5.3.3.7 Eavesdropping.....	19
5.3.4 Tampering.....	20
5.3.4.1 Software Tampering.....	20
5.3.4.2 Ownership File Misuse	20
5.3.4.3 External Device Boot	20
5.3.4.4 Log Tampering.....	20
5.3.4.5 OAM Traffic Tampering.....	20
5.3.4.6 File Write Permissions Abuse.....	21
5.3.4.7 User Session Tampering	21
5.3.5 Repudiation.....	21
5.3.5.1 Lack of User Activity Trace.....	21
5.3.6 Information disclosure	21
5.3.6.1 Poor key generation.....	21

5.3.6.2	Poor key management	22
5.3.6.3	Weak cryptographic algorithms	22
5.3.6.4	Insecure Data Storage	22
5.3.6.5	System Fingerprinting	22
5.3.6.6	Malware	22
5.3.6.7	Personal Identification Information Violation.....	23
5.3.6.8	Insecure Default Configuration.....	23
5.3.6.9	File/Directory Read Permissions Misuse	23
5.3.6.10	Insecure Network Services.....	23
5.3.6.11	Unnecessary Services.....	23
5.3.6.12	Log Disclosure	24
5.3.6.13	Unnecessary Applications.....	24
5.3.6.14	Eavesdropping.....	24
5.3.6.15	Security threat caused by lack of GNP traffic isolation	24
5.3.7	Denial of service.....	25
5.3.7.1	Compromised/Misbehaving User Equipments.....	25
5.3.7.2	Implementation Flaw	25
5.3.7.3	Insecure Network Services.....	25
5.3.7.4	Human Error	25
5.3.8	Elevation of privilege.....	26
5.3.8.1	Misuse by authorized users	26
5.3.8.2	Over-Privileged Processes/Services.....	26
5.3.8.3	Folder Write Permission Abuse	26
5.3.8.4	Root-Owned File Write Permission Abuse	26
5.3.8.5	High-Privileged Files	26
5.3.8.6	Insecure Network Services.....	27
5.3.8.7	Elevation of Privilege via Unnecessary Network Services	27
6	Generic assets and threats for network functions supporting SBA interfaces.....	27
6.1	Introduction	27
6.2	Generic critical assets.....	27
6.3	Generic threats.....	28
6.3.1	Introduction.....	28
6.3.2	Threats related to Service Based Interfaces	28
6.3.2.1	JSON Parser Exploits.....	28
6.3.2.2	JSON Parser not Robust.....	28
6.3.3	Threats related to service access	28
6.3.3.1	Elevation of privilege via incorrect verification of access tokens.....	28
6.3.4	Threats related to authentication for indirect communication	29
6.3.4.1	Incorrect validation of client credentials assertion.....	29
Annex A:	Aspects specific to the network product class MME	30
A.1	Network product class description for the MME	30
A.1.1	Introduction	30
A.1.2	Minimum set of functions defining the MME network product class	30
A.2	Assets and threats specific to the MME	30
A.2.1	Critical assets.....	30
A.2.2	Threats related to AKA procedures	31
A.2.2.1	Access to 2G.....	31
A.2.2.2	Resynchronization	31
A.2.2.3	Failed Integrity check of Attach message	31
A.2.2.4	Forwarding EPS authentication data to SGSN	31
A.2.2.5	Forwarding unused EPS authentication data between different security domains.....	31
A.2.3	Threats related to security mode command procedure	32
A.2.3.1	Bidding Down.....	32
A.2.3.2	NAS integrity selection and use.....	32
A.2.3.3	NAS NULL integrity protection	32
A.2.3.4	NAS confidentiality protection.....	32
A.2.4	Threats related to security in Intra-RAT mobility	32
A.2.4.1	Bidding down on X2-Handover.....	32

A.2.4.2	NAS integrity protection algorithm selection in MME change	33
A.2.5	Threats related to security in Inter-RAT mobility	33
A.2.5.1	2G SIM access via idle mode mobility	33
A.2.5.2	2G SIM access via handover.....	33
A.2.5.3	2G SIM access via SRVCC	33
A.2.6	Threats related to release of non-emergency bearer	33
Annex B: Aspects specific to the network product class PGW		35
B.1	Network product class description for the PGW	35
B.1.1	Introduction	35
B.1.2	Minimum set of functions defining the PGW network product class.....	35
B.2	Assets and threats specific to the PGW	35
B.2.1	Critical assets.....	35
B.2.2	Threats related to IP Address Allocation.....	36
B.2.2.1	IP Address Reallocation Continuously	36
B.2.3	Packet Forwarding.....	36
B.2.3.1	Sending unauthorized packets to other UEs	36
B.2.4	Emergency PDN Connection	36
B.2.4.1	Inactive Emergency PDN Connection Release.....	36
B.2.5	Threats related to charging relevant data.....	36
B.2.5.1	Failure to assign unique TEID or Charging ID for a session.....	36
Annex C: Aspects specific to the network product class eNB		38
C.1	Network product class description for the eNB	38
C.1.1	Introduction.....	38
C.1.2	Minimum set of functions defining the eNB network product class	38
C.2	Assets and threats specific to the eNB	38
C.2.1	Critical assets.....	38
C.2.2	Threats related to Control plane and User plane	39
C.2.2.1	Control plane data confidentiality protection.....	39
C.2.2.2	Control plane data integrity protection	39
C.2.2.3	User plane data ciphering and deciphering at eNB	39
C.2.2.4	User plane data integrity protection	39
C.2.3	Threats related to key reuse	40
C.2.3.1	Key reuse for eavesdropping	40
Annex D: Aspects specific to the network product class gNB.....		41
D.1	Network product class description for the gNB	41
D.1.1	Introduction.....	41
D.1.2	Minimum set of functions defining the gNB network product class	41
D.2	Assets and threats specific to the gNB	41
D.2.1	Critical assets.....	41
D.2.2	Threats related to Control plane and User plane in the network.....	42
D.2.2.1	Control plane data confidentiality protection.....	42
D.2.2.2	Control plane data integrity protection	42
D.2.2.3	User plane data confidentiality protection at gNB	42
D.2.2.4	User plane data integrity protection.....	42
D.2.2.5	AS algorithm selection and use.....	43
D.2.2.6	Bidding down on Xn-Handover.....	43
D.2.2.7	Key Reuse.....	43
D.2.2.8	Security Policy Enforcement	43
D.2.2.9	State transition from inactive state to connected state	43
Annex E: Aspects specific to the network product class UDM.....		45
E.1	Network product class description for the UDM	45
E.1.1	Introduction	45
E.1.2	Minimum set of functions defining the UDM network product class	45

E.2	Assets and threats specific to the UDM	45
E.2.1	Critical assets.....	45
E.2.2	Threats related to UDM assets	46
E.2.2.1	Incorrect SUCI de-concealment.....	46
E.2.2.2	Synchronization failure.....	46
E.2.2.3	Failure to store the authentication status.....	46
E.2.2.4	Incorrect security enforcement configuration	46
E.2.2.5	Incorrect UP security policy configuration for 5G LAN service	46
Annex F:	Aspects specific to the network product class AUSF	48
F.1	Network product class description for the AUSF.....	48
F.1.1	Introduction.....	48
F.1.2	Minimum set of functions defining the AUSF network product class	48
F.2	Assets and threats specific to the AUSF.....	48
F.2.1	Critical assets.....	48
F.2.2	Threats related to authentication procedures	49
Annex G:	Aspects specific to the network product class SEPP.....	50
G.1	Network product class description for the SEPP.....	50
G.1.1	Introduction	50
G.1.2	Minimum set of functions defining the SEPP network product class	50
G.2	Assets and threats specific to the SEPP.....	50
G.2.1	Critical assets.....	50
G.2.2	Threats related to cryptographic material in the SEPP.....	51
G.2.2.1	Misusing cryptographic material of peer SEPPs and IPX providers.....	51
G.2.2.2	Misusing cryptographic material beyond connection-specific scope.....	51
G.2.3	Threats related to error handling in the SEPP	51
G.2.3.1	Incorrect handling for PLMN ID mismatch.....	51
G.2.3.2	Incorrect handling for protection policies mismatch	52
G.2.4	Threats related to sensitive information exposure	52
G.2.4.1	Weak JWS algorithm	52
G.2.4.2	Exposure of confidential IEs in N32-f message.....	53
G.2.5	Threats related to TLS protection between NF and SEPP	53
G.2.5.1	Inter-PLMN routing using the incorrect reference.....	53
G.2.5.2	Tampering of Target API Root.....	53
Annex H:	Aspects specific to the network product class NRF	55
H.1	Network product class description for the NRF.....	55
H.1.1	Introduction	55
H.1.2	Minimum set of functions defining the NRF network product class.....	55
H.2	Assets and threats specific to the NRF.....	55
H.2.1	Critical assets.....	55
H.2.2	Threats related to NRF authorization	56
H.2.2.1	No slice specific authorization for NF discovery.....	56
Annex I:	Aspects specific to the network product class NEF	57
I.1	Network product class description for the NEF	57
I.1.1	Introduction.....	57
I.1.2	Minimum set of functions defining the NEF network product class	57
I.2	Assets and threats specific to the NEF	57
I.2.1	Critical assets.....	57
I.2.2	Threats related to NEF assets	58
I.2.2.1	No authentication on application function	58
I.2.2.2	No authorization on northbound APIs	58
Annex J:	Aspects specific to the network product class SMF	59

J.1	Network product class description for the SMF.....	59
J.1.1	Introduction.....	59
J.1.2	Minimum set of functions defining the SMF network product class.....	59
J.2	Assets and threats specific to the SMF.....	59
J.2.1	Critical assets.....	59
J.2.2	Threats related to SMF assets.....	60
J.2.2.1	Priority of UP security policy	60
J.2.2.2	TEID uniqueness failure	60
J.2.2.3	Charging ID Uniqueness failure	60
J.2.2.3	UP security policy check	60
Annex K:	Aspects specific to the network product class AMF	61
K.1	Network product class description for the AMF.....	61
K.1.1	Introduction	61
K.1.2	Minimum set of functions defining the AMF network product class.....	61
K.2	Assets and threats specific to the AMF	61
K.2.1	Critical assets.....	61
K.2.2	Threats related to AKA procedures	62
K.2.2.1	Resynchronization	62
K.2.2.2	Failed Integrity check of Initial Registration message.....	62
K.2.2.3	RES* verification failure	62
K.2.3	Threats related to security mode command procedure	62
K.2.3.1	Bidding Down.....	62
K.2.3.2	NAS integrity selection and use.....	63
K.2.3.3	NAS NULL integrity protection	63
K.2.3.4	NAS confidentiality protection	63
K.2.4	Threats related to security in Intra-RAT mobility	63
K.2.4.1	Bidding down on Xn-Handover.....	63
K.2.4.2	NAS integrity protection algorithm selection in AMF change	63
K.2.5	Threats related to release of non-emergency bearer	64
K.2.6	Threats related to initial registration procedure.....	64
K.2.6.1	Invalid or unacceptable UE security capabilities	64
K.2.7	Threats related to 5G-GUTI allocation.....	64
K.2.7.1	Failure to allocate new 5G-GUTI	64
K.2.8	NAS based redirection from 5GS to EPS in 5G CIoT.....	64
K.2.9	Threat related to Security for 5G CIoT	65
K.2.9.1	Failed Verification of UE Identity during RRC Reestablishment Procedure for CP CIoT 5GS Optimization	65
K.2.10	Threats related to session establishment procedure.....	65
K.2.10.1	Incorrect validation of S-NSSAIs	65
Annex L:	Aspects specific to the network product class UPF.....	66
L.1	Network product class description for the UPF	66
L.1.1	Introduction	66
L.1.2	Minimum set of functions defining the UPF network product class	66
L.2	Assets and threats specific to the UPF	66
L.2.1	Critical assets.....	66
L.2.2	Threats related to user plane data transport	67
L.2.3	Threats related to signalling data.....	67
L.2.4	Threats related to TEID.....	67
L.2.5	Threats related to user plane data forwarding.....	67
L.2.6	Threats related to malformed GTP-U messages.....	68
Annex M:	Void	69
Annex N:	Aspects specific to the network product class NWDAF	70
N.1	Network product class description for the NWDAF	70
N.1.1	Introduction	70

N.1.2	Minimum set of functions defining the NWDAF network product class	70
N.2	Assets and threats specific to the NWDAF	70
N.2.1	Critical assets	70
N.2.2	Void	71
Annex O: Aspects specific to the IMS network product classes		72
O.1	Network product class description for the IMS	72
O.1.1	Introduction	72
O.1.2	Minimum set of functions defining the IMS network product classes	72
O.2	Assets and threats specific to the P-CSCF	72
O.2.1	Critical assets	72
O.2.2	Threats related to set-up of security associations	73
O.2.2.1	High-priority algorithm selection	73
O.2.2.2	Bidding down on security association set-up	73
O.2.3	Threats related to IMS signalling transport	73
O.2.4	Threats related to SPI allocation	73
O.3	Assets and threats specific to the S-CSCF	74
O.3.1	Critical assets	74
O.3.2	Threats related to de-registration during the authentication	74
O.3.3	Threats related to authenticated re-registration	75
O.3.3.1	Unprotected register message	75
O.3.3.2	No resynchronization	75
O.4	Assets and threats specific to the I-CSCF	75
O.4.1	Critical assets	75
O.4.2	Threats related to network hiding	76
O.4.2.1	encryption in network hiding	76
O.5	Assets and threats specific to the IBCF	76
O.5.1	Critical assets	76
O.5.2	Threats related to network hiding	77
O.5.2.1	encryption in network hiding	77
O.5.2.2	replacement in network hiding	77
O.6	Assets and threats specific to the AS	77
O.6.1	Critical assets	77
O.6.2	Threats related to authorization	78
O.6.2.1	No user authorization	78
O.6.2.1	No ID privacy	78
O.7	Assets and threats specific to the MRFC	78
O.7.1	Critical assets	78
O.8	Assets and threats specific to the IMS AGW	79
O.8.1	Critical assets	79
O.9	Assets and threats specific to the MRFP	79
O.9.1	Critical assets	79
O.10	Assets and threats specific to the IMS MGW	80
O.10.1	Critical assets	80
O.11	Assets and threats specific to the TrGW	80
O.11.1	Critical assets	80
O.12	Assets and threats specific to the MGCF	81
O.12.1	Critical assets	81
Annex P: Aspects specific to the network product class NSSAAF		82
P.1	Void	82
P.2	Network product class description for the NSSAAF	82
P.2.1	Introduction	82

P.2.2	Minimum set of functions defining the NSSAAF network product class	82
P.3	Assets and threats specific to the NSSAAF	82
P.3.1	Critical assets.....	82
P.3.2	Threats related to NSSAAF.....	83
P.3.2.1	Threats related to impersonating attack by AAA-S	83
P.3.2.2	Threat to select AAA-P and AAA-S	83
Annex Q (normative): Aspects specific to the network product class SCP		84
Q.1	Network product class description for the SCP.....	84
Q.1.1	Introduction	84
Q.1.2	Minimum set of functions defining the SCP network product class	84
Q.2	Assets and Threats specific to SCP	84
Q.2.1	Threats related to tokens handled by the SCP	84
Q.2.1.1	Token forwarded to a wrong pNF instance.....	84
Q.2.1.2	Swapped token forwarded to the target pNF.....	85
Annex R: Change history		86
History		87

iTech Standards
(<https://standards.iteh.ai>)
Document Preview

[ETSI TR 133 926 V17.9.0 \(2024-04\)](https://standards.iteh.ai/catalog/standards/etsi/cd631f6f-8388-4214-b179-7d43ee024073/etsi-tr-133-926-v17-9-0-2024-04)

<https://standards.iteh.ai/catalog/standards/etsi/cd631f6f-8388-4214-b179-7d43ee024073/etsi-tr-133-926-v17-9-0-2024-04>

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 Standards
(<https://standards.iteh.ai>)
Document Preview

[ETSI TR 133 926 V17.9.0 \(2024-04\)](https://standards.iteh.ai/catalog/standards/etsi/cd631f6f-8388-4214-b179-7d43ee024073/etsi-tr-133-926-v17-9-0-2024-04)

<https://standards.iteh.ai/catalog/standards/etsi/cd631f6f-8388-4214-b179-7d43ee024073/etsi-tr-133-926-v17-9-0-2024-04>

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.